

CA Enterprise Log Manager

Implementation Guide

Release 12.5.01



This documentation, which includes embedded help systems and electronically distributed materials, (hereinafter referred to as the "Documentation") is for your informational purposes only and is subject to change or withdrawal by CA at any time.

This Documentation may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of CA. This Documentation is confidential and proprietary information of CA and may not be disclosed by you or used for any purpose other than as may be permitted in (i) a separate agreement between you and CA governing your use of the CA software to which the Documentation relates; or (ii) a separate confidentiality agreement between you and CA.

Notwithstanding the foregoing, if you are a licensed user of the software product(s) addressed in the Documentation, you may print or otherwise make available a reasonable number of copies of the Documentation for internal use by you and your employees in connection with that software, provided that all CA copyright notices and legends are affixed to each reproduced copy.

The right to print or otherwise make available copies of the Documentation is limited to the period during which the applicable license for such software remains in full force and effect. Should the license terminate for any reason, it is your responsibility to certify in writing to CA that all copies and partial copies of the Documentation have been returned to CA or destroyed.

TO THE EXTENT PERMITTED BY APPLICABLE LAW, CA PROVIDES THIS DOCUMENTATION "AS IS" WITHOUT WARRANTY OF ANY KIND, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT WILL CA BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, FROM THE USE OF THIS DOCUMENTATION, INCLUDING WITHOUT LIMITATION, LOST PROFITS, LOST INVESTMENT, BUSINESS INTERRUPTION, GOODWILL, OR LOST DATA, EVEN IF CA IS EXPRESSLY ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE.

The use of any software product referenced in the Documentation is governed by the applicable license agreement and such license agreement is not modified in any way by the terms of this notice.

The manufacturer of this Documentation is CA.

Provided with "Restricted Rights." Use, duplication or disclosure by the United States Government is subject to the restrictions set forth in FAR Sections 12.212, 52.227-14, and 52.227-19(c)(1) - (2) and DFARS Section 252.227-7014(b)(3), as applicable, or their successors.

Copyright © 2011 CA. All rights reserved. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

CA Technologies Product References

This document references the following CA Technologies 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 Technologies

Contact CA Support

For your convenience, CA Technologies provides one site where you can access the information you need for your Home Office, Small Business, and Enterprise CA Technologies 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 Technologies product documentation, you can send a message to techpubs@ca.com.

If you would like to provide feedback about CA Technologies 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:

- Integrating CA Enterprise Log Manager with CA Access Control—Changes to the Considerations for CA Access Control Users chapter to change the reference to the Connector Guide for CA Access Control.
- Securing CA Enterprise Log Manager using CA Access Control—Changes to the Considerations for CA Access Control Users chapter to document the feature. The changes include information about securing CA Enterprise Log Manager using CA Access Control.
- Virtualization—Changes to the Virtualization chapter to address the change in the required parameters to deploy an OVF template.

More information:

[Integrating with CA Access Control](#) (see page 223)

[Securing CA Enterprise Log Manager Using CA Access Control](#) (see page 248)

[Creating CA Enterprise Log Manager Servers using Virtual Appliances](#) (see page 282)

Contents

Chapter 1: Introduction 15

About This Guide	15
------------------------	----

Chapter 2: Planning Your Environment 17

Server Planning	18
Server Roles	19
Example: Network Architectures	23
Log Collection Planning	26
Disk Space Planning	28
About the CA EEM Server	28
Log Collection Guidelines	29
Federation Planning	30
Create a Federation Map	31
Example: Federation Map for a Large Enterprise	32
Example: Federation Map for a Mid-Sized Enterprise	34
User and Access Planning	36
User Store Planning	36
Users with Administrator Role	40
Password Policy Planning	40
Subscription Update Planning	42
The Subscription Service	43
How Subscription Works	44
How to Plan Subscription Updates	46
Example: Subscription Configuration with Six Servers	51
Agent Planning	53
About Syslog Event Collection	53
Agents and the Agent Certificate	55
About Agents	55
About Integrations	56
About Connectors	57
Sizing Your CA Enterprise Log Manager Network	58

Chapter 3: Installing CA Enterprise Log Manager 61

Understanding the CA Enterprise Log Manager Environment	61
Create the Installation DVDs	63
Installing a CA Enterprise Log Manager Server	64

CA Enterprise Log Manager Server Worksheet	65
Install CA Enterprise Log Manager	69
Verify that the iGateway Process is Running	70
Verify the CA Enterprise Log Manager Server Installation	73
View Self-Monitoring Events	74
Upgrade Existing CA Enterprise Log Manager Servers and Agents for FIPS Support	74
Prerequisites for Upgrade for FIPS Support	77
Upgrade Guidelines	77
Upgrading a Remote CA EEM Server	78
Disable ODBC and JDBC Access to the Event Log Store	78
Enable FIPS Mode Operation	78
View Agent Dashboard	79
Adding New CA Enterprise Log Manager Servers to an Existing FIPS Mode Federation	80
Installation Considerations for a System with SAN Drives	82
Install with Disabled SAN Drives	82
Install with Enabled SAN Drives	88
Initial CA Enterprise Log Manager Server Configurations	89
Default User Accounts	90
Default Directory Structure	90
Customized Operating System Image	91
Default Port Assignments	91
List of Related Processes	93
OS Hardening	95
Redirect Firewall Ports for syslog Events	95
Install the ODBC Client	96
Prerequisites	96
Configure the ODBC Server Service	97
Install the ODBC Client on Windows Systems	98
Create an ODBC Data Source on Windows Systems	98
Test the ODBC Client's Connection to the Database	100
Test Server Retrieval from the Database	101
Installing the JDBC Client	101
JDBC Client Prerequisites	102
Install the JDBC Client on Windows Systems	102
Install the JDBC Client on UNIX Systems	103
JDBC Connection Parameters	103
JDBC URL Considerations	103
Installation Troubleshooting	104
Resolve Network Interface Configuration Error	106
Verify that the RPM Package is Installed	106
Register CA Enterprise Log Manager Server with the CA EEM Server	107
Acquire Certificates from CA EEM Server	107

Import CA Enterprise Log Manager Reports	108
Import CA Enterprise Log Manager Data Mapping Files	109
Import Common Event Grammar Files	109
Import Correlation Rule Files	110
Import Common Agent Management Files	111
Import CA Enterprise Log Manager Configuration Files	111
Import Suppression and Summarization Files	112
Import Parsing Token Files	113
Import CA Enterprise Log Manager User Interface Files	113

Chapter 4: Configuring Basic Users and Access 115

About Basic Users and Access	115
Configuring the User Store	116
Accept the Default User Store	116
Reference an LDAP Directory	117
Reference CA SiteMinder as the User Store	118
Configure Password Policies	119
Preserving Predefined Access Policies	120
Create the First Administrator	121
Create a New User Account	121
Assign a Role to a Global User	122

Chapter 5: Configuring Services 125

Event Sources and Configurations	125
Edit Global Configurations	126
Working with Global Filters and Settings	128
Select Use of Federated Queries	129
Configure the Global Update Interval	130
Configuring the Event Log Store	130
About the Event Log Store Service	131
About Archive Files	131
About Auto Archive	132
Database Move and Backup Strategy Flowchart	133
Configuring Non-Interactive Authentication for Auto Archive	134
Example: Configure Non-Interactive Authentication for Hub and Spoke	135
Example: Configure Non-Interactive Authentication Across Three Servers	142
Example: Auto-Archiving Across Three Servers	143
Event Log Store Settings in the Basic Environment	148
Set Event Log Store Options	150
Configuring the Correlation Service	151
Apply Correlation Rules and Incident Notifications	152

Using Pre-Defined Correlation Rules	153
Set Collection Servers	156
How to Design and Apply Incident Notifications	156
How to Create a Notification Destination	157
Incident Service Considerations	160
ODBC Server Considerations	160
Report Server Considerations	162
How to Configure Subscription	163
Configure an Online Subscription Proxy	163
Configure an Offline Subscription Proxy	165
Configure a Subscription Client	166
Configure Proxy Lists	167
About Modules to Download	168
Set a Subscription Schedule	173
 Chapter 6: Configuring Event Collection	 175
Installing Agents	175
Using the Agent Explorer	176
Configuring the Default Agent	177
Review syslog Integrations and Listeners	177
Create a syslog Connector for the Default Agent	178
Verify that CA Enterprise Log Manager Is Receiving syslog Events	178
Example: Enable Direct Collection Using the ODBCLogSensor	179
Example: Enable Direct Collection Using the WinRMLinuxLogSensor	184
View and Control Agent or Connector Status	188
 Chapter 7: Creating Federations	 191
Queries and Reports in a Federated Environment	191
Hierarchical Federations	192
Hierarchical Federation Example	192
Meshed Federations	193
Meshed Federation Example	194
Configuring a CA Enterprise Log Manager Federation	195
Configure a CA Enterprise Log Manager Server as a Child Server	195
View Federation Graph and Server Status Monitor	196
 Chapter 8: Working with the Event Refinement Library	 199
About the Event Refinement Library	199
Supporting New Event Sources with the Event Refinement Library	199
Mapping and Parsing Files	200

Appendix A: Considerations for CA Audit Users **201**

Understanding Differences in Architectures	201
CA Audit Architecture	202
CA Enterprise Log Manager Architecture	204
Integrated Architecture	206
Configuring CA Technologies Adapters	207
About the SAPI Router and Collector	208
About the iTechnology Event Plug-in	210
Sending CA Audit Events to CA Enterprise Log Manager	211
Configure iRecorder to Send Events to CA Enterprise Log Manager	211
Modify an Existing CA Audit Policy to Send Events to CA Enterprise Log Manager	212
Modify an Existing r8SP2 Policy to Send Events to CA Enterprise Log Manager	214
When to Import Events	215
About the SEOSDATA Import Utility	215
Importing from a Live SEOSDATA Table	216
Importing Data from a SEOSDATA Table	216
Copy the Event Import Utility to a Solaris Data Tools Server	217
Copy the Import Utility to a Windows Data Tools Server	217
Understand the LMSeosImport Command Line	218
Create an Event Report	220
Preview Import Results	221
Import Events from a Windows Collector Database	222
Import Events from a Solaris Collector Database	222

Appendix B: Considerations for CA Access Control Users **223**

Integrating with CA Access Control	223
How to Modify CA Audit Policies to Send Events to CA Enterprise Log Manager	224
Configure the SAPI Collector Adapter to Receive CA Access Control Events	225
Modify an Existing CA Audit Policy to Send Events to CA Enterprise Log Manager	227
Check and Activate the Changed Policy	233
How to Configure a CA Access Control iRecorder to Send Events to CA Enterprise Log Manager	234
Configure the iTech Event Plugin for CA Access Control Events	234
Download and Install a CA Access Control iRecorder	235
Configure a Standalone CA Access Control iRecorder	235
How to Import CA Access Control Events from a CA Audit Collector Database	237
Prerequisites for Importing CA Access Control Events	237
Create a SEOSDATA Event Report for CA Access Control Events	239
Preview a CA Access Control Event Import	241
Import CA Access Control Events	244
View Queries and Reports to See CA Access Control Events	245
Securing CA Enterprise Log Manager Using CA Access Control	248

Prerequisites	249
Appendix C: CA IT PAM Considerations	251
Scenario: How to Use CA EEM on CA Enterprise Log Manager for CA IT PAM Authentication	251
CA IT PAM Authentication Implementation Process	252
Prepare to Implement CA IT PAM Authentication on a Shared CA EEM	253
Copy an XML File to the Management CA Enterprise Log Manager	253
Register CA IT PAM with a Shared CA EEM	254
Copy the Certificate to the CA IT PAM Server	255
Set Passwords for the Predefined CA IT PAM User Accounts	255
Install the Third-Party Components Required by CA IT PAM	257
Install the CA IT PAM Domain	257
Start the CA ITPAM Server Service	258
Launch and Log in to the CA IT PAM Server Console	259
Appendix D: Disaster Recovery	261
Disaster Recovery Planning	261
About Backing Up the CA EEM Server	262
Back Up a CA EEM Application Instance	262
Restore a CA EEM Server for Use with CA Enterprise Log Manager	263
Back Up a CA Enterprise Log Manager Server	264
Restore a CA Enterprise Log Manager Server from Backup Files	265
Restore a CA Enterprise Log Manager Server After Subscription Update	266
Replace a CA Enterprise Log Manager Server	266
Appendix E: CA Enterprise Log Manager and Virtualization	269
Deployment Assumptions	269
Considerations	269
Creating CA Enterprise Log Manager Servers Using Virtual Machines	270
Adding Virtual Servers to Your Environment	270
Creating a Completely Virtual Environment	274
Deploying Virtual CA Enterprise Log Manager Servers Rapidly	277
Creating CA Enterprise Log Manager Servers using Virtual Appliances	282
About CA Enterprise Log Manager Virtual Appliances	283
How to Use the Virtual Appliance	283
Virtual Appliance Installation Worksheet	284
Adding Virtual Servers to Your Environment	286
Creating a Completely Virtual Environment	309
Deploying Virtual Servers Rapidly	332
Post Installation Tasks	342

Glossary	345
Index	369

Chapter 1: Introduction

This section contains the following topics:

[About This Guide](#) (see page 15)

About This Guide

This *CA Enterprise Log Manager Implementation Guide* provides the instructions you need for planning, installing, and configuring CA Enterprise Log Manager to receive event logs from events sources in your network. The guide is organized so that tasks start with a description of the process and its goals. Processes are generally followed by relevant concepts, and then one or more procedures to accomplish the goal.

The *CA Enterprise Log Manager Implementation Guide* is designed for system administrators who have responsibility for installing, configuring and maintaining a log collection solution, creating users and assigning or defining their roles and access, and maintaining backup data.

This guide also assists any personnel who need information on how to do the following:

- Configure a connector or adapter to collect event data
- Configure services to control reporting, data retention, backup, and archive
- Configure a federation of CA Enterprise Log Manager servers
- Configure subscription to get content, configuration, and operating system updates

A summary of the contents follows:

Section	Description
Planning Your Environment	Describes planning activities for areas such as log collection, agents, federation, user and access management, subscription updates, and disaster recovery.
Installing CA Enterprise Log Manager	Provides work sheets for gathering required information, and detailed instructions on how to install CA Enterprise Log Manager and verify proper installation.
Configuring Basic Users and Access	Provides instructions for identifying a user store and creating the initial administrative user for the configuration of other user and access details.

Section	Description
Configuring Services	Provides instructions for configuring services including global and local filters, the event log store, report server, and subscription options.
Configuring Event Collection	Provides concepts and instructions for using or configuring the event refinement library components including the mapping and parsing files, and the CA Technologies adapters.
Creating Federations	Describes different types of federations and provides instructions for creating federated relationships between CA Enterprise Log Manager servers and viewing a federation graph.
Working with the Event Refinement Library	Provides high-level information about working with message parsing and data mapping files.
Considerations for CA Audit Users	Describes the interactions you can implement between CA Enterprise Log Manager and CA Audit, how to configure iRecorders and policies, and how to import data from your CA Audit Collector database.
Considerations for CA Access Control Users	Describes how to integrate with CA Access Control, how to modify CA Audit policies to send events to CA Enterprise Log Manager, how to configure a CA Access Control iRecorder to send events to CA Enterprise Log Manager, and how to import CA Access Control events from a CA Audit Collector database,
CA IT PAM Considerations	Describes the process of installing CA IT PAM such that the EEM component on the management CA Enterprise Log Manager handles authentication.
Disaster Recovery	Describes backup, restoration, and replacement procedures for ensuring recovery of your log management solution in case of disaster.
CA Enterprise Log Manager and Virtualization	Describes the process to use to create and configure a virtual machine to contain a CA Enterprise Log Manager server.

Note: For details on operating system support or system requirements, see the *Release Notes*. For a basic CA Enterprise Log Manager overview and use scenario, see the *Overview 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.

Chapter 2: Planning Your Environment

This section contains the following topics:

[Server Planning](#) (see page 18)

[Log Collection Planning](#) (see page 26)

[Federation Planning](#) (see page 30)

[User and Access Planning](#) (see page 36)

[Subscription Update Planning](#) (see page 42)

[Agent Planning](#) (see page 53)

Server Planning

The first step in planning your environment is to determine how many CA Enterprise Log Manager servers you need and what role each server will perform. Roles include:

- **Management**
Stores predefined and user-defined content and configurations. Also authenticates users and authorizes feature access.
- **Collection**
Receives event logs from its agents; refines events.
- **Correlation**
Receives event logs from agents or collection servers; filters events and creates incidents according to its applied correlation rules.
- **Reporting**
Processes queries on collected events, both on-demand queries and reports and also scheduled alerts and reports.
- **Restore point**
Receives restored event log databases for investigation of past events

The first server you install is the management server; this server can perform other roles as well. You can have only one management server in a single CA Enterprise Log Manager network. Every CA Enterprise Log Manager network must have one management server.

Possible architectures include:

- Single-server system, where the management server performs all the other roles
- Two-server system, where the management server performs all roles but collection. Collection is performed by a server dedicated to this role.
- Multiple-server system, where each server is dedicated to a single role.

Details on server roles and architectures follow.

Server Roles

A CA Enterprise Log Manager system can have one or more servers. Dedicating different servers to different roles optimizes performance. But, you can use any server to perform multiple roles or all roles, at your discretion. Consider the processing burden associated with each server role with regard to other relevant factors in your environment when determining how to dedicate each server you install.

■ Management server

The management server role is, by default, performed by the first CA Enterprise Log Manager server you install. The management server performs these major functions:

- Acts as a common repository for all servers that register with this server. Specifically, it stores application users, application groups (roles), policies, calendars, and AppObjects.
- If you configure the user store as the internal store, it stores global users, global groups, and password policies. If the configured user store is a reference to an external user store, it loads the global user account details and global group details from the referenced user store.
- Handles user entitlements with a high-speed memory-mapped file. Authenticates users at login based on user and group configuration. Authorizes users to access various parts of the user interface based on policies and calendars.
- Receives all content and configuration updates downloaded through subscription.

There can be only one active management server in a CA Enterprise Log Manager network of servers, but you can have a failover (inactive) management server. If you create more than one CA Enterprise Log Manager network, each must have its own active management server.

■ Collection server

In a single-server system, the management server performs the role of a collection server. In a system of two or more servers, consider a dedicated collection server. A collection server performs these functions:

- Supports the configuration of connectors.
- Accepts incoming event logs from connectors on its agents.
- Accepts incoming refined event logs, which are parsed and mapping into the CEG format that allows uniform presentation of event data from disparate event sources.
- Inserts event logs into the hot database and compresses the hot database when it reaches the configured size into a warm database.
- Allows auto-archiving, which moves warm database information to the related reporting server on the configured schedule.

Important! When you dedicate separate servers to collection and reporting, you must configure non-interactive authentication and hourly auto archiving from the collection server to the reporting server.

Consider the event volume generated by your event sources when determining whether to dedicate servers to event collection and refinement. Also consider how many collection servers are to auto-archive their data to a single reporting server.

■ Correlation server

In a single-server system, the management server performs the role of a correlation server. In a system of two or more servers, consider a dedicated correlation server. A correlation server performs these functions:

- Supports the configuration and application of correlation rules and notifications.
- Accepts incoming event logs from collection servers.
- Filters incoming events and creates incidents according to correlation rule conditions.
- Stores incidents in the Incident Database, and their component events in the Incident Event Database.

Important! When you dedicate separate servers to correlation, you must select every collection server whose events you want to correlate when configuring the correlation service.

■ Reporting server

In a single-server or two-server system, the management server performs the role of a reporting server. In a system with many servers, consider dedicating one or more servers to reporting. A reporting server performs these functions:

- Because non-interactive authentication and auto-archiving is configured, receives new databases of refined events from its collection servers.
- Processes on-demand prompts, queries, and reports.
- Processes scheduled alerts and reports.
- Supports wizards for creating custom queries and reports.
- If non-interactive authentication and auto archiving is configured from the reporting server to a remote storage server, moves old databases to a remote storage server.

If you plan to generate many complex reports and alerts on a server with high on-demand activity, consider dedicating a server to reporting.

■ Remote storage server

A remote storage server, which may not be a CA Enterprise Log Manager server, performs this function:

- Receives highly-compressed, auto-archived databases from reporting servers at configured intervals, before these databases are set for deletion due to age or lack of free disk space. Auto archiving saves you the effort of manually moving databases.
- Stores cold databases locally. Optionally, you can move or copy these databases to an off-site location for long-term storage. Cold databases are typically retained for the number of years mandated by government regulatory agencies.

Remote storage servers are never part of a CA Enterprise Log Manager federation. However, they deserve consideration when you plan your architecture.

■ Restore point server

Reporting servers typically act as restore point servers for the databases they once held. If your network is large, consider dedicating a CA Enterprise Log Manager server to this role. A restore point server performs these functions:

- Is used to investigate the logs of old events.
- Receives restored databases from a remote storage server that holds all cold databases. You can use the `restore-ca-elm.sh` utility to move databases to the restore point if you first configure non-interactive authentication from the storage server to the restore point.
- Recatalogs the archive catalog to add the restored databases to its records.
- Retains restored records for different configured lengths of time, depending on the restoration method.

The advantage of having a dedicated restore point is that you can exclude this server from your federation to ensure that no federated reports contain old, restored data. All reports generated on the restore point server reflect only event data from the restored databases.

Dedicating a server to a certain role does not mean you cannot perform functions from it that are associated with other roles. Consider an environment with dedicated collection servers and a reporting server. If you want to schedule an alert to check for a condition on a collection server because it is time-critical that you be notified as soon as possible, you have this flexibility.

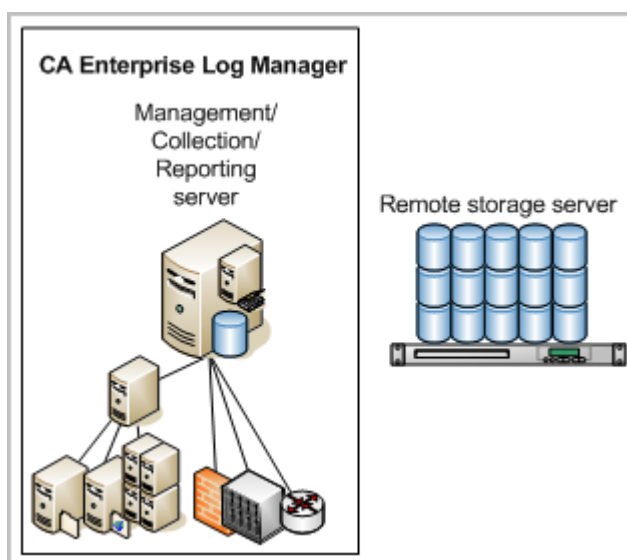
Example: Network Architectures

The simplest CA Enterprise Log Manager architecture is a single-server system, where one CA Enterprise Log Manager server performs all roles:

- The management, collection, reporting CA Enterprise Log Manager handles configuration/content management, event collection/refinement and correlation, as well as queries and reports.

Note: A non-CA Enterprise Log Manager remote server stores archived event log databases.

This setup is appropriate for processing a low event volume and few scheduled reports, as in a test system.

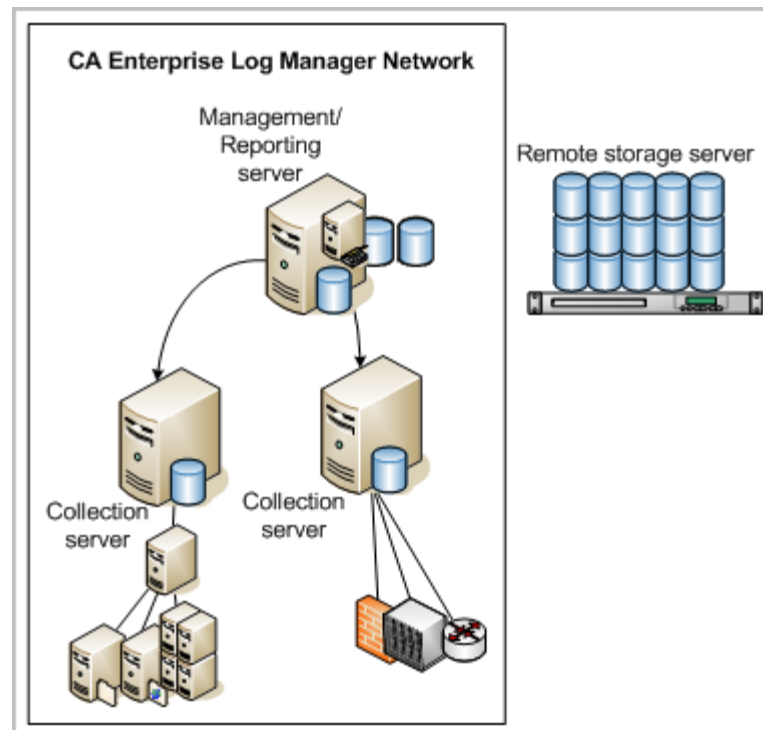


The next simplest architecture is a multi-server system where the first CA Enterprise Log Manager installed performs most roles:

- The management, reporting CA Enterprise Log Manager handles configuration/content management as well as queries and reports, and event correlation.
- The collection CA Enterprise Log Managers handle event collection and refinement.

Note: A non-CA Enterprise Log Manager remote server is set up to store archived databases of event logs.

This architecture is suitable for a network with moderate event volume. The arrows depict that the management functionality of the Management/Reporting server maintains the global settings that apply to all servers. When there are many collection servers, this architecture is termed "hub and spoke."

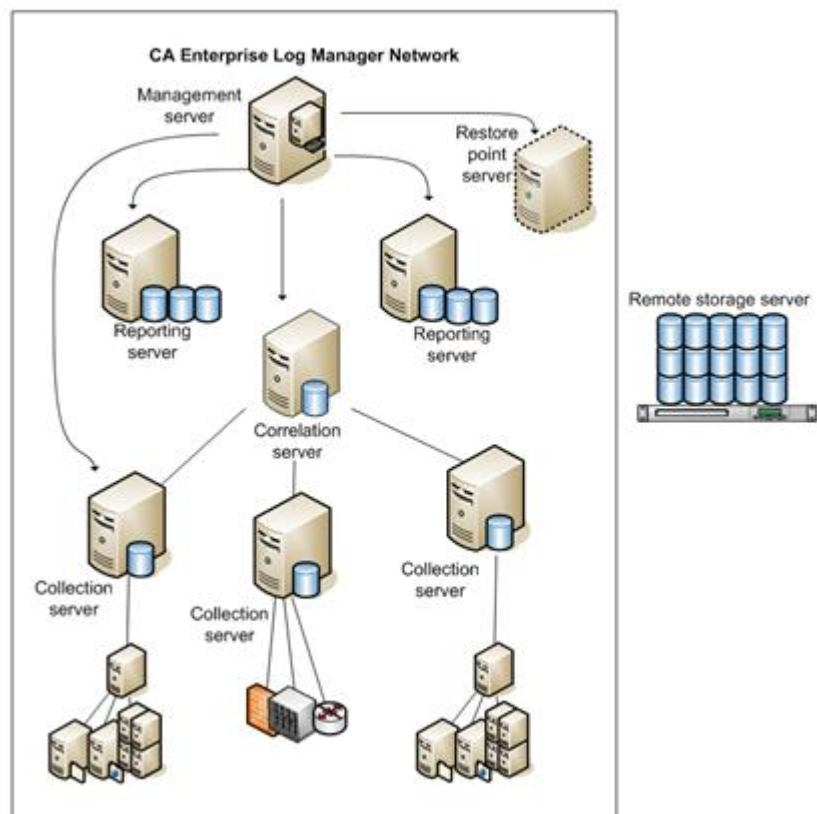


In a large network with high event volume, many complex scheduled reports and alerts, and ongoing customization, you can dedicate one or more CA Enterprise Log Manager servers to single roles:

- The management CA Enterprise Log Manager handles configuration/content management.
- The reporting CA Enterprise Log Manager handles queries and reports.
- The collection CA Enterprise Log Managers handle event collection and refinement.
- The correlation CA Enterprise Log Manager handles event correlation.
- Optionally, a restore point CA Enterprise Log Manager handles the investigation of events from restored archive databases.

Note: A non-CA Enterprise Log Manager remote server is set up to store archived databases of event logs.

This setup is ideal for very large networks. The arrows depict that the Management server maintains the global settings that apply to all servers.



Log Collection Planning

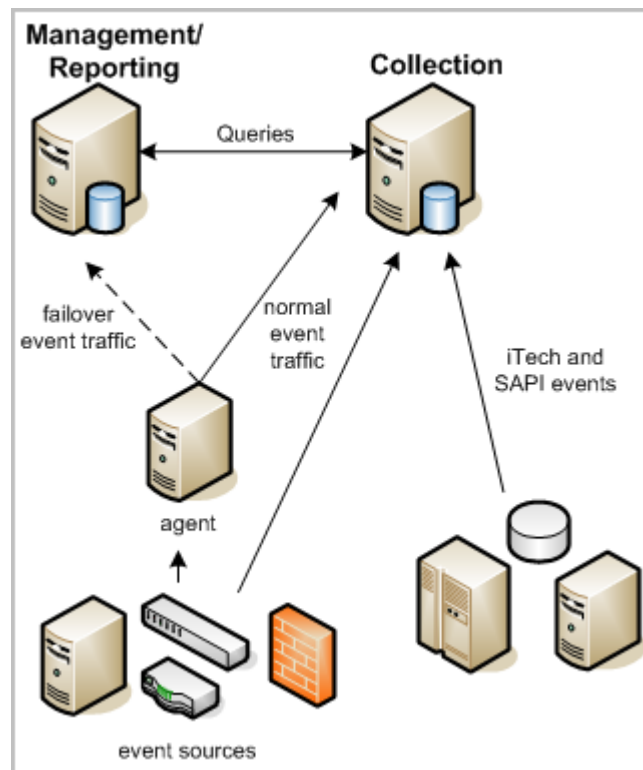
Log collection planning for your network is based upon the number of events per second (eps) you need to process for storage and the length of time you need to retain the data online. (In this sense, *online* means in an immediately searchable state.) Typically, you have only 30-90 days' worth of data online.

Each network has its own event volumes as a function of the number of devices, device types, and the degree to which network devices and applications like firewalls are tuned to fit the enterprise's event information needs. For example, some firewalls can generate huge volumes of unneeded events based on how they are configured.

We recommend planning your event collection so that your total event volume is spread evenly across your CA Enterprise Log Manager servers without forcing any of them to go beyond the normal constant duty rating. To maintain peak performance at enterprise event volumes, we recommend that you install at least two, federated CA Enterprise Log Manager servers:

- One reporting CA Enterprise Log Manager server to handle queries and reports, alerts and alert management, subscription updates, and user authentication and authorization.
- One or more collection CA Enterprise Log Manager servers specifically configured to maximize database inserts.

The following illustration shows a simple example of this kind of federated CA Enterprise Log Manager network. Two CA Enterprise Log Manager servers, one for reporting and one for collection, handle event traffic from a variety of event sources. Both servers can share data between them for queries, reporting, and alerting.



The *collection* server primarily handles the incoming event log traffic and focuses on database inserts. It uses a short data retention policy of 24 hours or less. An automated script moves stored event logs to a reporting server daily or more often depending on event volume. Federation and the use of federated queries between the two servers ensures that you receive accurate reports from the event logs on *both* servers.

The *reporting* server performs several functions:

- Processes queries and reports
- Schedules and manages alerts
- Moves archived files to a remote storage server
- Provides failover collection of connector-gathered events for the collection server

An automated backup script moves data from the reporting server to a remote server (cold storage). If you decide to restore data from cold storage, you generally will do so on the reporting server. If space on the reporting server is limited, you can also restore to the collection server. Since the collection server does not store large amounts of data and is federated, the report results are the same.

In addition, the reporting server can function as a failover receiver for events collected by a connector on a remote agent, if the collection server stops receiving events for some reason. You can configure failover at the agent level. Failover processing sends events to one or more alternate CA Enterprise Log Manager servers. Failover event collection is not available for events from legacy event sources collected through the SAPI and iTech listeners.

More information:

[CA Enterprise Log Manager and Virtualization](#) (see page 269)

Disk Space Planning

When you plan your environment, ensure that you have sufficient disk space to support high event volumes. For the collection server, this means enough disk space for each collection server to accommodate its share of peak loads as well as standard event volumes. For a reporting server, disk space is calculated based on event volume and the required online retention period.

Hot databases are not compressed. Warm databases are compressed. Both the hot and warm databases are considered to be online. You can search or report on their data. You would typically have at most between 30 and 90 day's worth of data ready for reporting and immediate search at any one time. Records older than that are stored on a remote server. You can restore them for search and reporting as needed.

Collection servers support both hot and warm databases. Since the retention period for a collection server is very short, from one to 23 hours, long term storage is not a factor.

A hot database exists on a management server for inserting self monitoring event messages.

Reporting servers support smaller hot databases and a large number of warm databases. Reporting servers must also have enough additional space to support restored files for some term. When you use direct attached storage, the partitions are automatically extended to allow for greater storage capacity.

About the CA EEM Server

CA Enterprise Log Manager uses the CA Embedded Entitlements Manager (CA EEM) server internally to manage configurations, authorize and authenticate users, coordinate subscription updates to content and binaries, and perform other management functions. In the basic CA Enterprise Log Manager environment, you install CA EEM when you install the management CA Enterprise Log Manager server. From there CA EEM manages the configurations of all of the collection CA Enterprise Log Manager servers and their agents and connectors.

You can also choose to install the CA EEM server on a remote server using the supplied install packages on the Application installation disk, or you can use an existing CA EEM server if you have one in use with other CA Technologies products.

The CA EEM server offers its own web interface. However, almost all of your configuration and maintenance activities take place within the CA Enterprise Log Manager user interface. You should not normally need to interact directly with the embedded CA EEM server functions except for failover configurations and the backup and restore functions that are part of disaster recovery.

Note: The CA Enterprise Log Manager server installation requires that you use the password for the CA EEM default administration account, EiamAdmin, for proper registration of a CA Enterprise Log Manager server. When you install the first management CA Enterprise Log Manager server, you create this new password as part of the installation. When you install subsequent CA Enterprise Log Manager servers using the same application instance name, you automatically create a network environment in which you can later set up federation relationships between the CA Enterprise Log Manager servers.

Log Collection Guidelines

Consider the following log collection guidelines during your planning phase:

- Traffic from the agent to the CA Enterprise Log Manager server is always encrypted, whether using agentless or agent-based log collection.
- Consider employing a syslog local collection mechanism as a workaround for the potential problems with guaranteed delivery.

When determining whether to use direct collection by the default agent, agent-based collection where the agent is installed on the host with the event source, or agentless collection where the agent is installed on a collection point remote from the event sources, consider these factors:

- Platform support
For example, WMI only works on Windows for the log sensor.
- Driver support for certain log sensors
For example, you need an ODBC driver for ODBC to work.
- Whether the log source can be accessed remotely
For example, for file-based logs, you need a shared-drive in order for those to work remotely.

Federation Planning

For CA Enterprise Log Manager, a *federation* is a network of servers that store, report on, and archive event data. A federation allows you to control how your data is grouped and reviewed in a network. You can configure how your servers relate to one another, and thus how queries are sent from one server to another. In addition, you can turn federated queries on and off for specific queries as needed.

The decision to use a federation is based on a combination of required event volume and your business needs for separating and reporting on log data. CA Enterprise Log Manager supports hierarchical and meshed federations, and configurations that blend the two types. All the CA Enterprise Log Manager servers you want to federate must use the same application instance name in CA EEM. Each CA Enterprise Log Manager server installation automatically registers with the CA EEM server using an application instance name.

You can configure a federation at any time after you install your first CA Enterprise Log Manager server and at least one additional server. However, the best results come from planning your federation *before* installation. Creating a detailed federation map helps you complete the configuration tasks quickly and accurately.

At the *network* level, having multiple CA Enterprise Log Manager servers allows you to handle greater event volumes. From a *reporting* perspective, using a federation allows you to control who can access event data and how much of that data they can see.

In a basic two-server environment, the management server takes the role of a reporting server. The internal CA EEM server on the management CA Enterprise Log Manager server manages federation configurations centrally and globally. (You can change the configuration options from any CA Enterprise Log Manager server in the network.) You configure the collection CA Enterprise Log Manager server as a child of the reporting server, so that queries and reports include the most recent data.

Note: If you have an existing CA EEM server that you plan to use with CA Enterprise Log Manager, configure the CA Enterprise Log Manager servers in the same way. The dedicated, remote CA EEM server stores these configurations.

You can also set local configuration options to override the global configurations, allowing selected CA Enterprise Log Manager servers to perform differently than others. Examples include sending email reports and alerts through a different mail server, or scheduling reports specific to a branch of the network at different times.

More information:

[Hierarchical Federations](#) (see page 192)

[Meshed Federations](#) (see page 193)

[Queries and Reports in a Federated Environment](#) (see page 191)

[Configuring a CA Enterprise Log Manager Federation](#) (see page 195)

Create a Federation Map

Creating a federation map is a useful step in planning and implementing your federation configuration. The larger your network is, the more helpful this map is during the actual configuration tasks. You can use any commercial graphics or drawing program, or you can sketch the map by hand. The more details you can supply in your map, the faster you can complete the configuration.

To create a federation map

1. Start your map with the two basic CA Enterprise Log Manager servers, management and collection, and provide the details for each.
2. Decide whether you need additional collection servers and whether they represent the top of a hierarchy or a unit in a mesh.
3. Decide which type of federation best suits your needs, hierarchical or meshed.
4. Identify opportunities for hierarchies, branches, or interconnections based on your business reporting, compliance, and event throughput needs.

For example, if your company has offices on three continents, you may decide to create three hierarchical federations. You may further decide to mesh the hierarchies at a high level, so that senior executives and security management can produce reports that cover the entire network. You should at a minimum federate the basic environment's insert and query CA Enterprise Log Manager servers.

5. Decide how many total CA Enterprise Log Manager servers you need to deploy.
This value is based on the number of devices in your network and the event volume they generate.
6. Decide how many layers of federated servers you need.
This number is based in part on the decisions you take in steps 2 and 3.
7. Identify the event types that each of the CA Enterprise Log Manager servers in the federation receives.

If your network has a large number of syslog-based devices and only a few Windows servers, you may decide to allocate one CA Enterprise Log Manager server expressly for Windows event collection. You may need several servers to handle the syslog event traffic. Planning ahead which CA Enterprise Log Manager servers receive which kinds of events makes configuration of the local listeners and services easier.

8. Sketch a map of this network to use during configuration of the federated (child) CA Enterprise Log Manager servers.

Include DNS names and IP addresses on your map, if known. You will use the DNS names of the CA Enterprise Log Manager servers to configure the federation relationships between them.

Example: Federation Map for a Large Enterprise

When creating a federation map, consider the types of reports for which you want different sets of consolidated data. For example, consider the scenario where you want consolidated data using three types of server groupings:

- All servers

For system reports on self-monitoring events, including all servers lets you evaluate the health of your entire CA Enterprise Log Manager network of servers at once.

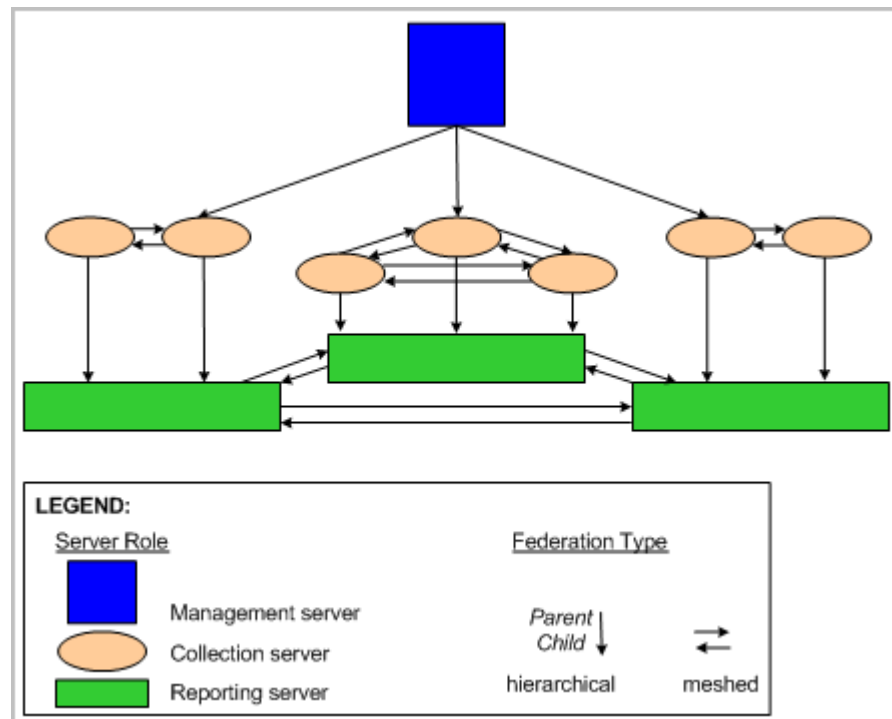
- All reporting servers

For summary and trend reports, where you want to examine data collected by all agents that send data to all collection servers while sparing your collection servers from processing queries on new, hot events, you need to run federated reports that include only reporting servers.

- A set of collection servers with their reporting server

For reports where you want data limited to a locale with one reporting server, but you want that report to include the events not yet sent to that server by its collection servers, you need to run federated reports on this subset of servers.

An example federation map that lets you meet these reporting objectives follows:



To implement the design of this federation map, you would take the following actions:

- Create a hierarchical federation from the management server to one collection server related to each reporting server, where the management server is the Parent and each collection server is the Child.
- Create a fully meshed federation among collection servers for each reporting server.
- Create a hierarchical federation from each collection server to its reporting server, where the collection server is the Parent and the reporting server is the Child.
- Create a fully meshed federation among the reporting servers.

To meet a given reporting objective, it is important to run the report from a server represented by a particular location on your federation map. Examples follow:

- To generate a system report on self-monitoring events that occur on each CA Enterprise Log Manager in your network, run the report from the management server.
- To generate summary and trend reports from all reporting servers on your network, run the report from any reporting server.
- To generate a report on data residing on a reporting server and its collection servers, run the report from one of those collection servers.

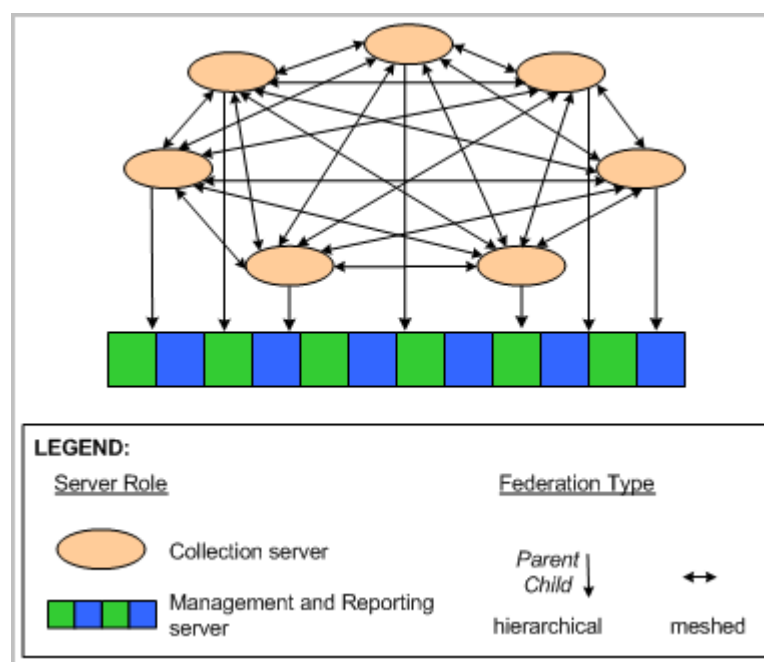
Example: Federation Map for a Mid-Sized Enterprise

Before you create a federation map, determine the number of servers you plan to devote to each server role. In the following example, one server is devoted to management and reporting and the remaining servers are devoted to collection. We recommend this configuration for a mid-sized environment. You can think of the architecture of the management/reporting server and collection servers as hub and spoke, where the management/reporting server is the hub. The federation map diagram does not mirror this configuration; instead, it shows the tiers so you can easily differentiate pairs that are federated hierarchically from the meshed ones.

When creating a federation map, consider the reports and alerts for which you want different sets of consolidated data. For example, consider the scenario where you want consolidated data using two types of server groupings:

- Only the management/reporting server
For most reports, where you want to examine recently archived (warm) events while sparing your collection servers from processing queries on new (hot) events
Note: Events are typically archived from collection servers (spokes) to the reporting server (hub) every hour.
- All servers
For system reports on self-monitoring events, where you want to evaluate the health of all your CA Enterprise Log Manager servers at once
For alerts, where it is important to query for new events from all collection servers

An example federation map that lets you meet these reporting objectives follows:



To implement the design of this federation map, you would take the following actions:

- Create a fully meshed federation among collection servers. (Every collection server is both Parent and Child to every other collection server.)
- Create a hierarchical federation from each collection server to the management/reporting server, where the collection server is the Parent and the management/reporting server is the Child.

To meet a given objective, it is important to run the report or alert from a server represented by a particular location on your federation map and correctly specify whether federation is needed. Examples follow:

- To schedule a system report on self-monitoring events that occur on each CA Enterprise Log Manager server in your network, run the report from the management/reporting server and specify federated.
- To schedule a report on recent (warm) events, run the report from the management/reporting server and clear the request for federated. Such a report includes recently archived data collected by all collection servers. Federation is not needed.
- To schedule an alert that includes new (hot) events from each collection server and archived (warm) events on the management/reporting server, run the alert from any collection server and specify federated. You can limit what is returned to the collection servers by specifying as result conditions the predefined range, within the last hour.

More information:

[Configure a CA Enterprise Log Manager Server as a Child Server](#) (see page 195)
[Example: Auto-Archiving Across Three Servers](#) (see page 143)

User and Access Planning

After you install the first CA Enterprise Log Manager server and access it as the EiamAdmin user, you can configure the user store, configure a user as an Administrator, and set password policies.

User and access planning is limited to the following:

- Determining whether to accept the default user store on this CA Enterprise Log Manager server or configure an external user store. If configuration is needed, record the required values on the supplied work sheets.
- Identifying the user who will act as the first Administrator. Only an Administrator can configure CA Enterprise Log Manager settings.
- Defining password policies with the goal of promoting strong passwords for CA Enterprise Log Manager users.

Note: You can configure password policies only when you configure the user store as the user store on this CA Enterprise Log Manager.

More information:

[External LDAP Directory Worksheet](#) (see page 37)
[CA SiteMinder Worksheet](#) (see page 39)

User Store Planning

After installing the first CA Enterprise Log Manager server, log into CA Enterprise Log Manager and configure the user store. The configured user store is where user names and passwords, used for authentication, and other global details are stored.

With all user store options, application user details are stored in the CA Enterprise Log Manager user store. This includes information such as roles, user favorites, and last login time.

Consider the following when planning the user store to configure:

- Use the CA Enterprise Log Manager user store (default)
Users are authenticated with the user names and passwords created in CA Enterprise Log Manager. You configure password policies. Users can change their own passwords and unlock other user accounts.

- Reference from CA SiteMinder

User names, passwords, and global groups are loaded from CA SiteMinder to the CA Enterprise Log Manager user store. Users are authenticated with the referenced user names and passwords. You can assign the global group to a new or existing policy. You cannot create new users, change passwords, or configure password policies.

- Reference from LDAP (Lightweight Directory Access Protocol) directory

User names and passwords are loaded from the LDAP directory to the CA Enterprise Log Manager user store. Users are authenticated with the referenced user names and passwords. The loaded user account information become global user accounts. You can assign the global users a user role corresponding to the access you want them to have in CA Enterprise Log Manager. You cannot create new users or configure password policies.

Important! We recommend that you back up the predefined access policies that are provided with CA Enterprise Log Manager before you or any Administrator begins working with them. For details, see the *CA Enterprise Log Manager Administration Guide*.

More information:

[Accept the Default User Store](#) (see page 116)

[Reference an LDAP Directory](#) (see page 117)

[Reference CA SiteMinder as the User Store](#) (see page 118)

External LDAP Directory Worksheet

Before you reference an external LDAP directory, gather the following configuration information:

Required information	Value	Comments
Type		Note the type of directory you are using. CA Enterprise Log Manager supports several different directories including Microsoft Active Directory, and Sun ONE Directory. Refer to the user interface for a complete list of supported directories.
Host		Record the host name of the server for the external user store or directory.
Port		Record the port number on which the external user store or directory server listens. Port 389 is the well-known port for LDAP (Lightweight Directory Access Protocol). If your registry server does not use port 389, record the correct port number.

Required information	Value	Comments
Base DN		Record the LDAP distinguished name (DN) that is used as the base. The DN is a unique identifier for an entry in an LDAP directory tree structure. No spaces are allowed in the Base DN. Only global users and groups discovered underneath this DN are mapped and can be assigned a CA Enterprise Log Manager application group or role.
Password		Enter and confirm the password for the user listed in the User DN row.
User DN		<p>Enter the valid user credentials for any valid user in the user registry whose user record is searchable. Enter the complete distinguished name (DN) of the user.</p> <p>You can log in with any user ID that has an administrative role. The User DN and associated password are the credentials used to attach to the external directory host.</p>
Use Transport Layer Security (TLS)		Specifies whether your user store is to use the TSL framework to protect plain text transmissions. When selected, TLS is used when making the LDAP connection to the external directory.
Include Unmapped Attributes		Specifies whether to include fields that are not synchronized from the LDAP directory. External attributes that are not mapped can be used for searching and as filters.
Cache Global Users		Specifies whether to store global users in memory for quick access. Selection allows for faster lookups at the cost of scalability. For a small test environment, selection is recommended.
Cache Update Time		If you selected to cache Global Users, specify the frequency, in minutes, for updating the cached global groups and users to include new and changed records.
Retrieve Exchange Groups as Global User Groups		If the type of external directory is Microsoft Active Directory, this option specifies that you want to create global groups from Microsoft Exchange group information. If selected, you can write policies against members of distribution lists.

CA SiteMinder Worksheet

Before you reference CA SiteMinder as the user store, gather the following configuration information:

Required information	Value	Comments
Host		Defines the host name or IP address of the referenced CA SiteMinder system. You can use IPv4 or IPv6 IP addresses.
Admin Name		The user name for the CA SiteMinder super user who maintains system and domain objects.
Admin Password		The password for the associated user name.
Agent Name		The name of the agent provided to the Policy Server. The name is not case-sensitive.
Agent Secret		The case-sensitive shared secret as defined to CA SiteMinder. The agent secret is case-sensitive.
Cache Global Users		Specifies whether to cache global users in memory, which allows for faster lookups at the cost of scalability. Note: Global user <i>groups</i> are always cached.
Cache Update Time		The interval in minutes after which the user cache is automatically updated.
Include Unmapped Attributes		Specifies whether to include external attributes that are not mapped for use as filters or in searches.
Retrieve Exchange Groups as Global User Groups		If the type of external directory is Microsoft Active Directory, this option specifies that you want to create global groups from Microsoft Exchange group information. If selected, you can write policies against members of distribution lists.
Authorization Store Type		Defines the type of user store in use.
Authorization Store Name		Specifies the assigned name of the user store referenced in the Authorization Store Type field.

Users with Administrator Role

Only users assigned the role of Administrator can configure CA Enterprise Log Manager components.

After installing the first CA Enterprise Log Manager, you access the CA Enterprise Log Manager through a browser, log in with your EiamAdmin credentials, and configure the user store.

The next step is to assign the Administrator application group to the account of the user who is to do the configuration. If you configured the user store as the CA Enterprise Log Manager user store, the default, you create a new user account and assign it the Administrator role. If you referenced an external user store, you cannot create a new user. In this case, you search for the user record of the individual who is to be the administrator, and add the Administrator application group to this user's account.

Password Policy Planning

If you accept the default user store, you define new users and set password policies for these user accounts from within CA Enterprise Log Manager. Using strong passwords helps protect your computing resources. Password policies help enforce the creation of strong passwords and can help prevent the use of weak passwords.

The default password policies provided with CA Enterprise Log Manager provide for a very *soft* form of password protection. For example, the default policy allows users to use their user name as their password and allows them to unlock passwords. It allows passwords never to expire and does no locking based on failed login attempts. The default options are intentionally set to a very low-level of password security to allow you to create your own, custom password policies.

Important! You should modify the default password policies to match the password restrictions in use at your company. We do not recommend running CA Enterprise Log Manager in production environments with the default password policies!

You can disallow these activities, enforce policies on the password attributes such as length, character type, age, and reuse, and establish a lock policy based on a configurable number of failed login attempts as part of your custom password policy.

More information:

[Configure Password Policies](#) (see page 119)

User Name as Password

For passwords to be strong, security best practices mandate that passwords should not contain or match the user name. The default password policy enables this option. While this option may seem useful when setting the temporary password for new users, it is a good practice to clear this password policy selection. Clearing this option prevents users from using this kind of weak password.

Password Age and Reuse

Consider the following guidelines when determining age and reuse policies:

- The password reuse policy can ensure that a given password is not re-used frequently. This policy creates a password history. A setting of 0 means that password history is not enforced. A setting greater than 0 specifies the number of passwords that are saved and used for comparison when the password is changed. A strong password policy should prevent users from reusing a password for at least a year.
- The recommended *maximum age* for a password varies with password length and complexity. One general rule is that an acceptable password is one that cannot be broken by a brute-force attack in less than the maximum allowed age of the password. A good standard for maximum age is 30 to 60 days.
- Setting a *minimum age* prevents users from resetting passwords many times during a single session to work around a reuse restriction policy. A common best practice recommendation is 3 days.
- If you set a password age, it is recommended that you warn users to reset their passwords. You can set the warning to occur at the midpoint of the age or closer to expiration.
- You should lock user accounts after a reasonable number of failed logins. This can help prevent successful password guessing by hackers. Three to five attempts is a standard number after which an account is locked.

Password Length and Format

Consider the following guidelines when determining whether to enforce length requirements:

- Because of the way passwords are encrypted, the most secure passwords are seven or 14 characters long.
- Take care not to exceed password length limitations imposed by any old operating systems on your network.

Consider the following guidelines when determining whether to enforce policies on maximum repeating characters or minimum number or numeric characters.

- Strong passwords are not found in any dictionary.
- Strong passwords include one or more characters from at least three of the four sets of lower case letters, upper case letters, digits, and special characters.

Subscription Update Planning

This section contains information and procedures on planning subscription updates for your CA Enterprise Log Manager environment.

More information:

[The Subscription Service](#) (see page 43)

[How Subscription Works](#) (see page 44)

[How to Plan Subscription Updates](#) (see page 46)

[Subscription Architecture](#) (see page 47)

[Offline Subscription Architecture](#) (see page 49)

The Subscription Service

Your environment can have one server performing all tasks, or it can have several servers, each dedicated to performing one or more specific roles, such as collection, correlation and reporting. You use the Subscription Service to keep all of your servers up to date with the latest content, operating system and product updates.

The Subscription Service uses a proxy-client system to deliver updates. CA Technologies publishes updates, packaged into *modules*, to the CA Technologies Subscription Server. One or more servers in your environment act as subscription *proxies*. These proxies contact the CA Technologies Subscription Server over the Internet, download update modules, and self-install them. All other servers in your environment are subscription clients, downloading updates from the proxies in turn.

In some environments, security policies or other considerations restrict network access to the Internet. In these cases, you update your CA Enterprise Log Manager environment through offline subscription. Offline subscription requires you to download updates from the CA Technologies offline subscription FTP site. You then manually copy the updates to a CA Enterprise Log Manager proxy that does not have internet access, called an *offline proxy*. Updates proceed normally, with subscription clients downloading and installing updates from this offline proxy.

Note: By default, the Subscription Service is not configured to perform automatic updates. To use the Subscription Service, you must configure settings, such as choosing modules and setting an update schedule.

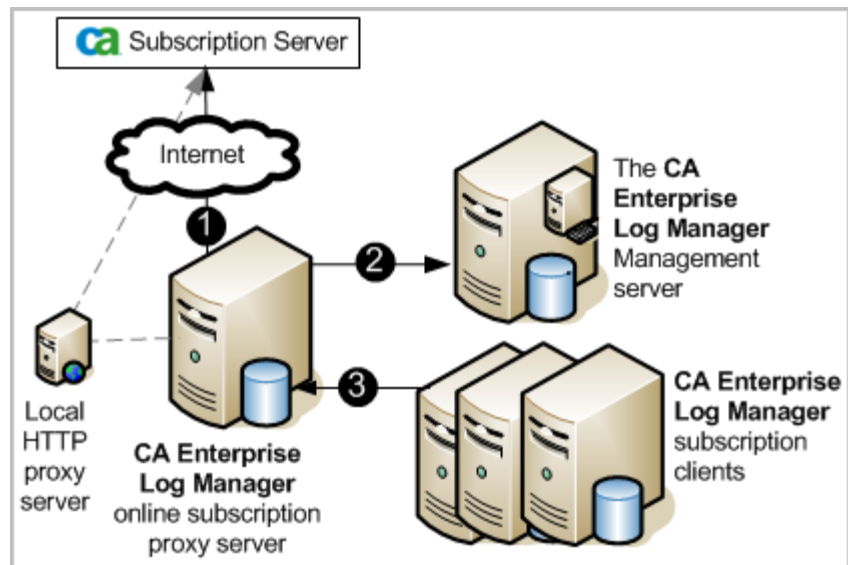
How Subscription Works

Subscription involves the following components:

- CA Technologies Subscription Server
- HTTP proxy server (optional)
- One or more CA Enterprise Log Manager subscription proxy servers
- CA Enterprise Log Manager management server
- One or more CA Enterprise Log Manager subscription clients

You can configure subscription updates to proceed automatically, according to a subscription schedule you set. You can also perform subscription updates on demand, manually starting the update process as needed.

The following diagram illustrates the Subscription Service process in detail.



1. The subscription proxy server contacts the CA Technologies Subscription Server. You can configure proxy servers to contact the Subscription Server either directly or through your local HTTP proxy. Proxies contact the CA Technologies Subscription Server either automatically, according to a schedule you set, or on demand, whenever you manually begin an update. The proxy server downloads and self-installs any operating system and product updates.

If you are using offline subscription, you manually download the update files to a system separate from your CA Enterprise Log Manager environment, and copy them to the offline proxy server.

2. The subscription proxy pushes content and integration updates to the management server. The management server is, by default, the first CA Enterprise Log Manager server you install, and stores all content information, such as reports, integrations and correlation rules, for your environment.
3. Subscription clients contact the subscription proxy for updates, either automatically or on demand. Clients download and self-install the updates.

Note: Subscription proxies install any updates they download before making them available to clients.

How to Plan Subscription Updates

Planning the architecture of subscription updates for your CA Enterprise Log Manager environment lets you ensure that all servers receive the updates you select, in a timely and secure manner.

To plan subscription updates for your CA Enterprise Log Manager environment, complete the following process. For details, see the related procedures.

1. Begin by designing a proxy-client structure for your CA Enterprise Log Manager servers. Decide which servers to designate as proxies and which to designate as clients, keeping in mind the role of each server, and network traffic considerations.
2. Consider any Internet access limitations in your environment, and decide whether you need one or more offline proxies.
3. Consider any Internet security and traffic concerns, and decide whether to include a local HTTP proxy in your subscription architecture. Online subscription proxies can contact the CA Technologies Subscription Server directly, or using your local HTTP proxy.
4. Consider whether you want to download all updates automatically, according to the subscription schedule you set, or if there are some update types you want to download manually. For example, internal security policies may require that you test certain upgrades before applying them to your environment.
5. Consider how frequently to update your CA Enterprise Log Manager environment. Updates are available on a regular basis; the frequency depends on the type of update. For details on update types, see About Modules to Download in the More Information section.

Note: Confirm that you have adequate disk space to download subscription updates to each CA Enterprise Log Manager server, before proceeding with subscription updates. If the available disk space on a server is less than 5 GB, the Subscription Service issues a self-monitoring event and suspends the download process.

More information:

[Subscription Architecture](#) (see page 47)

[Offline Subscription Architecture](#) (see page 49)

[About Modules to Download](#) (see page 168)

Subscription Architecture

Your CA Enterprise Log Manager environment can be a single-server system, or it can include two or more servers. Design your subscription architecture based on the number and roles of the CA Enterprise Log Manager servers in your environment. Possible subscription architectures include:

- Single-server environment
- Multiple-server environment with one subscription proxy
- Multiple-server environment with multiple subscription proxies

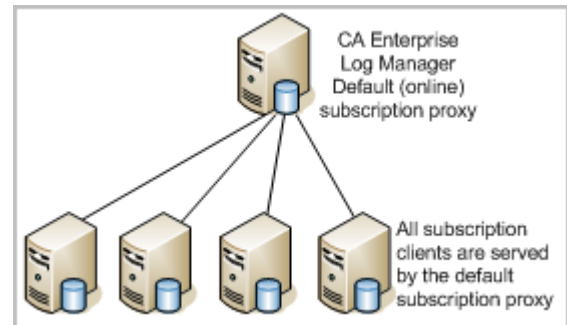
Note: When choosing a subscription architecture, consider whether you need one or more offline proxies. For details, see *Offline Subscription Architecture* in the *More Information* section.

The first CA Enterprise Log Manager server you install is configured upon installation as the *default subscription proxy*, which downloads and installs subscription updates if no other proxy is configured or available. Subsequent CA Enterprise Log Manager servers are, by default, configured as subscription clients. You can change the configuration of any CA Enterprise Log Manager server to act as an online or offline subscription proxy, or as a subscription client. You can also choose any online subscription proxy in your environment to act as the default subscription proxy.

The *content server* provides content and integration updates to the management server, which stores and retrieves application content for your environment. This server can be the default subscription proxy, or you can configure any online subscription proxy in your environment to act as the content server.

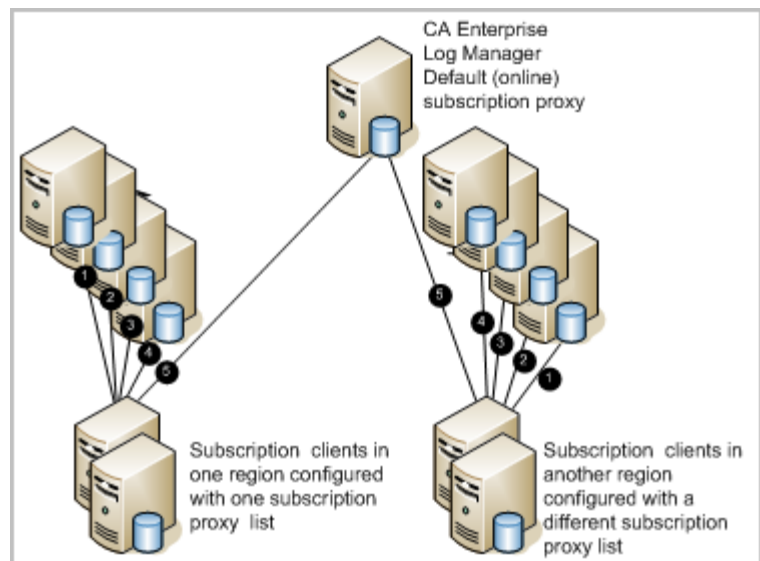
In a single-server environment, the sole CA Enterprise Log Manager server is configured as a subscription proxy. The server downloads and self-installs CA Enterprise Log Manager updates through the Subscription Service. The server also acts as the content server for the environment.

In a small environment with two or more servers, you can configure one server as both the subscription proxy and the content server, and all other servers as subscription clients. You can choose the default subscription proxy to act as the subscription proxy for your environment, or you can select any other CA Enterprise Log Manager server to be the proxy. The subscription proxy downloads and self-installs CA Enterprise Log Manager updates, and subscription clients contact the proxy to download their updates in turn. You can configure clients to download the same updates as the proxy downloads, or a subset of that group.



In a large multiple-server environment, you can configure multiple servers as subscription proxies, each one providing updates to a limited group of subscription clients. This allows the Subscription Service to work efficiently by balancing traffic to the subscription proxies.

With multiple proxies, you can also configure subscription proxy lists. Proxy lists help ensure that all CA Enterprise Log Manager servers successfully receive current updates in a timely manner. If a given proxy is unavailable when a client requests CA Enterprise Log Manager updates, the client contacts each proxy on its proxy list in turn until it succeeds in downloading the updates. You can configure a global proxy list for client updates, as well as for content updates, for your entire CA Enterprise Log Manager environment. You can also set a custom proxy list for client updates for each CA Enterprise Log Manager server.



More information

[How to Plan Subscription Updates](#) (see page 46)

[Offline Subscription Architecture](#) (see page 49)

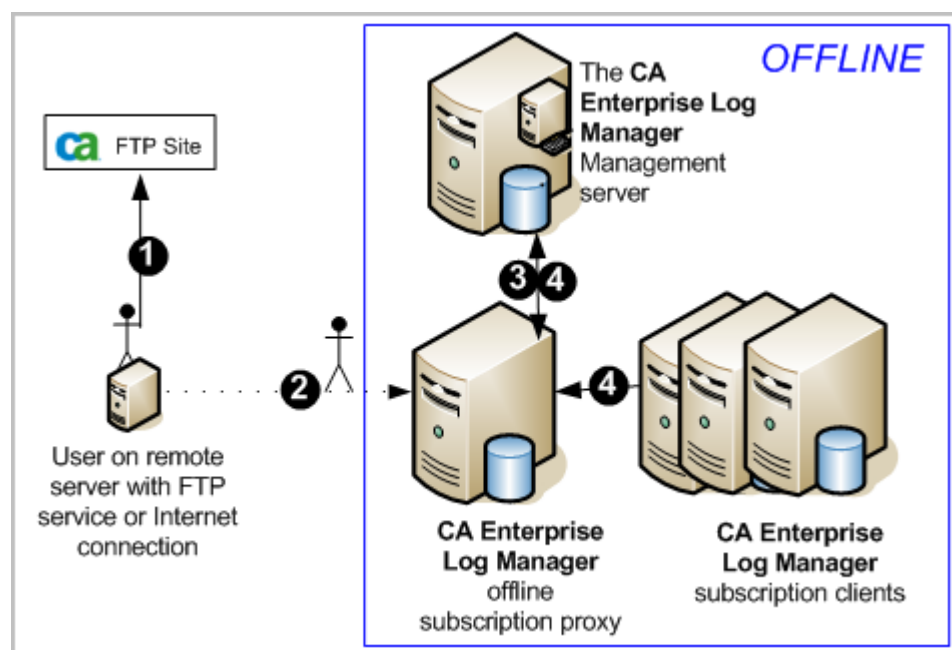
Offline Subscription Architecture

If security policies or other considerations restrict network access to the Internet, you can update your CA Enterprise Log Manager environment through offline subscription. Offline subscription allows you to isolate some or all of your servers from the Internet while still keeping your CA Enterprise Log Manager environment up to date. Circumstances in which it is necessary to configure offline subscription include:

- No servers in your CA Enterprise Log Manager environment are permitted to internet access.
- Some servers in your network are allowed internet access, while others are not allowed even a connection to a server with internet access.

The only difference between online and offline subscription is how update files are delivered to the subscription proxy. In online subscription, the proxy contacts the CA Technologies Subscription Server over the Internet. In offline subscription, you download updates from a CA Technologies FTP site, then manually copy them to a CA Enterprise Log Manager server configured as an offline proxy.

The following diagram illustrates the offline subscription process. In this example, the entire CA Enterprise Log Manager environment is offline.



1. A system administrator downloads updates from a CA Technologies FTP site to a system that is allowed Internet or FTP access.
2. The system administrator manually copies the update files to an offline CA Enterprise Log Manager proxy. You can transfer the files using physical media such as a disk, or using scp, which is included with CA Enterprise Log Manager.
3. Updates then proceed exactly as in online subscription. The offline proxy self-installs the updates and pushes content updates to the management server.

Note: You can allow the offline proxy to update itself as scheduled, it is good practice to perform a manual update on the offline proxy when you transfer new files. This practice ensures that the updates are available when subscription clients request them.

4. Clients of the offline proxy download the updates, according the schedule you set or when you perform a manual update.

Note: Offline subscription clients always receive all updates that are manually installed on the offline proxy server. Subscription modules selected for an offline subscription client at the local level have no effect.

A subscription architecture can also be "mixed." For example, you can designate only one proxy as offline, while you designate others as online. The offline proxy and any clients assigned to it remain isolated from the Internet, while the rest of your CA Enterprise Log Manager environment receives updates through online subscription. Because of its complexity, a mixed architecture is not considered best practice. Carefully consider and plan your overall subscription strategy before implementing this architecture.

Important! In a mixed subscription environment, do not include offline proxies in the proxy list for any online subscription client. If you do, the online subscription client automatically receives all updates that are manually installed, instead of the modules you selected globally for your CA Enterprise Log Manager environment or locally for that client.

More information

[How to Plan Subscription Updates](#) (see page 46)

[Subscription Architecture](#) (see page 47)

Example: Subscription Configuration with Six Servers

When you approach subscription configuration, consider the other roles the servers are performing before deciding on their subscription role. By default, the management server, the first server you install, is the default subscription proxy. All other servers are subscription clients of the default subscription proxy. While acceptable, it is better to configure an online subscription proxy and have the default proxy act as a failover or redundant proxy. A good practice is to assign the online proxy role to the least active server.

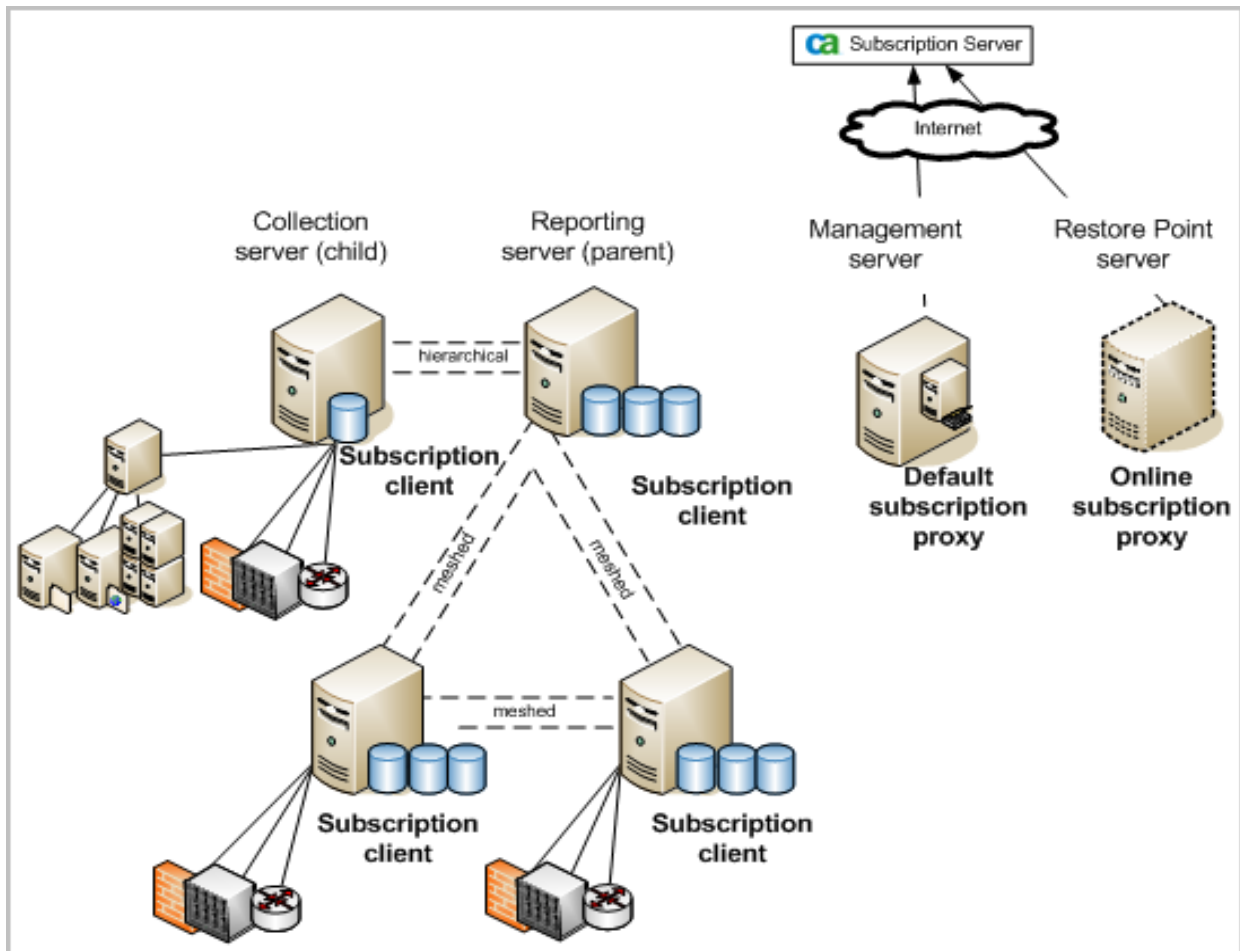
Example: Six Servers Where the Least Busy Server is the Online Subscription Proxy

Consider a scenario of six CA Enterprise Log Manager servers. The management server is dedicated to authenticating and authorizing users at login and storing application content. Four federated servers handle event processing and reporting. A sixth server is a dedicated restore point for investigating events from restored databases. An advantage of having a dedicated restore point is that you can keep old data from being included on current reports by not including this server in your federation.

In this example, the two servers labeled collection and reporting represent a configuration with exceptionally high processing requirements. These servers are federated in a hierarchical configuration, where the collection server is the child of the reporting server. The two servers that act as both collection and reporting servers represent a configuration with normal event volumes and scheduled reports. They are federated with each other and the dedicated reporting server in a meshed federation; that is, the three servers are peers. The purpose of federating servers is to extend the ability to get query results from the servers you federate. A federated query from any of the meshed servers returns events from itself and the other three servers in the federation.

Note: If you want to run consolidated reports on self-monitoring events, include the management server in the federation.

In this scenario, the recommended solution is to configure the restore point as the online subscription proxy because it is the least active server. Then configure each client to point to this online proxy, so the default proxy can act as a backup, if the online proxy is busy or unavailable.



More information:

[Configuring a CA Enterprise Log Manager Federation](#) (see page 195)

Agent Planning

Agents use connectors to collect events and transport them to the CA Enterprise Log Manager server. You can configure a connector on the default agent that is installed with the CA Enterprise Log Manager server, or you can install an agent on a server or event source in your network. The decision to use external agents is based on event volume, agent location, data filtering needs, and other considerations. Planning for agent installation involves the following:

- Understanding the relationships between the following components:
 - Integrations and listeners
 - Agents
 - Connectors
- Sizing your network to decide how many agents to install

You should install agents relatively close to the event sources from which you want to collect event logs. Most connectors collect events from one and only one event source. For syslog events, a single syslog listener can receive events from multiple event source types. An agent can control and handle event traffic from more than one connector.

About Syslog Event Collection

CA Enterprise Log Manager can receive events directly from syslog sources. Syslog collection differs from the other collection methods because several different log sources can send events to CA Enterprise Log Manager simultaneously. Consider a network router and a VPN concentrator as two possible event sources. Both can send events to CA Enterprise Log Manager directly using syslog, but the log formats and structures are different. A syslog agent can receive both kinds of events at the same time using the supplied syslog listener.

Generally speaking, event collection falls into two categories:

- CA Enterprise Log Manager *listens* for syslog events on configurable ports.
- CA Enterprise Log Manager *monitors* other event sources for their events, for example, using WMI to collect Windows events.

More than one syslog event source can transmit events through a single connector, since the listener receives all of the traffic on a specified port. CA Enterprise Log Manager can listen for syslog events on any port. (If you are running an agent as a non-root user there may be restrictions on the use of ports lower than port 1024.) The standard ports may be receiving an event stream composed of many different types of syslog events. These might include UNIX, Linux, Snort, Solaris, CiscoPIX, Check Point Firewall 1, and others. CA Enterprise Log Manager handles syslog events using listeners which are a specialized type of integration component. You build syslog connectors based on listeners and integrations:

- The listener provides the connection information such as ports or trusted hosts.
- The integration defines the message parsing (XMP) and data mapping (DM) files.

Because a single syslog connector may receive events from many event sources, you should consider whether to route syslog events based on their type or source. The size and complexity of your environment determine how you balance your syslog event reception:

Many syslog types : 1 Connector

If a single connector has to process events from different syslog sources, and event volume is high, the connector has to parse through all of the applied integrations (XMP files) until it finds a match for an event. This can cause slower performance because there is much more processing to do. However, if event volume is not too high, a single connector on the default agent may be enough to collect all of the required events for storage.

1 syslog type : 1 Connector

If you configure a series of single connectors to process events from a single syslog type, you can lighten the processing load by spreading it across several connectors. However, having too many connectors running on a single agent can also degrade performance, as each is a separate instance requiring individual processing.

Some syslog types : 1 Connector

If your environment has a heavier event volume for certain types of syslog events, you may want to configure a connector to collect only that type. You could then configure one or more other connectors to collect more than one syslog event types that have a lighter event volume in your environment. In this way, you can balance the syslog event collection load across a smaller number of connectors ensuring better performance.

You should not necessarily need to create your own syslog listeners, though you can do so if necessary. You could create separate syslog listeners with different default values for ports, trusted hosts, and so forth. This can help to simplify the creation of connectors if you have many connectors to create for each type of syslog event, for example.

More information:

[Default User Accounts](#) (see page 90)

[Redirect Firewall Ports for syslog Events](#) (see page 95)

Agents and the Agent Certificate

The predefined CAELM_AgentCert.cer certificate is used by all agents to communicate with their CA Enterprise Log Manager server.

If you choose to replace this certificate with a custom certificate, we recommend you do this before installing any agents. If you implement a custom certificate after agents are installed and registered with a CA Enterprise Log Manager server, you must uninstall each agent, delete the agent entry from the Agent Explorer, reinstall the agent, and reconfigure the connectors.

About Agents

Agents run as a service or daemon after installation and are optional product components, used in one or more of the following situations:

- A small, remote site needs to collect event data but does not require a full CA Enterprise Log Manager soft appliance.
- You need to filter data at the event source to reduce network traffic or the amount of data being stored.
- You need to guarantee event delivery to the event log store for compliance.
- You need to secure log transmission across the network with data encryption.

Agents act as process managers for connectors that collect event data from specific applications, operating systems, or databases. Agents deliver connector management commands such as start, stop, and restart from the Agent Explorer interface in the CA Enterprise Log Manager. Agents also apply connector configuration changes and binary updates.

You can install agents on individual event sources, or you can install agents on remote host servers to gather events from more than one event source. The CA Enterprise Log Manager server installation automatically installs its own agent. You can use this default agent for direct syslog event collection.

You can also view the status of any agent from the Agent Explorer on any CA Enterprise Log Manager server in the network. Agents have a watchdog service that restarts an agent in the event that it stops unexpectedly, and monitors for agent and connector binary updates. Agents also send self-monitoring events to the event log store for tracking of changes and status.

About Agent Groups

You can also create agent groups, which are logical groupings of agents that facilitate their management. After you make an agent part of an agent group, you can change configurations, and start and stop all of the connectors in a group at the same time. As an example, you might decide to group agents by their physical, geographical region.

You can create groups and move agents between groups in the Agent Explorer. If you do not define an agent group, then all agents reside in a default group created when you install CA Enterprise Log Manager.

Agent configurations and agent group records are stored in the management server. Each time you install an agent, the management server makes the new agent available in the Agent Explorer for every CA Enterprise Log Manager server that it has registered under the same application instance name. This allows you to configure and control any agent from any CA Enterprise Log Manager server in the network.

Agent User Account Privileges

Agents can run with low-privilege user accounts. You should create a group and a service user account on the target host before you install an agent. You will specify the user name during the agent installation, and the install program sets the permissions appropriately. On Linux systems, the agent user owns all of the agent binaries, except for the watchdog binary which the root user owns.

About Integrations

The set of out-of-box integrations is essentially a library of templates. These templates provide the code specific to collecting events from a particular kind of log source. An integration becomes a connector when taken from the library, configured, and applied to an event source. Integrations contain the following kinds of information:

- Data access file with information for a particular kind of event source
- Message parsing file that creates name-value pairs from collected event logs
- Data mapping file that maps the parsed name-value pairs to the common event grammar that forms the database schema for the CA Enterprise Log Manager server's event log store

CA Enterprise Log Manager provides a variety of integrations for popular and common event sources including CA Technologies products, popular firewalls, databases, operating systems, applications, and so forth. You can get additional integrations in the following ways:

- Subscription updates that include new integrations or new versions of existing ones
- Create custom integrations using the supplied wizard

You use integrations to specify the kind of event collection you want to do when you configure connectors.

About Connectors

Connectors listen for events and also periodically send status events to the agent for transport to the CA Enterprise Log Manager server. A *connector* is a process that uses a log sensor and an integration to create a configuration for collecting events from a particular event source. Other than for syslog, a connector uses an integration as its configuration template. Syslog connectors are based on listeners.

Agents use connectors to collect events. After you install an agent, you can use the Agent Explorer on any CA Enterprise Log Manager server to configure one or more connectors on that agent. (The CA Enterprise Log Manager servers must be registered under the same management server (or external CA EEM server) and with the same application instance name to configure agents in this way.)

Note: While you can theoretically configure up to 256 connectors on a given agent, performance decreases with a large number of connectors. We recommend configuring no more than 70 connectors per agent for best performance.

There is generally one connector for each event source in the network. For syslog events, there may be one connector for many event sources, depending on your configuration choices. You can create several connectors that use the same integration but that have slightly different configuration details for accessing different event sources. Some connectors offer configuration helpers which gather information needed for access to the event source. If you need a connector for which there is currently no integration provided, you can create an integration using the integration wizard.

About Log Sensors

A *log sensor* is the component in a connector that understands how to access event sources. CA Enterprise Log Manager provides log sensors for the following different types of event sources and log formats:

ACLogsensor

This log sensor reads CA Access Control events when CA Access Control uses selogrd for routing events.

FileLogSensor

This log sensor reads events from a file.

LocalSyslog

This log sensor collects events from any UNIX server's local syslog files.

ODBCLogSensor

This log sensor uses ODBC to connect to, and to retrieve events from, a database event source.

OPSELogSensor

This log sensor reads events from a Check Point OPSEC event source.

SDEELogSensor

This log sensor reads events from Cisco devices.

Syslog

This log sensor listens for syslog events.

TIBCOLogSensor

This log sensor reads events from a TIBCO Event Message Service (EMS) queue in CA Access Control implementations.

W3CLogSensor

This log sensor reads events from a W3C log format file.

WinRMLinuxLogSensor

This log sensor enables the default (Linux) agent on the CA Enterprise Log Manager server to collect Windows events.

WMILogSensor

This log sensor collects events from Windows event sources using Windows Management Instrumentation (WMI).

Other log sensors may be made available through subscription updates. More information on configuring log sensors is available in the online help and the *Administration Guide*.

Sizing Your CA Enterprise Log Manager Network

When planning the number of agents needed, consider using a simple sizing scheme such as the following. First, determine the number of connectors you need. You do not have to install an agent on every event source. But you configure one connector for each non-syslog event source from which you plan to collect events. (You can collect WMI events from multiple event sources on a single connector by adding a log sensor for each event source. Be sure to consider aggregate event volumes when configuring a connector in this way.)

You can configure syslog connectors in various ways. For example, you can configure a single syslog connector to receive all syslog events regardless of type. However, a good practice is to base your syslog connectors on the event volumes from specific syslog event sources.

You can install agents on an individual event source. We recommend this approach when the event count from that source is high. Your plan should distinguish between agents on an event source and agents on a host that act as a collector of different kinds of events.

Suppression Rule Effects

During planning, you may want to consider the effect of *suppression rules*, which prevent events either from being inserted into the event log store or collected by a connector. Suppression rules are always attached to a connector. You can apply suppression rules at either the agent or group level, or at the CA Enterprise Log Manager server itself. The placement locations have different effects:

- Suppression rules applied at the agent or group levels prevent events from being collected and thus reduce the amount of network traffic *sent* to the CA Enterprise Log Manager server.
- Suppression rules applied at the CA Enterprise Log Manager server prevent events from being *inserted* into the database and thus reduce the amount of information being stored.

There are potential performance considerations in applying suppression rules to events after they arrive at the CA Enterprise Log Manager server, especially if you create multiple suppression rules or the event flow rate is high.

For example, you might want to suppress *some* of the events from a firewall or from some Windows servers that produce duplicate events for the same action. Not collecting these events can speed up the transport of the event logs you do want to keep, and saves processing time on the CA Enterprise Log Manager server. In such cases, you would apply one or more appropriate suppression rules on agent components.

If you want to suppress all events of a certain type from multiple platforms or across your entire environment, you would apply one or more appropriate suppression rules at the CA Enterprise Log Manager server. Evaluation of events with regard to suppression occurs when events arrive at the CA Enterprise Log Manager server. Applying a large number of suppression rules at the server may lead to slower performance as the server must apply suppression rules in addition to inserting events into the event log store.

For smaller implementations, you can perform suppression at the CA Enterprise Log Manager server. You may also choose to apply suppression at the server for deployments where summarization (aggregation) is in use. If you are only inserting a few of the events from an event source that generates large amounts of event information, you may still choose to suppress unwanted events at the agent or agent group level to save processing time on the CA Enterprise Log Manager server.

Chapter 3: Installing CA Enterprise Log Manager

This section contains the following topics:

[Understanding the CA Enterprise Log Manager Environment](#) (see page 61)

[Create the Installation DVDs](#) (see page 63)

[Installing a CA Enterprise Log Manager Server](#) (see page 64)

[Upgrade Existing CA Enterprise Log Manager Servers and Agents for FIPS Support](#) (see page 74)

[Adding New CA Enterprise Log Manager Servers to an Existing FIPS Mode Federation](#) (see page 80)

[Installation Considerations for a System with SAN Drives](#) (see page 82)

[Initial CA Enterprise Log Manager Server Configurations](#) (see page 89)

[Install the ODBC Client](#) (see page 96)

[Installing the JDBC Client](#) (see page 101)

[Installation Troubleshooting](#) (see page 104)

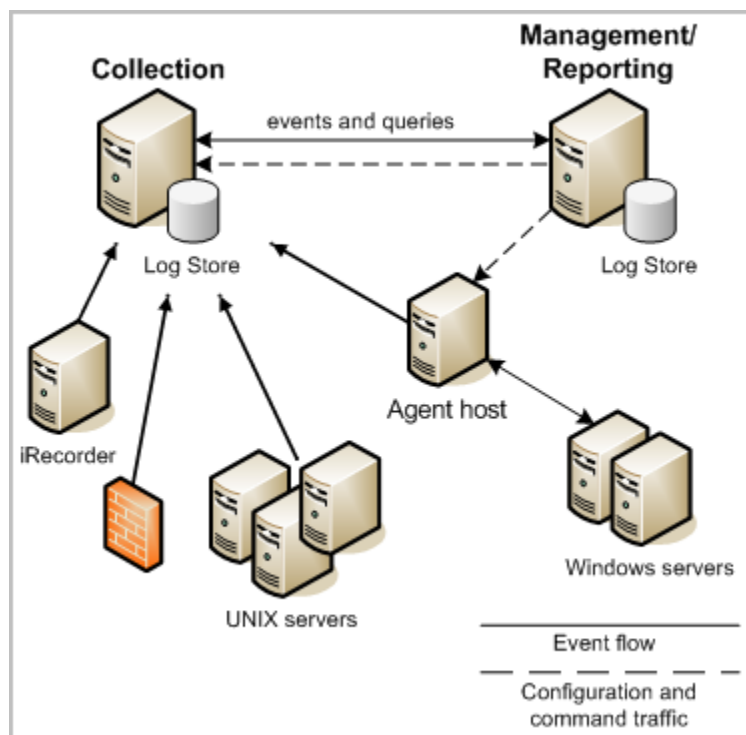
Understanding the CA Enterprise Log Manager Environment

CA Enterprise Log Manager is designed to be up and running in a short time from the start of install to the time that the product is collecting log information and generating reports. You must install the CA Enterprise Log Manager soft appliance on a dedicated system.

Important! Since the CA Enterprise Log Manager server is dedicated to high-performance event log collection, you should not install other applications on the server that hosts it. Doing so could have an adverse affect on performance.

There are a variety of ways that you can configure your environment. We recommend the following, specific configuration to help ensure handling of high event volumes in enterprise environments.

For a basic enterprise-level, production environment, install at least two CA Enterprise Log Manager servers into your existing network. The CA Enterprise Log Manager servers use the existing DNS servers in your network to work with named event sources and agent hosts. One server focuses on collection and the other on reporting of collected event logs. In a two-server environment, the management server you install first takes the role of a reporting server. As management server, it performs user authentication and authorization, and other management functions. The following illustration shows this basic environment with some event sources:



Solid lines in this diagram show event flow from event sources to the collection server, or to an agent host and then to the collection server. You can collect syslog events directly using the default agent on the collection CA Enterprise Log Manager server. You could also configure one or more connectors on a separate agent host to collect from multiple syslog sources (not shown in this diagram).

Windows event collection uses Windows Management Instrumentation (WMI) to monitor Windows servers for their events. This requires that you configure a WMI connector on an agent installed on a Windows host as an event collection point. For some other event types, you may decide to use a standalone CA Technologies iRecorder on a host server.

You can configure and manage the agents and connectors for these event sources from any CA Enterprise Log Manager server in the network. Dashed lines in the diagram represent configuration and control traffic between the management server and agents, and each of the other CA Enterprise Log Manager servers. In the environment represented in this diagram, you perform configurations from the management server. This allows the collection server to focus on processing events.

The log collection environment into which you install CA Enterprise Log Manager servers has the following characteristics:

- The management CA Enterprise Log Manager server handles user authentication and authorization as well as managing the configurations of all of the CA Enterprise Log Manager servers, agents, and connectors in your network using its local CA EEM server.

Depending on the size of your network and its event volume, you may choose to install more than one management server and build federations of collection servers under each one. Or, you can dedicate multiple servers to reporting, where all reporting servers register with your one management server. In this scenario, the event flow passes from event sources to the configured collection server to its configured reporting server.

- One or more collection CA Enterprise Log Manager servers process and store incoming events.
- Events flow through your log collection network from a variety of event sources *after* you configure their corresponding connectors or adapters.

Create the Installation DVDs

The CA Enterprise Log Manager software is available as downloadable, zipped ISO images. After you download the software, you need to create DVD media before you can install. Use this procedure to download the ISO images and then create the installation disks.

To create the installation DVDs

1. Access the download server at <http://ca.com/support> from an Internet-connected computer.
2. Click the Technical Support link and then click the Download Center link.
3. Choose CA Enterprise Log Manager in the Select a Product field, and then choose the release in the Select a Release field.
4. Check the Select all components check box and then click Go.

The Published Solutions Downloads page appears.

5. Select the download package.

The solutions document page appears.

6. Scroll to the bottom of the page and select the Download link opposite the package name.

The download of the package starts.

Note: The download may take some time to complete, depending upon your connection speed.

7. Unzip the two installation images.
8. Create two separate installation disks by burning the operating system and CA Enterprise Log Manager ISO disk images onto separate DVD-RW media.

The two installation disks contain all of the operating system and product components, respectively, for your CA Enterprise Log Manager environment. You may decide to use other components such as SAPI recorders or iRecorders in your environment. These are separate downloads available on the CA Technologies Support web site.

9. Use the newly-created installation disks for the installations.

Installing a CA Enterprise Log Manager Server

The installation process involves the following steps:

- Complete the CA Enterprise Log Manager server worksheet
- Install the CA Enterprise Log Manager management server

Note: If using SAN storage, take precautions to avoid installing on a SAN drive.

- Install one or more CA Enterprise Log Manager collection servers
- (Optional) Install one or more reporting servers

Note: If you do not install a server dedicated to reporting, you can use the management server for this reporting server role.

- (Optional) Install a restore point server
- Verify the installation
- View self-monitoring events

Important! Configure your storage disks in a RAID array *before* you begin the CA Enterprise Log Manager installation. Configure the first two disks as RAID 1 and make this array the bootable array. Configure the remaining disks as a single RAID 5 array. Failure to configure the RAID array could result in a loss of data.

As part of the overall security of the CA Enterprise Log Manager server itself, during installation the Grand Unified Boot-loader (GRUB) utility is password-protected.

More information:

[Install with Disabled SAN Drives](#) (see page 82)

[Install with Enabled SAN Drives](#) (see page 88)

CA Enterprise Log Manager Server Worksheet

Before you install a CA Enterprise Log Manager server, gather the information in the following table. After you complete the worksheet, you can use it as you work through the installation prompts. You can print and complete a separate worksheet for each CA Enterprise Log Manager server you plan to install.

CA Enterprise Log Manager Information	Value	Comments
OS Disk		
Keyboard Type	<i>appropriate value</i>	Specify the keyboard type you want to use by its national language setting. The default value uses hardware settings for the keyboard you have connected to the server when it starts.
Time Zone Selection	<i>your desired time zone</i>	Select the time zone where this server resides.
Root Password	<i>new root password</i>	Create and confirm a new root password for this server.
Application Disk		
New Hostname	<i>hostname for this CA Enterprise Log Manager server</i> For example: CA-ELM1	Specify the hostname for this server using only supported characters for hosts. Industry standards recommend A-Z (case-insensitive), 0-9, and hyphen, where the first character is a letter and the final character is alphanumeric. Do not use the underscore character in a host name. Note: Do not append a domain name to this host name value.
Select a device	<i>device name</i>	Select the name of the network adapter to use for event log collections and communications. Press the space bar to enter the configuration for the device.

CA Enterprise Log Manager Information	Value	Comments
IP Address, Subnet Mask, and Default Gateway	<i>relevant IP values</i>	Enter a valid IP address for this server. Enter a valid subnet mask and default gateway for use with this server.
Domain name	<i>your domain name</i>	Enter the fully-qualified domain name in which this server operates, for example, mycompany.com. Note: The domain name must be registered with the Domain Name Server (DNS) server in your network to enable resolution of the hostname to IP address.
List of DNS servers	<i>relevant IPv4 or IPv6 addresses</i>	Enter one or more DNS server IP addresses in use in your network. The list is comma-separated with <i>no</i> spaces between entries. If your DNS servers use IPv6 addressing, enter these addresses in that format.
System Date and Time	<i>local date and time</i>	Enter a new system date and time if needed.
Update Time through NTP?	Yes (recommended) or No	Indicate whether you want to configure the CA Enterprise Log Manager server to update its date and time from an established Network Time Protocol (NTP) server. Note: Time synchronization helps ensure alerts contain complete data.
NTP Server Name or Address	<i>relevant hostname or IP address</i>	Enter the host name or the valid IP address of the NTP server from which this CA Enterprise Log Manager server gets date and time information.
Sun Java JDK EULA	Yes	Read through the license agreement, paging down until you reach the question, Do you agree to the above license terms? [yes or no].
CA EULA	Yes	Read through the license agreement, paging down until you reach the question, Do you agree to the above license terms? [yes or no].

CA Enterprise Log Manager Information	Value	Comments
Local or Remote CA Embedded Entitlements Manager server?	Local - for the first installed server (management server) Remote - for each additional server	<p>Indicate whether you plan to use a local or a remote CA EEM server.</p> <p>For a management CA Enterprise Log Manager server, choose Local. The installation prompts you to create a password for the default EiamAdmin user account.</p> <p>For each additional server, choose Remote. The installation prompts you for the management server name.</p> <p>Regardless of whether you chose local or remote, you must use the EiamAdmin account ID and password to log into <i>each</i> CA Enterprise Log Manager server the first time.</p>
Enter name of the CA EEM server	<i>IP address or hostname</i>	<p>This prompt displays only if you select Remote for the Local or Remote server prompt.</p> <p>Enter the IP address or host name of the management CA Enterprise Log Manager server that you installed first.</p> <p>The host name must be registered with the DNS Server.</p>

CA Enterprise Log Manager Information	Value	Comments
CA EEM Server Admin password	<i>EiamAdmin account password</i>	<p>Record the password for the default administrator account, EiamAdmin.</p> <p>Your CA Enterprise Log Manager server <i>requires</i> these account credentials for the initial login.</p> <p>If you are installing the management server, you are creating and confirming a new EiamAdmin password here.</p> <p>Make a note of this password as you will use it again during the installations of other CA Enterprise Log Manager servers and agents.</p> <p>Note: The password you enter here is also the initial password for the default caelmadmin account that you will use to access the CA Enterprise Log Manager server directly through ssh.</p> <p>You can create additional administrator accounts to access the CA EEM functions after installation, if desired.</p>
Application Instance Name	CAELM	<p>When you install the first CA Enterprise Log Manager server in your network, you create an application instance value in this prompt.</p> <p>Subsequent CA Enterprise Log Manager servers use this value to register with the management server.</p> <p>The default application instance name is CAELM.</p> <p>You can use any name for this value.</p> <p>Make a note of the application instance name for use with later CA Enterprise Log Manager installations.</p>

CA Enterprise Log Manager Information	Value	Comments
Do you want to run CAELM Server in FIPS Mode?	yes or no	<p>Your response to this prompt determines whether the CA Enterprise Log Manager server will start up in FIPS mode.</p> <p>Note: If you are adding a server to an existing CA Enterprise Log Manager deployment, the CA Enterprise Log Manager management server or remote CA EEM server must also be in FIPS mode. Otherwise the new server cannot register and you will have to reinstall the new server again.</p>

Note: The install provides you with a chance to review and to change the CA EEM server details before it attempts connection.

If the installation program is unable to connect with the management server you specify, and you decide to continue the installation, you can register the CA Enterprise Log Manager server with the embedded CA EEM functionality manually. If this happens, you must also import the content, CEG, and agent management files manually. Refer to the section on installation troubleshooting for more information and instructions.

More information:

[Register CA Enterprise Log Manager Server with the CA EEM Server](#) (see page 107)

[Acquire Certificates from CA EEM Server](#) (see page 107)

[Import CA Enterprise Log Manager Reports](#) (see page 108)

[Import CA Enterprise Log Manager Data Mapping Files](#) (see page 109)

[Import Common Event Grammar Files](#) (see page 109)

[Import Common Agent Management Files](#) (see page 111)

Install CA Enterprise Log Manager

Use this procedure to install a CA Enterprise Log Manager server.

To install the CA Enterprise Log Manager software

1. Boot the server with the OS installation DVD.
The operating system installation starts automatically.

2. Respond to the prompts using the information you gathered in the CA Enterprise Log Manager server worksheet.

Declining the license agreement stops the installation and shuts down the server.

3. Respond to the reboot prompt by first removing the media and then clicking Reboot.
4. Insert the CA Enterprise Log Manager Application disk when prompted and press Enter.

5. Respond to the prompts using the information you gathered in the work sheet.

The installation continues. When you see the message, "CA Enterprise Log Manager installation succeeded." the installation is complete.

Note: When you install a second or subsequent CA Enterprise Log Manager server, you may notice an error message in the installation log saying the application name that the installation attempted to register with the CA EEM server already exists. You can safely ignore this error, as each CA Enterprise Log Manager installation attempts to create the application name as if it was new.

After the installation is complete, you must configure your CA Enterprise Log Manager server before you can receive events. This may include configuring a connector on the default agent to receive syslog events.

More information

[Installation Troubleshooting](#) (see page 104)

[Configuring the Default Agent](#) (see page 177)

Verify that the iGateway Process is Running

If you are unable to access the CA Enterprise Log Manager server's web interface after installation, and you are sure that the network interface ports are correctly configured, it may be that the igateway process is not running.

You can perform a quick check of the iGateway process status using this procedure. The iGateway process must be running for the CA Enterprise Log Manager server to collect events and for the user interface to be accessible.

To verify the iGateway daemon

1. Access a command prompt on the CA Enterprise Log Manager server.
2. Log in with the caelmadmin account credentials.
3. Switch users to the root account with the following command:

```
su - root
```

4. Use the following command to verify that the iGateway process is running:

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

The operating system returns the iGateway process information and a list of processes running under iGateway.

More information:

[Resolve Network Interface Configuration Error](#) (see page 106)

Start the iGateway Daemon or Service

The iGateway daemon or service is the process that handles all calls to the user interface for both CA EEM and CA Enterprise Log Manager. The process must be running for you to access either application. Use this procedure to start the iGateway process if it is not running.

Note: If you are unable to start iGateway, ensure the "/" folder has available disk space. Lack of disk space can prevent you from successfully starting iGateway.

To start the iGateway daemon or service

1. Log in as the caelmadmin user for the CA Enterprise Log Manager server.
2. Switch users to the root account with the following command:

```
su -
```

3. Start the igateway process with the following command:

```
$IGW_LOC/S99igateway start
```

S99igateway is the start-up script for the igateway process and is owned by the root account. When the igateway process starts, it runs under the caelmservice user account.

Stop the iGateway Daemon or Service

The iGateway daemon or service is the process that handles all calls to the user interface for both CA EEM and CA Enterprise Log Manager. The process must be running for you to access either application. Use this procedure to stop the iGateway process. You might do this in preparation to restart the process or when removing a CA Enterprise Log Manager server from the network.

To stop the iGateway daemon or service

1. Log in as the caelmadmin user for the CA Enterprise Log Manager server.
2. Switch users to the root account with the following command:

```
su -
```

3. Stop the igateway process with the following command:

```
$IGW_LOC/S99igateway stop
```

S99igateway is the shut down script for the igateway process and is owned by the root account. When the igateway process starts, it runs under the caelmservice user account.

Start the CA Enterprise Log Manager Agent Daemon or Service

The CA Enterprise Log Manager agent daemon or service is the process that manages connectors which send collected events to a CA Enterprise Log Manager server. The process must be running for connectors to be able to collect events. Use this procedure to start the CA Enterprise Log Manager agent process if it is not running.

To start the CA ELM Agent daemon or service

1. Log in as a root or Windows Administrator user.
2. Access a command prompt and enter the following command:

```
Linux, UNIX, Solaris: /opt/CA/ELMAgent/bin/S99elmagent start
```

```
Windows: net start ca-elmagent
```


Stop the CA Enterprise Log Manager Agent Daemon or Service

The CA Enterprise Log Manager agent daemon or service is the process that manages connectors which send collected events to a CA Enterprise Log Manager server. The process must be running for connectors to be able to collect events. Use this procedure to stop the CA Enterprise Log Manager agent process. Normally, start and stop commands are issued from within the Agent Explorer on any CA Enterprise Log Manager server. You might use this command in preparation to restart an agent process and all of its connectors.

To stop the CA ELM Agent daemon or service

1. Log in as a root or Windows Administrator user.
2. Access a command prompt and enter the following command:

Linux, UNIX, Solaris: `/opt/CA/ELMAgent/bin/S99elmagent stop`

Windows: `net stop ca-elmagent`

Verify the CA Enterprise Log Manager Server Installation

You can verify the CA Enterprise Log Manager server installation using a web browser. You can perform an initial verification of the installation by logging into the CA Enterprise Log Manager server.

Note: When you log into the CA Enterprise Log Manager application for the first time, you must use the EiamAdmin user credentials with which you installed the CA Enterprise Log Manager server. After you log in with this user account, you can only see and use specific user and access management functions. You must then configure your user store and create a new CA Enterprise Log Manager user account to access the other CA Enterprise Log Manager functionality.

To verify the CA Enterprise Log Manager server

1. Open a web browser and enter the following URL:

`https://<server_IP_address>:5250/spin/calrm`

The CA Enterprise Log Manager login screen appears.

2. Log in as the EiamAdmin administrative user.

The Administration tab's User and Access Management subtab appears. You can consider the installation successful if you are able to log into the CA Enterprise Log Manager server.

Note: You must configure one or more event source services before you can receive event data and view reports.

View Self-Monitoring Events

You can use self-monitoring events to verify that CA Enterprise Log Manager server is installed properly. While you have some configuration tasks to complete before CA Enterprise Log Manager can collect and report on event log data from around your network, you can see self-monitoring events generated by the CA Enterprise Log Manager server right away.

Logging into the CA Enterprise Log Manager server is the first and best test of a successful installation. Self-monitoring events are another way to check on the status of the CA Enterprise Log Manager server. There are a number of self-monitoring event types available. Use this procedure to see additional event data from events generated by the CA Enterprise Log Manager server itself.

To view self-monitoring events

1. Log into the CA Enterprise Log Manager server.
2. Access the Reports tab.
3. Click the System tag and select the report, Self Monitoring Events Detail.

The self-monitoring events report loads.

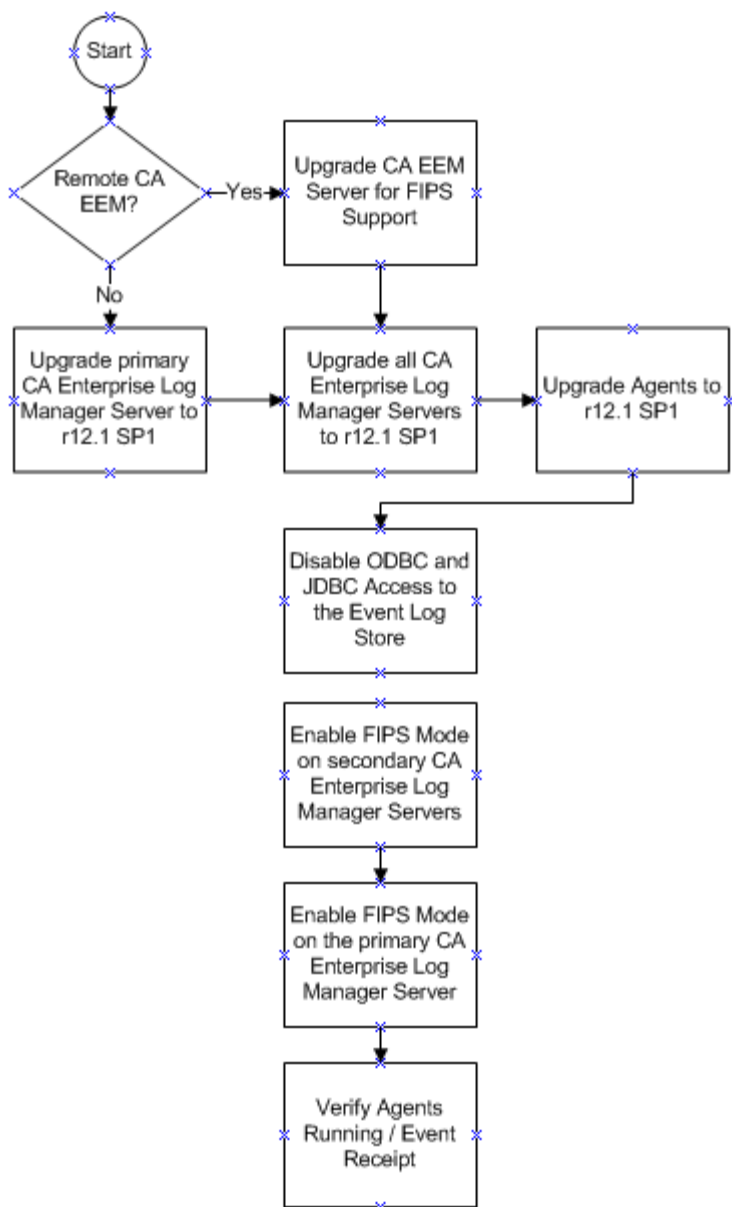
4. Verify that the self-monitoring events for your login and other preliminary configuration actions are present in the report.

Upgrade Existing CA Enterprise Log Manager Servers and Agents for FIPS Support

You can upgrade existing CA Enterprise Log Manager servers and agents for FIPS support using the Subscription Service. This upgrade process assumes the following:

- You installed CA Enterprise Log Manager r12.1, or upgraded to that level from r12.0 SP3.
- You want to enable FIPS mode for your CA Enterprise Log Manager federation.

Use the following process to upgrade your servers:



The upgrade and FIPS enablement process includes the following steps:

1. Upgrade the primary or Management server to r12.1 SP1.

If you use a remote CA EEM server, ensure that it is at a release level that supports FIPS operation. See the *CA EEM Release Notes* for more information about upgrading for FIPS support.

Detailed instructions for using the Subscription Service to upgrade both CA Enterprise Log Manager servers and agents are available in the *Administration Guide* section on subscription.

2. Upgrade all other CA Enterprise Log Manager servers in the federation to r12.1 SP1.
3. Upgrade all the agents to r12.1 SP1 and update the connector log sensors as needed.

Important! If you deployed a connector that uses the syslog log sensor on a Windows host, update all of these connector configurations to use the latest syslog sensor for this release, when running in FIPS mode. Refer to the CA Enterprise Log Manager Product Integration Matrix https://support.ca.com/irj/portal/anonymous/phpdocs?filePath=0/8238/8238_integration_certmatrix.html for the latest list of integrations that use the syslog log sensor.

4. Disable ODBC and JDBC access to the event log store.
5. Enable FIPS mode on each of the secondary CA Enterprise Log Manager servers in the federation.

Agents automatically detect the operating mode from the CA Enterprise Log Manager server that manages them.

6. Enable FIPS mode on the primary or Management server.
7. Verify that the agents are running in FIPS mode using the Agent Explorer dashboard.

You can also verify that the agents are sending events using a query or report, or by examining the self monitoring events tab in the System Status Service area.

When you upgrade an existing agent to r12.1 SP1, the subscription processing updates the agent in non-FIPS mode by default. You set the FIPS mode for the CA Enterprise Log Manager server that manages an agent. An agent detects the FIPS mode of its managing server and restarts itself in the corresponding mode as needed. Use the Agent Explorer dashboard in the CA Enterprise Log Manager user interface to view the FIPS mode for an agent, if you have Administrator user privileges. See the upgrade information in the *Implementation Guide* section on installing CA Enterprise Log Manager, or the online help for agent management tasks for more information.

More information:

[Enable FIPS Mode Operation](#) (see page 78)

[View Agent Dashboard](#) (see page 79)

Prerequisites for Upgrade for FIPS Support

The following are prerequisites for upgrading CA Enterprise Log Manager to support FIPS 140-2:

- Begin with an installation of either CA Enterprise Log Manager r12.0 SP3 or r12.1
- Upgrade to CA Enterprise Log Manager r12.1 SP1 through subscription

More information:

[Adding New CA Enterprise Log Manager Servers to an Existing FIPS Mode Federation](#)
(see page 80)

Upgrade Guidelines

The following guidelines apply to upgrading to CA Enterprise Log Manager with FIPS support:

- If you have more than one CA Enterprise Log Manager server in a federation, upgrade the primary or Management CA Enterprise Log Manager server to r12.1 SP1 first. Then you can upgrade all other servers in any order. The upgraded server starts in non-FIPS mode only. Enabling FIPS mode requires an Administrator user to set the operating mode manually.

Important! Do not switch to FIPS mode on any secondary CA Enterprise Log Manager server during subscription processing. This can cause subscription processing to fail.

- CA Enterprise Log Manager servers at r12.1 SP1 can communicate with r12.1 agents, but agent-level FIPS support is not available until you upgrade to r12.1 SP1.
- When you enable FIPS mode, only r12.1 SP1 FIPS-enabled agents and later can communicate with the CA Enterprise Log Manager server. When you enable *non-FIPS* mode, the CA Enterprise Log Manager server is fully backward compatible with older agents, but FIPS mode operation is not available. We recommend that you install *only* r12.1 SP1 agents after upgrading your CA Enterprise Log Manager servers to r12.1 SP1.
- Agents associated with a CA Enterprise Log Manager server automatically detect server mode changes and restart themselves in the corresponding mode.
- Adding a new CA Enterprise Log Manager server to an existing federation running in FIPS mode requires special handling. See the *Implementation Guide* section on adding a new CA Enterprise Log Manager server to an existing federation for more information.

Upgrading a Remote CA EEM Server

If you are using a stand-alone CA EEM server with your CA Enterprise Log Manager installation, upgrade it for FIPS support before upgrading any of your CA Enterprise Log Manager servers or agents. See the instructions in the *CA EEM Getting Started* guide for details and instructions.

Disable ODBC and JDBC Access to the Event Log Store

You can prevent ODBC and JDBC access to the events in the event log store using options in the ODBC Service configuration dialog. If you plan to run your federated network in FIPS mode, disable the ODBC and JDBC access to remain in compliance with federal standards.

To disable ODBC and JDBC access

1. Log in to the CA Enterprise Log Manager server and access the Administration tab.
2. Click the Services subtab and then expand the ODBC Service node.
3. Select the desired server.
4. Clear the Enable Service check box and then click Save.

Note: Disable the ODBC option for *each* CA Enterprise Log Manager server in a federation to verify that ODBC and JDBC are disabled.

Enable FIPS Mode Operation

You can use the FIPS Mode options in the System Status service to turn FIPS mode on and off. The default FIPS mode is non-FIPS. Administrator users must set the FIPS mode for each CA Enterprise Log Manager server in a federation.

Important! You cannot operate with mixed modes within the same federation of servers. Any server in a federation running in a different mode is not able to gather query and report data, or respond to requests, from the other servers.

To switch between FIPS and non-FIPS modes

1. Log in to the CA Enterprise Log Manager server.
2. Access the Administration tab, and then click the Services subtab.
3. Expand the System Status service node and select the desired CA Enterprise Log Manager server.

The System Status Service Configuration dialog appears.

4. Select the desired FIPS mode, On or Off, from the drop-down list.
5. Click Save.

The CA Enterprise Log Manager server restarts in the selected mode. You can log in again to view agent FIPS mode from the Agent Explorer.

6. Verify the CA Enterprise Log Manager server operating mode by checking the System Status service dialog after the server restarts.

You can also use self monitoring events to verify that the CA Enterprise Log Manager server started in the desired mode. Look for the following events in the Self Monitoring Events tab in the System Status dialog:

Successfully turned Server FIPS mode ON
Successfully turned Server FIPS mode OFF
Failed to turn Server FIPS mode ON
Failed to turn Server FIPS mode OFF

Disabling FIPS mode for the primary or Management server stops all federated queries and reports returning data. In addition, scheduled reports do not run. This condition continues until all servers in the federation are running in the same mode again.

Note: Disabling FIPS on the Management or remote CA EEM server is one of the requirements for adding a new CA Enterprise Log Manager server to a federation of server running in FIPS mode.

View Agent Dashboard

You can view the agent dashboard to view the status of agents in your environment. The dashboard also displays details such as the current FIPS mode (FIPS or non-FIPS), and usage details. These include events per second load, CPU percentage use, and most recent update date and time.

To view the agent dashboard

1. Click the Administration tab, and then the Log Collection subtab.

The Log Collection folder list appears.

2. Select the Agent Explorer folder.

Agent management buttons appear in the details pane.

3. Click Agent Status Monitor and Dashboard: 

The agent search panel appears, displaying status for all available agents in a details chart. For example:

Total: 10 Running: 8 Pending: 1 Stopped: 1 Not Responding: 0

4. (Optional) Select agent search criteria to narrow the list of displayed agents. You can select any one or more of the following criteria:
- Agent Group—returns only agents assigned to the selected group
 - Platform—returns only agents running on the selected platform
 - Status—returns only agents with the Status you select, Running, for example.
 - Agent name pattern—returns only agents containing the specified pattern.
5. Click Show Status.

A list of agents meeting your search criteria appears, displaying information including:

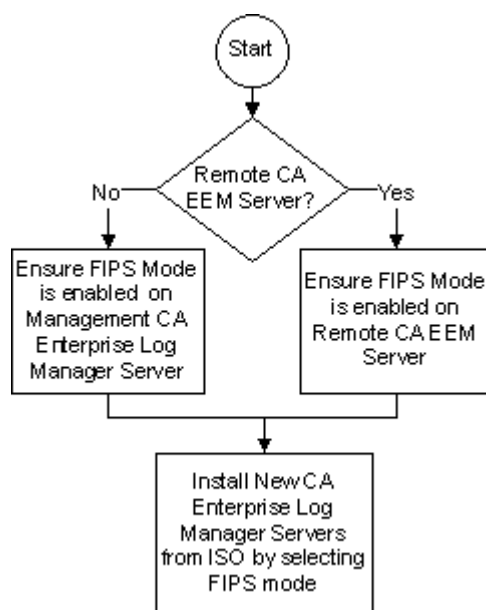
- Local connector name and version
- Current CA Enterprise Log Manager server
- Agent FIPS Mode (FIPS or non-FIPS)
- Last recorded event per second load handled by the agent
- Last recorded CPU usage value
- Last recorded memory usage value
- Most recent configuration update
- Configuration update status

Adding New CA Enterprise Log Manager Servers to an Existing FIPS Mode Federation

There are some special guidelines for adding a new CA Enterprise Log Manager server to a federation of servers already running in FIPS mode. Unless you specify FIPS mode during the installation, newly-installed CA Enterprise Log Manager servers run in *non-FIPS* mode by default. Servers running in non-FIPS mode cannot communicate with servers running in FIPS mode.

As part of its installation, a new CA Enterprise Log Manager server must register with the local, embedded CA EEM server on the Management server, or with a stand-alone remote CA EEM server. The processes for adding a server to an existing network are based on the location of the managing CA EEM server.

Consider the following workflow:



The process for adding a new server includes the following steps:

1. Ensure FIPS mode is enabled on the Management (primary) CA Enterprise Log Manager server, or on the remote CA EEM server.
2. Using the ISO image or DVDs for CA Enterprise Log Manager 12.1 SP1 or above, install one or more new CA Enterprise Log Manager secondary servers.

Important! Be sure you specify FIPS mode during the installation. Otherwise the newly installed server will not be able to communicate with the management server or remote CA EEM server and you will have to reinstall the new CA Enterprise Log Manager server again.

Because the CA Enterprise Log Manager management server or remote CA EEM server is operating in FIPS mode, the new CA Enterprise Log Manager server is able to register and join the federation.

More information:

[Enable FIPS Mode Operation](#) (see page 78)

[View Agent Dashboard](#) (see page 79)

Installation Considerations for a System with SAN Drives

When you install the operating system for the CA Enterprise Log Manager appliance on a system with SAN drives, take precautions to prevent CA Enterprise Log Manager from being installed on a SAN drive. Such an installation fails.

Take one of the following approaches to help ensure a successful installation:

- Disable the SAN drives. Install the operating system and the CA Enterprise Log Manager application as usual. Then, configure the SAN drives for CA Enterprise Log Manager and recycle CA Enterprise Log Manager to activate the SAN configuration.
- Leave the SAN drives enabled. Begin the operating system installation. Exit this procedure as described to change the sequence of operations defined in the kickstart file. Resume the installation process and finish it as documented.

More information:

[Install with Disabled SAN Drives](#) (see page 82)

[Install with Enabled SAN Drives](#) (see page 88)

Install with Disabled SAN Drives

CA Enterprise Log Manager is currently supported using fixed hardware configurations provided by Dell, IBM, and HP. The following example assumes that the hardware consists of HP Blade Servers using a QLogic Fiber Channel card to connect to a storage area network (SAN) for data storage. The HP Blade Servers come with SATA hard drives configured in RAID-1 (mirrored) configuration.

If you use the kickstart boot file as is, be sure to disable the SAN drives before beginning the installation. Start the installation process with the OS5 DVD and complete the installation as documented.

Note: If you do not start the installation with the SAN drives disabled, CA Enterprise Log Manager is installed on the SAN. In this case, a red screen appears with the message, Illegal Opcode, after CA Enterprise Log Manager reboots.

Use the following sequence of procedures to install a CA Enterprise Log Manager appliance on a system with SAN drives, where you disable the SAN drives before installing the operating system.

1. Disable the SAN drives.
2. Install the operating system on the appliance.
3. Install the CA Enterprise Log Manager server.
4. Set up a multipath configuration for SAN storage.
5. Create a logical volume.
6. Prepare the logical volume for CA Enterprise Log Manager.
7. Recycle the CA Enterprise Log Manager.
8. Verify installation success.

When installing the operating system with disabled SAN drives, you work with the following files:

lvm.conf

The configuration file for the Linux Logical Volume Manager (LVM2).

multipath.conf (/etc/multipath.conf)

The configuration file for Linux multipathing.

fstab (/etc/fstab)

The file systems table file that maps devices to directories in a Linux system.

More Information:

[Disable the SAN Drives](#) (see page 83)

[Install CA Enterprise Log Manager](#) (see page 69)

[Set Up a Multipath Configuration for SAN Storage](#) (see page 84)

[Create a Logical Volume](#) (see page 85)

[Prepare the Logical Volume for CA Enterprise Log Manager](#) (see page 86)

[Recycle the CA Enterprise Log Manager Server](#) (see page 87)

[Verify the CA Enterprise Log Manager Server Installation](#) (see page 73)

Disable the SAN Drives

Use the procedures recommended by your SAN drive vendor to disable the SAN drives on the hardware on which you plan to install the soft appliance.

Disable the SAN drives before installing the soft appliance operating system or the CA Enterprise Log Manager application.

Set Up a Multipath Configuration for SAN Storage

Setting up a multipath configuration is required for a CA Enterprise Log Manager system installed on a RAID system that is to use SAN storage. Physical disks on the SAN are partitioned into logical storage spaces named logical unit numbers (LUNs).

Set up a multipath configuration for SAN storage

1. Log on to the CA Enterprise Log Manager appliance and su to root.
2. (Optional) Do a directory listing of /dev/mapper to view the state of the configuration before setting up multipathing and logical volumes. Results resemble the following:

```
drwxr-xr-x 2 root root    120 Jun 18 12:09 .
drwxr-xr-x 11 root root   3540 Jun 18 16:09 ..
crw----- 1 root root   10, 63 Jun 18 12:09 control
brw-rw---- 1 root disk 253,  0 Jun 18 16:09 VolGroup00-LogVol00
brw-rw---- 1 root disk 253,  2 Jun 18 12:09 VolGroup00-LogVol01
brw-rw---- 1 root disk 253,  1 Jun 18 16:09 VolGroup00-LogVol02
```

3. Open the .../etc/multipath.conf file for edit and proceed as follows:
 - a. Add the following section under "device {" for each LUN provided by the SAN administrator:

```
device {
    vendor            "NETAPP"
    product           "LUN"
    path_grouping_policy multibus
    features           "1 queue_if_no_path"
    path_checker       readsector0
    path_selector      "round-robin 0"
    failback           immediate
    no_path_retry      queue
}
```

- b. Uncomment the 'blacklist' section for all devices. The blacklist section enables multipathing on default devices.

```
blacklist {
    devnode "^(ram|raw|loop|fd|md|dm-|sr|scd|st)[0-9]*"
    devnode "^hd[a-z]"
    devnode "^cciss!c[0-9]d[0-9]*"
}
```

- c. Save and close the multipath.conf file.
4. Verify that Multipath is turned on and that the LUNs are listed by running the following:

```
multipath -l
```

Note: Paths display as 'mpath0' and 'mpath1'. If the LUNs are not shown, reboot and run multipath again.

5. View the available drives.

```
fdisk -l
```

6. List the available partitions and verify that 'mpath0' and 'mpath1' are listed.

```
ls -la /dev/mapper
```

7. Map the first partition as follows:

```
kpartx -a /dev/mapper/mpath0
```

8. Map the second partition as follows:

```
kpartx -a /dev/mapper/mpath1
```

Create a Logical Volume

You can use volume manager software to combine multiple LUNs into a logical volume for CA Enterprise Log Manager to access. Logical Volume Manager (LVM) manages disk drives and similar mass-storage devices on the Linux operating system. Storage columns created under the LVM can be resized or moved on to backend devices like SAN storage.

To create a logical volume

1. Create the first physical volume:

```
pvcreate /dev/mapper/mpath0
```

2. Create the second physical volume:

```
pvcreate /dev/mapper/mpath1
```

3. Show all the physical volumes on the system:

```
pvdisplay
```

4. Create the VolGroup01 volume group. (The VolGroup00 volume group exists.)

```
vgcreate VolGroup01 /dev/mapper/mpath0 /dev/mapper/mpath1
```

Note: This command creates a volume and makes the two physical volumes part of the group.

5. Create a logical volume within the volume group:

```
lvcreate -n LogVol00 -l 384030 VolGroup01
```

6. Create a file system:

```
mkfs -t ext3 /dev/VolGroup01/LogVol00
```

Prepare the Logical Volume for CA Enterprise Log Manager

After you create a logical volume, you populate it with the expected directory structure and assign the ownership and group associations required by CA Enterprise Log Manager. You use vi to modify the fstab file to point to the logical volume you created and then you mount the new data directory.

To prepare the logical volume for CA Enterprise Log Manager

1. Create a temporary directory, /data1, change the ownership of the /data1 directory to caelmservice, and change the group associated with this directory to caelmservice:

```
mkdir /data1
chown caelmservice /data1
chgrp caelmservice /data1
```

2. Stop the CA Enterprise Log Manager server iGateway processes:

```
/opt/CA/SharedComponents/iTechnology/S99igateway stop
```

3. Change directories to the directory where the CA Enterprise Log Manager agent is running, stop the agent, and verify that the services are stopped:

```
cd /opt/CA/ELMAgent/bin/
./caelmagent -s
ps -ef | grep /opt/CA
```

4. Change directory to /data1.

5. Mount the new file system on /data1, copy the contents of the /data directory into the /data1 directory, and verify that the two directories are the same:

```
mount -t ext3 /dev/VolGroup01/LogVol00 /data1
cp -pR /data/* /data1
diff -qr /data /data1
```

6. Unmount the existing data mount point and then unmount the data1 mount point:

```
umount /data
umount /data1
```

7. Delete the /data directory and rename the /data1 directory to /data.

```
rm -rf /data
mv /data1 data
```

8. Modify the line in `/etc/fstab` that references the `/data` directory and point it to the new Logical Volume. That is, change `/dev/VolGroup00/LogVol02` to `/dev/VolGroup01/LogVol00`. The changed data is shown in boldface type in the following rendering of a sample `fstab` file.

device name	mount point	fs-type	options	dump-freq pass-num
none	<code>/dev/VolGroup00/LogVol00/</code>	ext3	defaults	1 1
none	<code>/dev/VolGroup01/LogVol00/data</code>	ext3	defaults	1 2
<code>LABEL=/boot</code>	<code>/boot</code>	ext3	defaults	1 2
tmpfs	<code>/dev/shm</code>	tmpfs	defaults	0 0
devpts	<code>/dev/pts</code>	devpts	<code>gid=5,mode=620</code>	0 0
sysfs	<code>/sys</code>	sysfs	defaults	0 0
proc	<code>/proc</code>	proc	defaults	0 0
none	<code>/dev/VolGroup00/LogVol01</code>	swap	defaults	0 0

9. Mount the new data directory and verify all the partitions in `/etc/fstab` are mounted:

```
mount -a
```

```
mount
```

Recycle the CA Enterprise Log Manager Server

After you create a logical volume, recycle CA Enterprise Log Manager so that you can use the logical volume. To verify success, browse to CA Enterprise Log Manager and view events returned by the System All Events Details query.

To recycle the CA Enterprise Log Manager server

1. Start the CA Enterprise Log Manager server iGateway processes:
`/opt/CA/SharedComponents/iTechnology/S99igateway start`
2. Start the ELMAgent service
`/opt/CA/ELMAgent/bin/caelmagent -b`
3. Reboot the CA Enterprise Log Manager server.

Install with Enabled SAN Drives

The topic, Example: Set Up SAN Storage for CA Enterprise Log Manager, includes the recommendation to disable the SAN drives (LUNs) before installing the operating system on the CA Enterprise Log Manager appliance.

An alternative is to leave the SAN drives enabled but to modify the kick-start file, `ca-elm-ks.cfg`, with an ISO editing tool, after starting the operating system installation. The modification helps ensure that the install and boot are done from the local hard disk, not from the SAN.

To boot from the local disk (not SAN)

1. Boot the server with the OS installation DVD
2. Respond to the first prompt for keyboard type.
3. Press Alt-F2 to display the Anaconda/Kickstart prompt.
4. Type the following:

```
list-harddrives
```

The list of available drives displays, where the list resembles the following:

```
cciss/c0d0 – 68GB RAID 1 (cciss is HP Smart Array)
Sda – 500GB SAN (sda – h is the SAN Multipathed)
Sdb – 500GB SAN
Sdc – 500GB SAN
Sdd – 500GB SAN
Sde – 500GB SAN
Sdf – 500GB SAN
Sdg – 500GB SAN
Sdh – 500GB SAN
```

5. Identify the local hard drive. In this case, it is `cciss/c0d0`.

6. Take the following steps:
 - a. Open the CA Enterprise Log Manager operating system kickstart file, `ca-elm-ks.cfg` for edit. Use an ISO editor.
 - b. Locate the following line to edit:

```
bootloader --location=mbr --driveorder=sda,sdb
```


Change it to the following:

```
bootloader --location=mbr --driveorder=cciss/c0d0
```


This change specifies to boot from the local disk only.
 - c. Locate the following lines to edit:

```
clearpart --all --initlabel  
part /boot --fstype "ext3" --size=100  
part pv.4 --size=0 --grow
```


Change these lines to the following:

```
part /boot --fstype "ext3" --size=100 --ondisk cciss/c0d0  
part pv.4 --size=0 --grow --ondisk cciss/c0d0
```


This change to the partition definition lines helps ensure that the partitions are created on the `cciss/c0d0` disk by name. Using `--ondisk`, replaces the existing `$disk1` and `$disk2` variables.
 - d. If appropriate for your case, remove the IF/When clause for the number of disk drives, retaining only the first set of disk commands (lines 57 - 65).
 - e. Save the new ISO image.
7. Exit the Anaconda prompt to return to the operating system installation prompts.
8. Continue with the installation, using the documented procedures.

Initial CA Enterprise Log Manager Server Configurations

Installation of the first CA Enterprise Log Manager server creates an application name whose default value is CAELM. The installation registers this name with the embedded CA EEM server. When subsequent installations use the same application instance name, the management CA Enterprise Log Manager server manages all of the configurations under that same application instance name.

When the installation is complete, the server has both an operating system and a CA Enterprise Log Manager server. The 32-bit operating system supports both 32- and 64-bit hardware. The initial configurations include the following areas:

- Default user accounts
- Default directory structure
- Customized operating system image
- Default port assignments

Default User Accounts

The CA Enterprise Log Manager installation creates a default administrative user, `caelmadmin`, which has its own password. When you need to access the host server directly, you must use this account to login because the root account login capability is restricted after installation. The `caelmadmin` account allows only a login action. From there you must switch users to the root account using its separate password to access utilities for OS-level system administration.

The default password for this account is the same password you created for the `EiamAdmin` account. We recommend that you change the password for the `caelmadmin` account immediately after installation.

The installation also creates a default service user account, `caelmservice`, which you *cannot* use to log into the system. You can switch users to this user to start and stop processes, if needed. The `iGateway` process and the embedded CA EEM server (if one is installed on the CA Enterprise Log Manager server) run under this user account to provide an additional layer of security.

The `iGateway` process does not run under a root user account. Port forwarding is automatically enabled to allow HTTPS requests on ports 80 and 443 to access the CA Enterprise Log Manager user interface, in addition to port 5250.

Default Directory Structure

The CA Enterprise Log Manager installation places software binaries under the directory structure, `/opt/CA`. If the system has a second disk drive, it is configured as `/data`. The installation creates a symbolic link from the directory, `/opt/CA/LogManager/data` to the directory, `/data`. The following represents the default installation directory structure:

File Types	Directory
iTechnology-related files (iGateway)	/opt/CA/SharedComponents/iTechnology
CA Enterprise Log Manager EEM server-related files	/opt/CA/LogManager/EEM

File Types	Directory
CA Enterprise Log Manager installation-related files	/opt/CA/LogManager/install
Data files (links to /data in case of multiple drives)	/opt/CA/LogManager/data
Log files	/opt/CA/SharedComponents/iTechnology

Under normal circumstances, you should not need to access the *ssh* utility on the CA Enterprise Log Manager server, except to move archive files for backup and long term storage, and to add disk drives.

Customized Operating System Image

The installation process customizes the operating system by creating a minimal image and limiting access to as few channels as possible. Non-essential services are not installed. The CA Enterprise Log Manager server listens on a small number of ports and specifically turns off unused ports.

During the operating system installation, you create a password for the root account. After the CA Enterprise Log Manager installation is complete, the root is restricted to allow no subsequent logins. The CA Enterprise Log Manager installation creates a default user, *caelmadmin* that has only login capability and no other permissions.

For root level access to the CA Enterprise Log Manager server, you can access the server with this account and then switch users to the root account for use of administration tools. This means that you will need to know both the *caelmadmin* and *root* passwords to gain access to the system as a root user.

No other specific security-related software is installed with CA Enterprise Log Manager. To maintain peak performance, do not install other applications on the CA Enterprise Log Manager server.

Default Port Assignments

The CA Enterprise Log Manager server is configured by default to listen on port 5250, and on ports 80 and 443 using the HTTPS protocol. CA Enterprise Log Manager processes and daemons do not run under the root account, so they cannot open ports below port 1024. As a result, the installation automatically creates a redirection (through iptables) to port 5250 for incoming user interface requests on ports 80 and 443.

The CA Enterprise Log Manager server's local operating system syslog daemon is not configured because CA Enterprise Log Manager uses its self-monitoring events to track system status. You can see other local events and report on actions taken on the local CA Enterprise Log Manager server using self-monitoring events.

A list of ports used by the CA Enterprise Log Manager environment follows:

Port	Component	Description
53	CA Enterprise Log Manager server	TCP/UDP port that must be available for DNS communications to resolve host names to IP addresses of servers such as CA Enterprise Log Manager servers, the remote CA EEM server, if configured, and the NTP server if you selected NTP time synchronization at install time. DNS communications is not needed if you map host names to IP addresses in the local /etc/hosts file.
80	CA Enterprise Log Manager server	TCP communications with CA Enterprise Log Manager server user interface over HTTPS; automatically redirected to port 5250.
111	Portmapper (SAPI)	Audit client communications with PortMapper process to receive dynamic port assignments.
443	CA Enterprise Log Manager server	TCP communications with CA Enterprise Log Manager server user interface over HTTPS; automatically redirected to port 5250.
514	Syslog	Default UDP syslog listening port; this port value is configurable. For the default agent to run as a non-root user, the default port is set to 40514, and the installation applies a firewall rule to the CA Enterprise Log Manager server.
1468	Syslog	Default TCP syslog listening port; this port value is configurable.
2123	DXadmin	CA Directory LDAP DXadmin port, if you are using a CA EEM server on the same physical server as the CA Enterprise Log Manager server (the management server).
5250	CA Enterprise Log Manager server	TCP communications with the CA Enterprise Log Manager server user interface using iGateway. TCP communications between: <ul style="list-style-type: none">■ CA Enterprise Log Manager server and CA EEM server■ Federated CA Enterprise Log Manager servers■ Agent and CA Enterprise Log Manager server for status updates
6789	Agent	Agent command and control listening port. Note: If you do not allow outbound traffic, you will need to open this port to enable proper operations.

Port	Component	Description
17001	Agent	<p>TPC port for secure agent to CA Enterprise Log Manager server communications; this port value is configurable.</p> <p>Note: If you do not allow outbound traffic, you will need to open this port to enable proper operations.</p>
17002	ODBC/JDBC	Default TCP port used for communications between ODBC or JDBC driver and the CA Enterprise Log Manager event log store.
17003	Agent	TCP port used for communications by the Qpid message bus for r12.1 agents.
17200	Dispatcher SME Listener	TCP port used for the Dispatcher service on the agent localhost to listen for self monitoring events between agent processes.
17201	Dispatcher Event Listener	TCP port used for the Dispatcher service on the agent localhost to listen for events from client connectors.
random	SAPI	UDP ports used for event collection assigned by the port mapper; you can also configure the SAPI router and collector to use any fixed port value above 1024.

List of Related Processes

The following table represents a list of the processes that run as part of a CA Enterprise Log Manager implementation. The list does not include system processes related to the underlying operating system.

Process Name	Default Port	Description
caelmagent	6789, 17001	This is the CA Enterprise Log Manager agent process.
caelmconnector	Dependent upon what it listens for, or to what it connects.	This is the CA Enterprise Log Manager connector process. There will be a separate connector process running for each connector that is configured on an agent.
caelmdispatcher		This CA Enterprise Log Manager process handles event submission and status information between the connector and agent.
caelmwatchdog	None	CA Enterprise Log Manager watchdog process that monitors other processes to ensure continuity of operations.
caelm-agentmanager		This CA Enterprise Log Manager process handles agent management tasks such as status and subscription.

Process Name	Default Port	Description
caelm-alerting		This CA Enterprise Log Manager process handles alert messages sent via email, IT PAM, and SNMP trap.
caelm-correlation		This CA Enterprise Log Manager process handles correlation rules, communicating with the Correlation service when a correlation rule triggers.
caelm-eemsessionsponsor		CA EEM main process that manages all communications to CA EEM for local sponsors running under safetynet on the CA Enterprise Log Manager server. This process may run under safetynet.
caelm-incidentservice		This CA Enterprise Log Manager process handles incident generation and logging configuration, handling information from the Correlation service when a Correlation rule triggers.
caelm-logdepot	17001	The CA Enterprise Log Manager event log store process that handles event storage, archive file creation, and other functions. This process may run under safetynet.
caelm-queryservice		This CA Enterprise Log Manager process handles the configuration and management of queries.
caelm-reporter		This CA Enterprise Log Manager process handles configuration and management of scheduled reports, report exports, and action alerts.
caelm-ruletest		This CA Enterprise Log Manager process manages rule tests performed on an ad-hoc basis.
caelm-sapicollector		This is the SAPI collector service process. This process may run under safetynet.
caelm-sapirouter		This is the SAPI router service process. This process may run under safetynet.
caelm-systemstatus		This process gathers system status for display in the CA Enterprise Log Manager user interface. This process may run under safetynet.
dxadmind		CA Directory process that runs on the server where CA EEM is installed.
dxserver		CA Directory process that runs on the server where CA EEM is installed.
igateway	5250	CA Enterprise Log Manager main process; must be running to collect and store events.

Process Name	Default Port	Description
message broker		CA Enterprise Log Manager process that communicates between the agent and the CA Enterprise Log Manager server to send events.
oaserver	17002	CA Enterprise Log Manager process that runs to handle server-side processing for ODBC and JDBC requests for access to the event log store.
safetynet		CA Enterprise Log Manager process framework that runs to ensure continuity of operations.
ssld		CA Directory process that runs on the server where CA EEM is installed.

OS Hardening

The CA Enterprise Log Manager soft appliance contains a streamlined and hardened copy of the Red Hat Linux operating system. The following hardening techniques apply:

- Access to SSH as the root user is disabled.
- Use of the Ctrl-Alt-Del key sequence to reboot the server from the console without logging in is disabled.
- Redirections are applied in iptables for the following ports:
 - TCP Port 80 and 443 are redirected to 5250
 - UDP port 514 is redirected to 40514
- The GRUB package is password-protected.
- Installation adds the following low-privilege users:
 - caelmadmin - an operating system account with login rights to the CA Enterprise Log Manager server console
 - caelmservice - service account under which the iGateway and Agent processes run; you cannot login directly using this account

Redirect Firewall Ports for syslog Events

You can redirect traffic on standard ports to another port if you are using a firewall between an agent and the CA Enterprise Log Manager server.

Security best practices dictate the least user privilege required to run application processes and daemons. UNIX and Linux daemons running under non-root accounts cannot open ports below 1024. The standard UDP syslog port is 514. This can create a problem for devices such as routers and switches that cannot use non-standard ports.

To resolve this problem, you can configure the firewall to listen for incoming traffic on port 514 and then send to the CA Enterprise Log Manager server on a different port. The redirection occurs on the same host as the syslog listener. Choosing to use a non-standard port instead means that you would have to reconfigure each event source to send its events on that port.

To redirect event traffic through a firewall

1. Log in as a root user.
2. Access a command prompt.
3. Enter a command to redirect the ports for your specific firewall.

An example of the command line entries for the netfilter/iptables packet filtering tool running on a Red Hat Linux operating system resembles the following:

```
chkconfig --level 345
```

```
iptables on iptables -t nat -A PREROUTING -p udp --dport 514 -j REDIRECT --to  
<yournewport>
```

```
service iptables save
```

4. Replace the variable value, *<yournewport>* with an available port number greater than 1024.

For other implementations, refer to the instructions for handling ports provided by your firewall vendor.

Install the ODBC Client

Installing an ODBC client on Windows systems involves the following steps:

1. Verify that you have necessary permissions and obtain a license key for the ODBC client driver (prerequisites).
2. Install the ODBC client.
3. Create a data source using the Windows Data Source (ODBC) utility.
4. Configure the connection details for ODBC client.
5. Test the connection to the database.

Prerequisites

ODBC access to the event log store is available only in CA Enterprise Log Manager r12.1 and later releases. See the ODBC data source considerations for needed information before you begin the installation.

Users of this feature must belong to a user group that has the *dataaccess* privilege in the Default Data Access Policy (in the CALM access policies). See the *CA Enterprise Log Manager r12.1 Administration Guide* for more information about access policies.

For an ODBC client, the following prerequisites apply:

- You must have administrator privileges to install the ODBC client on a Windows server.
- The ODBC client installation requires the Microsoft Windows Installer service, and displays a message if it is not found.
- Configure the ODBC Server service in CA Enterprise Log Manager, ensuring that you select the Enable Service check box
- Configure an ODBC Data Source for Windows systems using the Data Sources (ODBC) utility on the Control Panel.
- You must have rights to create files in the directory where you want to install the client on UNIX and Linux systems.

See the CA Enterprise Log Manager Support Certification Matrix on <http://www.ca.com/Support> for details on the specific platforms supported for use with the ODBC and JDBC feature.

Configure the ODBC Server Service

You can configure ODBC and JDBC access to the CA Enterprise Log Manager event log store using this procedure.

To configure ODBC and JDBC access

1. Log in to the CA Enterprise Log Manager server as an Administrator user.
2. Access the Administration tab, and then click the Services subtab.
3. Click the ODBC Server service to open the global settings, or expand the node and select a specific CA Enterprise Log Manager server.
4. Set a port value for the Service Port field, if you decide to use a port other than the default value.
5. Specify whether to enable SSL to encrypt data transport between the ODBC client and the CA Enterprise Log Manager server.

Note: The Service Port and SSL Enabled settings must match on both the server and the ODBC client. The default value for port is 17002, and SSL encryption is enabled. If these settings do not match the settings on the ODBC client, connection attempts fail.

Install the ODBC Client on Windows Systems

Use this procedure to install the ODBC client on a Windows system.

Note: You need a Windows Administrator account to install the ODBC client.

To install the ODBC client

1. Locate the ODBC client directory in the Application DVD or installation image, in the directory \CA\ELM\ODBC.
2. Double-click the application, Setup.exe.
3. Respond to the license agreement and click Next.
The Choose Destination Location panel appears.
4. Enter a destination location or accept the default location and click Next.
The Select Program Folder panel appears.
5. Select a program folder or accept the default selection and click Next.
The Start Copying Files panel appears.
6. Click Next to begin copying files.
The Setup Status panel displays the progress of the installation. When the installation finishes copying files, the InstallShield Wizard Complete panel appears.
7. Click Finish to complete the installation.

Create an ODBC Data Source on Windows Systems

Use this procedure to create the required ODBC data source on Windows systems. You can create the data source as either a user DSN or a System DSN.

To create the data source

1. Access the Windows Control Panel, and open the Administrative Tools.
2. Double-click the utility, Data Sources (ODBC). The ODBC Data Source Administrator window appears.
3. Click Add to display the Create New Data Source window.
4. Select the entry, CA Enterprise Log Manager ODBC Driver, and then click Finish.
The CA Enterprise Log Manager ODBC Driver Setup window appears.
5. Enter values for the fields as described in the section on ODBC Data Source Considerations, and then click OK.

ODBC Data Source Considerations

The following are the descriptions of the ODBC data source fields as they relate to CA Enterprise Log Manager:

Data Source Name

Create a name for this data source. Client applications that want to use this data use this name to connect to the data source.

Service Host

Specifies the name of the CA Enterprise Log Manager server which the client connects. You can use either a hostname or an IPv4 address.

Service Port

Specifies the TCP service port on which the CA Enterprise Log Manager server listens for ODBC client connections. The default value is 17002. The value you set here must match the setting for the ODBC Server service or the connection fails.

Service Data Source

Leave this field blank, otherwise the connection attempt fails.

Encrypted SSL

Specifies whether to use encryption on the communications between the client and the CA Enterprise Log Manager server. The default value is to have SSL enabled. The value you set here must match the setting for the ODBC Server service or the connection fails.

Custom Properties

Specifies the connection properties for use with the event log store. The delimiter between the properties is a semi-colon with no space. The recommended default values include the following:

querytimeout

Specifies the timeout value in seconds with no data returned after which the query is closed. The following is the syntax for this property:

```
querytimeout=300
```

queryfederated

Specifies whether to perform a federated query. Setting this value to false performs a query only on the CA Enterprise Log Manager server to which the database connection is made. The following is the syntax for this property:

```
queryfederated=true
```

queryfetchrows

Specifies how many rows to retrieve in a single fetch operation, if the query is successful. The minimum value is 1, and the maximum value is 5000. The default value is 1000. The following is the syntax for this property:

```
queryfetchrows=1000
```

offsetmins

Specifies the offset for the timezone for this ODBC client. A value of 0 uses GMT. You can use this field to set your own timezone offset from GMT. The following is the syntax for this property:

```
offsetmins=0
```

suppressNoncriticalErrors

Indicates the Interface Provider's behavior in case of noncritical errors such as a database not responding or a host not responding.

The following is the syntax for this property:

```
suppressNoncriticalErrors=false
```

Test the ODBC Client's Connection to the Database

The ODBC client is installed with a command line interactive SQL Query tool, ISQL. You can use this tool for testing your configuration settings and the connectivity between the ODBC client and the CA Enterprise Log Manager event log store.

To test the client connection to the database

1. Access a command prompt and navigate to the directory where you installed the ODBC client.
2. Start the ISQL utility, odbcisql.exe.
3. Enter the following command to test the client connection to the database:

```
connect User*Password@DSN_name
```

Use the data source name you created for this ODBC connection to the database for the DSN_name value. If your connection parameters are correct, you see a return message similar to following:

```
SQL: connecting to database: DSN_name  
Elapsed time 37 ms.
```

Note: If your password contains the @ symbol, the ISQL utility fails to run properly, reading everything after the "@" as the DSN name. To avoid this problem, enter the password in quotes:

```
Connect User*"Password"@DSN_name
```

Test Server Retrieval from the Database

Use this test query to determine whether an ODBC client application is able to retrieve data from a CA Enterprise Log Manager event log store using the established database connection. This procedure uses the same ISQL utility you used to test the ODBC connection.

Note: Do not copy and use the SQL queries provided in the CA Enterprise Log Manager queries and reports to test your ODBC connection. Those SQL statements are only for the CA Enterprise Log Manager server to use with the event log store. Build your ODBC SQL queries using standard constructs according to the ANSI SQL standard.

To test the server component data retrieval

1. Access a command prompt and navigate to the directory where you installed the ODBC client.
2. Start the ISQL utility, odbcisql.exe.
3. Enter the following SELECT statement to test retrieval from the event log store:

```
select top 5 event_logname, receiver_hostname, SUM(event_count) as Count from  
view_event where event_time_gmt < now() and event_time_gmt >  
timestampadd(mi, -15, now()) GROUP BY receiver_hostname, event_logname;
```

Installing the JDBC Client

The JDBC client provides JDBC access through any Java-enabled applet, application, or application server. It delivers high-performance point-to-point and n-tier access to data sources. The client is optimized for the Java environment, allowing you to incorporate Java technology and extend the functionality and performance of your existing system.

The JDBC client runs on 32-bit and 64-bit platforms. No changes are required to existing applications to enable them to run on 64-bit platforms.

Installing the JDBC client involves the following steps:

1. Ensure that a web application server with connection pool configuration capabilities is installed and running.
2. Obtain the license key for the JDBC client driver.
3. Install the JDBC client.
4. Configure the connection to the database using your web application server's connection pool management functions.
5. Test the connection to the database.

JDBC Client Prerequisites

JDBC access to the event log store is available only CA Enterprise Log Manager r12.1 and later releases. You can install the JDBC client on Windows and UNIX systems.

Users of this feature must belong to a CA Enterprise Log Manager user group that has the *dataaccess* privilege in the Default Data Access Policy (in the CALM access policies). See the *CA Enterprise Log Manager r12.1 Administration Guide* for more information about access policies.

For a JDBC client, the following prerequisites apply:

- You must have administrator privileges to install the JDBC client on a Windows server.
- Verify that the ODBC Server configuration window shows that the Enable Service check box is selected (enabled)
- You must have rights to create files in the directory where you want to install the client on UNIX and Linux systems.
- For applications running under the J2SE v 1.4.2.x, set your database connections programmatically, as defined in a specific application.
- For applications running under J2EE 1.4.2.x and later versions, use a web application server such as Oracle WebLogic or Red Hat JBoss to configure connection pool management.

See the CA Enterprise Log Manager Support Certification Matrix on <http://www.ca.com/Support> for details on the specific platforms supported for use with the ODBC and JDBC feature.

Install the JDBC Client on Windows Systems

Use this procedure to install the JDBC client driver on a Windows system.

To install the JDBC driver

1. Locate the following two .jar files in the Application DVD or installation image, in the directory CA/ELM/JDBC:

LMjc.jar
LMssl14.jar

2. Copy the .jar files to the desired directory on the destination server and make a note of the location.

Install the JDBC Client on UNIX Systems

Use this procedure to install the JDBC client driver on a UNIX system.

To install the JDBC driver

1. Locate the following two .jar files in the Application DVD or installation image, in the directory CA/ELM/JDBC:

LMjc.jar
LMssl14.jar
2. Copy the .jar files to the desired directory on the destination server and make a note of the location.
3. Execute the following (or similar) command manually from the installation directory after installing the JDBC client for JDBC on UNIX:

```
chmod -R ugo+x file_location
```

The value for *file_location* is the directory where you installed the JDBC client. This step enables you to execute shell scripts supplied with the installed client.

JDBC Connection Parameters

Various applications require certain connection parameters to use the JDBC client driver. The usual parameters include the following:

- Connection string or connection URL
- Class name

The JDBC connection string (URL) is in the following format:

```
jdbc:ca-elm://[CA-ELM_host_name]:[ODBC/JDBCport];ServerDataSource=Default;
```

The JDBC driver class name is:

```
com.ca.jdbc.openaccess.OpenAccessDriver
```

JDBC URL Considerations

When using the JDBC client to access event data stored in CA Enterprise Log Manager, you need both the JDBC Classpath and a JDBC URL. The JDBC Classpath names the driver JAR file locations. The JDBC URL defines the parameters the classes in the JARs use when they load.

The following is a complete, sample JDBC URL:

```
jdbc:ca-elm://127.0.0.1:17002;encrypted=1;ServerDataSource=Default;CustomProperties=(querytimeout=600;queryfederated=true;queryfetchrows=1000;offsetmins=0;suppressNoncriticalErrors=false)
```

The following descriptions explain the URL components:

jdbc:ca-elm:

Defines the protocol:subprotocol string that designates the JDBC driver provided with CA Enterprise Log Manager.

//IP Address:Port;

Names the IP address that represents the CA Enterprise Log Manager server whose data you want to access. The port number is the port to use for the communications, and must match the setting in the CA Enterprise Log Manager ODBC Service configuration panel. If the ports do not match, the connection attempt fails.

encrypted=0|1;

Determines whether SSL encryption is used for the communications between the JDBC client and the CA Enterprise Log Manager server. The default value is 0, not encrypted, and does not require specification in the URL. Setting encrypted=1 turns encryption on. Set the connection to encryption explicitly. In addition, this setting must match what you configure in the CA Enterprise Log Manager ODBC Service dialog or the connection attempt fails.

ServerDataSource=Default

Specifies the name of the data source. Set this value to *Default* for access to the CA Enterprise Log Manager event log store.

CustomProperties=(x;y;z)

These properties are the same as the ODBC custom properties. If you do not specify them explicitly, the default values shown in the example URL apply.

More information

[ODBC Data Source Considerations](#) (see page 99)

Installation Troubleshooting

You can review the following installation log files to begin troubleshooting your installation:

Product	Log File Location
CA Enterprise Log Manager	/tmp/pre-install_ca-elm.log
	/tmp/install_ca-elm.<timestamp>.log
	/tmp/install_ca-elmagent.<timestamp>.log
CA Embedded Entitlements Manager	/opt/CA/SharedComponents/EmbeddedIAM/eiam-install.log

Product	Log File Location
CA Directory	/tmp/etrdir_install.log

The CA Enterprise Log Manager installation copies content and other files to the CA EEM server for management. From the perspective of the CA EEM server, the CA Enterprise Log Manager reports and other files are *imported*. If the installation cannot connect to the CA EEM server, the installation of CA Enterprise Log Manager continues without importing the content files. You can import the content files manually when the installation is complete.

If you encounter any errors during installation, you may need to perform one or more of the following actions to complete your installation. Each of these actions involves logging into the CA Enterprise Log Manager server using the default account, caelmadmin, and then switching users to the root account.

- Resolve network interface configuration error
- Verify that the rpm package was installed
- Verify that the iGateway daemon is running
- Register the CA Enterprise Log Manager application with the CA EEM server
- Acquire digital certificates
- Import CA Enterprise Log Manager reports
- Import Data Mapping files
- Import Message Parsing files
- Import common event grammar (CEG) files
- Import common agent management files

Resolve Network Interface Configuration Error

After installation, if you are unable to access the CA Enterprise Log Manager server's user interface, you may have a network interface configuration error. You have two options to resolve the error:

- Remove the physical network cable and insert it into another port.
- Reconfigure the logical network interface adapters from a command line.

To reconfigure network adapter ports from a command line

1. Log into the soft appliance as the caelmadmin user and access a command prompt.
2. Switch users to the root user using the following command:

```
su -
```

3. Enter the root user password to confirm access to system.
4. Enter the following command:

```
system-config-network
```

The user interface to configure the network adapters displays.

5. Set the port configurations as desired and exit.
6. Restart the network services for your changes to take effect with the following command:

```
service network restart
```

Verify that the RPM Package is Installed

You can perform a quick check of the installation by verifying that the appropriate rpm package is installed.

To verify the rpm package

1. Access a command prompt on the CA Enterprise Log Manager server.
2. Log in with the caelmadmin account credentials.
3. Switch users to the root account with the following command:

```
su - root
```

4. Verify that the ca-elm-<version>.i386.rpm package is installed with the following commands:

```
rpm -q ca-elm  
rpm -q ca-elmagent
```

The operating system returns the full name of the package if it is installed.

Register CA Enterprise Log Manager Server with the CA EEM Server

Symptom:

During installation, the CA Enterprise Log Manager application did not register successfully with the CA EEM server. The CA Enterprise Log Manager application depends on the CA EEM server for the management of user accounts and service configurations. If the CA Enterprise Log Manager application is not registered, the software will not run properly.

The shell script mentioned in the procedure that follows is automatically copied to the named directory during installation.

Solution:

Register the CA Enterprise Log Manager application with the CA EEM server manually.

To register the CA Enterprise Log Manager application

1. Access a command prompt on the CA Enterprise Log Manager server.
2. Log in with the caelmadmin account credentials.
3. Switch users to the root user with the following command:

```
su -
```

4. Navigate to the directory, /opt/CA/LogManager/EEM.
5. Execute the following command:

```
./EEMRegister.sh
```

The shell script registers the CA Enterprise Log Manager application with the CA EEM server.

Acquire Certificates from CA EEM Server

Symptom:

During installation, the digital certificates were not acquired from the CA EEM server correctly. Digital certificates are required to start and run the CA Enterprise Log Manager application.

The shell script mentioned in the procedure that follows is automatically copied to the named directory during installation.

Solution:

Acquire the certificates from the CA EEM server manually.

To acquire the digital certificates

1. Access a command prompt on the CA Enterprise Log Manager server.
2. Log in with the caelmadmin account credentials.
3. Switch users to the root user with the following command:

```
su -
```

4. Navigate to the directory, /opt/CA/LogManager/EEM.
5. Execute the following command:

```
./EEMAcqCert.sh
```

The shell script performs the processing necessary to acquire the needed digital certificates.

Import CA Enterprise Log Manager Reports

Symptom:

During installation, the CA EEM server did not successfully import report content from the CA EEM server. You must import the report content to see event data after it is stored in the event log store.

The shell script mentioned in the procedure that follows is automatically copied to the named directory during installation.

Solution:

Import the report content manually.

To import report content

1. Access a command prompt on the CA Enterprise Log Manager server.
2. Log in with the caelmadmin account credentials.
3. Switch users to the root user with the following command:

```
su -
```

4. Navigate to the directory, /opt/CA/LogManager/EEM/content.
5. Execute the following command:

```
./ImportCALMContent.sh
```

The shell script downloads the report content from the CA EEM server.

Import CA Enterprise Log Manager Data Mapping Files

Symptom:

During installation, the CA EEM server did not successfully import the data mapping (DM) files. You must have the DM files to map incoming event data into the event log store.

The shell script mentioned in the procedure that follows is automatically copied to the named directory during installation.

Solution:

Import the DM files manually.

To import DM files

1. Access a command prompt on the CA Enterprise Log Manager server.
2. Log in with the caelmadmin account credentials.
3. Switch users to the root user with the following command:

```
su -
```

4. Navigate to the directory, /opt/CA/LogManager/EEM/content.
5. Execute the following command:

```
./ImportCALMDM.sh
```

The shell script imports the DM files from the CA EEM server.

Import Common Event Grammar Files

Symptom:

During installation, the CA EEM server did not successfully import the common event grammar (CEG) files. The CEG forms the underlying database schema for the event log store. You will not be able to store events in the CA Enterprise Log Manager event log store without the CEG files.

The shell script mentioned in the procedure that follows is automatically copied to the named directory during installation.

Solution:

Import the CEG files manually.

To import CEG files

1. Access a command prompt on the CA Enterprise Log Manager server.
2. Log in with the caelmadmin account credentials.
3. Switch users to the root user with the following command:

```
su -
```

4. Navigate to the directory, /opt/CA/LogManager/EEM/content.
5. Execute the following command:

```
./ImportCALMCEG.sh
```

The shell script imports the common event grammar files.

Import Correlation Rule Files

Symptom:

During installation, the CA EEM server did not successfully import the correlation rule files. Correlation rules allow you to identify patterns of events that require investigation. You can import correlation groups or rule themselves.

The shell script mentioned in the procedure that follows is automatically copied to the named directory during installation.

Solution:

Import the correlation rule files manually.

To import correlation rule files

1. Access a command prompt on the CA Enterprise Log Manager server.
2. Log in with the caelmadmin account credentials.
3. Switch users to the root user with the following command:

```
su -
```

4. Navigate to the directory, /opt/CA/LogManager/EEM/content.
5. Execute one of the following commands:

```
./ImportCALMCorrelationGroups.sh
```

The shell script imports correlation rule groups.

```
./ImportCALMCorrelationRules.sh
```

The shell script imports the correlation rule files.

Import Common Agent Management Files

Symptom:

During installation, the CA EEM server did not successfully import the common agent management files. You cannot manage agents in the CA Enterprise Log Manager user interface without these files.

The shell script mentioned in the procedure that follows is automatically copied to the named directory during installation.

Solution:

Import the agent management files manually.

To import common agent management files

1. Access a command prompt on the CA Enterprise Log Manager server.
2. Log in with the caelmadmin account credentials.
3. Switch users to the root user with the following command:

```
su -
```

4. Navigate to the directory, /opt/CA/LogManager/EEM/content.
5. Execute the following command:

```
./ImportCALMAgentContent.sh
```

The shell script imports the common agent management files.

Import CA Enterprise Log Manager Configuration Files

Symptom:

During installation, the CA EEM server did not successfully import the configuration files. You can start CA Enterprise Log Manager but certain settings and values are missing from the Services configuration areas, and you cannot configure individual hosts centrally without these files.

The shell script mentioned in the procedure that follows is automatically copied to the named directory during installation.

Solution:

Import the configuration files manually.

To import configuration files

1. Access a command prompt on the CA Enterprise Log Manager server.
2. Log in with the caelmadmin account credentials.
3. Switch users to the root user with the following command:

```
su -
```

4. Navigate to the directory, /opt/CA/LogManager/EEM/content.
5. Execute the following command:

```
./ImportCALMConfig.sh
```

The shell script imports the configuration files.

Import Suppression and Summarization Files

Symptom:

During installation, the CA EEM server did not successfully import the suppression and summarization files. You cannot use the out-of-the-box suppression and summarization rules in the CA Enterprise Log Manager user interface without these files.

The shell script mentioned in the procedure that follows is automatically copied to the named directory during installation.

Solution:

Import the suppression and summarization files manually.

To import suppression and summarization files

1. Access a command prompt on the CA Enterprise Log Manager server.
2. Log in with the caelmadmin account credentials.
3. Switch users to the root user with the following command:

```
su -
```

4. Navigate to the directory, /opt/CA/LogManager/EEM/content.
5. Execute the following command:

```
./ImportCALMSAS.sh
```

The shell script imports the suppression and summarization files.

Import Parsing Token Files

Symptom:

During installation, the CA EEM server did not successfully import the parsing token files. You cannot use out-of-the-box parsing tokens in the Message Parsing Wizard without these files.

The shell script mentioned in the procedure that follows is automatically copied to the named directory during installation.

Solution:

Import the parsing token files manually.

To import parsing token files

1. Access a command prompt on the CA Enterprise Log Manager server.
2. Log in with the caelmadmin account credentials.
3. Switch users to the root user with the following command:

```
su -
```

4. Navigate to the directory, /opt/CA/LogManager/EEM/content.
5. Execute the following command:

```
./ImportCALMTOK.sh
```

The shell script imports the parsing token files.

Import CA Enterprise Log Manager User Interface Files

Symptom:

During installation, the CA EEM server did not successfully import the user interface files. You cannot see or use the values in the dynamic time range drop down fields without these files.

The shell script mentioned in the procedure that follows is automatically copied to the named directory during installation.

Solution:

Import the user interface files manually.

To import user interface files

1. Access a command prompt on the CA Enterprise Log Manager server.
2. Log in with the caelmadmin account credentials.
3. Switch users to the root user with the following command:

```
su -
```

4. Navigate to the directory, /opt/CA/LogManager/EEM/content.
5. Execute the following command:

```
./ImportCALMFlexFiles.sh
```

The shell script imports the user interface files.

Chapter 4: Configuring Basic Users and Access

This section contains the following topics:

[About Basic Users and Access](#) (see page 115)

[Configuring the User Store](#) (see page 116)

[Configure Password Policies](#) (see page 119)

[Preserving Predefined Access Policies](#) (see page 120)

[Create the First Administrator](#) (see page 121)

About Basic Users and Access

Configuration begins with setting the user store, creating one or more users with the predefined Administrator role, and configuring password policies. Typically, this configuration is performed by the installer, who can log onto CA Enterprise Log Manager with the EiamAdmin credentials. After this configuration is complete, the users defined as Administrators configure CA Enterprise Log Manager.

If the default user store configuration is accepted, the minimum configuration that must be completed by the EiamAdmin user is the account for the first Administrator. The first Administrator can configure password policies before configuring the other CA Enterprise Log Manager components.

Note: For details on creating other users, or creating custom roles with and custom access policies, see the *CA Enterprise Log Manager Administration Guide*.

Configuring the User Store

The user store is the repository for global user information. You can configure the user store as soon as you install a CA Enterprise Log Manager server. Only the EiamAdmin user can configure the user store, this is usually done immediately after the first logon.

Configure the user store in one of the following ways:

- Accept the default, Store in internal datastore
Note: The default option could be displayed as the CA Management Database if, during installation, you pointed to a standalone CA EEM.
- Select Reference from an external directory, which can be an LDAP directory such as Microsoft Active Directory, Sun One, or Novell CA Directory
- Select Reference from CA SiteMinder

If you configure the user store as an external directory, you cannot create new users. You can only add predefined and user defined application groups, or roles, to the read-only global user records. You must add new users in the external user store and then add the CA Enterprise Log Manager permissions to the global user records.

Accept the Default User Store

You do not have to configure the user store if you accept the default, which is the internal datastore. This applies if there is no external user store to reference.

To verify that the default repository is configured as the user store

1. Log into a CA Enterprise Log Manager server as a user with Administrator privileges or with the EiamAdmin user name and associated password.
2. Click the Administration tab.
If you log in as the EiamAdmin user, this tab displays automatically.
3. Select the User and Access Management subtab, and then click the User Store button on the left pane.
The EEM Server Configuration for Global Users/Global Groups appears.
4. Verify that the option, Store in internal datastore, is selected.
5. Click Save and then click Close.

Note: With the default user store set, you can create new users, set temporary passwords, and set password policies.

More information:

[User Store Planning](#) (see page 36)

Reference an LDAP Directory

Configure the user store as a reference to an LDAP directory when global user details are stored in Microsoft Active Directory, Sun One, or Novell Directory.

Note: Application details are stored in the default repository. Referencing an external user store does not update that user store.

To reference an LDAP directory as the user store

1. Log into a CA Enterprise Log Manager server as a user with administrator privileges or as the EiamAdmin user.
2. Click the Administration tab.

If you log in as the EiamAdmin user, this tab displays automatically.

3. Select the User and Access Management subtab, and then click User Store on the left pane.

The CA EEM Server configuration for User Store appears.

4. Select Reference from an external directory.

Fields for the LDAP configuration appear.

5. Complete these fields as planned on the external directory worksheet.

Consider the following example for binding to Active Directory objects, with the following binding string:

Set objUser = Get Object ("LDAP://cn=Bob, cn=Users, ou=Sales, dc=MyDomain, dc=com"), where cn is the Common Name, ou is the Organizational Unit, and dc is composed of two Domain Components that make up the full DNS name. For User DN, you would enter:

```
cn=Bob,cn=Users,ou=Sales,dc=MyDomain,dc=com
```

6. Click Save.

Saving this reference loads user account information into CA EEM. This makes it possible for you to access these user records as global users and then add application-level details such as application user group, the name for user role.

7. Review the displayed status to verify that the external directory bind is successful and that data is loaded.

If the status displays a warning, click Refresh status. If the status displays an error, correct the configuration, click Save, and repeat this step.

8. Click Close.

More information:

[User Store Planning](#) (see page 36)

[External LDAP Directory Worksheet](#) (see page 37)

Reference CA SiteMinder as the User Store

If your user accounts are already defined to CA SiteMinder, reference this external directory when you configure the user store.

To reference CA SiteMinder as the user store

1. Log into a CA Enterprise Log Manager server as a user with administrator privileges or as the EiamAdmin user.

2. Click the Administration tab.

If you log in as the EiamAdmin user, this tab displays automatically.

3. Select the User and Access Management subtab, and then click the User Store button on the left pane.

The CA EEM Server configuration for User Store appears.

4. Select the option, Reference from CA SiteMinder.

CA SiteMinder-specific fields appear.

- a. Complete these fields as planned on the SiteMinder Worksheet.
- b. To view or change connections and ports used by CA SiteMinder, click the ellipsis to display the Connection Attributes panel.

5. Click Save.

Saving this reference loads user account information into CA EEM. This makes it possible for you to access these user records as global users and then add application-level details such as application user group, the name for user role.

6. Review the displayed status to verify that the external directory bind is successful and that data is loaded.

If the status displays a warning, click Refresh status. If the status displays an error, correct the configuration, click Save, and repeat this step.

7. Click Close.

More information:

[User Store Planning](#) (see page 36)

[CA SiteMinder Worksheet](#) (see page 39)

Configure Password Policies

You can set password policies to ensure that the passwords users create for themselves meet the standards you set and are changed with the frequency you set. Set password policies after configuring the internal user store. Only the EiamAdmin user or a user assigned the Administrator role can set or modify password policies.

Note: CA Enterprise Log Manager password policies do not apply to user accounts created in an external user store.

To configure password policies

1. Log into a CA Enterprise Log Manager server as a user with Administrator privileges or as the EiamAdmin user.

2. Click the Administration tab.

If you log in as the EiamAdmin user, this tab displays automatically.

3. Select the User and Access Management subtab, and then click the Password Policies button on the left pane.

The Password Policies panel appears.

4. Specify whether to allow passwords to be the same as the user name.
5. Specify whether to enforce length requirements.
6. Specify whether to enforce policies on maximum repeating characters or minimum number or numeric characters.
7. Specify age and reuse policies.
8. Verify your settings, then click Save.
9. Click Close.

The configured password policies apply to all CA Enterprise Log Manager users.

More information:

[Password Policy Planning](#) (see page 40)

[User Name as Password](#) (see page 41)

[Password Age and Reuse](#) (see page 41)

[Password Length and Format](#) (see page 41)

Preserving Predefined Access Policies

If you plan to use only the predefined application user groups, or roles, with the associated predefined policies, there may be little risk that predefined policies would ever get deleted or corrupted. However, if your Administrators plan to create user-defined roles and associated access policies, the predefined policies will be accessed, edited, and vulnerable to undesired changes. It is good practice to keep a backup of the original predefined policies that you can restore if needed.

Create a backup file containing each type of predefined policy using the Export function. You can copy these files to an external media or leave them on the disk of the server on which the Export was initiated.

Note: For procedures on backing up predefined policies, see the *CA Enterprise Log Manager Administration Guide*.

Create the First Administrator

The first user you create must be assigned the Administrator role. Only users who are assigned the Administrator role can perform configuration. You can assign an Administrator role to a new user account you create or to an existing user account retrieved into CA Enterprise Log Manager.

Use the following process:

1. Log into the CA Enterprise Log Manager server as the EiamAdmin default user.
2. Create the first administrator.

The method you use to create the first CA Enterprise Log Manager Administrator depends on how you configure the user store.

- If you configure CA Enterprise Log Manager to use the internal user store, you create a new user account with the Administrator role.
- If you configure CA Enterprise Log Manager to use an external user store, you use an existing LDAP user to bind to the directory. Once you bind to an external directory, you retrieve from the external user store the account of the user to whom you want to assign a CA Enterprise Log Manager role. User accounts from external user stores are retrieved as global users. You cannot modify existing user account information, but you can add a new CAELM application user group, or role. For the first user, you assign the role, Administrator.

Note: You cannot create new users from CA Enterprise Log Manager when you configure an external user store.

3. Log off the CA Enterprise Log Manager server
4. Log back on to the CA Enterprise Log Manager server with the new user account credentials.

You are then ready to perform configuration tasks.

Create a New User Account

You can create a user account for each individual who is to use CA Enterprise Log Manager. You provide the credentials the user is to log on with for the first time and you specify their role. The three predefined roles include Administrator, Analyst, and Auditor. When a new user who is assigned the role of Analyst or Auditor logs on, CA Enterprise Log Manager authenticates the user with the saved credentials and authorizes usage to various functionality based on the role you assign.

To create a new user

1. Log into the CA Enterprise Log Manager server as the EiamAdmin default user.

The Administration tab and User and Access Management subtab displays.

2. Click Users on the left pane.
3. Click New User to the left of the Users folder.
The New User details screen appears on the right side of the window.
4. Type a user name in the Name field. User names are not case-sensitive.
5. Click Add Application User Details.
6. Select the role associated with tasks this user is to perform. Use the shuttle control to move it to the Selected User Groups list.
7. Provide values for the remaining fields in the screen as needed. You must provide a case-sensitive password with confirmation in the authentication group box.
8. Click Save, and then click Close.

More information:

[Assign a Role to a Global User](#) (see page 122)

Assign a Role to a Global User

You can search for an existing user account and assign the application user group for the role you want the individual to perform. If you reference an external user store, the search returns global records loaded from that user store. If your configured user store is the CA Enterprise Log Manager user store, the search returns records created for users in CA Enterprise Log Manager.

Only Administrators can edit user accounts.

To assign a role, or application user group, to an existing user

1. Click the Administration tab and the User and Access Management subtab.
2. Click Users on the left pane.
The Search Users and Users panes appear.
3. Select Global Users, enter search criteria, and click Go.

If the search is for loaded user accounts, the Users pane shows the path and the path labels reflect the referenced external directory.

Important! Always enter criteria when searching to avoid displaying all entries in an external user store.

4. Select a Global User that has no membership in a CA Enterprise Log Manager application group.

The User page displays with the folder name, global user details, and, if applicable, global group membership.

5. Click Add Application User Details.

The "CAELM" User Details pane expands.

6. Select the desired group from Available User Groups and click the right arrow.

The selected group appears in the Selected User Groups box.

7. Click Save.

8. Verify the addition.

- a. On the Search Users pane, click Application User Details and click Go.
- b. Verify that the name of the new application user appears in the displayed results.

9. Click Close.

Chapter 5: Configuring Services

This section contains the following topics:

- [Event Sources and Configurations](#) (see page 125)
- [Edit Global Configurations](#) (see page 126)
- [Working with Global Filters and Settings](#) (see page 128)
- [Configuring the Event Log Store](#) (see page 130)
- [Configuring the Correlation Service](#) (see page 151)
- [Incident Service Considerations](#) (see page 160)
- [ODBC Server Considerations](#) (see page 160)
- [Report Server Considerations](#) (see page 162)
- [How to Configure Subscription](#) (see page 163)

Event Sources and Configurations

Most networks have some Windows and some syslog-based devices whose event logs must be collected, stored, monitored, and audited. Your network can also have other device types, including applications, databases, badge readers, biometric devices, or existing CA Audit Recorders and iRecorders. The CA Enterprise Log Manager services, adapters, agents, and connectors represent the configurations required to connect to these event sources to receive event data.

CA Enterprise Log Manager services include the following areas for configurations and settings:

- Global configurations
- Global filters and settings
- Alerting Service
- Correlation Service
- Event log store settings
- Incident Service
- ODBC server settings
- Report server settings
- Rule Test Service
- Subscription service configuration
- System status access panel

Service configurations can be global, meaning that they affect all CA Enterprise Log Manager servers installed under a single application instance name in the management server. Configurations can also be local, affecting only a selected server. Configurations are stored in the management server with a local copy on the collection CA Enterprise Log Manager server. In this way, if network connectivity is lost or the management server goes down for some reason, event logging continues without interruption on the collection servers.

The System Status access panel provides you with tools to affect a CA Enterprise Log Manager server and its services, and to gather information for Support. Additional information about this area is available in the Administration Guide and online help.

Edit Global Configurations

You can set global configurations for all services. If you attempt to save values outside the allowed range, CA Enterprise Log Manager defaults to the minimum or maximum as appropriate. Several of the settings are interdependent.

To edit global settings

1. Click the Administration tab and the Services subtab.

The Service List appears.

2. Click Global Configuration in the Service List.

The Global Service Configuration details pane opens.

3. Change any of the following configuration settings:

Update Interval

Specifies the frequency, in seconds, at which server components apply configuration updates.

Minimum: 30

Maximum: 86400

Session Timeout

Specifies the maximum length of an inactive session. If auto-refresh is enabled, a session never times out.

Minimum: 10

Maximum: 600

Allow Auto Refresh

Lets users auto-refresh reports or queries. This setting lets administrators globally disable auto-refresh.

Auto Refresh Frequency

Specifies the interval, in minutes, at which the report views refresh. This setting depends on the selection of Allow Auto Refresh.

Minimum: 1

Maximum: 60

Enable Auto Refresh

Sets auto-refresh in all sessions. Auto-refresh is not enabled, by default.

Viewing Action Alerts Requires Authentication

Prevents Auditors or third-party products from viewing Action Alert RSS feeds. This setting is enabled by default.

Default Report

Specifies the default report.

Enable Default Report Launch

Displays the default report when you click the Reports subtab. This setting is enabled by default.

4. Change any of the following report or query tag settings:

Hide Report Tags

Prevents specified tags from appearing in any tag list. Hiding report tags streamlines the view of the available reports.

Hide Query Tags

Lets you hide chosen tags. Hidden tags do not appear in the main query list or the action alert scheduling query list. Hiding query tags customizes the view of the available queries.

5. Change any of the following Dashboard settings:

Enable Default Dashboard Launch

Displays the default dashboard when you click the Queries and Reports tab.
This setting is enabled by default.

Default Dashboard

6. Change any of the following Profiles settings:

Enable Default Profile

Lets you set the default profile.

Default Profile

Specifies the default profile.

Hide Profiles

Lets you hide chosen profiles. When the interface refreshes or the Update Interval expires, the hidden profiles do not appear. Hiding profiles customizes the view of the available profiles.

Note: Click Reset to restore the last saved values. You can reset a single change or multiple changes until you save changes. After you save changes, reset your changes individually.

7. Click Save.

Working with Global Filters and Settings

You can set global filters and settings as part of configuring your CA Enterprise Log Manager server. Global settings are saved for the current session only and do not persist after you log off of the server, unless you select the option, Use as default.

A global *quick filter* controls the initial time interval on which to report, offers simple matching text filtering, and allows you to use specific fields and their values to affect the data that displays in a report.

A global *advanced filter* allows you to use SQL syntax and operators to scope your report data further. Global settings allow you to set a time zone, and to use special queries that retrieve data from other CA Enterprise Log Manager servers in a federation, as well as enabling automatic refresh of reports during viewing.

You should set global filters that make sense for use in multiple report areas. By setting options that narrow the global filter, you can control the amount of data that is shown in a report. The initial tasks for the global filters and settings include the following:

- Configure global quick filters to provide an initial time that affects the reports you view from this CA Enterprise Log Manager server
- Select federated queries in the Settings tab to see data from CA Enterprise Log Manager servers that you have federated under this server
- Decide whether you want reports to be refreshed automatically
- Set the interval at which you want the data in reports to be refreshed

Note: Setting the global filter so that it is too narrow or specific can prevent data from displaying in some reports.

More information about global filters and their use is available in the online help.

Select Use of Federated Queries

You can select whether you want to execute queries on federated data. If you plan to use more than one CA Enterprise Log Manager server in a federated network, you may want to select the Use Federated Queries check box. This option enables you to gather event data for reporting from all of the CA Enterprise Log Manager servers that are federated to (acting as children of) this CA Enterprise Log Manager server.

You may also choose to turn off federated queries for a specific query, if you want to see data from only the current CA Enterprise Log Manager server.

To set use of federated queries

1. Log into the CA Enterprise Log Manager server.
2. Click the Show/Edit Global Filters button.

The button is located to the right of the current CA Enterprise Log Manager server name and just above the main tabs.

3. Click the Settings tab.
4. Choose whether you want to use federated queries.

If you do turn off the select federated queries option, reports that you view will *not* contain event data from any servers that you have configured as children of this server.

More information:

[Configuring a CA Enterprise Log Manager Federation](#) (see page 195)

[Configure a CA Enterprise Log Manager Server as a Child Server](#) (see page 195)

Configure the Global Update Interval

You can set the interval at which the CA Enterprise Log Manager services check for configuration changes. The default value, after installation, is five minutes, and is expressed in seconds. Setting this value for very long intervals may result in needed configuration changes being delayed in their application.

To configure the update interval

1. Log into the CA Enterprise Log Manager server and click the Administration tab.
2. Click the Services tab and then click the Global Configuration service node.
3. Enter a new value for the update interval.

The default and recommended value is 300 seconds.

Configuring the Event Log Store

The event log store is the underlying proprietary database that contains collected event logs. The configuration options you set for the event log store service can be global or local, and affect the CA Enterprise Log Manager servers' storage and archival of events. The process for configuring the event log store includes the following:

- Understand the event log store service
- Understand how the event log store handles archive files
- Configure the event log store's global and local values

This includes setting database size, basic archive file retention values, summarization rules, suppression rules, federation relationships, correlation settings, data integrity checks, and auto-archive options.

CA Enterprise Log Manager automatically closes active database files and creates archive files when the active databases reach the capacity you define for this service. Then CA Enterprise Log Manager opens new, active files to continue event logging operations. You can set auto-archive options for handling these files, but only as a local configuration for each CA Enterprise Log Manager server.

About the Event Log Store Service

The event log store service handles database interactions such as the following:

- Inserting new events into the current (hot) database
- Retrieving events from local and remote federated databases for queries and reports
- Creating new databases when the current database is full
- Creating new archive files and deleting old archive files
- Managing the archive query cache
- Applying selected summarization and suppression rules
- Applying selected event forwarding rules
- Defining CA Enterprise Log Manager servers that act as federated children to this CA Enterprise Log Manager server

About Archive Files

The CA Enterprise Log Manager server automatically creates warm database files, called *archive* files, when a hot database reaches the Maximum Rows setting you specify in the event log store service. Hot database files are not compressed.

When you configure auto archiving from a collection server to a reporting server, the warm databases on the collection server are deleted after the databases are copied to the reporting server. The Max Archive Days does not apply here.

When you configure auto archiving from a reporting server to a remote storage server, the warm databases on the reporting server are not deleted after being copied to the remote storage server. Rather, these warm databases are retained on the reporting server until the Max Archive Days value is reached. Then, they are *deleted*. However, a record of these deleted, cold databases is retained so you can query the archive database for details, should you ever need this information for performing a restore.

When determining how to set Max Archive Days, consider your available disk space on the reporting server. Your configuration for Archive Disk Space sets the threshold. If available disk space falls below the set percentage, event log data is deleted to make more room even when the Max Archive Days for that data has not elapsed.

When you do not configure auto archiving from a reporting server to a remote storage server, you must manually back up the warm databases and manually move the copy to a remote storage location at a frequency greater than the configured Max Archive Days. Otherwise, you risk losing data. We recommend that you back up archive files daily to avoid a potential data loss and to maintain adequate disk space. The event log store service manages its own internal cache for queries on archived databases to improve performance when running repeated or very broad queries.

More information on working with archive files is available in the *CA Enterprise Log Manager Administration Guide*.

More information:

[Example: Auto-Archiving Across Three Servers](#) (see page 143)

About Auto Archive

Management of stored event logs requires careful handling of backups and restored files. The event log store service configuration provides you with a central place to configure and tune internal database sizes, retention, and to set auto archive options. CA Enterprise Log Manager provides the following scripts to help with these tasks:

- `backup-ca-elm.sh`
- `restore-ca-elm.sh`
- `monitor-backup-ca-elm.sh`

Note: Use of these scripts assumes that you have established non-interactive authentication between the two servers using RSA keys.

The *backup* and *restore* scripts use the LMArchive utility to facilitate copying warm databases to or from remote hosts. The scripts automatically update the appropriate catalog files when the tasks finish. You can copy to remote servers or to other CA Enterprise Log Manager servers. If the remote host to which you send files is a CA Enterprise Log Manager server, the scripts automatically update the catalog files on the receiving server as well. The scripts also delete the archive files from the local machine to avoid duplication in federated reports. This ensures that data is available for query and reporting. Off-system storage is called cold storage. You can restore files moved to cold storage for queries and reporting.

The *monitor* script runs the backup script automatically using the settings you specify in the auto archive portion of the event log store service configuration.

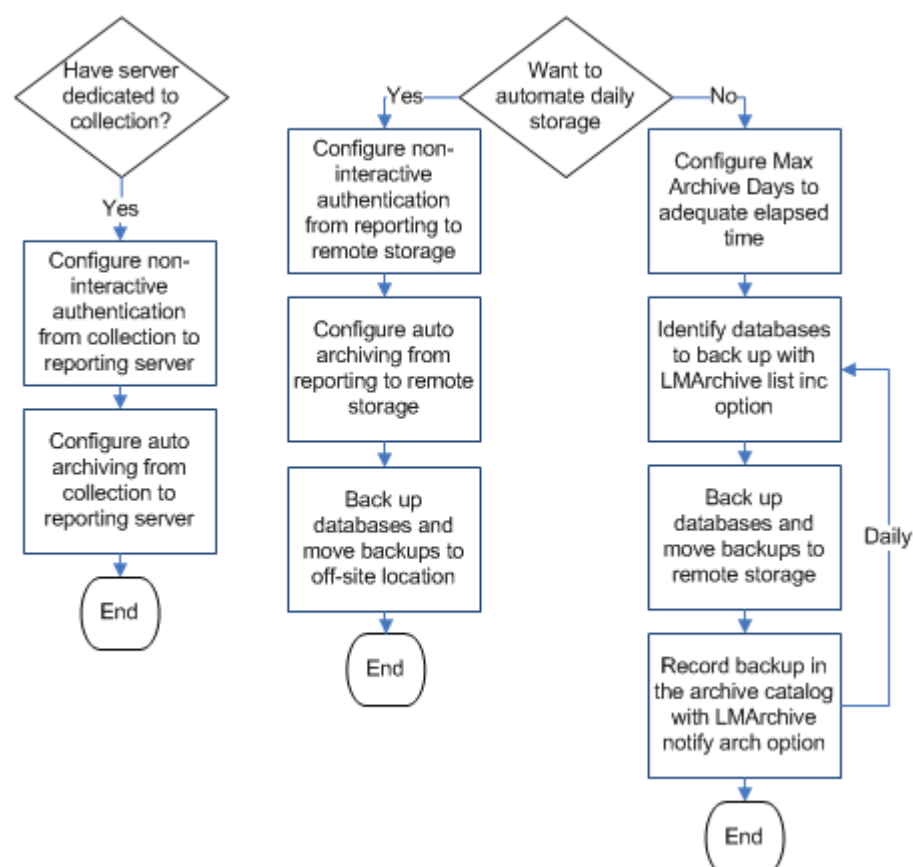
More information:

[Example: Auto-Archiving Across Three Servers](#) (see page 143)

Database Move and Backup Strategy Flowchart

You can perform both event collection and reporting on each CA Enterprise Log Manager server or you can dedicate different servers to collection and reporting. If you dedicate servers to collection, then automating hourly moves from collection servers to a reporting server is required; otherwise, it is not applicable. If you have no dedicated server roles, interpret the flowchart references "from reporting to remote storage" as "from a non-dedicated CA Enterprise Log Manager to remote storage."

A backup strategy implies having two copies of each database, where one is considered the backup. You can achieve this goal with or without auto archiving to a remote storage server. The backup strategy with auto archive results in the original databases on the remote storage server and the backups in an off-site location. The backup strategy without auto archive results in the original databases on the CA Enterprise Log Manager server and the backups on a remote storage server. Whether you can store the original databases on the CA Enterprise Log Manager where they were initially archived depends on the available space for long-term storage and storage policies. If these criteria are met, the decision rests on personal preference.



More information:

[Event Log Store Settings in the Basic Environment](#) (see page 148)

[Configuring Non-Interactive Authentication for Auto Archive](#) (see page 134)

Configuring Non-Interactive Authentication for Auto Archive

You can configure auto archiving between servers having different roles. For example:

- From one or more collection servers to a single reporting server.
- From one or more reporting servers to a single remote storage server.

Before configuring auto archiving from one server to another, configure non-interactive *ssh* authentication from the source server to the destination server. *Non-interactive* means that one server can move files to another server without requiring passwords.

- If you have only three servers, a collection server, a reporting server, and a remote storage server, you configure non-interactive authentication twice:
 - From the collection server to the reporting server
 - From the reporting server to the remote storage server.
- If you have six servers with four collection servers, one reporting server, and one remote storage server, you configure non-interactive authentication five times:
 - From collection server 1 to the reporting server.
 - From collection server 2 to the reporting server.
 - From collection server 3 to the reporting server.
 - From collection server 4 to the reporting server.
 - From the reporting server to the remote storage server.

Configuring non-interactive *ssh* authentication between two servers uses RSA key pairs, a private key and a public key. You copy the first public key you generate to the destination server as `authorized_keys`. When you configure multiple instances of non-interactive authentication to the same destination reporting server, you copy the additional public keys to unique filenames to avoid overwriting the original `authorized_keys`. Then you concatenate these filenames to `authorized_keys`. For example, you would append `authorized_keys_ELM-C2` and `authorized_keys_ELM-C3` to the `authorized_keys` file from ELM-C1.

More information:

[Example: Configure Non-Interactive Authentication for Hub and Spoke](#) (see page 135)

[Example: Configure Non-Interactive Authentication Across Three Servers](#) (see page 142)

Example: Configure Non-Interactive Authentication for Hub and Spoke

The existence of non-interactive authentication between two servers is a prerequisite for auto archiving from the source to the destination server. A common scenario for configuring non-interactive authentication is one where multiple source servers dedicated to collection have a common destination server dedicated to reporting/management. This example assumes a mid-sized CA Enterprise Log Manager federation with one reporting/management server (hub), four collection servers (spokes), and a remote storage server. Names for servers in each server role follow:

- CA Enterprise Log Manager Reporting/management server: ELM-RPT
- CA Enterprise Log Manager Collection servers: ELM-C1, ELM-C2, ELM-C3, ELM-C4
- Remote storage server: RSS.

The procedures for enabling non-interactive authentication for CA Enterprise Log Manager federation follow:

1. From the first collection server, generate an RSA key pair as caelmservice and copy the public key as `authorized_keys` to the `/tmp` directory on the destination reporting server.
2. From each additional collection server, if any, generate an RSA key pair and copy the public key as `authorized_keys_n`, where `n` uniquely identifies the source.
3. From the `/tmp` directory of the reporting server, concatenate the contents of these public key files to the original `authorized_keys`. Create an `.ssh` directory and change directory ownership to caelmservice, move `authorized_keys` to the `.ssh` directory, and set the key file ownership and required permissions.
4. Verify that non-interactive authentication exists between each collection server and the reporting server.
5. From the remote storage server, create a directory structure for the `.ssh` directory, where the default is `/opt/CA/LogManager`. Create an `.ssh` directory on the destination, change ownership to caelmservice.
6. From the reporting server, generate an RSA key pair as caelmservice and copy the public key as `authorized_keys` to the `/tmp` directory on the destination remote storage server.
7. From the remote storage server, move `authorized_keys` from `/tmp` to the `.ssh` directory and set the key file ownership to caelmservice with the required permissions.
8. Verify that non-interactive authentication exists between the reporting server and the remote storage server.

More information:

[Configure Keys for First Collection-Reporting Pair](#) (see page 136)

[Configure Keys for Additional Collection-Reporting Pairs](#) (see page 137)

[Create a Single Public Key File on the Reporting Server and Set File Ownership](#) (see page 138)

[Validate Non-Interactive Authentication Between Collection and Reporting Servers](#) (see page 139)

[Create a Directory Structure with Ownerships on the Remote Storage Server](#) (see page 140)

[Configure Keys for the Reporting-Remote Storage Pair](#) (see page 141)

[Set Key File Ownership on the Remote Storage Server](#) (see page 141)

[Validate Non-Interactive Authentication Between Reporting and Storage Servers](#) (see page 142)

Configure Keys for First Collection-Reporting Pair

Configuring non-interactive authentication for a hub and spoke architecture begins with generating an RSA public key/private key pair on a collection server and copying the public key to its reporting server. You copy the public key file with the name *authorized_keys*. Assume that this key is the first public key copied to the specified reporting server.

To generate a key pair on the first collection server and copy the public key to a reporting server

1. Log into the ELM-C1 through ssh as the caelmadmin user.
2. Switch users to root.

su –
3. Switch users to the caelmservice account.

su – caelmservice
4. Generate the RSA key pair using the following command:

ssh-keygen -t rsa
5. Press Enter to accept the default when each of the following prompts appears:
 - Enter file in which to save the key (/opt/CA/LogManager/.ssh/id_rsa):
 - Enter passphrase (empty for no passphrase):
 - Enter same passphrase again:

6. Change directories to `opt/CA/LogManager`.
7. Change the permissions of the `.ssh` directory using the following command:

```
chmod 755 .ssh
```
8. Navigate to `.ssh`, where `id_rsa.pub` key is saved.

```
cd .ssh
```
9. Copy the `id_rsa.pub` file to ELM-RPT, the destination CA Enterprise Log Manager server, using the following command:

```
scp id_rsa.pub caelmadmin@ELM-RPT:/tmp/authorized_keys
```

This creates the `authorized_keys` file on the reporting server with the content of the public key.

Configure Keys for Additional Collection-Reporting Pairs

The second step of configuring non-interactive authentication for a hub and spoke architecture is to generate an RSA key pair on each additional collection server and copy it to the `/tmp` directory of the common reporting server as `authorized_keys_n`, where `n` uniquely references the source collection server.

To generate an RSA key pair on additional collection servers and copy the public key to a common reporting server.

1. Log into the second collection server ELM-C2 through ssh as `caelmadmin`.
2. Switch users to root.
3. Switch users to the `caelmservice` account.

```
su - caelmservice
```
4. Generate the RSA key pair using the following command:

```
ssh-keygen -t rsa
```
5. Press Enter to accept the default when each of the following prompts appears:
 - Enter file in which to save the key (`/opt/CA/LogManager/.ssh/id_rsa`):
 - Enter passphrase (empty for no passphrase):
 - Enter same passphrase again:
6. Change directories to `/opt/CA/LogManager`.
7. Change the permissions of the `.ssh` directory using the following command:

```
chmod 755 .ssh
```
8. Navigate to `.ssh`, where `id_rsa.pub` key is saved.

9. Copy the `id_rsa.pub` file to ELM-RPT, the destination CA Enterprise Log Manager server, using the following command:

```
scp id_rsa.pub caelmadmin@ELM-RPT:/tmp/authorized_keys_ELM-C2
```

This creates the `authorized_keys_ELM-C2` file on the reporting server with the content of the public key.

10. Type `yes` followed by the `caelmadmin` password of ELM-RPT
11. Type `exit`.
12. Repeat steps 1-11 of this procedure on collection servers ELM-C3. For Step 9 specify the following:

```
scp id_rsa.pub caelmadmin@ELM-RPT:/tmp/authorized_keys_ELM-C3
```

13. Repeat steps 1-11 of this procedure on collection servers ELM-C4. For Step 9 specify the following:

```
scp id_rsa.pub caelmadmin@ELM-RPT:/tmp/authorized_keys_ELM-C4
```

Create a Single Public Key File on the Reporting Server and Set File Ownership

In our scenario thus far, we have generated key pairs on each collection server and copied the public key portion to the reporting server as the following files:

- `authorized_keys`
- `authorized_keys_ELM-C2`
- `authorized_keys_ELM-C3`
- `authorized_keys_ELM-C4`

Step 3 is to concatenate these files, move the resulting RSA public key file to the correct directory, and set directory and file ownership to `caelmservice`.

To create a combined public key file in the correct directory on the reporting server and set file ownership

1. Log into the reporting CA Enterprise Log Manager server through `ssh` as `caelmadmin`.
2. Switch users to `root`.
3. Change directories to the CA Enterprise Log Manager folder:

```
cd /opt/CA/LogManager
```
4. Create the `.ssh` folder:

```
mkdir .ssh
```
5. Change the ownership of the new folder to the `caelmservice` user and group:

```
chown caelmservice:caelmservice .ssh
```

6. Change directories to /tmp
7. Add the contents of the public keys from the collection servers ELM-C2, ELM-C3, and ELM-C4 to the authorized_keys file that contains the public key from ELM-C1.

```
cat authorized_keys_ELM-C2 >> authorized_keys
cat authorized_keys_ELM-C3 >> authorized_keys
cat authorized_keys_ELM-C4 >> authorized_keys
```

8. Change directories to opt/CA/LogManager/.ssh
9. Copy the authorized_keys file from the /tmp folder to the current folder, .ssh:

```
cp /tmp/authorized_keys .
```

10. Change the ownership of the authorized_keys file to the caelmservice account:

```
chown caelmservice:caelmservice authorized_keys
```

11. Change the permissions on the file:

```
chmod 755 authorized_keys
```

755 means read and execute access for everyone and read, execute, and write access for the owner of the file

This completes the configuration of password-less authentication between the collection servers and the reporting server.

Validate Non-Interactive Authentication Between Collection and Reporting Servers

You can validate the configuration of non-interactive authentication between the source and destination servers of both phases of auto-archive.

To validate the configuration between the collection and reporting servers

1. Log into the collection server ELM-C1 through ssh as caelmadmin.
2. Switch users to root.
3. Switch users to the caelmservice account.

```
su - caelmservice
```

4. Enter the following command:

```
ssh caelmservice@ELM-RPT
```

Being logged into ELM-RPT without entering a passphrase confirms non-interactive authentication between ELM-C1 and ELM-RPT.

5. Log on to ELM-C2 and repeat.
6. Log on to ELM-C3 and repeat.
7. Log on to ELM-C4 and repeat.

Create a Directory Structure with Ownerships on the Remote Storage Server

The following procedure assumes the remote storage server is not a CA Enterprise Log Manager server and that you need to create new users, a group, and a directory structure that mirrors that of a CA Enterprise Log Manager server. You must perform this procedure before you send the key from the reporting server, since you use the caelmadmin account you create to communicate with the reporting server.

To create a file structure and set file ownerships on the remote storage server

1. Log into the remote storage server, RSS, through ssh as root.
2. Create a new user called caelmadmin.
3. Create a group called caelmservice and then create a new user called caelmservice.
4. Create the directory to use as the Remote Location, where the default is /opt/CA/LogManager.

Note: To use a different directory, be sure to specify that directory when you configure Remote Location for Auto Archive.

5. Change the home directory for caelmservice to /opt/CA/LogManager or the planned Remote Location directory. The following example assumes the default directory:

```
usermod -d /opt/CA/LogManager caelmservice
```

6. Set the file permissions for caelmservice. The following example assumes the default Remote Location directory:

```
chown -R caelmservice:caelmservice /opt/CA/LogManager
```

7. Change directories to /opt/CA/LogManager or the Remote Location alternative.
8. Create the .ssh folder.
9. Change the ownership of the .ssh folder to the caelmservice user and group:

```
chown caelmservice:caelmservice .ssh
```

10. Log off of the remote storage server.

Configure Keys for the Reporting-Remote Storage Pair

After you configure and validate non-interactive authentication from each collection server to the reporting server, you configure and validate non-interactive authentication from the reporting server to the remote storage server.

For the example scenario, configuration begins with generating a new RSA key pair on the reporting server, ELM-RPT, and copying the public key as `authorized_keys` to the `/tmp` directory of the remote storage server, RSS.

To generate an RSA key pair on the reporting server and copy it to the remote storage server

1. Log into the reporting server as `caelmadmin`.
2. Switch users to root.
3. Switch users to the `caelmservice` account.

```
su - caelmservice
```

4. Generate the RSA key pair using the following command:

```
ssh-keygen -t rsa
```

5. Press Enter to accept the default when each of the following prompts appears:

- Enter file in which to save the key (`/opt/CA/LogManager/.ssh/id_rsa`):
- Enter passphrase (empty for no passphrase):
- Enter same passphrase again:

6. Change directories to `opt/CA/LogManager`.
7. Change the permissions of the `.ssh` directory using the following command:

```
chmod 755 .ssh
```

8. Navigate to the `.ssh` folder.
9. Copy the `id_rsa.pub` file to RSS, the destination remote storage server, using the following command:

```
scp id_rsa.pub caelmadmin@RSS:/tmp/authorized_keys
```

This creates the `authorized_keys` file in the `/tmp` directory on the remote storage server with the content of the public key.

Set Key File Ownership on the Remote Storage Server

You can set key file ownership and permissions on a remote storage server after you generate a key pair on the reporting server and copy the public key to that remote storage server.

To move the public key file to the correct location on the remote storage server and set file ownership

1. Log into the remote storage server as caelmadmin.
2. Switch users to root.
3. Change directories to /opt/CA/LogManager/.ssh.
4. Copy the authorized_keys file from the /tmp directory to the current directory .ssh:

```
cp /tmp/authorized_keys .
```

5. Change the ownership of the authorized_keys file with the command:

```
chown caelmservice:caelmservice authorized_keys
```

6. Change the permissions on the authorized_keys file:

```
chmod 755 authorized_keys
```

Non-interactive authentication is now configured between a CA Enterprise Log Manager reporting server and the remote host used for storage.

Validate Non-Interactive Authentication Between Reporting and Storage Servers

Confirm that non-interactive authentication is set between the reporting server and the remote storage server. For the example scenario, the remote storage server is named RSS.

To validate non-interactive authentication between the reporting CA Enterprise Log Manager and the storage server

1. Log into the reporting server as root.
2. Switch users to the caelmservice.

```
su - caelmservice
```

3. Enter the following command:

```
ssh caelmservice@RSS
```

This logs you into the remote storage server without entering a passphrase.

Example: Configure Non-Interactive Authentication Across Three Servers

The simplest scenario for configuring non-interactive authentication, a prerequisite for auto archiving, is one with two CA Enterprise Log Manager servers, one collection server and one reporting/management server, and a remote storage system on any UNIX or Linux server. This example assumes that the three servers being prepared for auto archiving are named:

- NY-Collection-ELM
- NY-Reporting-ELM
- NY-Storage-Svr

The procedures for enabling non-interactive authentication follow:

1. From NY-Collection-ELM, generate the RSA key pair as caelmservice and copy the public key of this pair as `authorized_keys` to the `/tmp` directory on NY-Reporting-ELM.
2. Create an `.ssh` directory on NY-Reporting-ELM, change ownership to caelmservice, move `authorized_keys` from the `/tmp` directory to the `.ssh` directory and set the key file ownership to caelmservice with the required permissions.
3. Validate non-interactive authentication from NY-Collection-ELM to NY-Reporting-ELM.
4. From NY-Reporting-ELM, generate another RSA key pair as caelmservice and copy the public key as `authorized_keys` to the `/tmp` directory of NY-Storage-Svr.
5. From NY-Storage-Svr, create the directory structure `/opt/CA/LogManager`. From this path, create an `.ssh` directory, change ownership to caelmservice, move `authorized_keys` to this directory and set the key file ownership to caelmservice with the required permissions.
6. Validate non-interactive authentication from NY-Reporting-ELM to NY-Storage-Svr.

The details for these steps are similar to those of the hub and spoke scenario. For a three server scenario, you skip Step 2 on additional collection-reporting pairs and skip the Step 3 instructions on concatenating the files to `authorized_keys`.

More information:

[Example: Auto-Archiving Across Three Servers](#) (see page 143)

Example: Auto-Archiving Across Three Servers

When using the collection-reporting architecture, you must configure auto-archiving from the collection server to a reporting server. This configuration automates the move of a warm database of collected and refined event log data to the reporting server where you can report on it. It is a good practice to schedule this auto-archiving to recur hourly, rather than daily, to avoid devoting an extended period of time every day for doing huge data transfers. Choose a schedule based on your load and whether it is better to consolidate processing or spread it out over the day. When databases are copied through auto archiving from a collection server to its reporting server, those databases are deleted from the collection server.

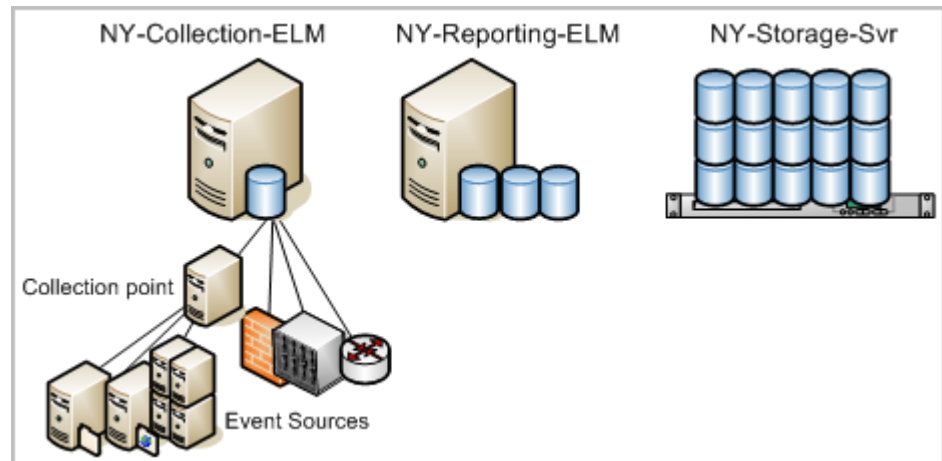
After you identify a local server with a lot of storage space, you can configure auto-archiving from the reporting server to this remote storage server. When databases are copied through auto archiving from a reporting server to a remote storage server, those databases stay intact on the reporting server until the time you configure as Max Archive Days has elapsed. At that point, they are deleted. The benefit of this phase of auto-archiving is to protect archived databases from being lost due to not being manually moved to a long-term storage location before auto-deletion.

Note: Before you configure a remote server to receive auto-archived databases, you must set up a directory structure on this destination server like that on the source CA Enterprise Log Manager server and assign various ownerships and permissions for authentication. For details, see "Configuring Non-Interactive Authentication" in the *Implementation Guide*. Be sure to follow instructions described in "Set Key File Ownership on a Remote Host."

For this example scenario, assume you are a CA Enterprise Log Manager Administrator in a New York data center with a network of CA Enterprise Log Manager servers, each with a dedicated role, plus a remote server with a lot of storage capacity. Names of the servers used in auto-archiving follow:

- NY-Collection-ELM
- NY-Reporting-ELM
- NY-Storage-Svr

Note: This example assumes the existence of a management server dedicated to managing the CA Enterprise Log Manager system of servers. This server is not depicted here because it has no direct role in auto-archiving.



To configure auto-archiving from a collection server to a reporting server and then from the reporting server to a remote storage server, use the following example as a guide:

1. Select the Administration tab and the Log Collection subtab.
2. Expand the Event Log Store folder and select a collection server.



3. Specify Auto-archiving to recur hourly, where the destination is the reporting server. Enter credentials of a CA Enterprise Log Manager user with an Administrator role. If you have custom policies, this must be a user with edit rights to the Database resource, which grants the ability to delete the archived database.

Auto Archive			
<input checked="" type="checkbox"/> Enabled	Backup Type: Incremental		
Frequency: Hourly	Start Time (24-hour clock): 0		
EEM User: Administrator1	EEM Password: *****		
Remote Server: NY-Reporting-ELM	Remote User: caelmservice		
Remote Location: /opt/CA/LogManager	<input checked="" type="checkbox"/> Remote ELM Server		

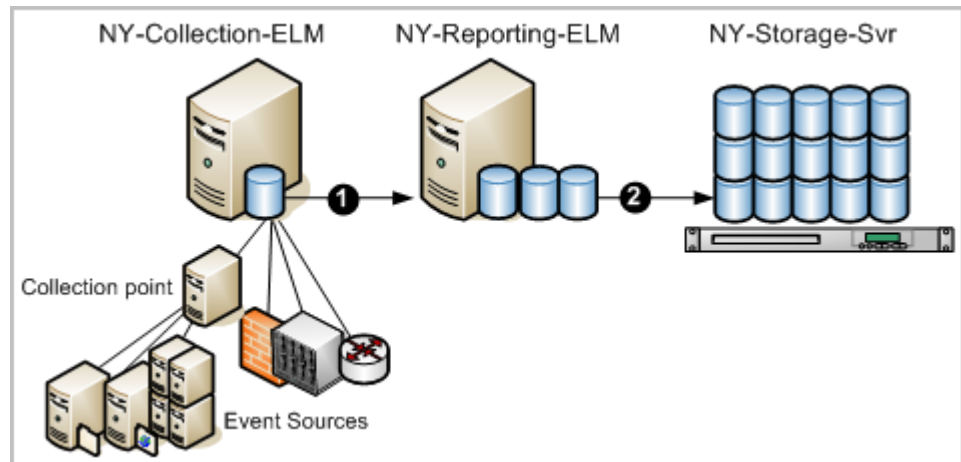
4. Select the reporting server from the Services list.



- Specify Auto-archiving to recur daily, where the destination is a remote server that is used for storage. Enter credentials of a user account with an Administrator role. Optionally, create a CALM access policy with the edit action on the database resource and assign a user as the Identity. Enter the credentials of that low-privileged user here.

Auto Archive	
<input checked="" type="checkbox"/> Enabled	Backup Type: Incremental ▼
Frequency: Daily ▼	Start Time (24-hour clock): 1 ▲▼
EEM User: Administrator1	EEM Password: *****
Remote Server: NY-Storage-Svr	Remote User: caelmservice
Remote Location: /opt/CA/LogManager	<input type="checkbox"/> Remote ELM Server

The numbers on the following diagram depict two configurations of auto-archiving: one from the collection server to the reporting server and another from the reporting server to a remote server on the network.

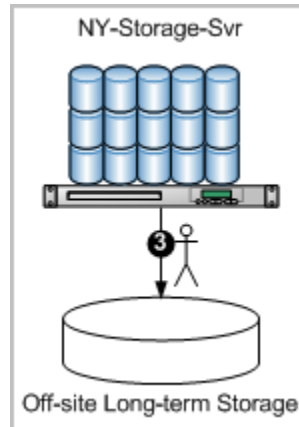


After such a configuration, that automatic processing works as follows:

- NY-Collection-ELM, the Collection CA Enterprise Log Manager server, collects and refines events and inserts them into the hot database. When the hot database reaches the configured number of records, the database is compressed into a warm database. Since auto-archiving is scheduled to recur hourly, each hour the system copies the warm databases and moves them to the NY-Reporting-ELM, the reporting CA Enterprise Log Manager server. The warm databases are deleted from NY-Collection-ELM when they are moved.
- NY-Reporting-ELM retains databases that can be queried until they are the age configured for Max Archived Days, after which they are deleted. Since auto-archiving is scheduled to recur daily, each day the system copies the warm databases and moves them as cold databases to NY-Storage-Svr. The cold databases can remain on the remote storage server for an extended period of time.

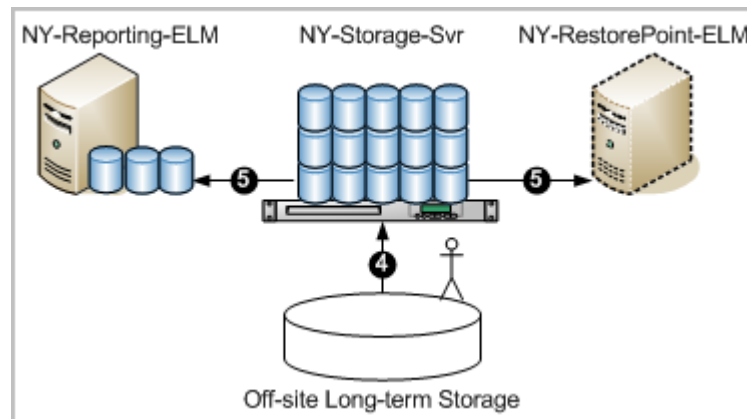
3. You move the cold databases stored on the network NY-Storage-Svr to an off-site long-term storage solution where they can remain for the mandated number of years.

The reason for archiving is to keep event logs available for restoration. Cold databases can be restored if a need arises to investigate old events that have been logged. The manual step of moving archived databases from the on-site storage server to an off-site long-term storage location is depicted on the following diagram.



4. Assume that a situation surfaces that makes it necessary to examine logs that have been backed up and moved off-site. To identify the name of the archived database to restore, search the local archive catalog on NY-Reporting-ELM. (Click the Administration tab, select Archive Catalog Query from the Log Collection Explorer, and click Query.)
5. Retrieve the identified archived database from off-site storage. Copy it back to the /opt/CA/LogManager/data/archive directory on the NY-Storage-Svr. Then, change the ownership of the archive directory to caelmservice user.

6. Restore the database either to its original reporting server or to a restore point dedicated to investigating logs from restored databases as follows:
 - If restoring to NY-Reporting-ELM, run the `restore-ca-elm.sh` script from NY-Reporting-ELM specifying NY-Storage-Svr as the remote host.
 - If restoring to NY-RestorePoint-ELM, run the `restore-ca-elm.sh` script from NY-RestorePoint-ELM specifying NY-Storage-Svr as the remote host.



Note: You can now query and report on the restored data.

More information:

[About Auto Archive](#) (see page 132)

[About Archive Files](#) (see page 131)

[Event Log Store Settings in the Basic Environment](#) (see page 148)

[Example: Federation Map for a Large Enterprise](#) (see page 32)

Event Log Store Settings in the Basic Environment

In an environment with separate CA Enterprise Log Manager servers performing roles of collection server and reporting server, you should configure the event log stores individually as local configurations. If you also choose to use the reporting server to handle failover traffic, you may want to set a higher value for the Maximum Rows field than that which is shown in the table. If you use your management server as a reporting server, consider that the management server does generate some event information itself in the form of self-monitoring events.

Note: You must configure each pair of servers that participate in auto archiving for non-interactive authentication for the auto archive configuration to operate properly.

The following table is an example, illustrating certain basic settings. The collection CA Enterprise Log Manager server is named CollSrvr-1. The reporting CA Enterprise Log Manager server named RptSrvr-1. For the example, there exists a remote storage server named RemoteStore-1 to store cold database files, and that the cold files are located in the directory, /CA-ELM_cold_storage.

Event Log Store field	Collection Server values	Reporting Server values
Maximum Rows	2000000 (default)	Not applicable to auto archive.
Max Archive Days	1 (Not applicable to auto archive.)	30 (Applicable to auto archive and when auto archive is not configured.)
Archive Disk Space	10	10
Export Policy	24	72
Secure Service Port	17001	17001
<i>Auto Archive Options</i>		
Enabled	Yes	Yes
Backup Type	Incremental	Incremental
Frequency	Hourly	Daily
Start Time	0	23
EEM User	<CA Enterprise Log Manager_Administrator>	<CA Enterprise Log Manager_Administrator>
EEM Password	<password>	<password>
Remote Server	RptSrvr-1	RemoteStore-1
Remote User	caelmservice	user_X
Remote Location	/opt/CA/LogManager	/CA-ELM_cold_storage
Remote CA-ELM Server	Yes	No

The auto archive options in this example move archive files (warm database files) on the collection server to the reporting server every hour. This keeps disk space available for incoming events. Both servers use an incremental backup to avoid having to move large volumes of data at any one time. After a warm database is moved to the reporting server, it is automatically deleted from the collection server.

Note: The 0 value for the Start Time does not have any effect when the backup Frequency is set to Hourly.

For EEM User and EEM Password, you specify the credentials of a CA Enterprise Log Manager user assigned either the predefined role of Administrator or a custom role associated with a custom policy that grants the ability to perform the edit action on the database resource.

For the reporting server, specify `/opt/CA/LogManager` for the Remote Location and `caelmservice` as the Remote User if auto archiving from the reporting server to the remote storage server. You create this path and this user when you configure non-interactive authentication between these servers.

The auto archive options in this example move archive files on the reporting server to the remote storage server daily starting at 11:00 pm. After a database is moved to cold storage on the remote server, it is retained on the reporting server for Max Archive Days.

If auto-archive is not enabled, warm databases are retained based on thresholds configured for Max Archive Days and Archive Disk Space, whichever occurs first. Archived databases would be retained on the reporting server for 30 days before being deleted unless the disk space drops below 10%. In that case, the reporting server generates a self-monitoring event and deletes the oldest databases until available disk space is above 10%. You can create an alert to notify you by email or RSS feed when this occurs.

When a database is restored from a remote storage server to its original reporting server, it is kept for 3 days (72 hours).

More information about each of these fields and their values is available in the online help.

Set Event Log Store Options

The Event Log Store configuration dialog allows you to set global options for all CA Enterprise Log Manager servers. You can also click the arrow next to the entry to expand the Event Log Store node. This action displays the individual CA Enterprise Log Manager servers in your network. Clicking on those server names allows you to set local configuration options that are specific to each server, if desired.

Users with the Administrator role can configure any CA Enterprise Log Manager server from any other CA Enterprise Log Manager server.

To set event log store options

1. Log into the CA Enterprise Log Manager server and select the Administration tab.
The Log Collection subtab displays by default.
2. Click the Services subtab.
3. Select the Event Log Store entry.

The default options provide a good starting configuration for a medium-sized network with moderate throughput.

Additional information about each field is available in the online help.

Note: The Federation Children and Auto Archive tables appear only when you display the local options for an individual CA Enterprise Log Manager server.

Configuring the Correlation Service

The correlation service controls how and where correlation rules are applied in your environment. When configuring the correlation service, you should consider:

- Whether or not you plan to deploy a dedicated correlation server.
- The names and locations of the collection servers that supply events for correlation.
- Types and specific names of the correlation rules you want to apply in your environment.
- Notification destinations you have created for your environment.

Apply Correlation Rules and Incident Notifications

You must apply correlation rules in order for them to take effect in your environment. When you apply correlation rules, you can also associate notification destinations for each rule.

To apply correlation rules and set notification destinations

1. Click Administration, then the Services subtab, and expand the Correlation Service node.
2. Select the CA Enterprise Log Manager server on which you want to apply correlation rules.

Correlation Server details appear in the right pane.
3. Click Add.

A rule and version dialog appears.
4. Select the check box beside rule category or rule you want to apply. You can select entire category folders, individual rules, or any combination.
5. Select the rule version you want for each rule you select to apply.
6. (Optional) Select a notification destination for any rule you have selected to apply. If you do not select a destination, the rule will have no automatic notification. You can still manually set a notification for incidents generated by any rule.
7. Select collection servers to route events for correlation from the available list of servers. You must select all the servers you want to send events for correlation. If no servers are selected, no events will be forwarded for correlation.
8. Click OK, or Apply.

Using Pre-Defined Correlation Rules

CA Enterprise Log Manager provides a large number of pre-defined correlation rules for use in your environment, organized by type or regulatory requirement. For example, in the Correlation rules folder of the Library interface, you can see a folder titled PCI, containing rules for various PCI requirements. You can also see a folder titled Identity, which contains general-purpose rules on authorization and authentication.

There are three main types of rules, any or all of which may be included in each category. This topic gives an example of choosing and applying one of each type.

Example - Select and Apply a Simple Rule

Simple correlation rules detect the presence of one state or occurrence. For example, you can apply a rule that alerts you to account creation activity outside normal office hours. Before applying any rule, you should ensure that you have created the Notification Destinations that you want for your environment.

To select and apply the Account Creation Outside Normal Office Hours rule

1. Click the Administration tab, then the Library subtab, and expand the Correlation Rules folder.
2. Expand the PCI folder, then the Requirement 8 folder, and select the Account Creation Outside Normal Office Hours rule.

The rule details appear in the right pane.

3. Review the rule details to ensure that the rule is appropriate for your environment. In this case, the filters define the account creation action, and set the normal business hours by time and day of the week.
4. (Optional) Click Edit at the top on the pane to modify the filter settings, if required. For example, you could change the normal work hours to fit your local specifications.

The Manage Rule wizard opens, populated with the rule details.

5. Add any notification details you want in the Manage Rule wizard. Notification details provide the message content that is delivered as specified in Notification Destinations.
6. Once you have finished preparing the rule, click Save and Close in the wizard. When you edit and save a pre-defined correlation rule, CA Enterprise Log Manager automatically creates a new version, preserving the original version.
7. Click the Services subtab, and expand the Correlation Service node.
8. Select the server you want to apply the rule on. If you have identified a Correlation Server you should select that server.
9. Click Apply in the Rule Configuration area, and select the new version of the Account Creation Outside Normal Business Hours rule, along with the Notification Destination you want associated with it.

10. Click OK to close the dialog and activate the rule.

Example - Select and Apply a Counting Rule

Counting correlation rules identify a series of identical states or occurrences. For example, you can apply a rule that alerts you to five or more failed logins by an Administrator account. Before applying any rule, you should ensure that you have created the Notification Destinations that you want for your environment.

To select and apply the 5 Failed Logins by Administrator Account rule

1. Click the Administration tab, then the Library subtab, and expand the Correlation Rules folder.
2. Expand the Threat Management folder, then the Suspicious Account and Login Activity folder, and select the 5 Failed Logins by Administrator Account rule.

The rule details appear in the right pane.

3. Review the rule details to ensure that the rule is appropriate for your environment. In this case, the filters define an Administrator account as a username belonging to the 'Administrators' keyed list, and sets the count threshold to 5 events in 60 minutes.
4. (Optional) Click Edit at the top on the pane to modify the filter settings, if required. For example, you could change the time threshold to 3 events in 30 minutes.

The Manage Rule wizard opens, populated with the rule details.

5. Add any notification details you want in the Manage Rule wizard. Notification details provide the message content that is delivered as specified in Notification Destinations.
6. Once you have finished preparing the rule, click Save and Close in the wizard. When you edit and save a pre-defined correlation rule, CA Enterprise Log Manager automatically creates a new version, preserving the original version.
7. Click the Services subtab, and expand the Correlation Service node.
8. Select the server you want to apply the rule on. If you have identified a Correlation Server you should select that server.
9. Click Apply in the Rule Configuration area, and select the new version of the 5 Failed Logins by Administrator Account rule, along with the Notification Destination you want associated with it.

10. Click OK to close the dialog and activate the rule.

Example - Select and Apply a State Transition Rule

State transition correlation rules identify a series of states or occurrences in turn. For example, you can apply a rule that alerts you to failed logins followed by a successful login from the same user account. Before applying any rule, you should ensure that you have created the Notification Destinations that you want for your environment.

1. Click the Administration tab, then the Library subtab, and expand the Correlation Rules folder.

2. Expand the Identity folder, then the Authentication folder, and select the Failed Logins Followed by Success rule.

The rule details appear in the right pane.

3. Review the rule details to ensure that the rule is appropriate for your environment. In this case, the details pane displays the two states that the rule tracks. The first is five or more failed logins by the same user account or identity. The second is a successful login by that same user or identity.

4. (Optional) Click Edit at the top on the pane to modify the state settings, if required.

The Manage Rule wizard opens, displaying the two states that make up the rule.

5. Double-click any state you want to change.

The State Definition wizard appears, displaying the details of the state.

6. Make any state changes you want to the state you selected., and click Save and Close to return to the Manage Rule wizard. For example, the first state checks for 5 failed logins in 10 minutes. You could change the failed login threshold, or the time, or both.

7. Add any notification details you want in the Manage Rule wizard. Notification details provide the message content that is delivered as specified in Notification Destinations.

8. Once you have finished preparing the rule, click Save and Close in the wizard. When you edit and save a pre-defined correlation rule, CA Enterprise Log Manager automatically creates a new version, preserving the original version.

9. Click the Services subtab, and expand the Correlation Service node.

10. Select the server you want to apply the rule on. If you have identified a Correlation Server you should select that server.

11. Click Apply in the Rule Configuration area, and select the new version of the Failed Logins Followed by Success rule, along with the Notification Destination you want associated with it.

12. Click OK to close the dialog and activate the rule.

More information:

[Apply Correlation Rules and Incident Notifications](#) (see page 152)

Set Collection Servers

You can set collection servers to route events for correlation in a multiserver environment. Setting collection servers allows you to administer and run correlation rules on one server, whether it is a dedicated correlation server, or one with shared roles. You can then view incidents from all the selected collection servers.

To set collection servers

1. Click Administration, then the Services subtab, and expand the Correlation Service node.
2. Select the CA Enterprise Log Manager server to which you want route events for correlation. If you have a dedicated correlation server, select that server name.
Correlation Server details appear in the right pane.
3. Use the Collection Servers shuttle control to select the servers you want. Ensure that all the servers that are collecting events for correlation are in the Selected column.

How to Design and Apply Incident Notifications

You can set up notifications for your correlation rules. Notifications allow you to pass key information on detected incidents to the staff you specify, or create CA IT PAM service desk tickets automatically.

Use the following process to design and set up notifications in your environment:

1. Plan and create notification destinations.
2. Select the pre-defined correlation rules, or create custom rules you want to use in your environment.
3. Add notification details to the rules for which you want to set notifications.
4. Apply correlation rules to CA Enterprise Log Manager servers, and assign notification destinations.

More information:

[How to Create a Notification Destination](#) (see page 157)

[Apply Correlation Rules and Incident Notifications](#) (see page 152)

How to Create a Notification Destination

You can create notification destination objects for use in correlation rules. Destinations allow you to apply common delivery settings to various rules; one destination can be assigned to multiple rules, as needed. They can be assigned during correlation rule application or after an incident is created.

You create a notification destination object using the following process:

1. Open the Manage Notification Destinations wizard and set a destination name and description.
2. Set parameters for the destination types you want:
 - a. Emails
 - b. CA IT PAM processes
 - c. SNMP traps

A notification destination object can have multiple notification types.

More information:

[Open the Manage Notification Destination Wizard](#) (see page 157)

[Set Email Destinations](#) (see page 158)

[Set a Process Destination](#) (see page 158)

[Set SNMP Destinations](#) (see page 159)

Open the Manage Notification Destination Wizard

To create a notification destination you must open the wizard.

To open the manage notification destination wizard

1. Click the Administration tab, the Library subtab, and the Notification Destinations folder.
2. Click New Notification.

The Manage Notification wizard opens.

More information:

[Set Email Destinations](#) (see page 158)

[Set a Process Destination](#) (see page 158)

[Set SNMP Destinations](#) (see page 159)

Set Email Destinations

You can set email destinations for notifications, to help inform proper personnel of incidents relating to their job role or responsibility.

To set email destinations

1. Open the Manage Notification Destination wizard.
2. Set the identification details, and advance to the Notifications step.
3. Click the email tab, and select Enable email notification.
4. Enter at least one recipient email address. You can enter multiple addresses separated by commas.
5. (Optional) Enter From email address.
6. Add any other destinations you want, or click Save and Close.

Set a Process Destination

You can set an IT PAM Process as a notification destination. The notification passes CA Enterprise Log Manager incident information to CA ServiceDesk or third party applications using IT PAM. You set a process destination by identifying a valid IT PAM process. You define the incident information you want to make up the process parameters using notification details.

For additional information on IT PAM processes, see the *CA Enterprise Log Manager Administration Guide*.

To set process destinations

1. Open the Manage Notification Destinations wizard, set identification details, and advance to the Notifications step.
2. Click the Process tab and select Enable Process Automation.
3. Enter the name of an IT PAM process to which you want to pass incident information, such as:

/CA_ELM/EventAlertOutput
4. Add any other destinations you want, or click Save and Close.

Set SNMP Destinations

You can set SNMP destinations, allowing you to use SNMP traps to send incident information to third-party management systems. For additional information on SNMP traps, see the *CA Enterprise Log Manager Administration Guide*.

To set SNMP destinations

1. Open the Manage Notification Destinations wizard, set the identification details, and advance to the Notifications step.
2. Click the SNMP tab, and select Enable SNMP Trap.
3. (Optional) To send the alert using SNMP v3, select SNMP Version 3. SNMP Version 2 is the default.
4. (Optional) If you select SNMP Version 3, click the V3 Security button to set authentication or encryption in the Security Parameters dialog.
5. Enter Destination Server and Destination Port information to identify the target of your SNMP-transmitted events.
6. (Optional) Select another Destination Server/Destination Port row, and enter another pair of server/port values.
7. Add any other destinations you want, or click Save and Close.

Incident Service Considerations

You can control the way in which the incident service stores events and creates incidents for a selected CA Enterprise Log Manager server. You can set the following values:

Expiration Time

Specifies how long in days the service retains incidents in the incident database. If the value is 0, events are never deleted. Expired incidents are not displayed.

Incident Generation Limit values

Specifies how often a single correlation rule can create incidents, allowing you to reduce unwanted multiple incidents. For the purposes of incident generation limits, different versions of a rule are considered separate rules. So if you have applied multiple versions of a rule in your environment, they are limited separately. Limit values include:

Enabled

Indicates whether incident generation limits are applied.

Count

Sets a threshold for the number of incidents generated by a single rule. This value works with the Time value, if that value is above 0. After these numbers are reached, the incident service applies the Blocked Time limit. So if you set Count to 3, and the Time to 10, the limit applies after a single rule generates more than 3 incidents in 10 seconds.

Time

Sets a threshold, in seconds, for the number of incidents generated by a single rule. This value works with the Count value, if that value is above 0. After these numbers are reached, the incident service applies the Blocked Time limit. So if you set Count to 3, and the Time to 10, the limit applies after a single rule generates more than 3 incidents in 10 seconds.

Blocked Time

Specifies an interval in seconds, when a rule is blocked from creating further incidents. When this limit is reached, the rule creates no incidents until the time expires.

ODBC Server Considerations

You can install an ODBC client or a JDBC client to access the CA Enterprise Log Manager event log store from an external application like SAP BusinessObjects Crystal Reports.

You can perform the following tasks from this configuration area:

- Enable or disable ODBC and JDBC access to the event log store.
- Set the service port used for communications between the ODBC or JDBC client and CA Enterprise Log Manager server.
- Specify whether communications between ODBC or JDBC client and CA Enterprise Log Manager server are encrypted.

The field descriptions are as follows:

Enable Service

Indicates whether the ODBC and JDBC clients can access data in the event log store. Select this check box to enable external access to events. Clear the check box to disable external access.

The ODBC service is not currently FIPS-compatible. Clear this check box to prevent ODBC and JDBC access if you intend to run in FIPS mode. This prevents non-compliant access to event data. If you intend to disable the ODBC and JDBC service for FIPS mode operations, ensure that you set this value for *each* server in a federation.

Server Listening Port

Specifies the port number used by the ODBC or JDBC services. The default value is 17002. The CA Enterprise Log Manager server refuses connection attempts when a different value is specified in the Windows Data Source or the JDBC URL string.

Encrypted (SSL)

Indicates whether to use encryption for communications between the ODBC client and the CA Enterprise Log Manager server. The CA Enterprise Log Manager server refuses connection attempts when the corresponding value in the Windows Data Source or JDBC URL does not match this setting.

Session Timeout (minutes)

Specifies the number of minutes to keep an idle session open before it is closed automatically.

Log Level

Defines the type and level of detail recorded in the logging file. The drop-down list is arranged in order of detail, with the first choice providing least detail.

Apply to all loggers

Controls whether the Log Level setting overrides all log settings from the properties file of the log. This setting only applies when the Log Level setting is lower (showing more detail) than the default setting.

Report Server Considerations

The Report Server controls the administration of automatically delivered reports, and their appearance in PDF format, and Action Alert and report retention. You can perform the following tasks from the report server configuration area:

- Control the company name and logo, fonts, and other PDF reports settings in the Report Configurations area.
- Set the total Actions Alerts retained, and number of days they are retained in the Alert Retention area:

Maximum Action Alerts

Defines the maximum number of action alerts the reporting server retains for review.

Minimum: 50

Maximum: 1000

Action Alerts Retention

Defines the number of days action alerts are retained, up to the maximum number.

Minimum: 1

Maximum: 30

- Set the retention policy for each scheduled report recurrence type in the Report Retention area.
- Set whether or how often the retention utility searches for reports to delete automatically based on those policies. For example, if the report retention utility runs daily, it deletes reports daily that are older than the specified maximum age.

How to Configure Subscription

Once you have planned your subscription architecture, you can configure your CA Enterprise Log Manager environment to implement subscription updates.

An overview of the subscription configuration process follows. For details on each step, see the related procedures.

1. Using your subscription architecture as a guide, configure each server as a subscription proxy or client. If needed, specify one or more proxies as offline proxies. You specify each server as a proxy or client at the local level.
2. Configure proxy lists for both client updates and content updates. You can specify a proxy list for client updates globally for your whole environment, or set local proxy lists for individual servers. For content updates, you can only specify a proxy list at the global level.
3. Select modules to download. You can select modules globally, or locally for individual servers.
4. Set your subscription schedule. You can schedule globally, or locally for individual servers.

More information:

[Configure an Online Subscription Proxy](#) (see page 163)

[Configure an Offline Subscription Proxy](#) (see page 165)

[Configure a Subscription Client](#) (see page 166)

[Configure Proxy Lists](#) (see page 167)

[Select Modules for Online Subscription](#) (see page 169)

[Download & Select Modules for Offline Subscription](#) (see page 171)

[Set a Subscription Schedule](#) (see page 173)

Configure an Online Subscription Proxy

An online subscription proxy contacts the CA Technologies Subscription Server to download the latest CA Enterprise Log Manager updates, and distributes them to subscription clients in turn.

The *default online subscription proxy* downloads updates to subscription clients if no other proxy is configured or available. The first CA Enterprise Log Manager server you install is configured upon installation as the default subscription proxy. However, you can specify any online proxy as the default subscription proxy. You can configure the default subscription proxy only at the global level.

To configure an online subscription proxy

1. Click the Administration tab and the Services subtab.
2. Click Subscription Service.

The Global Service Configuration: Subscription Service window appears.

Note: To specify a default subscription proxy different from the one configured upon installation, click Administration and enter the server name in the Default Subscription Proxy field.

3. In the Service List, expand Subscription Service, and select the server to configure.
The Subscription Service Configuration for the selected CA Enterprise Log Manager server appears.
4. Click the Administration tab.
5. Select the Subscription Proxy checkbox, and select Online Subscription Proxy.
6. Confirm that the RSS feed URL for subscription updates is correct. If you want this proxy to use an RSS feed different from the global setting, switch to local configuration and enter the correct RSS URL.
7. If this server is to contact the CA Technologies Subscription Server through an HTTP proxy server different from the inherited one, switch to local configuration and configure the desired HTTP proxy.
8. Click Save.

More information:

[How to Configure Subscription](#) (see page 163)

Configure an Offline Subscription Proxy

An offline subscription proxy provides CA Enterprise Log Manager updates to its clients without connecting to the Internet. This configuration allows you to isolate some or all of your CA Enterprise Log Manager servers from the Internet.

Before performing an offline subscription update, manually copy offline update files from a CA Technologies FTP site to any offline proxies, using physical media, or via scp, which is included with CA Enterprise Log Manager. Copy the update files to the following path: `/opt/CA/LogManager/data/subscription/offline`.

By design, subscription clients of offline proxy servers automatically receive all updates that are manually installed on the offline proxy, regardless of any modules selected for a client at the local level. Therefore, in a mixed subscription environment where you have configured both online and offline proxies, do not include offline proxies in the proxy list for any online subscription client. If you do, the online subscription client automatically receives all updates that are manually installed on the offline proxy server, instead of the modules you selected for that client.

To configure an offline subscription proxy

1. Click the Administration tab and the Services subtab.
2. Expand Subscription Service and select the server to configure.

The Subscription Service Configuration for the selected CA Enterprise Log Manager server appears.

3. Click the Administration tab.
4. Select the Subscription Proxy checkbox, and select Offline Subscription Proxy.
5. Select the .zip file containing the offline subscription files you want to install from the File drop-down list.

Note: This procedure presumes that you have already copied the offline subscription package to the correct location on this server. If you have not yet done so, a prompt appears.

6. Click Save.

More information:

[How to Configure Subscription](#) (see page 163)

Configure a Subscription Client

Subscription clients download the latest CA Enterprise Log Manager updates from subscription proxies. After a client retrieves updates, it installs the downloaded components.

All CA Enterprise Log Manager servers that are not configured as subscription proxies are subscription clients, by default. You do not need to configure a server locally as a client, unless you want to override subscription settings that you have set globally.

A subscription client cannot retrieve updates from a subscription proxy until that proxy has fully downloaded and installed the updates itself. A client attempts to retrieve updates from each server in its configured proxy list in turn. If no proxy has completed installation of the updates the client requests, the client retries the request every 5 minutes until the update is successful. If the client cannot download the updates after one hour of retries, the update is canceled, and the client reattempts update at the next scheduled time. Messages appear in the Self Monitoring Events log throughout this process, alerting you to the status of the update.

To configure a subscription client

1. Click the Administration tab and the Services subtab.
2. Expand Subscription Service and select the server to configure.
The Subscription Service Configuration for the selected CA Enterprise Log Manager server appears.
3. Identify the selected server as a client by leaving Subscription Proxy check box unselected.
4. Because subscription clients contact subscription proxies through the internal network, there is no need to configure local HTTP Proxy settings for an individual client server.
5. Click Save.

More information:

[How to Configure Subscription](#) (see page 163)

Configure Proxy Lists

If you configure multiple subscription proxies for your environment, you can configure proxy lists for client updates. If a given proxy is unavailable when a client requests updates, the client contacts each proxy on its proxy list in turn until it succeeds in downloading the updates. You can configure a proxy list for client updates globally for your entire CA Enterprise Log Manager environment, or locally for individual subscription clients.

With multiple subscription proxies, you can also configure a proxy list for content updates. These are servers that receive content updates, such as queries, reports and correlation rules, and distribute them to the Management Server where they are stored for use by CA Enterprise Log Manager. You can configure a proxy list for content updates only at the global level.

Proxy lists help ensure that subscription updates are successfully retrieved and distributed in a timely manner. Even in a small CA Enterprise Log Manager environment, it is good practice to configure at least one backup proxy for both client and content updates, in case the primary proxy is unavailable.

To configure a proxy list

1. Click the Administration tab and the Services subtab.
2. Click Subscription Service.

The Global Service Configuration for the Subscription Service appears.

3. Do one of the following:
 - To specify a global proxy list for your entire CA Enterprise Log Manager environment, click the Administration tab.

or

- To specify a local proxy list for a specific subscription client, click the server name, click the Administration tab, and switch to local configuration.
4. Add the desired proxy servers to the proxy lists.

Important! In a mixed subscription environment, where you have configured both online and offline subscription proxies, do not include offline proxies in the proxy list for any online subscription client. If you do, the online subscription client automatically receives all updates that are manually installed on the offline proxy server, instead of the modules you selected.

5. Click Save.

More information:

[How to Configure Subscription](#) (see page 163)

About Modules to Download

Updates are packaged into *modules*, which are downloaded through the CA Technologies Subscription Server. You access the list of available modules through an RSS feed URL provided by CA Technologies, or in the case of offline subscription, through a CA Technologies FTP site. CA Technologies determines what each module contains.

The following table describes each module, its function, and how frequently CA makes an update available:

Module Type	Description	Frequency
Content	Updates the Query List, Report List, and Correlation Rules with new content. The proxy for content updates automatically pushes this content to the management server repository.	Monthly
Integrations	Updates connectors when you run the Subscription Wizard and select Connector Updates.	Monthly
Operating System	Updates the operating system installed on each CA Enterprise Log Manager server.	Periodically
Agents	Updates agents when you run the Subscription Wizard and select Agent Updates.	Periodically
Log Manager Service Pack	Updates the CA Enterprise Log Manager product on each server with the indicated Service Pack.	Quarterly
Log Manager Version	Upgrades the CA Enterprise Log Manager product on each system to the indicated version.	Periodically

You can select the list of modules to download for your CA Enterprise Log Manager environment at a global level. Individual subscription proxy and client servers inherit these global settings. You can also override the global settings by configuring a local list of modules to download for an individual CA Enterprise Log Manager server.

Note: A subscription proxy cannot distribute a module to a client that the proxy has not, itself, installed. When selecting modules for a subscription proxy, include at minimum all modules selected for the proxy's clients.

You can perform updates to your CA Enterprise Log Manager environment using one, or both, of the following methods:

1. Automatically: You select modules in advance, and specify a schedule for download. The Subscription Service automatically downloads and installs the modules you select, according to the schedule you specify.
2. Manually: You select modules when needed, using the Update Now feature of the Subscription Service to download and install these modules at a time you choose.

Because Content, Integration, Operating System and Agent modules are updated regularly, consider setting your subscription schedule to download these modules automatically at least once per month. Log Manager Service Pack and Version updates are less frequent, and can require additional consideration and planning before you apply them to your CA Enterprise Log Manager environment. Consider downloading these types of updates manually, as needed.

As new modules become available, they appear in the Subscription RSS feed, or in the case of offline subscription, on the CA Technologies offline subscription FTP site. Because modules available for download vary with the update cycle, it is good practice to monitor the available list to be sure that all modules you need are selected. You can also check the CA Support Site at <http://ca.com/support> to learn when new Log Manager service packs and versions are available.

More information:

[Select Modules for Online Subscription](#) (see page 169)

[Download & Select Modules for Offline Subscription](#) (see page 171)

[How to Plan Subscription Updates](#) (see page 46)

[How to Configure Subscription](#) (see page 163)

Select Modules for Online Subscription

The CA Enterprise Log Manager subscription updates currently available are listed in the RSS feed provided by CA Technologies. The RSS feed URL is provided by default in the Subscription Service Administration tab upon installation.

As new modules become available, they appear in the Subscription RSS feed. Periodically monitor the list of available modules to be sure that all modules you need are selected. You can also check the CA Support Site at <http://ca.com/support> to learn when new Log Manager service packs and versions are available.

To select modules to download

1. Click the Administration tab and the Services subtab.
2. Click Subscription Service.

The Global Service Configuration for the Subscription Service appears.

3. Do one of the following:

- To select modules to download globally for your entire CA Enterprise Log Manager environment, click the Administration tab.

or

- To select modules to download locally for a specific server, click the server name, click the Administration tab and switch to local configuration in Modules Selected for Download.

4. Confirm that the correct RSS address appears in the RSS feed URL field, or to configure a custom RSS address for a specific server, switch to local configuration and enter the RSS URL.

5. Click Browse.

The Modules Available for Download dialog appears.

6. Select the modules you want to download.

Note: To receive new updates from CA as soon as they are available, select modules that are updated Monthly and Periodically, and set your subscription schedule to update automatically at least once per month. Service Pack and Version updates are less frequent, and can require additional consideration and planning before you apply them to your CA Enterprise Log Manager environment. Consider downloading these types of updates manually, as needed.

Note: Clients cannot download modules that their proxy has not also downloaded. Be sure that the modules selected for a subscription proxy include at minimum all modules selected in the download lists of that proxy's clients.

7. Click OK.

The Modules Available for Download dialog closes, and the modules you selected appear in the Modules Selected for Download list.

8. Click Save.

More information:

[How to Configure Subscription](#) (see page 163)

[About Modules to Download](#) (see page 168)

Download & Select Modules for Offline Subscription

Offline subscription update files are available at the CA Technologies offline subscription FTP site, packaged in .zip files. As new modules become available, they appear on the FTP site. Periodically monitor the list of available modules to be sure that you have downloaded the most recent updates. You can also check the CA Support Site at <http://ca.com/support> to learn when new Log Manager service packs and versions are available.

Before you can select modules to download for offline subscription proxies, download the offline update file package from the CA Technologies FTP site and manually copy it to your offline proxies. You can then select which modules to download and install. Offline subscription clients, by contrast, automatically receive all updates that are manually installed on their offline proxy, regardless of any modules selected for the client at the local level.

To download and select offline subscription modules

1. On a system with Internet or FTP access, navigate to the FTP offline subscription site:

`ftp://ftp.ca.com/pub/elm/connectors/ftp/outgoing/pub/elm/ELM_Offline_Subscription`

The directory index displays a folder for each major CA Enterprise Log Manager release.

2. Download the appropriate .zip file for the update you want to perform.

Note: The folder for the CA Enterprise Log Manager r12.5 release contains a subfolder as well as a .zip file. The subfolder contains modules for upgrading from any previous version to version r12.5. The .zip file contains the modules for performing routine, periodic updates to version r12.5. If you are using offline subscription to upgrade from a previous version to r12.5, see the Upgrading to CA Enterprise Log Manager topic in the *Release Notes*. If you are performing a routine update, select the .zip file.

3. Using physical media such as a disk, or using scp, manually copy the .zip file to the following file path on your offline proxies:

`/opt/CA/LogManager/data/subscription/offline.`

4. Log in to a system in your CA Enterprise Log Manager environment.

5. Click the Administration tab and the Services subtab.
6. Expand Subscription Service and select an offline proxy server to configure.

The Subscription Service Configuration for the selected CA Enterprise Log Manager server appears.

Note: Offline subscription clients automatically receive all modules that are manually installed on their offline proxy. The contents of the proxy server control which updates the subscription client receives. Modules selected at the local level for an offline client have no effect.

7. Click the Administration tab.
8. In the File drop-down, select the offline update .zip file you copied to the server, and click Browse.

The Modules Available for Download dialog appears.

9. Select the modules you want to download.
10. Click OK.

The Modules Available for Download dialog closes, and the modules you selected appear in the Modules Selected for Download list.

11. Click Save.

Offline subscription clients can now download these modules automatically according to the subscription schedule you set, or on demand when you begin a manual update.

12. (Optional) Click Update Now.

The offline proxy server updates itself with the selected modules.

Note: Though you can allow the offline proxy to update itself according to the subscription schedule you set, it is good practice to perform a manual update whenever you transfer new files. This practice ensures that the updates are available when offline subscription clients request them.

More information

[How to Configure Subscription](#) (see page 163)

[About Modules to Download](#) (see page 168)

Set a Subscription Schedule

You set a subscription schedule to define when, and how frequently, the Subscription Service performs automatic updates. You can set a subscription schedule globally, for your entire CA Enterprise Log Manager environment, or you can set a custom schedule for individual subscription proxies and clients.

To configure a subscription schedule

1. Click the Administration tab and the Services subtab.
2. Click Subscription Service.

The Global Service Configuration for the Subscription Service appears.

3. Do one of the following:
 - To specify a global subscription schedule for your entire CA Enterprise Log Manager environment, click the Administration tab.or
 - To specify a local subscription schedule for a specific server, click the server name, click the Administration tab, and switch to local configuration.
4. Set the subscription schedule. Select your time zone and a start time for updates, then specify the update frequency you want.

More information

[How to Configure Subscription](#) (see page 163)

Chapter 6: Configuring Event Collection

This section contains the following topics:

[Installing Agents](#) (see page 175)

[Using the Agent Explorer](#) (see page 176)

[Configuring the Default Agent](#) (see page 177)

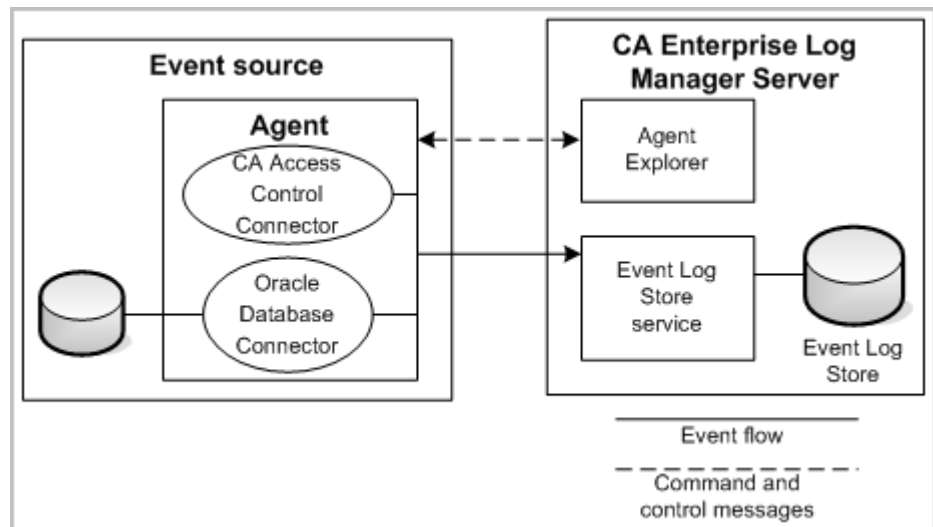
[Example: Enable Direct Collection Using the ODBCLogSensor](#) (see page 179)

[Example: Enable Direct Collection Using the WinRMLinuxLogSensor](#) (see page 184)

[View and Control Agent or Connector Status](#) (see page 188)

Installing Agents

With separate installations for specific platforms, CA Enterprise Log Manager agents provide the transport layer for getting events from event sources to the CA Enterprise Log Manager server's event log store. Agents use connectors to collect event logs from different event sources. The following diagram shows the interactions between agents and the CA Enterprise Log Manager server:



After you install an agent on an event source, you can configure one or more connectors to collect events from event sources such as devices, applications, operating systems, and databases. The examples in the diagram include connectors for CA Access Control and an Oracle database. You typically will install only one agent per host server or event source, but you can configure more than one type of connector on that agent. You can use the Agent Explorer that is part of the CA Enterprise Log Manager server to control agents and to configure and to control connectors on an agent. The Agent Explorer also allows you to create agent groups for easier management and control.

You base your configuration of a connector on either an integration or a listener, which are templates that can comprise files for data access, message parsing, and data mapping. CA Enterprise Log Manager provides a number of integrations for popular event sources out-of-the-box.

You can find more information and procedures for installing agents in the *CA Enterprise Log Manager Agent Installation Guide*.

More Information:

[View and Control Agent or Connector Status](#) (see page 188)

Using the Agent Explorer

Immediately after you install a CA Enterprise Log Manager server, you have a default agent listed in the Agent Explorer. That agent is installed when you install the CA Enterprise Log Manager server, and you use it for direct syslog event collection.

The Agent Explorer tracks and lists agents as you install them in your network, and provides a centralized place for configuration, command, and control of agents and connectors. Agents register with the CA Enterprise Log Manager server you specify the first-time you start them. When that registration takes place, the agent name appears in the Agent Explorer and you are ready to configure a connector to begin event log collection. Connectors gather event logs and send them to the CA Enterprise Log Manager server. One agent can control many connectors.

Using the Agent Explorer to install, configure, and control connectors and agents involves the following basic steps:

1. Download the agent binaries.
2. Create one or more agent groups (optional).
3. Create and configure a connector, including creating or applying suppression and summarization rules.
4. View agent or connector status.

See the *CA Enterprise Log Manager Administration Guide* for more information about creating and working with agent groups, connectors, and how to apply suppression rules on agents.

More information:

[About Agents](#) (see page 55)

[About Agent Groups](#) (see page 56)

[About Log Sensors](#) (see page 57)

[Suppression Rule Effects](#) (see page 59)

Configuring the Default Agent

The CA Enterprise Log Manager installation creates a default agent on the CA Enterprise Log Manager server that has two connectors ready for use, a `syslog_Connector` and a `Linux_local Connector`. The `syslog connector` is available for collection of `syslog` events sent to the CA Enterprise Log Manager server. The `Linux_local connector` is available for collection of OS-level events from the CA Enterprise Log Manager physical server, or from a `syslog` file.

In the basic two-server environment, configure one or more `syslog` connectors on the collection server to receive events.

The process for using the default agent includes the following steps:

1. (optional) Review the `syslog` integrations and listeners.
2. Create a `syslog` connector.
3. Verify that the CA Enterprise Log Manager server is receiving `syslog` events.

Review syslog Integrations and Listeners

You can review the default `syslog` integrations and listeners before you create a connector. Listeners are essentially a template for your `syslog` connectors that use specific `syslog` integrations provided as out-of-the-box content with your CA Enterprise Log Manager server.

To review syslog integrations

1. Log into CA Enterprise Log Manager and access the Administration tab.
2. Click the Library subtab and expand the Event Refinement Library node.
3. Expand both the Integrations node and the Subscription node.
4. Select an integration whose name ends with `..._Syslog`.

The integration details display in the right side window. You can review which message parsing and data mapping file the integration uses and other details such as version and lists of suppression rules and summarization rules.

To review a syslog listener

1. Expand both the Listeners node and the Subscription node.
2. Select the `Syslog` listener.

The default listener details display in the right side window. You can review details such as versions, suppression and summarization rules, the default ports on which to listen, a list of trusted hosts, and the listener's time zone.

Create a syslog Connector for the Default Agent

Create a syslog connector to receive syslog events using the default agent on the CA Enterprise Log Manager server.

To create a syslog connector for the default agent

1. Log into CA Enterprise Log Manager and access the Administration tab.
2. Expand the Agent Explorer and an agent group.

The default agent is automatically installed into the Default Agent Group. You can move this agent to another group.
3. Select the agent name.

The default agent has the same name you gave the CA Enterprise Log Manager server during installation.
4. Click Create New Connector to open the connector wizard.
5. Click the Listeners option and provide a name for this connector.
6. Apply suppression rules, and suppression rules as needed in the second and third pages of the wizard.
7. Select one or more targeted syslog integrations from the Available list to use with this connector, and move them to the Selected list.
8. Set UDP and TCP port values, if you are not using the defaults, and provide a list of trusted hosts if your implementation uses them.

Note: When a CA Enterprise Log Manager agent does not run as root, it cannot open a port below 1024. The default syslog connector therefore uses UDP port 40514. The installation applies a firewall rule to the CA Enterprise Log Manager server to redirect traffic from port 514 through 40514.
9. Select a time zone.
10. Click Save and Close to finish the connector.

The connector begins collecting syslog events that match the selected integrations on the ports you specified.

Verify that CA Enterprise Log Manager Is Receiving syslog Events

You can verify that the connector on the default agent is collecting syslog events with the following procedure.

To verify syslog event receipt

1. Log into CA Enterprise Log Manager and access the Queries and Reports tab.

2. Select the System query tag and open the System All Events Detail query.

You should see events listed for the default agent, if the you configured the connector correctly and the event source is actively sending events.

Example: Enable Direct Collection Using the ODBCLogSensor

You can enable direct collection of events generated by specific databases and CA products with the ODBCLogSensor. To do this, you create a connector on the default agent that is based on an integration that uses the ODBCLogSensor. Many integrations use this sensor, for example, CA_Federation_Manager, CAIdentityManager, Oracle10g, Oracle9i, and MS_SQL_Server_2005.

Following is a partial list of products that generate events that can be collected directly by the default agent on a CA Enterprise Log Manager server. For each product, a unique connector is used; each connector uses the ODBCLogSensor.

- CA Federation Manager
- CA SiteMinder
- CA Identity Manager
- Oracle 9i and 10g
- Microsoft SQL Server 2005

For a complete list, see the [Product Integration Matrix](#) on Support Online.

This example shows how to enable direct collection of events from a Microsoft SQL Server database. The connector deployed on the default agent is based on the MS_SQL_Server_2005 integration. In this example, the SQL Server database resides on an ODBC server. The connector deployed to the CA Enterprise Log Manager agent collects events from the MSSQL_TRACE table. Part of enabling the collection of events from a Microsoft SQL Server database is to direct selected events to this trace table. You can find explicit directions for doing this in the *CA Connector Guide for Microsoft SQL Server*.

To learn how to configure the Microsoft SQL Server event source

1. Select the Administration tab and the Library subtab.
2. Expand Event Refinement Library, expand Integrations, expand Subscription, and select MS_SQL_Server_2005.

The View Integration Details displays the sensor name, ODBCLogSensor. Supported platforms include both Windows and Linux.

3. Click the Help link on View Integration Details.

The Connector Guide for Microsoft SQL Server appears.

4. Review the Prerequisites and Microsoft SQL Server Configuration sections for guidelines.

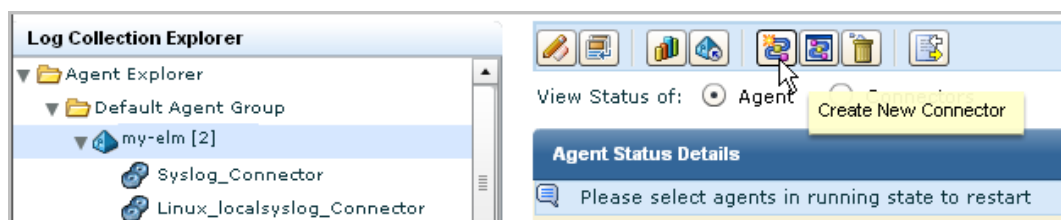
To configure the event source and verify logging

1. Gather the following details: the IP address of the ODBC server, the database name, the Administrator user name and password required to log on to the server, and the credentials of the low-privileged user used for SQL Server authentication. (This is the user defined to have read-only access to the trace table.)
2. Log on to the ODBC server with the Administrator user name and password.
3. Ensure connectivity over TCP/IP as specified in the *Connector Guide for Microsoft SQL Server*.
4. Configure the SQL Server and verify that events are being directed to the trace table as specified in the *Connector Guide for Microsoft SQL Server*.

Note: Keep a record of the name of the database under which you create the trace table. You must specify that database name in the connection string. For example: master.

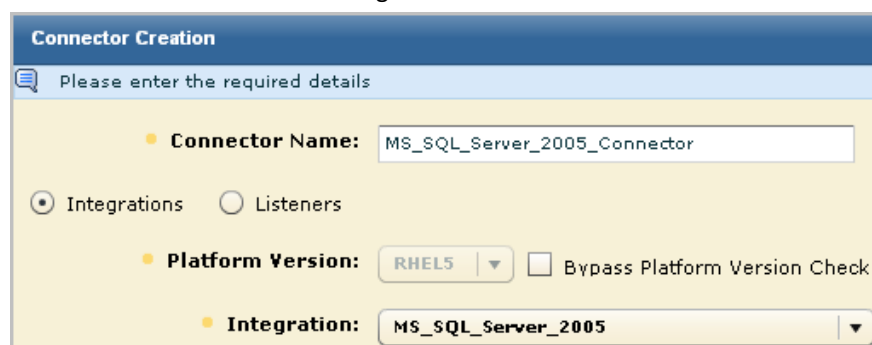
To create a connector on the default agent to retrieve events generated by a SQL Server database on an ODBC Server

1. Select the Administration tab and the Log Collection subtab.
2. Expand Agent Explorer, and expand the agent group containing the CA Enterprise Log Manager default agent
3. Select a default agent, that is, an agent with the name of a CA Enterprise Log Manager server.
The default agent can have other connectors deployed to it.
4. Click Create New Connector.



The New Connector Creation wizard opens with the Connector Details step selected.

5. Select the MS_SQL_Server_2005 integration from the Integration drop-down list.
This selection populates the Connector Name field with MS_SQL_Server_2005_Connector.
6. (Optional) Replace the default name with one that makes the connector easy for you to identify. Consider providing a unique name if you are monitoring several SQL Server databases with this same agent.



7. (Optional) Click the Apply Suppression Rules step and select rules associated with the supported events.
For example, select MSSQL_2005_Authorization 12.0.44.12.
8. Click the Connector Configuration step and click the Help link.
Instructions include CA Enterprise Log Manager Sensor Configuration Requirements for both Windows and Linux.

9. Review the steps for Linux, the platform of the default agent, and configure the Connection String and other fields as specified.
 - a. Enter the connection string as specified under Sensor Configuration--Linux, where the address is the host name or IP address of the event source and the database is the SQL Server database under which MSSQLSERVER_TRACE is created.

DSN=SQLServer Wire Protocol;Address=IPaddress,port;Database=databasename
 - b. Enter the name of the user with read-only event collection access rights. This user must be assigned the db_datareader and public roles to have read-only access.
 - c. Enter the password for the specified Username.
 - d. Specify the timezone of the database as an offset of GMT.

Note: On a Window server, this information appears on the Time Zone tab of Date and Time Properties. Open the clock on the system tray.
 - e. Select or clear Read from Beginning depending on whether you want the log sensor to read events from the beginning of the database.

A partial example follows:

The screenshot shows a 'Sensor Configuration' dialog box with the following fields and values:

- Connection String:** DSN=SQLServer Wire Protocol;Address=172.24.36.107,1433;Database=master
- Username:** ELMsqlagent
- Password:** *****
- TZ Offset Sign:** -
- TZ Offset Hours:** 5
- TZ Offset Minutes:** 0
- Event Log Name:** MS_SQL_Server
- UpdateAnchorRate:** 10
- PollInterval:** 10
- MaxEventsPerSecond:** 1000
- ☒ Read from Beginning

10. Click Save and Close.

The new connector name displays under the agent in the Agent Explorer.



11. Click the MS_SQL_Server_2005_Connector to view status details.

Initially, the status shows Configuration pending. Wait until that status shows Running.

Connector	Agent ▼	Agent Group	Platform	Integration	
MS_SQL_Server_2005_Connector_SQL2005	my-elm	Default Agent Group	Linux_X86_32	MS_SQL_Server_2005	Running

12. Select the connector and click Running to see event collection details.

Note: You can also run a report to view data from this database.

To verify that the default agent is collecting events from the target event source

1. Select the Queries and Reports tab. The Queries subtab is displayed.
2. Expand Prompts in the Query List and select Connector.
3. Enter the connector name and click Go.

Collected events are displayed. The first two are internal events. Those that follow are events collected from the MS SQL trace table you configured.

Note: If the expected events are not displayed, click Global Filters and Settings in the main toolbar, set the Time Range to No Limit, and save the setting.

4. (Optional) Select Show raw events and examine the result string for the first two event. The result string appears last in the raw event. The following values indicate a successful start.
 - result_string=ODBCSource initiated successfully - MSSQL_TRACE
 - result_string=<connector name> Connector Started Successfully

Example: Enable Direct Collection Using the WinRMLinuxLogSensor

You can enable direct collection of events generated by Windows applications or the Windows Server 2008 operating system with the WinRMLinuxLogSensor. To do this, you create a connector on the default agent that is based on an integration that uses the WinRMLinuxLogSensor. Many integrations use this sensor, for example, Active_Directory_Certificate_Services, Forefront_Security_for_Exchange_Server, Hyper-V, MS_OCS, and WinRM. The Microsoft Windows application and operating system that generate events that can be retrieved by the WinRMLinuxLogSensor are those for which Windows Remote Management is enabled.

Following is a partial list of products that generate events that can be collected directly by the default agent on a CA Enterprise Log Manager server. For each product, a unique connector is used; each connector uses the WinRMLinuxLogSensor.

- Microsoft Active Directory Certificate Services
- Microsoft Forefront Security for Exchange Server
- Microsoft Forefront Security for SharePoint Server
- Microsoft Hyper-V Server 2008
- Microsoft Office Communication Server
- Microsoft Windows Server 2008

For a complete list, see the [Product Integration Matrix](#) on Support Online.

This example shows how to enable direct collection of events using a connector based on the WinRM integration. When such a connector is deployed, it collects events from a Windows Server 2008 operating system event source. Collection begins after you configure the event sources to log events in the Windows Event Viewer and enable Windows Remote Management on the server as specified in the Connector Guide associated with this integration.

To learn how to configure the Windows Server 2008 event source

1. Select the Administration tab and the Library subtab.
2. Expand Event Refinement Library, expand Integrations, expand Subscription, and select WinRM.

The View Integrations Details displays the sensor name, WinRMLinuxLogSensor. Supported platforms include both Windows and Linux.

3. Click the Help link on the WinRM View Integration Details.

The Connector Guide for Microsoft Windows Server 2008--WinRM appears.

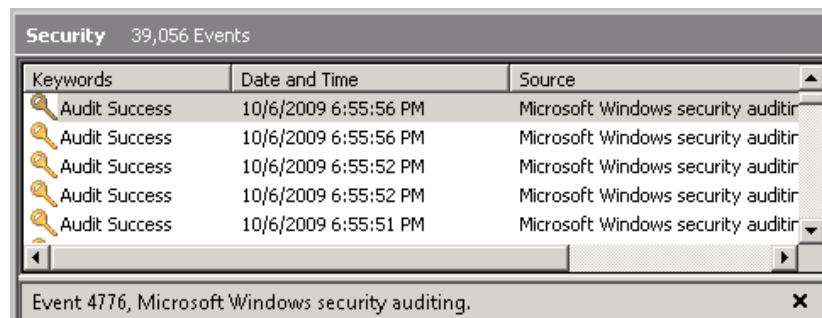
To configure the event source and verify logging

1. Log on to the target host with a Windows Server 2008 operating system.
2. Follow the directions in the *CA Connector Guide for Microsoft Windows Server 2008* to ensure events are displayed in the Windows Event Viewer and to ensure Windows Remote Management is enabled on the target server.

Note: Part of this process is creating the user name and password that you must enter when you configure the connector. These credentials enable authentication required to establish connectivity between the event source and CA Enterprise Log Manager.

3. Verify logging.
 - a. Open eventvwr from the Run dialog.
The Event Viewer appears.
 - b. Expand Windows Logs and click Security.

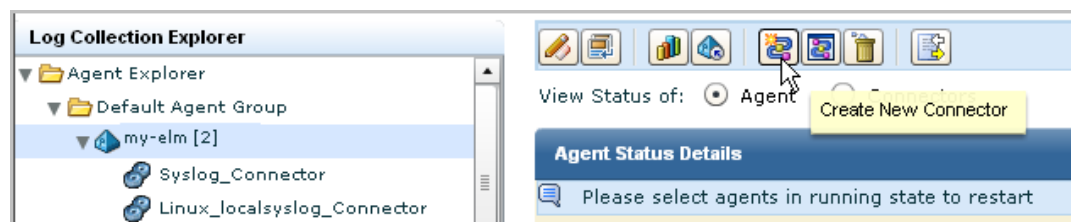
A display similar to the following indicates that logging is occurring.

**To enable direct collection of events from Windows event sources**

1. Select the Administration tab and the Log Collection subtab.
2. On the Log Collection Explorer, expand Agent Explorer, and expand the agent group containing the CA Enterprise Log Manager default agent.
3. Select a default agent, that is, an agent with the name of a CA Enterprise Log Manager server.

The default agent may have other connectors deployed to it.

4. Click Create New Connector



The New Connector Creation wizard opens with the Connector Details step selected.

5. Select an integration that uses the WinRM log sensor from the Integration drop-down list.

For example, choose WinRM.



The screenshot shows a 'Connector Creation' wizard window. At the top, it says 'Please enter the required details'. Below this, there are three main sections: 'Connector Name' with a text input field containing 'WinRM_Connector', 'Integrations' with a radio button selected (and 'Listeners' unselected), and 'Platform Version' with a dropdown menu showing 'RHEL5'. To the right of the platform version is a checkbox labeled 'Bypass Platform Version Check'. At the bottom, there is an 'Integration' dropdown menu showing 'WinRM'.

This selection populates the Connector Name field with WinRM_Connector

6. (Optional) Click Apply Suppression Rules and select rules associated with the supported events.
7. Click the Connector Configuration step and click the Help link.

Instructions include CA Enterprise Log Manager Sensor Configuration--WinRM.

[5.0 CA Enterprise Log Manager Sensor Configuration--WinRM](#)
[5.1 Fixed Parameter](#)

8. Follow the instructions in this Connector Guide to configure the sensor. Enter the IP address, rather than the hostname, of the host on which you configured Windows Remote Management. The Username and Password entries reflect credentials you added during configuration of Windows Remote Management.

An example follows:

Connector Configuration

Please enter the configuration details

Saved Configurations: Select Configuration ▼

Sensor Configuration

- Computer Name: 172.24.36.107
- Port: 80
- Username: ELMagent
- Password: *****
- Event Log Name: NT-Security
- PollInterval: 10
- UpdateAnchorRate: 10
- ☒ Read from Beginning
- SourceName: Security
- Channel (Log) Name: Security

9. Click Save and Close.
10. The new connector name displays under the agent in the Agent Explorer.



11. Click WinRM_Connector to view the status details.

Initially, the status shows Configuration pending. Wait until that status shows Running.

Status Details					
Restart	Start	Stop			
Connector	Agent	Agent Group	Platform	Integration	Status
WinRM_Connector	my-elm	Default Agent Group	Linux_X86_32	WinRM	Running

12. Click Running to get summary data such as the EPS (events per second).

Status:	Percentage CPU: 3.4 Memory Usage in MB: 12 Average EPS: 1519.95 Filtered Event Count: 0
----------------	--

To verify that the default agent is collecting events from the target event source

1. Select the Queries and Reports tab. The Queries subtab is displayed.
2. Expand Prompts in the Query List and select Connector.
3. Enter the connector name and click Go.
4. View the collected events.

View and Control Agent or Connector Status

You can monitor the status of agents or connectors in your environment, restart agents, and start, stop, and restart connectors as needed.

You can view agents or connectors from different levels of the Agent Explorer folder hierarchy. Each level narrows the available view accordingly:

- From the Agent Explorer folder, you can view all agents or connectors assigned to the current CA Enterprise Log Manager server.
- From a specific agent group folder, you can view agents and connectors assigned to that agent group.
- From an individual agent, you can view only that agent and any connectors assigned to it.

You can determine the FIPS mode (FIPS or non-FIPS) for an agent from all three levels.


To view agent or connector status

1. Click the Administration tab, and then the Log Collection subtab.

The Log Collection folder list appears.

2. Select the Agent Explorer folder.

Agent management buttons appear in the details pane.

3. Click Status and Command: 

The status panel appears.

4. Select Agents or Connectors.

The agent or connector search panel appears.

5. (Optional) Select agent or connector update search criteria. If you enter no search terms, all available updates appear. You can select any one or more of the following criteria to narrow your search:
 - Agent Group—returns only agents and connectors assigned to the selected group.
 - Platform—returns only agents and connectors running on the selected operating system.
 - Agent name pattern—returns only agents and connectors containing the specified pattern.
 - (Connectors only) Integration—returns only connectors using the selected integration.
6. Click Show Status.

A details chart appears, displaying status for agents or connectors that match your search. For example:

Total: 10 Running: 8 Pending: 1 Stopped: 1 Not Responding: 0
7. (Optional) Click the status display to view details in the Status pane at the bottom of the chart.

Note: You can click the On Demand button for an agent or connector to refresh the status display.
8. (Optional) If you are viewing connectors, select any connector and click Restart, Start, or Stop. If you are viewing agents, select any agent and click Restart.

Chapter 7: Creating Federations

This section contains the following topics:

[Queries and Reports in a Federated Environment](#) (see page 191)

[Hierarchical Federations](#) (see page 192)

[Meshed Federations](#) (see page 193)

[Configuring a CA Enterprise Log Manager Federation](#) (see page 195)

Queries and Reports in a Federated Environment

A single CA Enterprise Log Manager server returns data from its internal event database to respond to queries and populate reports. If you have a federation of CA Enterprise Log Manager servers, you can control how queries and reports return event information in the way you configure your federation relationships. You can also maintain query results from single servers by disabling the Use Federated Queries global setting.

By default the global setting, Use Federated Queries, is enabled. This causes queries from a parent CA Enterprise Log Manager server to be sent to all child CA Enterprise Log Manager servers. Each child CA Enterprise Log Manager server queries the active event log store and the archive catalog as well as querying all of its child CA Enterprise Log Manager servers. Each child CA Enterprise Log Manager server then creates a single results set to send to the requesting parent CA Enterprise Log Manager server. Protection against circular queries is built into CA Enterprise Log Manager to enable meshed configurations.

A typical enterprise CA Enterprise Log Manager implementation has from one to five servers. A large enterprise implementation may have ten or more servers. The way you configure your federation controls how much information is visible to the CA Enterprise Log Manager server that issues the query. The simplest query type comes from the primary CA Enterprise Log Manager server and returns information from all of the child servers configured under it.

When you query the federation from a child server, the results you see depend on how you have your federation configured. In a *hierarchical* federation, all of the servers that are configured as children under one server return query results to it. In a *meshed* federation, all of the interconnected servers return data to the server that issues the query.

Hierarchical Federations

Hierarchical federations use a top-down, pyramid structure to spread event collection loads over a wide area. The structure is similar to an organization chart. There is no set number of levels that you have to create - you can create the levels that make the most sense for your business needs.

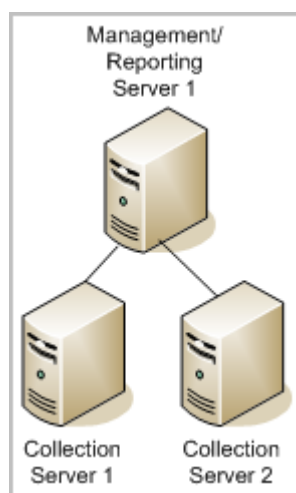
In a hierarchical federation, you can connect to any CA Enterprise Log Manager server to see reports on its event data and data from any of the child servers beneath it. The scope of the data that you can access is limited by where you start in the hierarchy. If you start in the middle of the hierarchy, you can see only that server's data, and any of its child server's data. The higher up you move in a hierarchical federation, the wider the scope of network data you have. At the top level, you have access to all of the data in the whole deployment.

Hierarchical federations are useful, for example, in regional deployments. Suppose that you want local resources to have access to event data within a certain hierarchy, or branch, of the network, but not the event data in other, parallel branches. You could create a hierarchical federation with two or more parallel branches to contain the data for each region. Each of the branches could report to a management CA Enterprise Log Manager server at the headquarters office for the top-down view of all event log reports.

Hierarchical Federation Example

In the federation map shown in the diagram that follows, the network uses the management CA Enterprise Log Manager server as a reporting server and multiple collection servers in a configuration that is similar to an organization chart. The management/reporting server acts as a parent CA Enterprise Log Manager server and provides user authentication, authorization, and major management functions as well as the reporting functions of handling queries, reports and alerts. The collection servers in this example would be children of Management/Reporting Server 1. You could arrange additional levels in the hierarchy. However, there can be no more than one management server. Additional levels would be composed of reporting servers as parents to collection servers.

As an example of this style of federation, Management/Reporting Server 1 might be located at your headquarters office, with collection servers located in regional or branch offices represented by Collection Servers 1 and 2. Each branch could get reporting information on its own data, but not the data from the other branch. For example, from Collection Server 1, you can query and report on data only on Collection Server 1. From Management/Reporting Server 1, however, you can query and report on data from the Management/Reporting Server 1, Collection Server 1 and Collection Server 2.



In a hierarchical federation, each CA Enterprise Log Manager server can have one or more children, but only one parent. You configure this type of federation in a top-down fashion, starting with the management server. Then you move through each downward layer to configure the child reporting and collection servers. The key to configuring a federation is in first making a map of the servers and the intended relationships. Then you can configure a CA Enterprise Log Manager server as a child server, to implement the relationships between them.

Meshed Federations

A *meshed federation* is similar to a hierarchical federation in that it may have tiers. The primary difference is in the configuration of the connections between the servers. A meshed federation can allow any CA Enterprise Log Manager server in the network to query, and report on, the data in all of the other CA Enterprise Log Manager servers. The capabilities for reporting depend on the relationships you create between the servers.

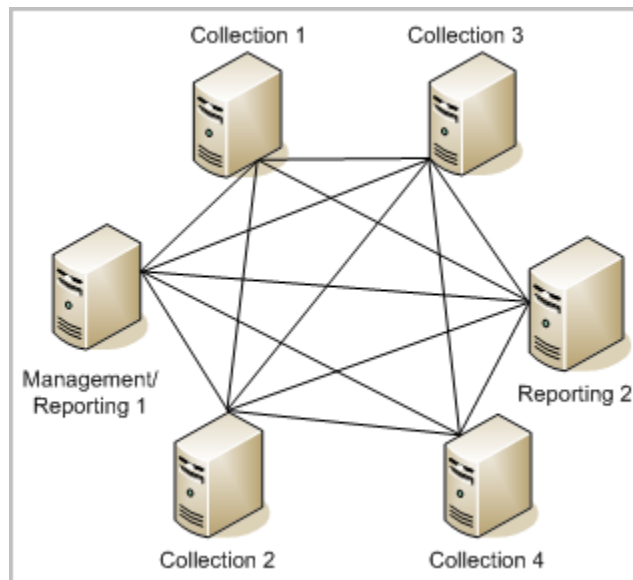
For example, in a meshed federation, the servers may interconnect only within a vertical branch. This means all CA Enterprise Log Manager servers in that branch would have access to all other CA Enterprise Log Manager servers in the same branch. This is in direct contrast to a CA Enterprise Log Manager server in a hierarchical federation, which can produce reports only on the servers beneath it in the hierarchy.

In a ring or star formation, every CA Enterprise Log Manager server is configured to be a child of all of the other servers. When you request report data from any one CA Enterprise Log Manager server, you see the data for all CA Enterprise Log Manager servers in the network.

The meshed federation allocates two or more CA Enterprise Log Manager servers as primary and uses servers in federation without respect to their placement in the network. The servers configured *as* children are also configured to view the children in the same or other branches as federated to them. For example, if you had two CA Enterprise Log Manager servers, A and B, you could create a meshed federation by making B a child of A, *and* A a child of B. This is the expected configuration when you are using two or more management servers.

Meshed Federation Example

Consider the following illustration of a fully meshed federation:



In the meshed federation shown in this diagram, four collection servers are federated to each other and to both reporting servers. Every server is both a parent and a child to every other server in the federation.

A potential benefit of this deployment over the strict hierarchical federation is that you can access the data from any point within the mesh, and get results from all other CA Enterprise Log Manager servers in that mesh, without regard to a hierarchy.

You can combine meshed and hierarchical federations to make any configuration that suits your needs. For example, a meshed configuration within a single branch could be very useful for global deployments. You could obtain a global overview of data from the parent reporting servers, while maintaining regional clusters (branches) that have access only to their own data.

Configuring a CA Enterprise Log Manager Federation

Each CA Enterprise Log Manager server that you add to a federation must reference the same application instance name on the management server. In this way, the management server can store and manage all of the configurations together, as global configurations.

You can configure the federation at any time, but it is useful to do so before you begin scheduling reports, if you want consolidated reports.

Configuring a federation involves the following activities:

1. Create a federation map.
2. Install the first CA Enterprise Log Manager, the management server.
3. Install one or more additional servers.
4. Configure the parent/child relationships. For example, begin by selecting federation children of the parent/child relationships. For example, begin by selecting federation children of the management server from this server's event log store settings.

This first group of child servers forms the second layer, or tier, of the federation if you are configuring a hierarchical federation.

5. View the Federation Graph to verify that the structure between the servers in the parent and child tiers is configured as you intended.

Configure a CA Enterprise Log Manager Server as a Child Server

Configuring one CA Enterprise Log Manager server as the child of another is the essential step in creating a federation. Use this procedure to add servers to your federation at any time. You must install all of the CA Enterprise Log Manager servers you want to federate under the same registered application instance name prior to performing this part of the configuration. As you install each new server, its name appears in the list of servers available for federation. You can perform this procedure as many times as is necessary to create the federated structure you want.

To configure a CA Enterprise Log Manager server as a child server

1. Log into any one of the CA Enterprise Log Manager servers that is registered under the same application instance name as the others in your intended federation.
2. Click the Administration tab and select the Services subtab.

3. Expand the Event Log Store service folder, and then select the server name for the parent CA Enterprise Log Manager server.
4. Scroll down to the Federation Children list.
5. Select one or more server names that you want to configure as children of the parent server from the servers in the Available list.
6. Use the arrow buttons to move your selections to the list of Selected servers.


The CA Enterprise Log Manager servers you selected and moved into the list are now federated children of the parent server.

More information:

[Select Use of Federated Queries](#) (see page 129)

View Federation Graph and Server Status Monitor

You can view a graph showing the CA Enterprise Log Manager servers in your environment, their federation relationships, and status information about individual servers. The federation graph lets you view the current federation structure, and view status details of each server. You can also select the local server that is queried within that session, setting it as the parent server.

To view the federation graph, click Show Federation Graph and Status Monitor at the top of the screen: 

A window appears showing a graphic display of all the event store hosts registered with the current management server:

- Event stores with federation children are displayed in light blue and with black connection lines showing the federation relationship.
- Event stores without federation children are displayed in light green.

You can select a current local server for query purposes.

You can also view status details for any of the displayed servers. Click a server in the federation graph to show status detail displays, including:

- CPU utilization percentage
- Available memory utilization percentage
- Available disk space utilization percentage
- Events per second received
- Event log store status master chart

More information:

[Example: Federation Map for a Mid-Sized Enterprise](#) (see page 34)

[Example: Federation Map for a Large Enterprise](#) (see page 32)

Chapter 8: Working with the Event Refinement Library

This section contains the following topics:

[About the Event Refinement Library](#) (see page 199)

[Supporting New Event Sources with the Event Refinement Library](#) (see page 199)

[Mapping and Parsing Files](#) (see page 200)

About the Event Refinement Library

The event refinement library provides you with tools to create new parsing and mapping files, or to modify copies of existing ones to provide support for new devices, applications, and so forth. The library includes the following options:

- Integrations
- Listeners
- Mapping and Parsing Files
- Suppression and Summarization Rules

Suppression rules prevent data from being collected, or prevent it from being inserted into the event log store. Summarization rules allow you to aggregate events to reduce the number of inserts for similar event types or actions. This is the most frequently used part of the library since suppression and summarization rules can help to tune both network and database performance.

You can use the integrations area to view predefined integrations and to create new integrations for your custom or proprietary devices, applications, files, or databases. More information is available in the *CA Enterprise Log Manager Administration Guide* and the online help.

Supporting New Event Sources with the Event Refinement Library

To support a device, application, database, or other event source that is not already supported, use the mapping and parsing file wizards and the integrations wizard to create the necessary components.

The process involves the following general steps:

1. Create parsing files to collect event data as name-value pairs.
2. Create mapping files to map the name-value pairs into the common event grammar.
3. Create new integrations and listeners to collect data from your event source.

Integrations, parsing and mapping files, and suppression and summarization rules are covered in depth in the *CA Enterprise Log Manager Administration Guide* and the online help.

Mapping and Parsing Files

During operation, CA Enterprise Log Manager reads incoming events and breaks them up into sections in an action called *parsing*. There are separate message parsing files for different devices, operating systems, applications, and databases. After the incoming events are parsed into name-value pairs, that data goes through a *mapping* module that places the event data into the fields in the database.

The mapping module uses data mapping files that are built for specific event sources similar to the message parsing files. The database schema is the common event grammar that is one of the central features of CA Enterprise Log Manager.

Parsing and mapping together are the means by which data is normalized and stored in a common database regardless of event type or message format.

The integration wizard and some of the CA Technologies Adapter modules require you to configure the mapping and parsing files that best describe the kinds of event data for which a connector or an adapter listens. In the configuration panels where these controls appear, the order of the message parsing files should reflect the relative number of events received of that type. The order of the data mapping files should also reflect the quantity of events received from a given source.

For example, if the syslog listener module for a specific CA Enterprise Log Manager server receives mostly Cisco PIX Firewall events, you should put the CiscoPIXFW.XMPS and CiscoPIXFW.DMS files first in each respective list.

Appendix A: Considerations for CA Audit Users

This section contains the following topics:

[Understanding Differences in Architectures](#) (see page 201)

[Configuring CA Technologies Adapters](#) (see page 207)

[Sending CA Audit Events to CA Enterprise Log Manager](#) (see page 211)

[When to Import Events](#) (see page 215)

[Importing Data from a SEOSDATA Table](#) (see page 216)

Understanding Differences in Architectures

In planning how you to use CA Audit and CA Enterprise Log Manager together, you first should understand the differences in the architectures and the effects they have on your network structure.

CA Enterprise Log Manager uses an embedded event log store, and provides an Agent Explorer to configure and manage agents. New technology coupled with a common event grammar allows for faster event throughput to storage while supporting a higher number of event sources. The common event grammar allows CA Enterprise Log Manager to normalize events from many different event sources into a single database schema.

CA Enterprise Log Manager integrates at a certain level with CA Audit, but by design it is not completely interoperable. CA Enterprise Log Manager is a new and separate server infrastructure that can run in parallel with CA Audit, with the following event handling considerations:

CA Enterprise Log Manager does...	CA Enterprise Log Manager does <i>not</i> ...
Receive event logs sent from CA Audit clients and iRecorders using configurable listeners.	Directly access event logs stored in the CA Audit collector database.
Provide a utility to import event log data stored in the CA Audit collector database (SEOSDATA table).	
Use agents to send event logs only to the CA Enterprise Log Manager server infrastructure.	
Permit CA Enterprise Log Manager agents and CA Audit clients with iRecorders to run on the same physical host.	Allow CA Enterprise Log Manager agents and CA Audit clients with iRecorders on the same host to access the same log sources simultaneously.

CA Enterprise Log Manager does...

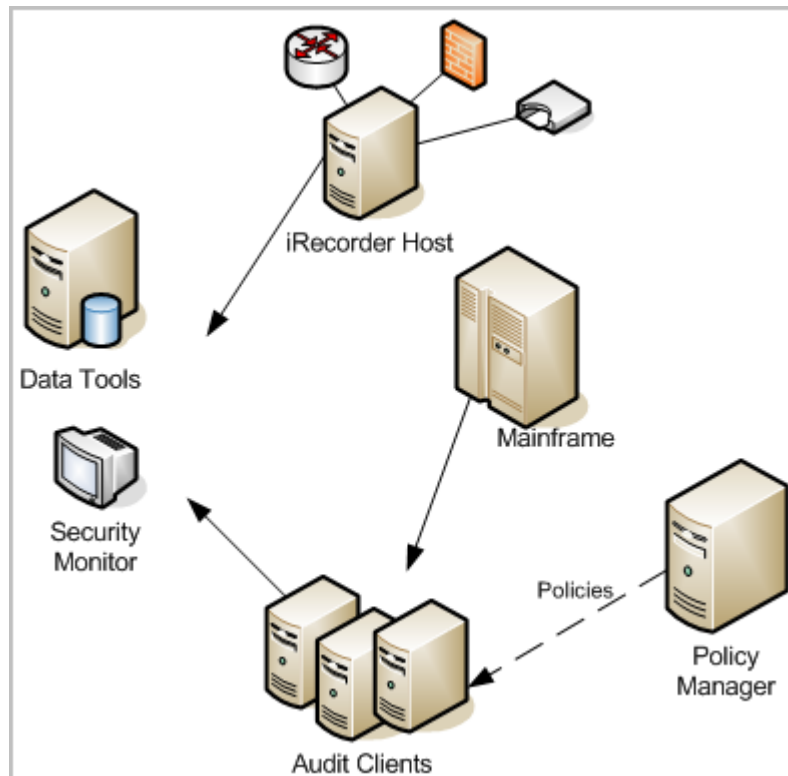
Use its built-in Agent Explorer to manage only CA Enterprise Log Manager agents. During side-by-side operation of the two systems, CA Audit uses its Policy Manager only to manage CA Audit clients

CA Enterprise Log Manager does *not*...

Migrate CA Audit data held in table collectors, report templates or custom reports, alert policies, collection/filtering policies, or role-based access control policies

CA Audit Architecture

The following illustration shows a simplified CA Audit implementation:



In some enterprise deployments of CA Audit, event data is stored by the collector service in a relational database running on the Data Tools server. A database administrator monitors and maintains this database, and works with a system administrator to ensure that the correct policies are in place to gather desired events, and to exclude events that are not needed.

Solid lines in this diagram show events flowing from CA Audit clients, recorder, and iRecorder hosts to the Data Tools server, or in some cases to an optional security monitor console. A dashed line represents the control flow between the Policy Manager server and the clients using policies.

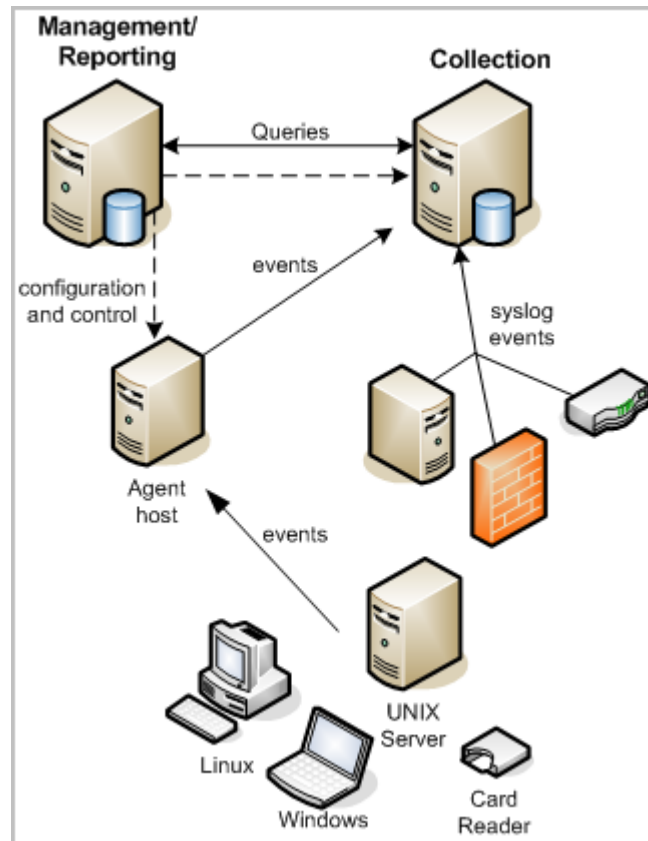
The Data Tools server provides basic reporting and visualization utilities as well as event storage. Custom queries and reports are the norm in enterprise implementations, and require significant time to create and to maintain.

This network topology allows for collection of a variety of event types from different devices, applications, and databases. You have central storage of collected events that is usually part of, or managed by, the Data Tools server which also offers some reports.

However, you need additional capabilities to scale your solution to handle rapidly increasing event volumes. You need to generate reports that demonstrate compliance with a variety of federal and international regulations. And you need to be able to find those reports quickly and easily.

CA Enterprise Log Manager Architecture

The following illustration shows a basic two-server CA Enterprise Log Manager implementation:



A CA Enterprise Log Manager system can have one or more servers, where the first installed server is the management server. There can be no more than one management server in a system, but you can have multiple systems. The management server maintains content and configuration for all CA Enterprise Log Manager servers and performs user authorization and authentication.

In a basic two-server implementation, the management server also performs the role of a reporting server. A reporting server receives refined events from one or more collection servers. The reporting server handles on demand queries and reports as well as scheduled alerts and reports. The collection server refines collected events.

Each CA Enterprise Log Manager server has its own internal event log store database. The event log store is a proprietary database that uses compression to enhance storage capacity, and to allow queries of active database files, files marked for archival, and defrosted files. No relational DBMS package is required for event storage.

The collection CA Enterprise Log Manager server can receive events directly using its default agent, or from an agent residing on the event source. Agents can also reside on a host that acts as a collector for other event sources in the network as for a VPN concentrator or router host.

Solid lines in this diagram represent event flows from event sources to agents to the collection server to the reporting role of the management/reporting server. The dashed lines show configuration and control traffic between the CA Enterprise Log Manager servers and from the management role of the management/reporting server to the agents. You can use any CA Enterprise Log Manager server in the network to control any agent in the network, so long as the CA Enterprise Log Manager servers were registered with the same application instance name in management server during installation.

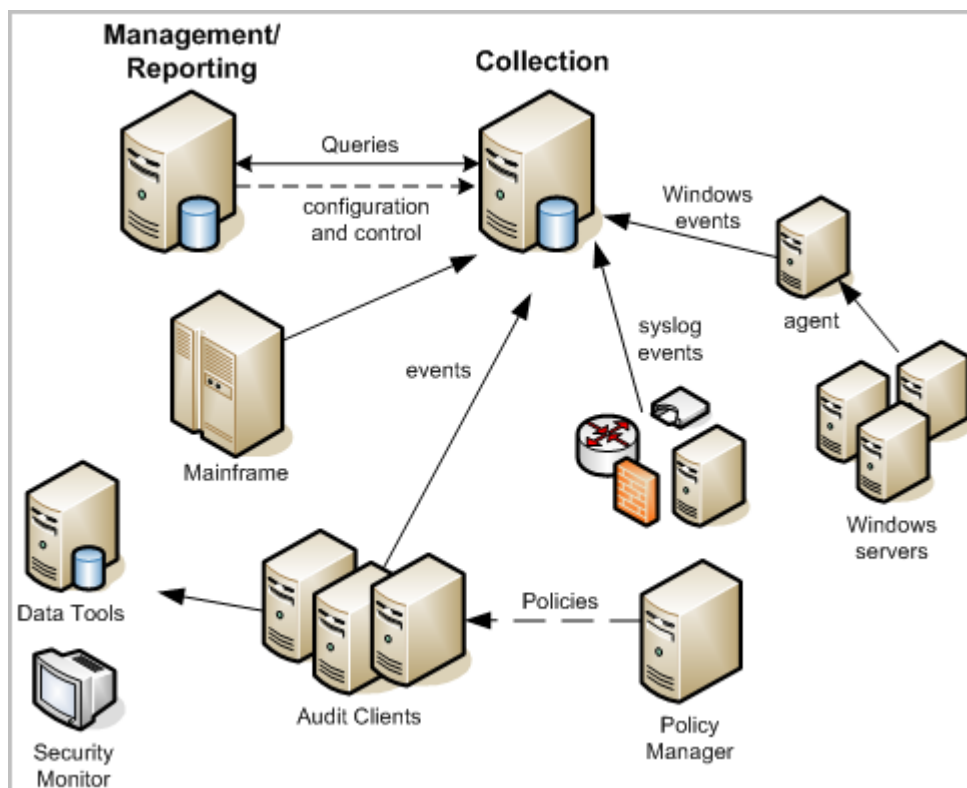
Agents use connectors (not shown) to collect events. A single agent can manage several connectors to collect multiple, different types of events at the same time. This means that a single agent deployed on an individual event source can collect different types of information. The CA Enterprise Log Manager server also offers listeners that allow event collection from other CA Technologies applications using the existing iRecorder and SAPI recorders from your CA Audit network.

You can federate CA Enterprise Log Manager servers to scale your solution and to share reporting data between them without having that data transported out of bounds. This can give you a network-wide view of compliance while still following regulations about maintaining physical data locations.

Subscription updates to predefined queries and reports mean that you no longer have to maintain queries and reports manually. Supplied wizards allow you to create your own custom integrations for third-party devices and applications not yet supported.

Integrated Architecture

The following diagram shows a typical CA Audit network with CA Enterprise Log Manager added to leverage its high volume event handling and compliance-based reporting capabilities:



CA Enterprise Log Manager uses an integrated Agent Explorer, an embedded event log store, and single user interface to centralize and simplify log collection. CA Enterprise Log Manager agent technology coupled with the common event grammar allows for faster event throughput to storage while handling a higher number of event sources. A single agent can handle multiple connectors to event sources, simplifying agent management tasks, and taking advantage of predefined integrations for popular or common event log sources.

In this implementation, the CA Enterprise Log Manager collection server receives the syslog, iTechnology-based, and SAPI recorder events directly. The collection server receives events from Windows event sources through a separate Windows-based CA Enterprise Log Manager agent. You may have several agents deployed in your network, each of which can gather many different kinds of event data through its connectors. This can help to reduce event traffic to the SEOSDATA database and leverage the queries and reports available in CA Enterprise Log Manager. A simple policy rule change allows the CA Audit clients to send collected events to both the Data Tools server and the CA Enterprise Log Manager server.

In addition to higher throughput, CA Enterprise Log Manager offers out-of-the-box queries and reports that help you to demonstrate compliance with regard to multiple standards like PCI (DSS) and SOX. When you couple the predefined queries and reports with your existing CA Audit and CA Security Command Center implementation, you can leverage your investments in your custom solutions while taking advantage of CA Enterprise Log Manager reports and higher throughput.

Configuring CA Technologies Adapters

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

Set the CA Technologies adapter configuration options prior to changing the configurations of CA Audit policies or iRecorders. This ensures that the listener processes are operating before the events arrive. This prevents incorrectly mapped event data.

If you send events through an iRecorder to CA Audit, or if you use a CA Audit client with iRecorder, you will use the CA Enterprise Log Manager SAPI adapters to receive events. To send events to CA Enterprise Log Manager, you will modify an existing CA Audit policy for CA Access Control events. You can add either a Collector action or a Route action to an existing rule.

- If you create a Collector action on a rule in an existing CA Audit policy, configure the SAPI Collector CA Technologies Adapter to receive the events.
- If you create a Route action on a rule in an existing CA Audit policy, configure the SAPI Router CA Technologies Adapter to receive the events.

Refer to the SAPI source documentation for instructions on how to reconfigure to send events directly to CA Enterprise Log Manager.

If you plan to install a standalone iRecorder or you plan to use an existing iRecorder, you will configure the iTech Event Plugin to receive the events. For example, use this approach if you do not have CA Audit installed, but want to use a CA Technologies iRecorder to gather events from a supported event source. The process includes the following steps:

- Configure the iTechnology event plug-in
- Configure the iRecorder or iTechnology-based product to send events directly to the CA Enterprise Log Manager server

About the SAPI Router and Collector

The SAPI services are generally used to receive events from existing CA Audit clients and integrated products. CA Enterprise Log Manager uses two instances of a SAPI listener service, one installed as the SAPI Collector, the other as the SAPI Router.

The SAPI modules use the iGateway daemon for command and control. The modules act as a SAPI router and a SAPI collector and uses either static ports or dynamic ports through the portmapper.

Use the SAPI collector when sending events from CA Audit clients so that you can use the built in fail-over support in the Audit Collector action.

Use the SAPI router when sending events from CA Audit clients using the Route action, or when sending events from SAPI recorders or integrations that support sending events directly to a CA Audit client. In this case you would configure the remote sender as if the CA Enterprise Log Manager server is the CA Audit client.

The SAPI listener opens its own port and listens passively for new events to be sent to it. Each instance of the SAPI module has its own configuration that specifies the following:

- Port on which to listen
- Data mapping (DM) files to load
- Encryption libraries to use

After receiving the event, the module submits it to the mapping library and then CA Enterprise Log Manager inserts it into the database.

Important: The data mapping library may contain one or more mapping files with the same name but different version numbers. The different files support varying release levels of the same event source, such as an operating system, a database, and so forth. It is critical that you select only one, version-relevant mapping file when you configure the SAPI collector or router.

If two files with the same name are present in the list of selected mapping files, the mapping engine uses only the first one in the list. If that is not the right file for the incoming event stream, the mapping engine cannot map the events correctly. This can, in turn, cause queries and reports to show information that doesn't include the mis-mapped events, or any events at all.

Configure the SAPI Collector Service

Use this procedure to configure the SAPI collector service.

You can modify CA Audit policies that use Collector actions to send events to a CA Enterprise Log Manager server in addition to, or in place of, sending events to the CA Audit collector database. Configure this service before you modify Audit policies to ensure that no events are lost.

To configure the SAPI collector service

1. Log into the CA Enterprise Log Manager server and select the Administration tab.
The Log Collection subtab displays by default.
2. Expand the CA Technologies Adapters entry.
3. Select the SAPI Collector service.
4. Refer to the online help for descriptions of each field.
5. Click Save when you are finished.

Configure the SAPI Router Service

Use this procedure to configure a SAPI router service.

You can modify CA Audit policies which use Route actions to send events to a CA Enterprise Log Manager server in addition to, or in place of, routing events to other destinations. You can also redirect SAPI recorder events to go directly to the SAPI router listener by modifying their configuration files. Configure this service before you modify Audit policies or SAPI recorder configurations to ensure that no events are lost.

To configure the SAPI router service

1. Log into the CA Enterprise Log Manager server and select the Administration tab.
The Log Collection subtab displays by default.
2. Expand the CA Technologies Adapters entry.
3. Select the SAPI Router service.
4. Refer to the online help for descriptions of each field.
5. Click Save when you are finished.

About the iTechnology Event Plug-in

The iTechnology event plug-in receives events sent through the iGateway event handling mechanism. Configure the iTechnology event plug-in if any of the following are true for your environment:

- You have existing iRecorders in your network that do not have CA Audit clients on the same system
- You have other products, such as CA EEM, that can forward events through iTechnology

After receiving an event, this service submits it to the mapping library after which CA Enterprise Log Manager inserts the mapped event into the event log store.

Configure the iTechnology Event Plug-in

Use this procedure to configure the iTechnology event plug-in to receive from iRecorders and other iTechnology event sources.

Use the iTechnology plug-in when you configure a standalone iRecorder to send its events to a CA Enterprise Log Manager server. Configure this service *before* you configure or install an iRecorder to ensure that no events are lost.

Note: If you want to send events from an external client to the iTechnology Event Plug-in listener, you must send these events only to the secondary CA Enterprise Log Manager server.

To configure the iTechnology event plug-in

1. Log into the CA Enterprise Log Manager server and select the Administration tab.
The Log Collection subtab displays by default.
2. Expand the CA Technologies Adapters entry.
3. Select the iTechnology Event Plug-in service.
4. Select one or more data mapping (DM) files from the Available DM Files list and use the arrows to move them to the Select DM Files list.

The event plug-in service is preconfigured to include most of the major data mapping files.

5. Click Save to store the changes in the management server configuration files.

Sending CA Audit Events to CA Enterprise Log Manager

You can integrate CA Enterprise Log Manager with your existing CA Audit implementation in the following ways:

- Reconfigure an iRecorder that is not on the same host as a CA Audit client to send events to CA Enterprise Log Manager
- Modify an existing CA Audit policy to send events to both CA Audit and CA Enterprise Log Manager

Configure iRecorder to Send Events to CA Enterprise Log Manager

CA Enterprise Log Manager receives events from iRecorders through the iTech Event Plugin Listener. You must configure the listener before you change the iRecorder's configuration. If you do not do this, you may lose event data. After you configure the Listener, use this procedure to configure the iRecorder to send events to the CA Enterprise Log Manager server.

iRecorders that are installed on the same computer as a CA Audit client send events to the client directly. For those machines, you should use the SAPI collector or router adapters.

Important! A standalone iRecorder can only send its events to a single destination. If you reconfigure an iRecorder using the procedure that follows, events are stored *only* in the CA Enterprise Log Manager event log store. If you need to retain events in both the event log store, and the CA Audit Collector database, modify a rule action on an existing policy, or create a new policy for a CA Audit client.

To configure the iRecorder to send events to CA Enterprise Log Manager

1. Log into the server that hosts the iRecorder as a user with Administrator privileges.
2. Navigate to the directory for your operating system:
 - UNIX or Linux: /opt/CA/SharedComponents/iTechnology
 - Windows: \Program Files\CA\SharedComponents\iTechnology
3. Stop the iGateway daemon or service with the following command:
 - UNIX or Linux: ./S99gateway stop
 - Windows: net stop igateway
4. Edit the iControl.conf file.
5. Specify the following RouteEvent value:

```
<RouteEvent>true</RouteEvent>
```

This entry tells the iGateway to send its events, including all iRecorder events, to the host named in the RouteHost tag pair.

6. Specify the following RouteHost value:

```
<RouteHost>CA_ELM_hostname</RouteHost>
```

This entry tells the iGateway to send its events to the CA Enterprise Log Manager server using its DNS name.

7. Restart the iGateway daemon or service with the following command:

- UNIX or Linux: `./S99gateway start`
- Windows: `net start igateway`

This action forces the iRecorder to use the new settings and starts the flow of events from the iRecorder to the CA Enterprise Log Manager server.

More information:

[About the SAPI Router and Collector](#) (see page 208)

[Configure the SAPI Collector Service](#) (see page 209)

[Configure the SAPI Router Service](#) (see page 209)

Modify an Existing CA Audit Policy to Send Events to CA Enterprise Log Manager

Use this procedure to enable a CA Audit client to send events to *both* CA Enterprise Log Manager and the CA Audit collector database. By adding a new target to the Route or Collector actions on an existing rule, you can send collected events to both systems. As an alternative, you can also modify specific policies or rules to send events *only* to the CA Enterprise Log Manager server.

CA Enterprise Log Manager collects events from CA Audit clients using the CA Audit SAPI Router and CA Audit SAPI Collector listeners. Collected events are stored in the CA Enterprise Log Manager event log store only *after* you push the policy to the clients and it becomes active.

Important: You must configure the CA Enterprise Log Manager listeners to receive events before you modify and activate the policy. If you do not do this configuration first, you may have incorrectly mapped events if events arrive between the time that the policy becomes active and the listeners can correctly map the events.

To modify an existing policy rule's action to send events to CA Enterprise Log Manager

1. Log into the Policy Manager server and access the My Policies tab in the left pane.
2. Expand the policy folder until you can see the desired policy.
3. Click the policy to display its basic information in the Details pane to the right.
4. Click Edit in the Details pane to add to the policy's rules. The rule wizard starts.

5. Click the Edit Actions next to the arrow for the wizard's step 3. The wizard's rule actions page displays.
6. Click the Collector action in the Browse Actions pane on the left. This displays the Action List to the right.

You can also use the Route action to create a rule to send events to a CA Enterprise Log Manager server.

7. Click New to add a new rule.
8. Enter the IP address or host name of the collection CA Enterprise Log Manager server.

For a CA Enterprise Log Manager implementations with two or more servers, you can enter a different CA Enterprise Log Manager host name or IP address in the Alternate Host Name field to take advantage of <Aus>'s automatic failover feature. If the first CA Enterprise Log Manager server is not available, CA Audit automatically sends events to the server named in the Alternate Host Name field.

9. Enter the name of the management CA Enterprise Log Manager server in the Alternate Host Name field, and then create a description for this new rule action.
10. Clear the check box, Perform this action on remote server, if it is checked.
11. Click Add to save the new rule action and then click Finish in the wizard window.
12. Select the Rules tab in the lower right pane, and then select a rule to check.
13. Click Check Policies to check the changed rule with the new actions to ensure that it compiles properly.

Make any needed modifications to the rule and ensure that it compiles correctly before you activate it.

14. Click Activate to distribute the checked policy that contains the new rule actions you added.
15. Repeat this procedure for each rule and policy with collected events you want to send to CA Enterprise Log Manager.

More information:

[About the SAPI Router and Collector](#) (see page 208)

[Configure the SAPI Collector Service](#) (see page 209)

[Configure the SAPI Router Service](#) (see page 209)

Modify an Existing r8SP2 Policy to Send Events to CA Enterprise Log Manager

Use this procedure to enable an r8 SP2 CA Audit client to send events to *both* CA Enterprise Log Manager and the CA Audit collector database. By adding a new target to the Route or Collector actions on an existing rule, you can send collected events to both systems. As an alternative, you can also modify specific policies or rules to send events *only* to the CA Enterprise Log Manager server.

More information on working with policies is available in the *CA Audit r8 SP2 Implementation Guide*. Refer to that resource for details on performing the steps in the procedure that follows.

CA Enterprise Log Manager collects events from CA Audit clients using the CA Audit SAPI Router and CA Audit SAPI Collector listeners. Collected events are stored in the CA Enterprise Log Manager event log store only *after* you push the policy to the clients and it becomes active.

Important: You must configure the CA Enterprise Log Manager listeners to receive events before you modify and activate the policy. If you do not do this configuration first, you may have incorrectly mapped events between the time that the policy becomes active and the listeners can correctly map the events.

To modify an existing r8 SP2 policy rule's action to send events to CA Enterprise Log Manager

1. Log into the Policy Manager server as a user with the Maker role.
2. Access the rule you want to edit by expanding its folder in the Policies pane and choosing the appropriate policy.

The policy appears in the Details pane, displaying its rules.
3. Click the rule you want to edit.

The rule appears, with its actions displayed, in the Details pane.
4. Click Edit.

The Edit Rule wizard appears.
5. Use the Edit Rule wizard to change the rule so that it sends events to the CA Enterprise Log Manager server, either in addition to or in place of the current destinations, and click Finish when done.
6. Check and commit the policy as the Maker user so that it can be approved by a user with the Checker role.
7. Log out, and then log back into the Policy Manager server as a user with the Checker role, if your enterprise uses the segregation of duties feature.

8. Review and approve the policy folder that contains the changed policy and rule.

After the policy is approved, the Policy Manager Distribution Server's settings determine when the new policy is distributed to the audit nodes. You can review the activation log to check on a policy's activation status.

9. Repeat this procedure for each rule and policy with collected events you want to send to CA Enterprise Log Manager.

When to Import Events

If you have an existing CA Audit Data Tools server with a Collector database, you have a SEOSDATA table that contains event data. To run your CA Audit and CA Enterprise Log Manager systems side-by-side and view reports on data you have already collected, you may want to import data from your SEOSDATA table.

You can run the SEOSDATA import utility to perform an import of event data from your Collector database to a CA Enterprise Log Manager event log store. Typically, you import event data immediately after you deploy a CA Enterprise Log Manager server. If you are integrating the two systems, you may decide to perform the import of data more than once, depending on your use and network configuration.

Note: Importing data from the SEOSDATA table does *not* remove or modify any of the data stored there. The import procedure copies the data, parses it, and maps it into the CA Enterprise Log Manager event log store.

About the SEOSDATA Import Utility

The import utility, LMSeosImport, uses a command line interface and supports both the Windows and Solaris operating systems. The utility performs the following actions:

- Connects to the SEOSDATA table to extract events in the manner you specify
- Parses the selected SEOSDATA events into name-value pairs
- Submits the events to the CA Enterprise Log Manager through the SAPI Event Sponsor or the iTech Event Sponsor for insertion into the event log store

The events are mapped to the common event grammar (CEG) that forms the basis for the event log store's database tables. You can then use the predefined queries and reports to gather information from your stored events.

Importing from a Live SEOSDATA Table

Running the LMSeosImport utility against a live SEOSDATA table is not recommended, but at times may be unavoidable. If you must run the utility against a live database, the utility imports only a certain section of data. This happens because events that are added to the database *after* the LMSeosImport utility starts are not imported during that import session.

For example, if you do not specify the -minid and -maxid parameters in the command line, when the utility starts, it queries the database for the minimum and maximum existing entry IDs. The utility then bases its queries and import activities on those values. Events inserted into the database after the utility starts have entry IDs outside that range and so are not imported.

When an import session completes, the utility displays the last entry ID that it processed. You may need to run more than one import session to get all of your events, or you may choose to wait for a period of lower network and event activity to run the import utility. You can run additional import sessions, if needed, using the last session's ending entry ID as the new session's -minid value.

Importing Data from a SEOSDATA Table

Use this process for importing data from a collector database (SEOSDATA table) to ensure the best results:

1. Copy the LMSeosImport utility to the iTechnology folder on a CA Audit Data Tools server.

Note: The LMSeosImport utility requires the *etsapi* and *etbase* supporting libraries that are supplied with the CA Audit Client.

2. Understand the LMSeosImport command line and options.
3. Create an Event report to discover the event types and counts, and the entry ID ranges.
4. Preview the import results with the parameters you expect to use.

You may decide to run the preview import again to refine the command line options, if needed.

5. Import events from a collector database using the refined command line options.

Copy the Event Import Utility to a Solaris Data Tools Server

Before you can import data from your SEOSDATA table, you must copy the LMSeosImport utility from the CA Enterprise Log Manager Application installation DVD-ROM to your Solaris Data Tools server.

Note: The LMSeosImport utility requires the presence of the *etsapi* and *etbase* libraries. These files are part of the base Data Tools server installation. Before you try to use the LMSeosImport utility, ensure that the CA Audit install directory is included in your system PATH statement. The default directory is `opt/CA/eTrustAudit/bin`.

Before you run the utility, set the following environment variables with the *env* command:

- `ODBC_HOME=<CA Audit data tools install directory>/odbc`
- `ODBCINI=<CA Audit data tools install directory>/odbc/odbc.ini`

To copy the utility

1. Access a command prompt on the Solaris Data Tools server.
2. Insert the CA Enterprise Log Manager Application installation DVD-ROM.
3. Navigate to the directory, `/CA/ELM/Solaris_sparc`.
4. Copy the LMSeosImport utility to the CA Audit Data Tools server's iTechnology directory, `/opt/CA/SharedComponents/iTechnology`.

The utility is ready for use after you copy it to the designated directory and set the required environment variables. There is no separate installation to run.

Copy the Import Utility to a Windows Data Tools Server

Before you can import data from your SEOSDATA table, you must copy the LMSeosImport utility from the CA Enterprise Log Manager Application installation DVD-ROM to your Windows Data Tools server.

Note: The LMSeosImport utility requires the presence of the *etsapi* and *etbase* dynamic link libraries. These files are part of the base Data Tools server installation. Before you try to use the LMSeosImport utility, ensure that the directory, `Program Files\CA\eTrust Audit\bin`, is included in your system PATH statement.

To copy the utility

1. Access a command prompt on the Windows Data Tools server.
2. Insert the CA Enterprise Log Manager Application installation DVD-ROM.
3. Navigate to the directory, `\CA\ELM\Windows`.

4. Copy the LMSeosImport.exe utility to the CA Audit Data Tools server's iTechnology directory, <drive>:\Program Files\CA\SharedComponents\iTechnology.

The utility is ready for use after you copy it to the designated directory. There is no separate installation to run.

Understand the LMSeosImport Command Line

The LMSeosImport utility offers a variety of command line arguments that let you control which events are migrated. Each event in the SEOSDATA table is a row, and has a unique *entry ID* to identify it. You can use the import utility to retrieve a report that lists several different kinds of useful information. The report lists the number of events in the SEOSDATA table (as a number of entry IDs), event counts by log type, and the date ranges of the events. The utility offers a retry option in case an error occurs during the import of an event.

You can also run a preview job to see what the import results would be with a specific command structure. Preview jobs do not actually import data. This allows you to refine your command line options prior to the actual migration.

You can run the migration utility more than once using different parameters to import different kinds of data. For example, you may choose to migrate your data in several, tailored sessions based on a range of entry IDs, the log type, or specific date ranges.

Note: The utility does *not* offer import tracking of prior sessions. It is possible to duplicate data in your CA Enterprise Log Manager database if you run the command with the same parameters more than once.

For the best results, break up your import by log type (using the -log option) or by entry ID (using the -minid and -maxid options) to improve import performance. Use the -retry option to help recover from any errors that may occur during event import. The utility uses a default -retry value of 300 seconds to maximize import success.

Import Utility Command and Options

The LMSeosImport utility supports the following command line syntax and options:

```
LMSeosImport -dsn dsn_name -user user_name -password password -target target_name
{-sid nnn -eid nnnn -stm yyyy-mm-dd -etm yyyy-mm-dd -log logname -transport
(sapi|itech) -chunk nnnn -pretend -verbose -delay -report -retry}
```

-dsn

Specifies the name of the host server where the SEOSDATA table resides. This parameter is required.

-user

Specifies a valid user ID that has at least Read access to the SEOSDATA table. This parameter is required.

-password

Specifies the password for the user account specified with the -user parameter. This parameter is required.

-target

Specifies the hostname or IP address of the CA Enterprise Log Manager server to receive the migrated events from the SEOSDATA table. This parameter is required.

-minid nnnn

Indicates the starting ENTRYID used when selecting events from the SEOSDATA table. This parameter is optional.

-maxid nnnn

Indicates the ending ENTRYID used when selecting events from the SEOSDATA table. This parameter is optional.

-mintm YYYY-MM-DD

Indicates the starting time (in YYYY-MM-DD format) used when selecting events from the SEOSDATA table. This parameter is optional.

-maxtm YYYY-MM-DD

Indicates the ending time (in YYYY-MM-DD format) used when selecting events from the SEOSDATA table. This parameter is optional.

-log logname

Specifies that the utility should select only event records with this specified logname. This parameter is optional. If the logname contains spaces, then it must be enclosed in double quotes.

-transport <sapi | itech >

Specifies the transport method that should be used between the import utility and CA Enterprise Log Manager. The default transport method is sapi.

-chunk nnnn

Specifies the number of event records to select from the SEOSDATA table on each pass. The default value is 5000 events (rows). This parameter is optional.

-preview

Outputs the results of the event record selections to STDOUT, but does not actually import the data. This parameter is optional.

-port

Specifies the port number to use if you set the transport option to SAPI and you configured the CA Enterprise Log Manager SAPI router to use a fixed port value (without using the portmapper).

-verbose

Specifies that the utility sends detailed processing messages to STDOUT. This parameter is optional.

-delay

Specifies the number of seconds to pause between the processing of each event. This parameter is optional.

-report

Displays a report of time range, ENTRYID range, and Log counts in the SEOSDATA table. This parameter is optional.

-retry

Specifies the total number of seconds during which retry attempts are made each time an error occurs during the import of an event. Processing continues when the send of that event is successful again. The utility automatically uses a default value of 300 seconds. You do not have to enter the parameter unless you want to specify a different value. Messages related to the retry status are sent to STDOUT.

LMSeosImport Command Line Examples

You can use the following command line examples to create your own custom command when using the SEOSDATA import utility.

To run an import of records between ENTRYIDs 1000 and 4000

Enter the command line:

```
LMSeosImport -dsn eAudit_DSN -user sa -password sa -target 130.200.137.192 -minid 1000 -maxid 4000
```

To run an import of records for only NT-Application events

Enter the command line:

```
LMSeosImport -dsn eAudit_DSN -user sa -password sa -target 130.200.137.192 -log NT-Application
```

Create an Event Report

Running a SEOSDATA event report prior to the actual import of data provides you with needed information about the events in the table. The report shows the event time range, the event count per log type, and the entry ID range. You can use the values displayed in the report to refine your command line options for either a preview command or the actual import command.

To show a report of current SEOSDATA event information on Windows

1. Access a command prompt on the CA Audit Data Tools server.
2. Navigate to the directory, \Program Files\CA\SharedComponents\iTechnology.
3. Enter the command line:

```
LMSeosImport -dsn eAudit_DSN -user sa -password sa -target  
<Log_Manager_host_name> -report
```

The generated report display is similar to the following example:

```
SEOSProcessor::InitOdbc: successfully attached to source [eAudit_DSN]
```

```
----- SEOSDATA Event Time Range -----
```

```
Minimum TIME = 2007-08-27  
Maximum TIME = 2007-10-06
```

```
----- Event Count Per Log -----
```

```
com.ca.iTechnology.iSponsor : 3052  
EiamSdk : 1013  
NT-Application : 776  
NT-System : 900
```

```
----- SEOSDATA EntryID Range -----
```

```
Minimum ENTRYID : 1  
Maximum ENTRYID : 5741
```

```
Report Completed.
```

Preview Import Results

You can run a test import with output to STDOUT to preview the import results without actually importing or migrating data. This is a good way to test the command line parameters you have entered for either a one-time migration or for a regularly scheduled import batch job.

To run a test import to preview import results

1. Access a command prompt on the CA Audit Data Tools server.
2. Navigate to the appropriate directory:

Solaris: /opt/CA/SharedComponents/iTechnology

Windows: \Program Files\CA\SharedComponents\iTechnology

3. Enter the command line:

For Solaris:

```
./LMSeosImport.sh -dsn eAudit_DSN -user sa -password sa -target  
<Log_Manager_host_name_or_IP> -minid 1000 -maxid 4000 -preview
```

For Windows:

```
LMSeosImport.exe -dsn eAudit_DSN -user sa -password sa -target  
<Log_Manager_host_name_or_IP> -minid 1000 -maxid 4000 -preview
```

Import Events from a Windows Collector Database

You can use this procedure to import event data from a Collector database that resides on a Windows Data Tools server.

To import events from a SEOSDATA table on a Windows server

1. Locate the name of the server on which the SEOSDATA table resides.
2. Ensure that you have user access credentials for that server with at least Read access to the SEOSDATA table.
3. Access a command prompt on the CA Audit Data Tools server.
4. Navigate to the directory, \Program Files\CA\Shared Components\iTechnology.
5. Start the import utility using the command syntax:

```
LMSeosImport.exe -dsn <dsname> -user <UID> -password <password> -target  
<targethostname> <optional flags>
```

Import Events from a Solaris Collector Database

You can use this procedure to import event data from a Collector database that resides on a Solaris Data Tools server.

To import events from a SEOSDATA table on a Solaris server

1. Locate the name of the server on which the SEOSDATA table resides.
2. Ensure that you have user access credentials for that server with at least Read access to the SEOSDATA table.
3. Access a command prompt on the CA Audit Data Tools server.
4. Navigate to the directory, /opt/CA/SharedComponents/iTechnology.
5. Start the import utility using the command syntax:

```
./LMSeosImport -dsn <dsname> -user <UID> -password <password> -target  
<targethostname> <optional flags>
```

Appendix B: Considerations for CA Access Control Users

This section contains the following topics:

[Integrating with CA Access Control](#) (see page 223)

[How to Modify CA Audit Policies to Send Events to CA Enterprise Log Manager](#) (see page 224)

[How to Configure a CA Access Control iRecorder to Send Events to CA Enterprise Log Manager](#) (see page 234)

[How to Import CA Access Control Events from a CA Audit Collector Database](#) (see page 237)

[Securing CA Enterprise Log Manager Using CA Access Control](#) (see page 248)

Integrating with CA Access Control

You can integrate CA Enterprise Log Manager with CA Access Control using one of several different release levels. The general approach is the following:

For CA Access Control releases that use a TIBCO message server for routing events, do the following:

- Install a CA Enterprise Log Manager agent
- Configure a connector that uses the `AccessControl_R12SP1_TIBCO_Connector` connector

For CA Access Control r12.5, see the *CA Access Control r12.5 Implementation Guide* and the *CA Enterprise Log Manager CA Access Control Connector Guide*.

For CA Access Control r12. SP1, see the *CA Access Control r12 SP1 Implementation Guide, 3rd Edition*, and the *Connector Guide for CA Access Control*.

Note: These implementations use components that are part of the CA Access Control Premium Editions.

For CA Access Control releases that use `selogrd` for routing events, do the following:

- Install a CA Enterprise Log Manager agent
- Configure a connector that uses the `ACSelogrd` integration

More information about configuring a connector to collect CA Access Control events is available in the *CA Access Control r8 SP1 Connector Guide*.

If you are currently sending CA Access Control events to CA Audit, use of the following methods to get events to CA Enterprise Log Manager:

- Modify an existing CA Audit policy to send events both to CA Audit and to CA Enterprise Log Manager, if you use a CA Audit iRecorder to collect events. You can also modify the policy to send events only to the CA Enterprise Log Manager server, if desired.
- Configure the control.conf file for an iRecorder to send events directly to CA Enterprise Log Manager.

The guidelines that follow use the r8 SP2-series for the Policy Manager user interface. The general procedures are the same when you are using earlier CA Audit releases, though the user interface is different.

How to Modify CA Audit Policies to Send Events to CA Enterprise Log Manager

The process for modifying an existing CA Audit policy to send events to CA Enterprise Log Manager involves the following steps:

- Gather the needed information:
 - Verify that you have user credentials for the CA Audit Policy Manager with the authority to create, verify, and activate policies.
 - Obtain the IP address or host name required to access the Audit Administrator user interface. The URL to access the r8 SP2-series Policy Manager server web application follows the form:

`https://<IP_address_of_CA_Audit_PM>:5250/spin/auditadmin`

- Configure the CA Enterprise Log Manager SAPI collector or SAPI router service, depending on how you intend to create the rule action.

If you plan to create a Collector action, configure the SAPI collector. If you plan to configure a Route action, configure the SAPI router.

Note: The example in this section uses the Collector action.

- Locate and modify an existing CA Access Control policy to send events to CA Enterprise Log Manager.
- Check and activate the changed policy to distribute it to the audit nodes.

Repeat this process to add new rule actions to other policy rules, as needed.

More information:

[About the SAPI Router and Collector](#) (see page 208)

Configure the SAPI Collector Adapter to Receive CA Access Control Events

Use this procedure to configure the SAPI collector adapter to receive CA Access Control events from a CA Audit implementation.

You can modify CA Audit policies that use Collector actions to send events to a CA Enterprise Log Manager server in addition to, or in place of, sending events to the CA Audit collector database. Configure this service *before* you modify CA Audit policies to verify that no events are lost.

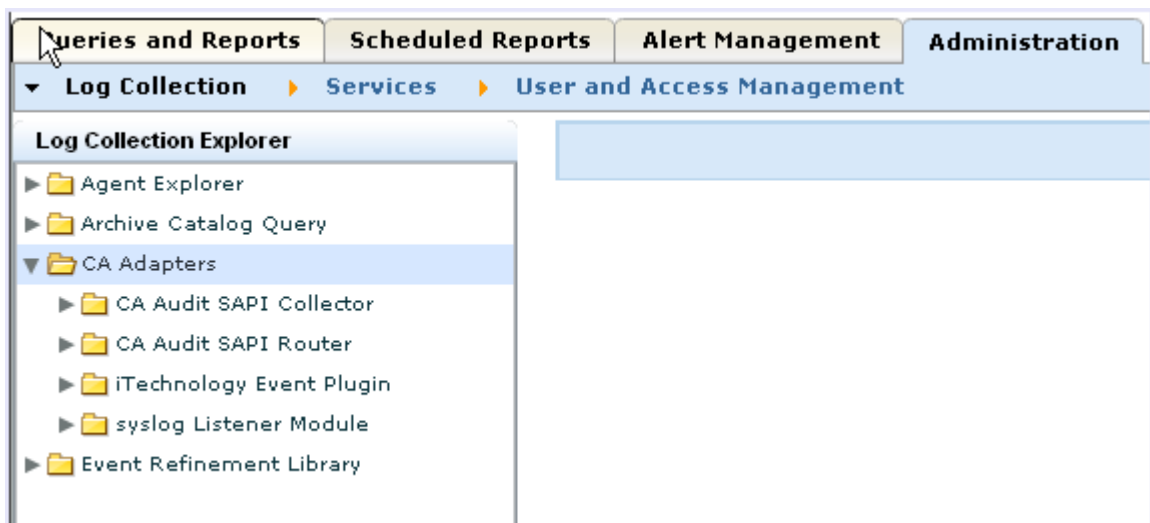
(You can configure a SAPI Router service in a similar way. If you use both the Router and Collector services, be sure that the ports listed are different, or that the port mapper service controls them.)

To configure the SAPI collector service

1. Log into the CA Enterprise Log Manager server as an Administrator user and select the Administration tab.

The Log Collection subtab displays by default.

2. Expand the CA Technologies Adapters entry.



3. Select the SAPI Collector service.

Global Service Configuration: CA Audit SAPI Collector

Administration **Self Monitoring Events** **Save** **Reset** **Use Defaults**

Global Service Configuration: CA Audit SAPI Collector

View or edit the details of this configuration.

☒ **EnableListener**

SapiPort: 0

☒ **Register**

Encryption Key:

☐ **Event Ordering**

Event Throttling: 10000

Thread Count per queue: 1

Ciphers

Available	Selected
	Aes256
	Aes128

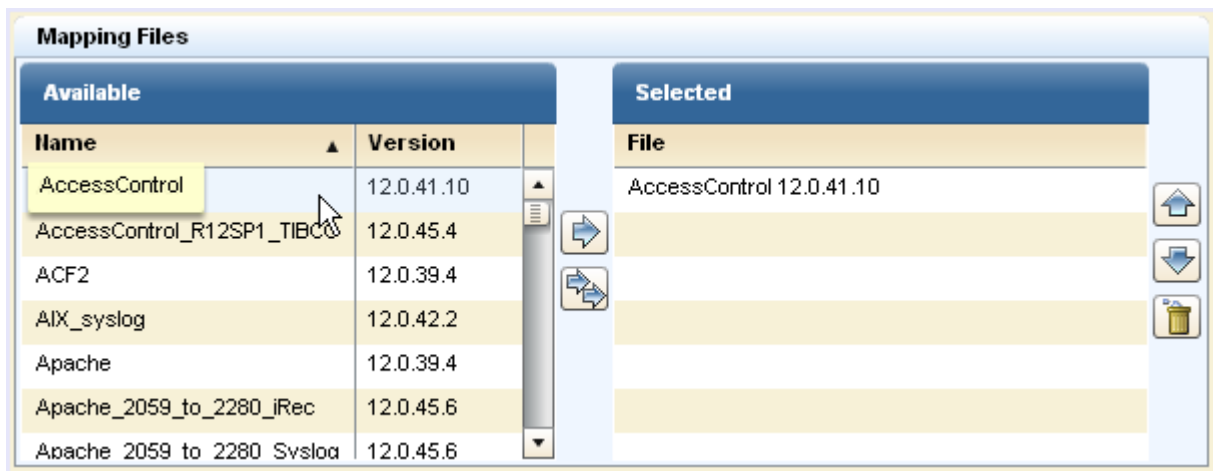
4. Select the EnableListener check box and set the SapiPort value to a value that matches what CA Audit uses.

The default CA Enterprise Log Manager value, 0, uses the Portmapper service to map the ports. If you have a port defined in CA Audit, use that setting here.

5. Accept the other field defaults, and scroll down to the list of Mapping Files.

If you select the Register check box, specify a SAPI port value.

6. Add the Access Control mapping file entry if it is not present, and remove the other mapping file selections from the list of Selected mapping files.



7. Click Save.

Modify an Existing CA Audit Policy to Send Events to CA Enterprise Log Manager

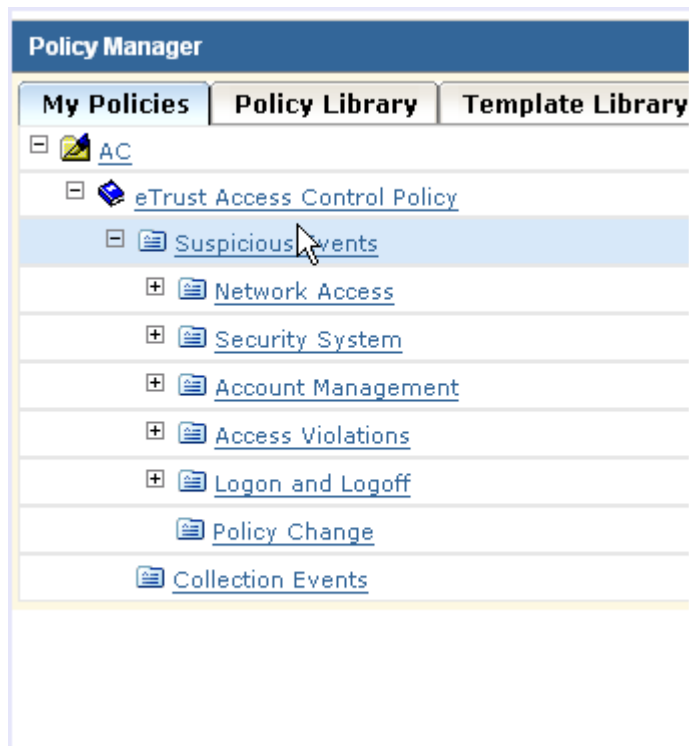
Use this procedure to enable a CA Audit client to send events to *both* CA Enterprise Log Manager and the CA Audit collector database. By adding a new target to the Route or Collector actions on an existing rule, you can send collected events to both systems. As an alternative, you can also modify specific policies or rules to send events *only* to the CA Enterprise Log Manager server.

CA Enterprise Log Manager collects events from CA Audit clients using the CA Audit SAPI Router and CA Audit SAPI Collector listeners. (CA Enterprise Log Manager can also collect events using the iTech plugin directly, if you configured any iRecorders to send directly to the CA Enterprise Log Manager server.) Collected events are stored in the CA Enterprise Log Manager event log store only *after* you push the policy to the clients and it becomes active.

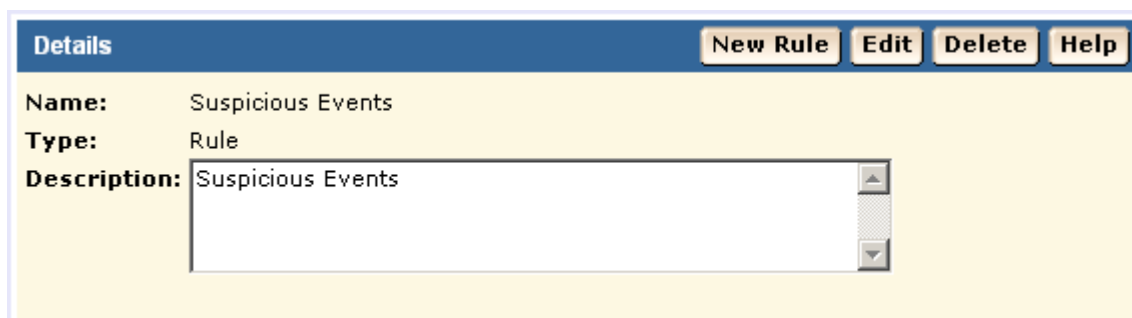
Important: Configure the CA Enterprise Log Manager listeners to receive events before you modify and activate the policy. If you do not do this configuration first, you can incorrectly map events between the time that the policy becomes active and the listeners can correctly map the events.

To modify an existing policy rule action to send events to CA Enterprise Log Manager

1. Log into the Policy Manager server and access the My Policies tab in the left pane.
2. Expand the policy folder until you can see the desired policy.



3. Click the policy to display its basic information in the Details pane to the right.



- Click Edit in the Details pane to add to the policy rules.

The rule wizard starts:

Edit a Rule: Information Back Next Finish Cancel Help

1 Edit Information 2 Edit Script 3 Edit Actions

Rule Information
Edit the rule name and the description of the rule.

Rule Name:
Suspicious Events

Rule Description:
Suspicious Events

Quick Help

- Edit the rule name and the description of the rule.

5. Click Edit Actions next to the arrow for the step 3.

The rule actions page displays:

Edit a Rule: Actions [Back](#) [Next](#) [Finish](#) [Cancel](#) [Help](#)

1 **Edit Information** 2 **Edit Script** 3 **Edit Actions**

Browse Actions [Help](#)

Browse the list of actions, and create actions to add to the rule.

- [Collector](#)
- [E-Mail](#)
- [eSCC Status Monitor](#)
- [External Program](#)
- [File](#)
- [c:\eacevents.txt](#)
- [Route](#)
- [Screen](#)
- [Security Monitor](#)
- [r8sp1cr3](#)
- [Snmp](#)
- [Unicenter](#)

- Click the Collector action in the Browse Actions pane to display the Action List to the right.

The screenshot shows the 'Edit a Rule: Actions' window. At the top, there are navigation buttons: Back, Next, Finish, Cancel, and Help. Below this is a progress bar with three steps: 1 Edit Information, 2 Edit Script, and 3 Edit Actions (which is highlighted with a yellow diamond). The main area is divided into two panes. The left pane is titled 'Browse Actions' and contains a list of actions: Collector, E-Mail, eSCC Status Monitor, External Program, and File. The 'Collector' action is selected. The right pane is titled 'Action List' and contains a table with the following columns: Host Name or IP Address, Use Remote Server, Optional Parameters, and Description. The table is currently empty.

Host Name or IP Address	Use Remote Server	Optional Parameters	Description
-------------------------	-------------------	---------------------	-------------

You could also use the Route action, but the collector action offers the additional benefit of an alternate host name for basic failover processing.

7. Click New to add a new rule.
8. Enter the IP address or host name of the collection CA Enterprise Log Manager server.

Edit a Rule: Actions [Back] [Next] [Finish] [Cancel] [Help]

1 Edit Information 2 Edit Script 3 Edit Actions

Browse Actions [Help]
Browse the list of actions, and create actions to add to the rule.

- Collector
- E-Mail
- eSCC Status Monitor
- External Program
- File
- c:\eacevents.txt
- Route
- Screen
- Security Monitor
- r8sn1cr3

Collector [Add] [Cancel]

Host Name or IP Address: CA-ELM-Collector

Alternate Host Name: CA-ELM-Management

Description: CA Enterprise Log Manager action

☐ **Perform this action on remote server**

☒ **Server is defined by AN Group**

☐ **Server is:** []

For a CA Enterprise Log Manager implementation with two or more servers, you can enter a different CA Enterprise Log Manager host name or IP address in the Alternate Host Name field. This takes advantage of CA Audit's automatic failover feature. If the first CA Enterprise Log Manager server is not available, CA Audit automatically sends events to the server named in the Alternate Host Name field.

9. Enter the name of the management CA Enterprise Log Manager server in the Alternate Host Name field, and then create a description for this new rule action.
10. Clear the check box, Perform this action on remote server, if it is checked.
11. Click Add to save the new rule action and then click Finish in the wizard window.

Note: Next you check and activate the policy, so do *not* log out of the CA Audit Policy Manager.

More information:

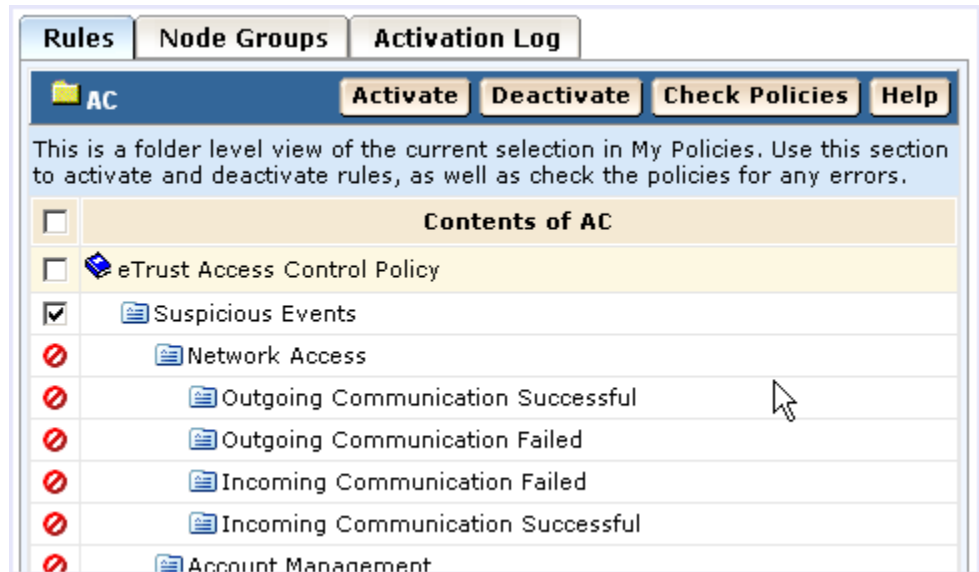
[Modify an Existing r8SP2 Policy to Send Events to CA Enterprise Log Manager](#) (see page 214)

Check and Activate the Changed Policy

After you change an existing policy to add a rule action, check (compile) it and then activate it.

To check and activate a CA Access Control policy

1. Select the Rules tab in the lower right pane, and then select a rule to check.



2. Click Check Policies to check the changed rule with the new actions to ensure that it compiles properly.
Make any needed modifications to the rule and ensure that it compiles correctly before you activate it.
3. Click Activate to distribute the checked policy that contains the new rule actions you added.
4. Repeat this procedure for each rule and policy with collected events you want to send to CA Enterprise Log Manager.

How to Configure a CA Access Control iRecorder to Send Events to CA Enterprise Log Manager

You can configure a standalone CA Access Control iRecorder to send the events it collects directly to the CA Enterprise Log Manager server for storage and reporting. The process includes the following steps:

1. Configure the iTech Event Plugin Listener to receive information from an CA Access Control iRecorder.
2. Download and install an CA Access Control iRecorder.
3. Configure the iRecorder to send its collected events directly to CA Enterprise Log Manager.
4. Verify that CA Enterprise Log Manager is receiving events.

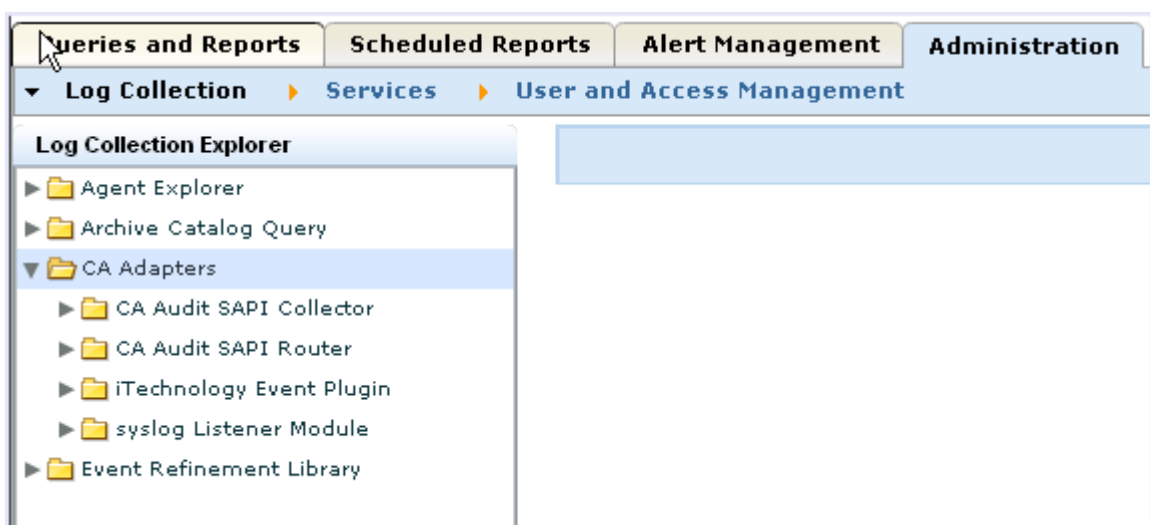
Note: iRecorders can send their events to only one destination. When you configure using this procedure, the only destination is the named CA Enterprise Log Manager server.

Configure the iTech Event Plugin for CA Access Control Events

Before you reconfigure an iRecorder to send events directly to CA Enterprise Log Manager, you need to configure a listener to receive those events.

To configure the listener

1. Log into the CA Enterprise Log Manager server as a user with the Administrator role.
2. Access the Administration tab and then expand the CA Adapters node.



3. Expand the iTechnology Event Plugin node.
4. Select the current CA Enterprise Log Manager server to display the local settings.
5. Ensure that the AccessControl mapping file is first in the list of Selected mapping files to ensure the most efficient operations.
6. Verify that the Log level value is set to NOTSET to collect all event levels.
7. Click Save.

Download and Install a CA Access Control iRecorder

You can collect CA Access Control events to send to a CA Enterprise Log Manager server even if you do not have CA Audit installed. When you collect events in this way, you are using an iRecorder in standalone mode. You can obtain an iRecorder from the CA Technologies Support web site.

Note: iRecorders are supported only with CA Access Control r8 and later releases.

To download and install a iRecorder

1. Access the following CA Technologies web site:

`https://support.ca.com/irj/portal/anonymous/phpdocs?filePath=0/154/cacirecr8-certmatrix.html#caacirec`
2. Select the appropriate iRecorder for your version of CA Access Control.
3. View and follow the installation instructions available from the Integration Guide link in the matrix.

Configure a Standalone CA Access Control iRecorder

Use this procedure to configure your iRecorder to send CA Access Control events to CA Enterprise Log Manager.

Important! A standalone iRecorder can only send its events to a single destination. If you configure an iRecorder using the procedure that follows, all of the iRecorders installed on this system will send their events *only* to the named CA Enterprise Log Manager event log store.

iRecorders that are installed on the same computer as a CA Audit client send events to the client directly. For those servers, you should modify an existing CA Audit policy to add rule actions and after configuring the CA Enterprise Log Manager SAPI collector or router adapters.

To configure the iRecorder to send events to CA Enterprise Log Manager

1. Log into the server that hosts the iRecorder as a user with Administrator or root privileges.
2. Navigate to the directory for your operating system:
 - UNIX or Linux: /opt/CA/SharedComponents/iTechnology
 - Windows: \Program Files\CA\SharedComponents\iTechnology
3. Stop the iGateway daemon or service with the following command:
 - UNIX or Linux: ./S99gateway stop
 - Windows: net stop igateway
4. Edit the iControl.conf file.

The following is a sample iControl file with the sections you need to change in boldface type:

```
<?xml version='1.0' encoding='UTF-8' standalone='no'?>
<iSponsor>
  <Name>iControl</Name>
  <ImageName>iControl</ImageName>
  <Version>4.5.0.2</Version>
  <DispatchEP>iDispatch</DispatchEP>
  <ISType>DSP</ISType>
  <Gated>>false</Gated>
  <PreLoad>>true</PreLoad>
  <RouteEvent>false</RouteEvent>
  <RouteEventHost>localhost</RouteEventHost>
  <EventsToCache>100</EventsToCache>
  <EventUseHttps>>true</EventUseHttps>
  <EventUsePersistentConnections>>true</EventUsePersistentConnections>
  <EventUsePipeline>>false</EventUsePipeline>
  <StoreEventHost max="10000">localhost</StoreEventHost>
  <RetrieveEventHost interval="60">localhost</RetrieveEventHost>
  <UID>ef1f44ef-r8splcr3596a1052-abcd28-2</UID>
  <PublicKey>Public_Key_Value</PublicKey>
  <PrivateKey>Private_Key_Value</PrivateKey>
  <EventsToQueue>10</EventsToQueue>
</iSponsor>
```

5. Specify the following RouteEvent value:

```
<RouteEvent>true</RouteEvent>
```

This entry tells the iGateway to send its events, including all iRecorder events, to the host named in the RouteEventHost tag pair.

6. Specify the following RouteEventHost value:

```
<RouteEventHost>Your_CA_Enterprise_Log_Manager_hostname</RouteEventHost>
```

This entry tells the iGateway to send its events to the CA Enterprise Log Manager server using its DNS name.

7. Save and close the file.
8. Restart the iGateway daemon or service with the following command:
 - UNIX or Linux: `./S99gateway start`
 - Windows: `net start igateway`

This action forces the iRecorder to use the new settings and starts the flow of events from the iRecorder to the CA Enterprise Log Manager server.

How to Import CA Access Control Events from a CA Audit Collector Database

The process for importing CA Access Control events from an existing SEOSDATA table includes the following:

1. Copy the LMSeosImport utility to the CA Audit Data Tools server.
2. Create an event report to determine if CA Access Control events are present in the database.
3. Run a preview of the import with CA Access Control-specific parameters.
4. Import the CA Access Control events.
5. Run CA Enterprise Log Manager queries and reports on the imported events.

Prerequisites for Importing CA Access Control Events

Before you using the LMSeosImport utility, do the following:

- Obtain a database user account with at least READ access to the CA Audit SEOSDATA table
- Copy the LMSeosImport utility to the CA Audit Data Tools server
- Access a command prompt on the Data Tools server and navigate to the appropriate directory:

Solaris: `/opt/CA/SharedComponents/iTechnology`

Windows: `\Program Files\CA\SharedComponents\iTechnology`

Copy the Import Utility to a Windows Data Tools Server

Before you can import data from your SEOSDATA table, you must copy the LMSeosImport utility from the CA Enterprise Log Manager Application installation DVD-ROM to your Windows Data Tools server.

Note: The LMSeosImport utility requires the presence of the *etsapi* and *etbase* dynamic link libraries. These files are part of the base Data Tools server installation. Before you try to use the LMSeosImport utility, ensure that the directory, Program Files\CA\eTrust Audit\bin, is included in your system PATH statement.

To copy the utility

1. Access a command prompt on the Windows Data Tools server.
2. Insert the CA Enterprise Log Manager Application installation DVD-ROM.
3. Navigate to the directory, \CA\ELM\Windows.
4. Copy the LMSeosImport.exe utility to the CA Audit Data Tools server's iTechnology directory, <drive>:\Program Files\CA\SharedComponents\iTechnology.

The utility is ready for use after you copy it to the designated directory. There is no separate installation to run.

Copy the Event Import Utility to a Solaris Data Tools Server

Before you can import data from your SEOSDATA table, you must copy the LMSeosImport utility from the CA Enterprise Log Manager Application installation DVD-ROM to your Solaris Data Tools server.

Note: The LMSeosImport utility requires the presence of the *etsapi* and *etbase* libraries. These files are part of the base Data Tools server installation. Before you try to use the LMSeosImport utility, ensure that the CA Audit install directory is included in your system PATH statement. The default directory is opt/CA/eTrustAudit/bin.

Before you run the utility, set the following environment variables with the *env* command:

- ODBC_HOME=<CA Audit data tools install directory>/odbc
- ODBCINI=<CA Audit data tools install directory>/odbc/odbc.ini

To copy the utility

1. Access a command prompt on the Solaris Data Tools server.
2. Insert the CA Enterprise Log Manager Application installation DVD-ROM.
3. Navigate to the directory, /CA/ELM/Solaris_sparc.

4. Copy the LMSeosImport utility to the CA Audit Data Tools server's iTechnology directory, /opt/CA/SharedComponents/iTechnology.

The utility is ready for use after you copy it to the designated directory and set the required environment variables. There is no separate installation to run.

Create a SEOSDATA Event Report for CA Access Control Events

To determine whether an existing SEOSDATA table contains CA Access Control events, and to decide upon an import method, you should run an event report. The logname for CA Access Control events is *eTrust Access Control*. The report lists all events in the database separated by their log names. The easiest way to import CA Access Control events is to import them based on their log name.

To create an event report

1. Create an event report so that you can see what CA Access Control events are present in the SEOSDATA table.

```
LMSeosImport -dsn My_Audit_DSN -user sa -password sa -report
```

After processing, the utility displays a report that resembles the following:

```
Import started on Fri Jan  2 15:20:30 2009
```

```
No transport specified, defaulting to SAPI...
```

```
Preparing ODBC connections...
```

```
Successfully attached to source [My_Audit_DSN]
```

```
----- SEOSDATA Event Time Range -----
```

```
Minimum TIME = 2008-05-27
```

```
Maximum TIME = 2009-01-02
```

```
----- Event Count Per Log -----
```

```
Unix : 12804
```

```
ACF2 : 1483
```

```
eTrust AC : 143762
```

```
com.ca.iTechnology.iSponsor : 66456
```

```
NT-Application : 5270
```

```
CISCO PIX Firewall : 5329
```

```
MS IIS : 6765
```

```
Netscape : 530
```

```
RACF : 14
```

```
Apache : 401
```

```
N/A : 28222
```

```
SNMP-recorder : 456
```

```
Check Point FW-1 : 1057
```

```
EiamSdk : 2790
```

```
MS ISA : 609
```

```
ORACLE : 2742
```

```
eTrust PCM : 247
```

```
NT-System : 680
```

```
eTrust Audit : 513
```

```
NT-Security : 14714
```

```
CISCO Device : 41436
```

```
SNORT : 1089
```

```
----- SEOSDATA EntryID Range -----
```



```
Minimum ENTRYID : 1
Maximum ENTRYID : 10000010243
```

Report Completed.

Successfully detached from source [My_Audit_DSN]

Exiting Import...

2. Review the report to ensure that events from CA Access Control are present.

The boldface line in this report excerpt shows that there are CA Access Control events contained in this SEOSDATA table.

```
----- Event Count Per Log -----
```

```
Unix : 12804
ACF2 : 1483
eTrust AC : 143762
com.ca.iTechnology.iSponsor : 66456
NT-Application : 5270
...
```

Preview a CA Access Control Event Import

You can use the import preview to fine-tune your import parameters. This example demonstrates two preview passes, based on a need to import events from a specific time period. The example assumes the following things:

- The CA Audit Data Tools server resides on a Windows computer.
- The database name for the SEOSDATA table is My_Audit_DSN.
- The database user name is sa with a password of sa.
- The import preview uses only the logname as the search and import criteria.

The output from the command with the -preview option sends sample import results to STDOUT. (This example uses the value *My_CA-ELM_Server* to represent a CA Enterprise Log Manager server name.)

To preview the import

1. Preview your CA Access Control event import with the following command:

```
LMSeosImport.exe -dsn My_Audit_DSN -user sa -password sa -target My_CA-ELM_Server  
-log "eTrust Access Control" -preview
```

The -preview command shows information like the following:

```
Import started on Fri Jan  2 15:35:37 2009
```

```
No transport specified, defaulting to SAPI...
```

```
Preparing ODBC connections...
```

```
Successfully attached to source [My_Audit_DSN]
```

```
No starting ENTRYID specified, using minimum ENTRYID of 1...
```

```
Import (preview) running, please wait...
```

```
.....
```

```
Import (preview) Completed (143762 records in 4 minutes 12 seconds).
```

```
----- Imported Events (preview) By Log -----
```

```
eTrust AC :      143762
```

```
Last EntryId processed: 101234500
```

```
Successfully detached from source [My_Audit_DSN]
```

```
Exiting Import...
```

The preview results note that there are a fairly large number of CA Access Control events to import. Suppose for this example that you only need to import the events that occurred in a two-month period. You can tailor the preview command to import a smaller group of events by date.

2. Change the import parameters to include a date range and run the preview again with the following command:

```
LMSeosImport.exe -dsn My_Audit_DSN -user sa -password sa -target My_CA-ELM_Server  
-log "eTrust Access Control" -mintm 2008-11-01 -maxtm 2009-12-31 -preview
```

The amended command shows information like the following:

```
Import started on Fri Jan  2 15:41:23 2009
```

```
No transport specified, defaulting to SAPI...
```

```
Preparing ODBC connections...
```

```
Successfully attached to source [My_Audit_DSN]
```

```
No starting ENTRYID specified, using minimum ENTRYID of 1...
```

```
Import (preview) running, please wait...
```

```
.....
```

```
Import (preview) Completed (143762 records in 4 minutes 37 seconds).
```

```
----- Imported Events (preview) By Log -----
```

```
eTrust AC :      2349
```

```
Last EntryId processed: 5167810102
```

```
Successfully detached from source [My_Audit_DSN]
```

```
Exiting Import...
```

This import preview shows that the date range results in a smaller subset of events to import. You are now ready to run the actual import.

More information:

[Understand the LMSeosImport Command Line](#) (see page 218)

[Preview Import Results](#) (see page 221)

Import CA Access Control Events

After you run the event report and an import preview, you are ready to import CA Access Control events from the SEOSDATA table.

To import CA Access Control events

Use the command from the preview without the -preview option to retrieve the CA Access Control events from the named date range:

```
LMSeosImport.exe -dsn [My_Audit_DSN] -user sa -password sa -target [My-CA-ELM-Server]  
-log "eTrust Access Control" -mintm 2008-11-01 -maxtm 2009-12-31
```

The utility displays results like the following:

```
Import started on Fri Jan  2 15:41:23 2009  
  
No transport specified, defaulting to SAPI...  
  
Preparing ODBC connections...  
  
Successfully attached to source [My_Audit_DSN]  
  
No starting ENTRYID specified, using minimum ENTRYID of 1...  
  
Import running, please wait...  
  
.....  
  
Import Completed (143762 records in 5 minutes 18 seconds).  
  
----- Imported Events (preview) By Log -----  
  
eTrust AC :      2241  
  
Last EntryId processed: 5167810102  
  
Successfully detached from source [My_Audit_DSN]  
  
Exiting Import...
```

More information:

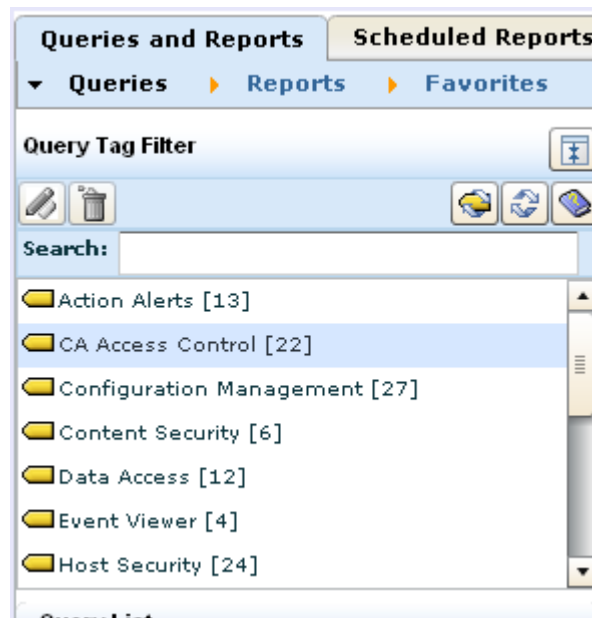
[Understand the LMSeosImport Command Line](#) (see page 218)
[Import Events from a Windows Collector Database](#) (see page 222)
[Import Events from a Solaris Collector Database](#) (see page 222)

View Queries and Reports to See CA Access Control Events

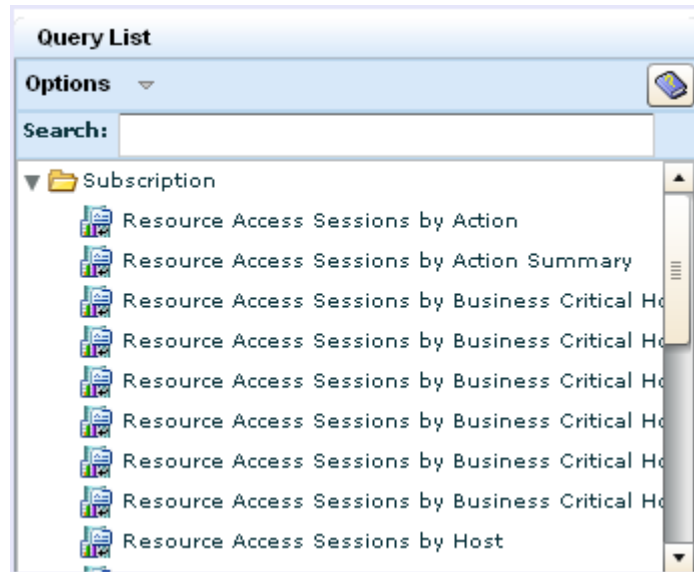
CA Enterprise Log Manager provides a number of queries and reports for examining events collected from CA Access Control. Use the procedure that follows to access CA Access Control queries and reports.

To access CA Access Control queries

1. Log into the CA Enterprise Log Manager server as a user with rights to view queries and reports.
2. Access the Queries sub-tab on the Queries and Reports tab, if it is not already displayed.



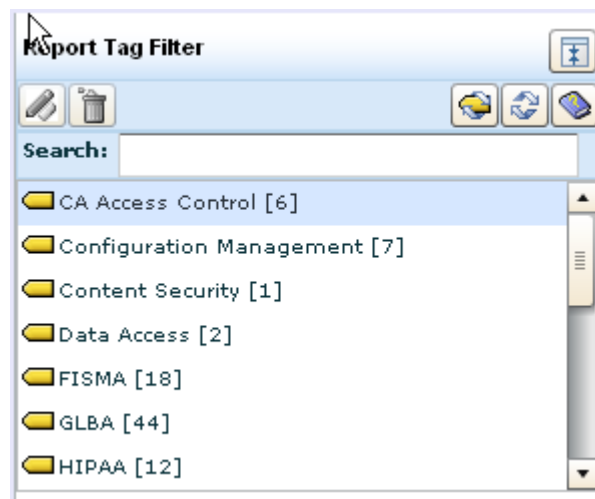
3. Click the CA Access Control query tag, to display the available queries in a list on the left.



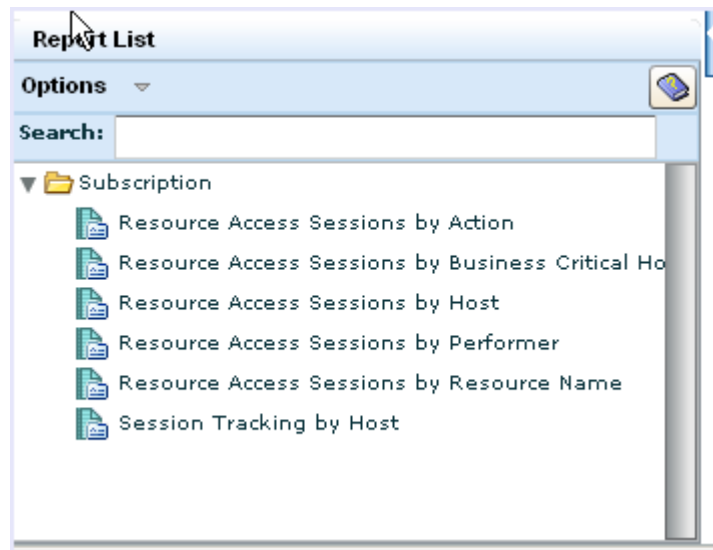
4. Select a query to view the event data.

To access CA Access Control reports

1. Log into the CA Enterprise Log Manager server as a user with rights to view queries and reports.
2. Access the Reports sub-tab on the Queries and Reports tab, if it is not already displayed.



3. Click the CA Access Control report tag to display the available reports in a list on the left.



4. Select a report to view the event data.

Securing CA Enterprise Log Manager Using CA Access Control

To secure CA Enterprise Log Manager using CA Access Control, you must install CA Access Control on CA Enterprise Log Manager. You can control user access and secure audit logs received from a product or generated by CA Enterprise Log Manager by creating rules on CA Access Control.

Note: For information about creating rules on CA Access Control, see the CA Access Control documentation set.

Example: Create a Rule that Monitors User Access to the /data Folder

Suppose that you want to create a rule on CA Access Control that monitors user access to the /data folder of CA Enterprise Log Manager, do the following:

1. Navigate to the installation path of CA Access Control.

Default Installation Path: /opt/CA/Access Control

2. Execute the following command:

```
seLang
```

The CA Access Control command line interpreter is displayed.

3. Execute the following command:

```
nr GFILE CA_ELM_DBFILES owner(nobody) warning
```

A new resource group CA_ELM_DBFILES is created for the DBFiles.

4. Execute the following command:

```
newres FILE /data/hot/* owner(nobody) defaccess(none) warning audit(failure)
```

A new resource rule is created for the CA Enterprise Log Manager hot database files.

5. Execute the following command:

```
newres FILE /data/raw/* owner(nobody) defaccess(none) warning audit(failure)
```

A new resource rule is created for the CA Enterprise Log Manager raw database files.

6. Execute the following commands:

```
editres GFILE CA_ELM_DBFILES mem+(/data/hot/*)
```

The resource rule for the CA Enterprise Log Manager hot database files is added to CA_ELM_DBFILES.

7. Execute the following commands:

```
editres GFILE CA_ELM_DBFILES mem+(/data/raw/*)
```

The resource rule for the CA Enterprise Log Manager raw database files is added to CA_ELM_DBFILES.

8. Execute the following command:

```
authorize GFILE CA_ELM_DBFILES uid(caelmservice) access(all)
```

The message 'Successfully added caelmservice to CA_ELM_DBFILES's ACL' is displayed. A rule is created to monitor user access to the /data folder of CA Enterprise Log Manager.

9. (Optional) Execute the following command to view the activities performed by a user on the hot database files and raw database files of CA Enterprise Log Manager:

```
seaudit -a
```

More information:

[Prerequisites](#) (see page 249)

Prerequisites

Before you create rules on CA Access Control, do the following:

- Verify that you have installed CA Enterprise Log Manager on a system where you want to install CA Access Control.
- Verify that you have created a Security Audit Group, Security Admin Group on CA Enterprise Log Manager to initiate the installation of CA Access Control on CA Enterprise Log Manager.
- Verify that you have created a user with administrator privileges on CA Enterprise Log Manager, and you have assigned the user to the Security Audit Group and Security Admin Group you created.
- Verify that you have installed CA Access Control using the created Security Audit Group, Security Admin Group, and administrator user credentials.
- Verify that you have created the CA Access Control audit logging config file, and you have edited the file to route generated events to the localhost by editing the **host loghost** parameter.
- Verify that you have enabled the CA Access Control audit login daemon.

Note: For information about installation procedures on Linux, see the CA Access Control documentation set.

Appendix C: CA IT PAM Considerations

This section contains the following topics:

[Scenario: How to Use CA EEM on CA Enterprise Log Manager for CA IT PAM](#)

[Authentication](#) (see page 251)

[CA IT PAM Authentication Implementation Process](#) (see page 252)

[Prepare to Implement CA IT PAM Authentication on a Shared CA EEM](#) (see page 253)

[Copy an XML File to the Management CA Enterprise Log Manager](#) (see page 253)

[Register CA IT PAM with a Shared CA EEM](#) (see page 254)

[Copy the Certificate to the CA IT PAM Server](#) (see page 255)

[Set Passwords for the Predefined CA IT PAM User Accounts](#) (see page 255)

[Install the Third-Party Components Required by CA IT PAM](#) (see page 257)

[Install the CA IT PAM Domain](#) (see page 257)

[Start the CA ITPAM Server Service](#) (see page 258)

[Launch and Log in to the CA IT PAM Server Console](#) (see page 259)

Scenario: How to Use CA EEM on CA Enterprise Log Manager for CA IT PAM Authentication

This appendix addresses the scenario where you plan to install CA IT PAM on a Windows server and share the CA EEM on the CA Enterprise Log Manager server for authentication. These procedures supplement those documented in the *CA IT Process Automation Installation Guide*.

Important! Sharing a CA EEM *is not* supported in FIPS mode as CA IT PAM is not FIPS compatible. If you upgrade your CA Enterprise Log Manager server to FIPS mode, the integration with CA IT PAM fails.

Note: If you plan to install CA IT PAM on a UNIX server or use LDAP or a local CA EEM for authentication, the documentation in this appendix is not for you. In these instances, you are not sharing the same CA EEM server. CA Enterprise Log Manager r12.1 SP1 can run in FIPS mode and it can communicate with CA IT PAM; however, those communication channels are not FIPS compatible.

For any installation scenario, download the *Installation Guide* for CA IT Process Automation Manager r2.1 SP03 from [Support Online](#). Also, download Adobe Acrobat reader so you can open the pdf.

The process that lets you use CA EEM on CA Enterprise Log Manager for CA IT PAM authentication involves two manual steps. You copy one file from the Windows server to the appliance and another file from the appliance to the Windows server. These steps are addressed in this appendix. They are not addressed in the CA IT PAM documentation.

CA IT PAM Authentication Implementation Process

The process of implementing CA IT PAM authentication using the CA EEM on the management CA Enterprise Log Manager server follows:

1. Prepare to implement CA IT PAM authentication.
 - a. Load the CA IT PAM installation package on the Windows server where you plan to install CA IT PAM.
 - b. (Optional) Change the default password for the itpamcert.p12 certificate.
2. Copy the ITPAM_eem.xml file from the host where you plan to install CA IT PAM to the CA Enterprise Log Manager appliance that includes CA EEM.
3. Register ITPAM as an application instance on the same CA EEM that CA Enterprise Log Manager uses. Running the safex command generates the itpamcert.p12 certificate and the ITPAM application instance with two user accounts, itpamadmin and itpamuser.

Note: For help on using the safex command, type ./safex.

4. Copy the itpamcert.p12 file from the CA Enterprise Log Manager appliance to the Windows host where you plan to install the CA IT PAM domain.
5. Browse to the ITPAM application and reset the passwords for itpamadmin and itpamuser.
6. Log on to the Windows server and install the third-party components using procedures documented in the *CA IT Process Automation Manager Installation Guide*.
7. Install the CA IT PAM domain using the guidelines presented in this appendix and the CA IT PAM installation instructions.
8. Start the CA ITPAM Server service.
9. Launch and log in to the CA IT PAM console.

More information:

[Prepare to Implement CA IT PAM Authentication on a Shared CA EEM](#) (see page 253)

[Copy an XML File to the Management CA Enterprise Log Manager](#) (see page 253)

[Register CA IT PAM with a Shared CA EEM](#) (see page 254)

[Copy the Certificate to the CA IT PAM Server](#) (see page 255)

[Set Passwords for the Predefined CA IT PAM User Accounts](#) (see page 255)

[Install the Third-Party Components Required by CA IT PAM](#) (see page 257)

[Install the CA IT PAM Domain](#) (see page 257)

[Start the CA ITPAM Server Service](#) (see page 258)

[Launch and Log in to the CA IT PAM Server Console](#) (see page 259)

Prepare to Implement CA IT PAM Authentication on a Shared CA EEM

After your installation package is loaded on the Windows server where you plan to install the CA IT PAM domain, you can set a password for the itpamcert.cer certificate.

To prepare to implement CA IT PAM authentication on the CA Enterprise Log Manager management server

1. Extract the CA IT PAM iso image to the Windows Server 2003 host where you plan to install CA IT PAM.

Note: You can find the CA IT PAM iso image on CD 2 of the CA IT PAM install source.

2. (Optional) Change the default password for the IT PAM certificate.

- a. Navigate to the <install path>\eem folder.

- b. Open the ITPAM_eem.xml file.

- c. Replace "itpamcertpass" in the following line:

```
<Register certfile="itpamcert.p12" password="itpamcertpass"/>
```

- d. Save the file.

Copy an XML File to the Management CA Enterprise Log Manager

The safex command generates CA IT PAM security objects from the ITPAM_eem.xml file. You must copy this file to the CA Enterprise Log Manager appliance where it can be accessed during safex processing.

To copy the ITPAM_eem.xml file to the CA Enterprise Log Manager appliance

Copy the ITPAM_eem.xml file located on the CA IT PAM installation disk to the CA Enterprise Log Manager appliance that includes CA EEM. If you extracted the iso file onto the Windows server, use Winscp to copy ITPAM_eem.xml to the /tmp directory of the appliance.

- Source file on the CA IT PAM installation disk:

ITPAM_eem.xml

- Destination path on the management CA Enterprise Log Manager:

/opt/CA/SharedComponents/iTechnology

Register CA IT PAM with a Shared CA EEM

You can register CA IT PAM with the CA EEM embedded in the CA Enterprise Log Manager management server. Registration with CA EEM adds CA IT PAM security objects.

CA IT PAM security objects added to CA EEM during registration include the following:

- The application instance, ITPAM
- Policies related to CA IT PAM access
- Groups and Users, including the predefined ITPAMAdmins, ITPAMUsers, itpamadmin, and itpamuser
- The certificate, itpamcert.p12

You can create the CA IT PAM security objects on the CA Enterprise Log Manager management server. Before you begin, obtain the caelmadmin password, if not already known.

To register CA IT PAM with the CA EEM on the CA Enterprise Log Manager management server

1. Log on to the CA Enterprise Log Manager appliance through ssh as the caelmadmin user.
2. Switch users to the root account.

```
su -
```

3. Change directories to the target path and list the contents.

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

4. Verify that the following files are listed:

- ITPAM_eem.xml
- safex

5. Execute the following command:

```
./safex -h <ELM_hostname> -u EiamAdmin -p <password> -f ITPAM_eem.xml
```

This process creates the CA IT PAM application in the CA Enterprise Log Manager management server, adds the default users, and generates the certificate needed during IT PAM installation. The certificate is generated with the password you specified in the ITPAM_eem.xml file, or if not changed, itpamcertpass.

Note: For help on using the safex command, type ./safex.

6. List the directory contents and verify that the itpamcert.cer is present.
7. Remove the CA IT PAM configuration XML file. This is recommended for security reasons.

```
rm ITPAM_eem.xml
```

Copy the Certificate to the CA IT PAM Server

When you ran the safex command from CA Enterprise Log Manager to register CA IT PAM with its CA EEM, this process generated the itpamcert.p12 certificate. You must copy this certificate to the Windows server where you plan to install the CA IT PAM domain. During CA IT PAM domain installation, you browse for this certificate file.

To copy the certificate from the CA Enterprise Log Manager appliance to the target Windows server

Copy the itpamcert.p12 file from the CA Enterprise Log Manager appliance that includes CA EEM to the host where you plan to install CA IT PAM.

- Source file on the management CA Enterprise Log Manager server:

```
/opt/CA/SharedComponents/iTechnology/itpamcert.p12
```

- Destination path on target Windows server:

```
<install path>
```

Note: You can copy this file to the path of your choice. You select this file from its location when you install the CA IT PAM domain.

Set Passwords for the Predefined CA IT PAM User Accounts

Execution of the safex command creates the following:

- IT PAM security groups:
 - ITPAMAdmins
 - ITPAMUsers
- IT PAM users
 - itpamadmin with a default password
 - itpamuser with a default password

You must reset the password for the two predefined IT PAM users.

To reset the passwords for itpamadmin and itpamuser in the IT PAM application on CA EEM

1. Browse to the URL of the server where the CA EEM used by CA Enterprise Log Manager is installed, for example, the CA Enterprise Log Manager management server:

`https://<ELM_managementserver>5250/spin/eiam`

The CA EEM logon screen appears. The Application pull-down list includes <Global>, CAELM, and ITPAM.
2. Log in to the IT PAM application:
 - a. Select ITPAM as the application.
 - b. Type EiamAdmin as the user name.
 - c. Type the password for the EiamAdmin user account.
 - d. Click Log In.
3. Click the Manage Identities tab.
4. In the Search Users dialog, type itpam for Value and click Go.

The following users appear in the list
 - itpamadmin
 - itpamuser
5. Reset the password for itpamadmin:
 - a. Select itpamadmin from the list and scroll to Authentication in the right pane.
 - b. Select Reset password.
 - c. Type the password for this account for New Password and again for Confirm Password.
 - d. Click Save.
6. Reset the password for itpamuser:
 - a. Select itpamuser from the list and scroll to Authentication in the right pane.
 - b. Select Reset password.
 - c. Type the password for this account for New Password and again for Confirm Password.
 - d. Click Save.
7. Click Log Out.

Install the Third-Party Components Required by CA IT PAM

JDK 1.6 or higher must be installed on your system before you install the third-party components. Run `Third_Party_Installer_windows.exe` on the Windows server where you plan to install CA IT PAM. See the *CA IT Process Automation Manager Installation Guide* for details.

Install the CA IT PAM Domain

Running the CA IT PAM wizard with the specifications described here links the certificate so that CA IT PAM and the CA EEM on the CA Enterprise Log Manager management server are trusted.

Have the following information at hand:

- The password for the EEM Certificate File, `itpamcert.p12`. You may have modified the default in the `ITPAM_eem.xml` file during the step, Prepare to Implement CA IT PAM Authentication on a Shared CA EEM.
- The host name of the CA Enterprise Log Manager management server. This is the server you logged into for the step, Register CA IT PAM with a Shared CA EEM.
- The `itpamadmin` password set during the Set Passwords for the Predefined CA IT PAM User Accounts step.
- The certificate password used to control access to the keys used to encrypt passwords. This is a new setting--not something that already exists.

For instructions on installing the CA IT PAM domain, see the *CA IT Process Automation Manager Installation Guide* that accompanies the software. Use the following procedure for specifics on configuring the EEM security settings.

To install the CA IT PAM domain

1. If the IT PAM installation wizard is not launched as a continuation of installing third-party components, launch `CA_ITPAM_Domain_windows.exe`.
2. Follow the instructions in your CA IT PAM documentation until you get to Select Security Server Type.
3. When the Select Security Server Type dialog appears, select EEM for Security Server and click Next.

The EEM Security Settings page appears.

4. Complete the EEM security settings as follows:
 - a. Enter the host name of the CA Enterprise Log Manager management server in the EEM server field.
 - b. Enter ITPAM in the EEM Application field.
 - c. Click Browse and navigate to the folder where you put itpamcert.p12.
 - d. Select itpamcert.p12.
 - e. Complete the EEM Certificate Password field in one of the following ways:
 - Enter the password you replaced in the ITPAM_eem.xml file during the preparation step.
 - Enter itpamcertpass, the default password.
5. Click Test EEM Settings.

The message "Performing a test...may take a few minutes" appears.
6. Click OK.

The Verify EEM settings dialog appears.
7. Enter itpamadmin as the user name. Enter the password you set for the itpamadmin user account and click OK.
8. Click Next. Follow IT PAM documented instructions to complete the rest of the wizard.

Start the CA ITPAM Server Service

Start the CA ITPAM Server service so that you and others can launch the CA IT PAM server.

To start the CA ITPAM Server service

1. Log on to the Windows server where you installed the CA IT PAM domain.
2. From the Start menu, select Programs, ITPAM Domain, Start Server Service.

Note: If this menu option is not displayed, select Administrative Tools, Component Services. Click Services, click CA IT PAM Server, and click Start the service.

Launch and Log in to the CA IT PAM Server Console

You can launch the CA IT PAM server from a browser on any system where Java JRE 1.6 or JDK 1.6 api is installed and integrated.

To launch the CA IT PAM management console

1. Enter the following URL in the address bar of a browser:

`http://<itpam_server_hostname>:8080/itpam/`

The CA IT Process Automation Manager logon screen appears.

2. Enter itpamadmin in the User Login field.
3. Enter the password you assigned for this user account in the Password field.
4. Click Log In.

The CA EEM on the CA Enterprise Log Manager appliance authenticates your login credentials and opens the CA IT Process Automation Manager.

For details on integrating and using CA IT PAM with CA Enterprise Log Manager, see the "Working with CA IT PAM Event/Output Processes" section of the Action Alerts chapter in the *CA Enterprise Log Manager Administration Guide*.

Appendix D: Disaster Recovery

This section contains the following topics:

[Disaster Recovery Planning](#) (see page 261)

[About Backing Up the CA EEM Server](#) (see page 262)

[Back Up a CA EEM Application Instance](#) (see page 262)

[Restore a CA EEM Server for Use with CA Enterprise Log Manager](#) (see page 263)

[Back Up a CA Enterprise Log Manager Server](#) (see page 264)

[Restore a CA Enterprise Log Manager Server from Backup Files](#) (see page 265)

[Restore a CA Enterprise Log Manager Server After Subscription Update](#) (see page 266)

[Replace a CA Enterprise Log Manager Server](#) (see page 266)

Disaster Recovery Planning

Planning for disaster recovery is a necessary part of every good network administration plan. CA Enterprise Log Manager disaster recovery planning is relatively simple and straightforward. The key to successful disaster recovery for CA Enterprise Log Manager is in keeping regular backups.

You need to make backups of the following information:

- CA Enterprise Log Manager application instance on the management server
- /opt/CA/LogManager/data folder on each CA Enterprise Log Manager server
- Certificate files in the /opt/CA/SharedComponents/iTechnology folder on each CA Enterprise Log Manager server

If maintaining high-throughput levels is critical to your implementation, you may choose to maintain a reserve server that has the same hardware characteristics as the one on which you install your other CA Enterprise Log Manager servers. If one CA Enterprise Log Manager server is disabled, you can install another one using the exact same name. When the new server starts, it receives the necessary configuration files from the management server. If this level of performance is not crucial to your implementation, you can install a CA Enterprise Log Manager server on any blank server that is capable of hosting the base operating system and meets the minimum memory and hard disk requirements.

More information about hardware and software requirements is available in the *CA Enterprise Log Manager Release Notes*.

The internal CA EEM server, installed on the management server, also has its own failover configuration processes for ensuring continuity of operations, covered in detail in the *CA EEM Getting Started Guide*.

About Backing Up the CA EEM Server

The configuration for each CA Enterprise Log Manager server, agent, and connector as well as queries, reports, alerts, and so forth is maintained separately in the management CA Enterprise Log Manager server's CA EEM repository. The key to successful server recovery is in maintaining regular backups of information stored in the CA Enterprise Log Manager application instance.

An *application instance* is a common space in the CA EEM repository that stores the following information:

- Users, groups, and access policies
- Agent, integration, listener, connector and saved configurations
- Customized queries, reports, and suppression and summarization rules
- Federation relationships
- Binary code management information
- Encryption keys

You can perform the CA EEM backup procedure from within the CA EEM web browser interface. Typically, all CA Enterprise Log Manager servers in an enterprise use the same application instance. The default CA Enterprise Log Manager application instance value is CAELM. You can install CA Enterprise Log Manager servers with different application instances, but you can only federate those servers that share the same application instance. Servers configured to use the same CA EEM server but with different application instances share only the user store, password policies, and global groups.

The *CA EEM Getting Started* has more information about backup and restore operations.

Back Up a CA EEM Application Instance

You can perform a backup of a CA Enterprise Log Manager application instance from the internal CA EEM server on the management server.

To back up an application instance

1. Access the CA EEM server with the following URL:

`https://<servername>:5250/spin/eiam`

2. Expand the Application list on the login page and select the application instance name you used when you installed your CA Enterprise Log Manager servers.

The default application instance name for CA Enterprise Log Manager is CAELM.

3. Log in as the EiamAdmin user or a user with the CA EEM Administrator role.
4. Access the Configure tab and then select the EEM Server subtab.
5. Select the Export Application item in the left side navigation pane.
6. Select all options except the check box, Override the Max Search Size.

Note: If you are using an external directory, do not select the options, Global Users, Global Groups, and Global Folders.

7. Click Export to create an XML export file for the application instance.

The File Download dialog displays the file name, *<AppInstanceName>.xml.gz*, for example CAELM.xml.gz and a Save button.

8. Click Save and select your backup location on a mapped, remote server. Or save the file locally and then copy or move this file to your backup location on another server.

Restore a CA EEM Server for Use with CA Enterprise Log Manager

You can restore a CA Enterprise Log Manager application instance to a management server. Restoring the management server's CA EEM functionality involves running the safex utility which imports the backed up application instance.

To restore a management server's CA EEM functionality from a backup

1. Install the CA Enterprise Log Manager soft appliance on a new hardware server.
2. Access a command prompt and navigate to the directory, */opt/CA/LogManager/EEM*.
3. Copy the backup file, *<AppinstanceName>.xml.gz*, to this directory from your external backup server.
4. Run the following command to retrieve the XML export file:

```
gunzip <AppinstanceName>.xml.gz
```

5. Execute the following command to restore the export file to the new management server

```
./safex -h eemserverhostname -u EiamAdmin -p password -f AppinstanceName.xml
```

If you are running in FIPS mode, be sure to include the `-fips` option.

6. Navigate to the directory, `/opt/CA/ELMAgent/bin`.
7. Replace the default `AgentCert.cer` file with the backed-up file, `CAELM_AgentCert.cer` to ensure proper agent startup.

Back Up a CA Enterprise Log Manager Server

You can back up an entire CA Enterprise Log Manager server from the `/opt/CA/LogManager/data` folder. This data folder is a symbolic link to the data folder under root directory (`/data`).

To back up a CA Enterprise Log Manager server

1. Log into the CA Enterprise Log Manager server as the `caelmadmin` user.
2. Access the root account using the `su` utility.
3. Navigate to the directory, `/opt/CA/LogManager`.
4. Execute the following TAR command to create a backup copy of the CA Enterprise Log Manager server files:

```
tar -hczvf backupData.tgz /data
```

This command creates the compressed output file, `backupData.tgz`, using the files from the `/data` directory.

5. Navigate to the directory, `/opt/CA/SharedComponents/iTechnology`.
6. Execute the following TAR command to create a backup copy of the digital certificates (all files with a `.cer` file extension):

```
tar -zcvf backupCerts.tgz *.cer
```

This command creates the compressed output file, `backupCerts.tgz`.

```
tar -hczvf backupCerts.tgz /data
```


Restore a CA Enterprise Log Manager Server from Backup Files

You can restore a CA Enterprise Log Manager server from backup files after you install the CA Enterprise Log Manager soft appliance on the new server.

To restore a CA Enterprise Log Manager server from backups

1. Stop the iGateway process on the new server.

To do this, navigate to the `/opt/CA/SharedComponents/iTechnology` folder and execute the following command:

```
./S99igateway stop
```

2. Copy the `backupData.tgz` and `backupCerts.tgz` files to the directory, `/opt/CA/LogManager` on the new server.
3. Expand the contents of the `backupData.tgz` file with the following command:

```
tar -xzvf backupData.tgz
```

This command overwrites the contents of the `data` folder with the contents of the backup file.

4. Navigate to the directory, `/opt/CA/SharedComponents/iTechnology`.
5. Expand the contents of the `backupCerts.tgz` file with the following command:

```
tar -xzvf backupCerts.tgz
```

This command overwrites the certificate (`.p12`) files in the current folder with the certificate files from the backup file.

6. Start the igateway process.

To do this, execute the following command:

```
./S99igateway start
```

Restore a CA Enterprise Log Manager Server After Subscription Update

You can restore a CA Enterprise Log Manager server after a failed or otherwise undesirable subscription update. Each subscription download creates backup files labeled with the date of the backup. This procedure restores only the log manager server itself, not EEM or other components.

To restore a server after subscription update

1. Stop the iGateway process on the new server.

To do this, navigate to the `/opt/CA/SharedComponents/iTechnology` folder and execute the following command:

```
./S99gateway stop
```

2. Navigate to the directory, `/opt/CA/SharedComponents/iTechnology`.
3. Enter the following command

```
sh ./restore.sh <backupdate> <backupversion>
```

For example:

```
sh ./restore.sh 22-Sep-2010 12.0.45.10
```

4. Navigate to the directory, `/opt/CA/SharedComponents/iTechnology`.
5. Start the igateway process.

To do this, execute the following command:

```
./S99gateway start
```

Replace a CA Enterprise Log Manager Server

Use this procedure to replace a collection CA Enterprise Log Manager server after a major disaster or failure. This procedure allows you to recover from a disaster situation by creating a new CA Enterprise Log Manager server to resume event collection in place of the failed server.

Note: This procedure does not recover event data that resides in the failed server's event log store. Use regular data recovery techniques to retrieve event data from the downed server's event log store.

To recover from a disabled CA Enterprise Log Manager server

1. Install the CA Enterprise Log Manager software appliance on a different server using the same host name that you assigned to the downed server.

When the install asks for the CA EEM application instance name, be sure that you use the same application instance that the old server used. This successful registration enables the CA EEM server to synchronize the configuration.

2. Start the new CA Enterprise Log Manager server and log in as the default administrative user, EiamAdmin.

When the new CA Enterprise Log Manager server starts, it automatically connects to the CA EEM server, which then downloads the configuration files. After receiving the configuration files, the new CA Enterprise Log Manager server resumes log collection.

Appendix E: CA Enterprise Log Manager and Virtualization

This section contains the following topics:

[Deployment Assumptions](#) (see page 269)

[Creating CA Enterprise Log Manager Servers Using Virtual Machines](#) (see page 270)

[Creating CA Enterprise Log Manager Servers using Virtual Appliances](#) (see page 282)

Deployment Assumptions

Using CA Enterprise Log Manager in a virtual environment, or a mixed environment that includes both appliance-class and virtual servers, assumes the following things:

- In an all-virtual environment, install at least one CA Enterprise Log Manager server as a management server. This management server manages configurations, subscription content, user-defined content, and communicates with agents. The management server does not receive event logs or handle queries and reports.
- In a mixed environment, install the management CA Enterprise Log Manager server on certified hardware.
- Each virtual machine host must have four, dedicated processors, which is the maximum permitted by VMware ESX Server 3.5.

Considerations

A dedicated CA Enterprise Log Manager server achieves optimal performance with eight or more processors. VMware ESX Server allows up to four processors for a single virtual machine. To attain performance similar to an eight-processor, dedicated server, install CA Enterprise Log Manager on two or more virtual machines and then federate them for consolidated reporting.

Two CA Enterprise Log Manager servers running as guests under VMware ESX Server v3.5 approximate the capacity of a single, dedicated CA Enterprise Log Manager server. Use the following table to help plan your virtual network:

CA Enterprise Log Manager Server Role	Number of Processors (minimum)	CPU Speed in GHz (per CPU)	Total Memory in GB (minimum requirement)
Management	8	3	8

CA Enterprise Log Manager Server Role	Number of Processors (minimum)	CPU Speed in GHz (per CPU)	Total Memory in GB (minimum requirement)
Reporting	8	3	8
Collection	4	3	8

Note: The maximum events per second is 1K in the medium deployment configuration is 1K, and is 5K in the large deployment configuration.

Creating CA Enterprise Log Manager Servers Using Virtual Machines

You can create virtual CA Enterprise Log Manager servers for your event log collection environment using the following scenarios:

- Adding virtual servers to an existing CA Enterprise Log Manager environment - creating a mixed environment
- Creating a virtual log collection environment
- Cloning and deploying virtual CA Enterprise Log Manager servers for rapid scalability
- Creating CA Enterprise Log Manager servers using virtual appliances

More information

[Adding Virtual Servers to Your Environment](#) (see page 286)

[Creating a Completely Virtual Environment](#) (see page 309)

[Deploying Virtual Servers Rapidly](#) (see page 332)

Adding Virtual Servers to Your Environment

If you already have an existing CA Enterprise Log Manager implementation, you can add virtual CA Enterprise Log Manager collection servers to handle an increased event volume in your network. This scenario assumes that you have already installed a CA Enterprise Log Manager management server and one or more CA Enterprise Log Manager servers for collection and reporting.

Note: To achieve the best performance, install CA Enterprise Log Manager on virtual servers to handle collection and reporting tasks only.

The process to add virtual collection servers to your environment includes the following procedures:

1. Create a new virtual machine.
2. Add virtual disk drives.
3. Install CA Enterprise Log Manager in the virtual machine.
4. Configure the CA Enterprise Log Manager server as described in the installation section.

After you install the virtual collection server, you can add it to your federation for querying and reporting.

Create a New Virtual Machine

Use this procedure to create a new virtual machine using the VMware Infrastructure Client. Use four processors for each virtual CA Enterprise Log Manager server to achieve acceptable performance.

To create a virtual machine

1. Access the VMware Infrastructure Client.
2. Right-click the ESX host in the left pane and select New Virtual Machine to invoke the new virtual machine wizard. This action displays a configuration type dialog.
3. Select Custom configuration and click Next. A name and location dialog appears.
4. Enter a name for the CA Enterprise Log Manager server you will install on this virtual machine and click Next.
5. Specify the storage settings for your virtual machine and then click Next.

Verify that your storage settings are large enough for your CA Enterprise Log Manager server. We recommend a minimum of 500 GB.

Note: You will set up additional virtual disk drives to store collected event logs in another procedure.

6. Select Red Hat Enterprise Linux 5 (32 bit) as your Guest Operating System and click Next.
7. Select 4 as the number of virtual processors from the drop-down list, Number of virtual processors.

Your physical host server must be able to devote four, physical CPUs *exclusively* to this CA Enterprise Log Manager instance. Click Next.

8. Configure the virtual machine memory size and then click Next. The *minimum* acceptable memory size for CA Enterprise Log Manager is 8 GB or 8192 MB.

9. Configure your network interface connection (NIC).CA Enterprise Log Manager requires at least one network connection. Select NIC x from the available NIC list, and set the Adapter value to Flexible.

Note: You do not have to configure a separate NIC for each CA Enterprise Log Manager server hosted on this physical server. However, you do have to allocate and assign a static IP address for each one.

10. Select the option, Connect at Power On, and then click Next. The I/O Adapter Types dialog appears.
11. Select LSI Logic for the I/O Adapter and then click Next. The Select a Disk dialog appears.
12. Select the option, Create a new virtual disk, and then click Next. A disk capacity and location dialog appears.
13. Specify your Disk Capacity and Location and then click Next. An advanced options dialog appears.

You can either store this disk with your virtual machine or you can specify another location. We recommend a minimum of 500 GB.
14. Accept the default values for the Advanced Options and click Next.
15. Confirm your settings and click Finish to create the new virtual machine.

Add Virtual Disk Drives

Use this procedure to add virtual disk drives for event log storage. Use these same settings regardless of the role a specific CA Enterprise Log Manager server plays in your network.

To edit the settings

1. Right-click your virtual machine in the VMware Infrastructure Client and select Edit Settings.

The Virtual Machine Properties dialog appears.
2. Highlight the CD/DVD Drive 1 properties.
3. Click the Host Device option button, and select your DVD-ROM drive from the drop-down list.
4. Select the Device Status option, Connect at power on.
5. Click Add to launch the Add Hardware Wizard and add a second hard disk.
6. Highlight Hard Disk in the device list and click Next. The Select a Disk dialog appears.
7. Select the option, Create a new virtual disk, and click Next.

8. Specify the size of your new disk and select the option, Specify a datastore to set its location.

CA Enterprise Log Manager detects this additional drive during installation and assigns it to data storage. We recommend maximizing the amount of storage that you can make available to CA Enterprise Log Manager.

Note: The default Block Size setting in VMware ESX Server is 1 MB, which limits the maximum disk space that you can create to 256 GB. If you need more space, up to 512 GB, increase the Block Size setting to 2 MB using this command:

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

Restart the ESX Server for the new setting to take effect. More information about this command and other commands is available in the VMware ESX Server documentation.

Click Next to display the Specify Advanced Options dialog.

9. Accept the default values for the Advanced Options and click Next. The Ready to Complete dialog appears.
10. Click Finish to store your changes to this virtual machine. This action returns you to the VMware Infrastructure Client dialog.

Install CA Enterprise Log Manager on the Virtual Machine

Use this procedure to install CA Enterprise Log Manager on a virtual machine that you created previously.

You can configure a virtual or dedicated CA Enterprise Log Manager server after installation to serve in one of several functional roles such as management, collection, or reporting. If you install a CA Enterprise Log Manager management server, do not use it to receive event logs or to run queries and reports. Install separate virtual CA Enterprise Log Manager servers to act as reporting and collection servers for the best performance.

Review the normal installation instructions before installing CA Enterprise Log Manager in a virtual environment. The installation worksheet helps you to gather the information you need.

To install CA Enterprise Log Manager on a virtual machine

1. Load your CA Enterprise Log Manager OS Install disk in the physical DVD-ROM drive, or locate the directory where you copied the installation image.
2. Highlight your virtual machine in the virtual machine inventory list, right-click on it, and select Power On.
3. Proceed with the normal CA Enterprise Log Manager installation.
4. Configure the installed CA Enterprise Log Manager server for the functional role you intend, using the information in the section on installing a CA Enterprise Log Manager server.

More information

[Install CA Enterprise Log Manager](#) (see page 69)

Creating a Completely Virtual Environment

If you do not yet have a CA Enterprise Log Manager environment implemented, you can create an all-virtual log collection environment. This scenario assumes that have a sufficient number of physical servers available, each with a group of at least four processors, to install each of the intended CA Enterprise Log Manager servers.

Install one CA Enterprise Log Manager server to act as a management server. During configuration, do not send event logs to this server or use this server to generate reports. Configuring your environment in this way maintains the event log collection throughput required for enterprise-level production.

Generally, you install two, four-processor CA Enterprise Log Manager servers in place of each of the appliance-class servers you would typically install when using certified hardware. (Appliance-class servers have a minimum of eight processors.)

The process you follow to create a virtual environment includes the following procedures.

1. Create a new virtual machine for each of the CA Enterprise Log Manager servers you intend to install.
2. Add virtual disk drives.
3. Install a virtual CA Enterprise Log Manager server for management functions on one of the virtual machine hosts.
4. Install two or more CA Enterprise Log Manager servers for collection and reporting.
5. Configure the CA Enterprise Log Manager servers as described in the section on installing a CA Enterprise Log Manager server.

Create a New Virtual Machine

Use this procedure to create a new virtual machine using the VMware Infrastructure Client. Use four processors for each virtual CA Enterprise Log Manager server to achieve acceptable performance.

To create a virtual machine

1. Access the VMware Infrastructure Client.
2. Right-click the ESX host in the left pane and select New Virtual Machine to invoke the new virtual machine wizard. This action displays a configuration type dialog.
3. Select Custom configuration and click Next. A name and location dialog appears.

4. Enter a name for the CA Enterprise Log Manager server you will install on this virtual machine and click Next.
5. Specify the storage settings for your virtual machine and then click Next.
Verify that your storage settings are large enough for your CA Enterprise Log Manager server. We recommend a minimum of 500 GB.
Note: You will set up additional virtual disk drives to store collected event logs in another procedure.
6. Select Red Hat Enterprise Linux 5 (32 bit) as your Guest Operating System and click Next.
7. Select 4 as the number of virtual processors from the drop-down list, Number of virtual processors.
Your physical host server must be able to devote four, physical CPUs *exclusively* to this CA Enterprise Log Manager instance. Click Next.
8. Configure the virtual machine memory size and then click Next. The *minimum* acceptable memory size for CA Enterprise Log Manager is 8 GB or 8192 MB.
9. Configure your network interface connection (NIC).CA Enterprise Log Manager requires at least one network connection. Select NIC x from the available NIC list, and set the Adapter value to Flexible.
Note: You do not have to configure a separate NIC for each CA Enterprise Log Manager server hosted on this physical server. However, you do have to allocate and assign a static IP address for each one.
10. Select the option, Connect at Power On, and then click Next. The I/O Adapter Types dialog appears.
11. Select LSI Logic for the I/O Adapter and then click Next. The Select a Disk dialog appears.
12. Select the option, Create a new virtual disk, and then click Next. A disk capacity and location dialog appears.
13. Specify your Disk Capacity and Location and then click Next. An advanced options dialog appears.
You can either store this disk with your virtual machine or you can specify another location. We recommend a minimum of 500 GB.
14. Accept the default values for the Advanced Options and click Next.
15. Confirm your settings and click Finish to create the new virtual machine.

Add Virtual Disk Drives

Use this procedure to add virtual disk drives for event log storage. Use these same settings regardless of the role a specific CA Enterprise Log Manager server plays in your network.

To edit the settings

1. Right-click your virtual machine in the VMware Infrastructure Client and select Edit Settings.
The Virtual Machine Properties dialog appears.
2. Highlight the CD/DVD Drive 1 properties.
3. Click the Host Device option button, and select your DVD-ROM drive from the drop-down list.
4. Select the Device Status option, Connect at power on.
5. Click Add to launch the Add Hardware Wizard and add a second hard disk.
6. Highlight Hard Disk in the device list and click Next. The Select a Disk dialog appears.
7. Select the option, Create a new virtual disk, and click Next.
8. Specify the size of your new disk and select the option, Specify a datastore to set its location.

CA Enterprise Log Manager detects this additional drive during installation and assigns it to data storage. We recommend maximizing the amount of storage that you can make available to CA Enterprise Log Manager.

Note: The default Block Size setting in VMware ESX Server is 1 MB, which limits the maximum disk space that you can create to 256 GB. If you need more space, up to 512 GB, increase the Block Size setting to 2 MB using this command:

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

Restart the ESX Server for the new setting to take effect. More information about this command and other commands is available in the VMware ESX Server documentation.

Click Next to display the Specify Advanced Options dialog.

9. Accept the default values for the Advanced Options and click Next. The Ready to Complete dialog appears.
10. Click Finish to store your changes to this virtual machine. This action returns you to the VMware Infrastructure Client dialog.

Install CA Enterprise Log Manager on the Virtual Machine

Use this procedure to install CA Enterprise Log Manager on a virtual machine that you created previously.

You can configure a virtual or dedicated CA Enterprise Log Manager server after installation to serve in one of several functional roles such as management, collection, or reporting. If you install a CA Enterprise Log Manager management server, do not use it to receive event logs or to run queries and reports. Install separate virtual CA Enterprise Log Manager servers to act as reporting and collection servers for the best performance.

Review the normal installation instructions before installing CA Enterprise Log Manager in a virtual environment. The installation worksheet helps you to gather the information you need.

To install CA Enterprise Log Manager on a virtual machine

1. Load your CA Enterprise Log Manager OS Install disk in the physical DVD-ROM drive, or locate the directory where you copied the installation image.
2. Highlight your virtual machine in the virtual machine inventory list, right-click on it, and select Power On.
3. Proceed with the normal CA Enterprise Log Manager installation.
4. Configure the installed CA Enterprise Log Manager server for the functional role you intend, using the information in the section on installing a CA Enterprise Log Manager server.

More information

[Install CA Enterprise Log Manager](#) (see page 69)

Deploying Virtual CA Enterprise Log Manager Servers Rapidly

You can clone a virtual CA Enterprise Log Manager server to create a deployable image for rapid scalability of your log collection environment.

Note: To achieve the best performance, we recommend that you install CA Enterprise Log Manager on virtual servers to handle only collection tasks. Do not clone a virtual machine that contains a management CA Enterprise Log Manager server.

Before you start with this scenario, verify that you have an existing environment, or install a CA Enterprise Log Manager server to perform management functions on either a dedicated or virtual server. You must also have the correct version of VMware software to support the cloning function.

The process you follow to create and clone a virtual CA Enterprise Log Manager server for collection includes the following procedures:

1. Create a new virtual machine.
2. Add virtual disk drives.
3. Install a CA Enterprise Log Manager server in the virtual machine.
4. Clone the virtual machine that contains your new CA Enterprise Log Manager server, using the vendor-supplied instructions.

Note: Create only a full clone image. Do not use linked clones with CA Enterprise Log Manager.

5. Import the cloned virtual machine to a physical target server.

6. Update the cloned virtual machine before connecting it to the network.
7. Configure the CA Enterprise Log Manager server as described in the *Implementation Guide*.

Create a New Virtual Machine

Use this procedure to create a new virtual machine using the VMware Infrastructure Client. Use four processors for each virtual CA Enterprise Log Manager server to achieve acceptable performance.

To create a virtual machine

1. Access the VMware Infrastructure Client.
2. Right-click the ESX host in the left pane and select New Virtual Machine to invoke the new virtual machine wizard. This action displays a configuration type dialog.
3. Select Custom configuration and click Next. A name and location dialog appears.
4. Enter a name for the CA Enterprise Log Manager server you will install on this virtual machine and click Next.
5. Specify the storage settings for your virtual machine and then click Next.

Verify that your storage settings are large enough for your CA Enterprise Log Manager server. We recommend a minimum of 500 GB.

Note: You will set up additional virtual disk drives to store collected event logs in another procedure.

6. Select Red Hat Enterprise Linux 5 (32 bit) as your Guest Operating System and click Next.
7. Select 4 as the number of virtual processors from the drop-down list, Number of virtual processors.

Your physical host server must be able to devote four, physical CPUs *exclusively* to this CA Enterprise Log Manager instance. Click Next.

8. Configure the virtual machine memory size and then click Next. The *minimum* acceptable memory size for CA Enterprise Log Manager is 8 GB or 8192 MB.
9. Configure your network interface connection (NIC). CA Enterprise Log Manager requires at least one network connection. Select NIC x from the available NIC list, and set the Adapter value to Flexible.

Note: You do not have to configure a separate NIC for each CA Enterprise Log Manager server hosted on this physical server. However, you do have to allocate and assign a static IP address for each one.

10. Select the option, Connect at Power On, and then click Next. The I/O Adapter Types dialog appears.
11. Select LSI Logic for the I/O Adapter and then click Next. The Select a Disk dialog appears.
12. Select the option, Create a new virtual disk, and then click Next. A disk capacity and location dialog appears.
13. Specify your Disk Capacity and Location and then click Next. An advanced options dialog appears.

You can either store this disk with your virtual machine or you can specify another location. We recommend a minimum of 500 GB.
14. Accept the default values for the Advanced Options and click Next.
15. Confirm your settings and click Finish to create the new virtual machine.

Add Virtual Disk Drives

Use this procedure to add virtual disk drives for event log storage. Use these same settings regardless of the role a specific CA Enterprise Log Manager server plays in your network.

To edit the settings

1. Right-click your virtual machine in the VMware Infrastructure Client and select Edit Settings.

The Virtual Machine Properties dialog appears.
2. Highlight the CD/DVD Drive 1 properties.
3. Click the Host Device option button, and select your DVD-ROM drive from the drop-down list.
4. Select the Device Status option, Connect at power on.
5. Click Add to launch the Add Hardware Wizard and add a second hard disk.
6. Highlight Hard Disk in the device list and click Next. The Select a Disk dialog appears.
7. Select the option, Create a new virtual disk, and click Next.

- Specify the size of your new disk and select the option, Specify a datastore to set its location.

CA Enterprise Log Manager detects this additional drive during installation and assigns it to data storage. We recommend maximizing the amount of storage that you can make available to CA Enterprise Log Manager.

Note: The default Block Size setting in VMware ESX Server is 1 MB, which limits the maximum disk space that you can create to 256 GB. If you need more space, up to 512 GB, increase the Block Size setting to 2 MB using this command:

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

Restart the ESX Server for the new setting to take effect. More information about this command and other commands is available in the VMware ESX Server documentation.

Click Next to display the Specify Advanced Options dialog.

- Accept the default values for the Advanced Options and click Next. The Ready to Complete dialog appears.
- Click Finish to store your changes to this virtual machine. This action returns you to the VMware Infrastructure Client dialog.

Install CA Enterprise Log Manager on the Virtual Machine

Use this procedure to install CA Enterprise Log Manager on a virtual machine that you created previously.

You can configure a virtual or dedicated CA Enterprise Log Manager server after installation to serve in one of several functional roles such as management, collection, or reporting. If you install a CA Enterprise Log Manager management server, do not use it to receive event logs or to run queries and reports. Install separate virtual CA Enterprise Log Manager servers to act as reporting and collection servers for the best performance.

Review the normal installation instructions before installing CA Enterprise Log Manager in a virtual environment. The installation worksheet helps you to gather the information you need.

To install CA Enterprise Log Manager on a virtual machine

- Load your CA Enterprise Log Manager OS Install disk in the physical DVD-ROM drive, or locate the directory where you copied the installation image.
- Highlight your virtual machine in the virtual machine inventory list, right-click on it, and select Power On.
- Proceed with the normal CA Enterprise Log Manager installation.
- Configure the installed CA Enterprise Log Manager server for the functional role you intend, using the information in the section on installing a CA Enterprise Log Manager server.

More information

[Install CA Enterprise Log Manager](#) (see page 69)

Clone a Virtual CA Enterprise Log Manager Server

You can use this procedure to clone a virtual CA Enterprise Log Manager server. This procedure assumes that you already created a new virtual machine, added disk drives to it, and installed CA Enterprise Log Manager.

To clone a virtual server

1. Access the VMware VirtualCenter and locate the virtual machine that contains CA Enterprise Log Manager.
2. Turn off the virtual machine, if it is running.
3. Select the Export option and designate a location for the exported virtual machine.

VMware ESX Server offers alternative methods for cloning virtual machines. See the VMware documentation for more information.

Import a Cloned Virtual Machine to a Target Server

Use this procedure to import a clone virtual machine to another server for activation.

To import a cloned VM

1. Verify that you have network access to the target host server.
2. Access the VMware VirtualCenter from the server that hosts VMware ESX.
3. Select the Import option and then locate target server, responding to additional prompts as required.

The Import action moves the cloned virtual machine to the target server. More information is available in the VMware ESX documentation.

Update a Cloned CA Enterprise Log Manager Server Before Deployment

Use this procedure to update a cloned, virtual CA Enterprise Log Manager server.

A cloned, virtual CA Enterprise Log Manager server retains the host name you gave it during installation. However, the host name for each, active CA Enterprise Log Manager server must be unique within your log collection implementation. So, before you can activate a cloned, virtual server, change the host name and IP address of the server with the *Rename_ELM.sh* script.

The update script performs actions including the following:

- Automatically stops and restarts the default agent
- Automatically stops and restarts the iGateway service
- Prompts you to change the hostname, IP address, and DNS IP address
- Automatically updates configuration files with encrypted passwords for the various certificates

To update a cloned virtual CA Enterprise Log Manager server

1. Log in to the physical target server as root.
2. Access the Application ISO image or DVD and navigate to the directory, /CA/Linux_x86.

You can also find the script in the file system of an installed CA Enterprise Log Manager server. The script resides in the directory, opt/CA/LogManager.
3. Copy the script, Rename_ELM.sh, to the target server.
4. Change the information for virtual CA Enterprise Log Manager server with the following command:

`./Rename_ELM.sh`
5. Respond to the prompts.
6. Start the virtual machine that contains the updated virtual server.

Creating CA Enterprise Log Manager Servers using Virtual Appliances

You can deploy CA Enterprise Log Manager as a virtual appliance in the Open Virtualization Format (OVF). The provisioning of virtual appliance requires less time than the time required to install or clone a CA Enterprise Log Manager server on a virtual machine.

About CA Enterprise Log Manager Virtual Appliances

OVF is an open standard for packaging and distributing virtual appliances. CA Enterprise Log Manager uses the Virtual Machine Disk (VMDK) file format based on OVF. The OVF package contains the following files:

OVF Descriptor XML File

An OVF descriptor XML file with the .ovf extension. This file contains the virtual hardware specifications, CA Enterprise Log Manager configuration parameters, and the license agreement.

Virtual Disk Files

The following VMware vSphere virtual disk files, which contain disk image files used for deploying the virtual appliance:

- CA Enterprise Log Manager 1.vmdk
- CA Enterprise Log Manager 2.vmdk
- CA Enterprise Log Manager 3.vmdk

Manifest File

The CA Enterprise Log Manager.mf file, which contains the signature of all the files.

Note: We highly recommend that you do not modify the virtual disk files or the manifest file, as modifying them might affect the performance of the virtual appliance.

By default, the VMware vSphere Client reads the details imported using the OVF template and provisions the virtual appliance.

How to Use the Virtual Appliance

You can use virtual appliance to create virtual CA Enterprise Log Manager servers for your event log collection environment using the following scenarios:

- Adding virtual servers to an existing CA Enterprise Log Manager environment - creating a mixed environment
- Creating a virtual log collection environment
- Deploying virtual CA Enterprise Log Manager servers for rapid scalability

Use VMware vSphere Client to install the virtual appliance, manually or silently. The OVF descriptor file contains the configuration parameters to configure CA Enterprise Log Manager. Enter a value for each configuration parameter during the installation.

Virtual Appliance Installation Worksheet

Before you install the virtual appliance, gather the information in the following table. After you complete the worksheet, you can use it as you work through the installation prompts. You can print and complete a separate worksheet for each CA Enterprise Log Manager server you plan to install.

Required information	Value	Comments
Host Specific Settings		
Host Name	<i>hostname for this CA Enterprise Log Manager server</i> For example: CA-ELM1	Specify the host name for this server using only supported characters for hosts. Industry standards recommend A-Z (case-insensitive), 0-9, and hyphen, where the first character is a letter and the final character is alphanumeric. Do not use the underscore character in a host name, or append a domain name to this host. Note: The host name must not exceed 15 characters.
Root Password	<i>new root password</i>	Create and confirm a new root password for this server.
IP Address	<i>relevant IPv4 address</i>	Enter a valid IP address for this server.
Subnet Mask	<i>relevant IP address</i>	Enter a valid subnet mask for use with this server.
Default Gateway	<i>relevant IP address</i>	Enter a valid default gateway for use with this server.
DNS Servers	<i>relevant IPv4 addresses</i>	Enter one or more DNS server IP addresses in use in your network. The list is comma-separated with no spaces between entries. If your DNS servers use IPv6 addressing, enter these addresses in that format.
Domain Name	<i>your domain name</i>	Enter the qualified domain name in which this server operates, for example, mycompany.com. Note: The domain name must be registered with the Domain Name Server (DNS) server in your network to enable resolution of the hostname to IP address.
EULA	Accept	Read through the CA license agreement, paging down until you reach the question, Click on Accept to Accept the agreement.

Required information	Value	Comments
Time Zone	<i>your desired time zone</i>	Select the time zone where this server resides.
NTP Server Location	<i>relevant hostname or IP address</i>	Enter the host name or the valid IP address of the NTP server from which the CA Enterprise Log Manager server gets date and time information.
Application Specific Settings		
Location of CA EEM Server	<p>Local - for the first installed server (management server)</p> <p>Remote - for each additional server</p>	<p>Indicate whether you plan to use a local or a remote CA EEM server.</p> <p>For a management CA Enterprise Log Manager server, choose Local. The installation prompts you to create a password for the default EiamAdmin user account.</p> <p>For each additional server, choose Remote. The installation prompts you for the management server name.</p> <p>Regardless of whether you chose local or remote, you must use the EiamAdmin account ID and password to log on to each CA Enterprise Log Manager server the first-time.</p>
Host Name or IP Address of the remote CA EEM Server	<i>IP address or hostname</i>	<p>Enter this value only if you select Remote in the Local or Remote server option.</p> <p>Enter the IP address or host name of the management CA Enterprise Log Manager server that you installed first.</p> <p>The host name must be registered with the DNS Server.</p> <p>If you want to use a local CA EEM server, the default value is none.</p>

Required information	Value	Comments
Password for CA EEM Server	<i>EiamAdmin account password</i>	<p>Record the password for the default administrator account, EiamAdmin.</p> <p>Your CA Enterprise Log Manager server requires these account credentials for the initial login.</p> <p>If you are installing the management server, you are creating and confirming a new EiamAdmin password here.</p> <p>Make a note of this password as you must use it during the installations of other CA Enterprise Log Manager servers and agents.</p> <p>Note: The password you enter here is also the initial password for the default caelmadmin account that you use to access the CA Enterprise Log Manager server directly through ssh.</p> <p>You can create additional administrator accounts to access the CA EEM functions after installation, if desired.</p>
FIPS	Yes or No	<p>Specifies if the virtual appliance must run in FIPS mode or non-FIPS mode. If you choose to use a local CA EEM server, you can choose any mode. If you choose to use a remote CA EEM server, you must choose the mode that the remote CA EEM server uses.</p>

Adding Virtual Servers to Your Environment

If you already have an existing CA Enterprise Log Manager implementation, you can add virtual CA Enterprise Log Manager collection servers to handle an increased event volume in your network. This scenario assumes that you have already installed a CA Enterprise Log Manager management server and one or more CA Enterprise Log Manager servers for collection and reporting.

Note: To achieve the best performance, install CA Enterprise Log Manager on virtual servers to handle collection and reporting tasks only.

The process to add virtual collection servers to your environment includes the following procedures:

1. Download the CA Enterprise Log Manager virtual appliance package.
2. Install a CA Enterprise Log Manager server using virtual appliance.
3. Configure the CA Enterprise Log Manager server as described in the installation section.

After you install the virtual collection server, you can add it to your federation for querying and reporting.

Important! If you want to provision a CA Enterprise Log Manager server using the virtual appliance, the Application Instance Name of the primary CA Enterprise Log Manager server must be CAELM.

Download the Virtual Appliance Package

The distribution image for the CA Enterprise Log Manager virtual appliance is available from Support Online from the Downloads link. There are five files that you must download:

- The manifest file
- The .ovf file
- Three virtual disk files

Install a CA Enterprise Log Manager Server Manually

When you install the virtual appliance manually, perform the following tasks:

1. Deploy an OVF template.
2. Set the Paravirtualization and Resource settings.
3. Power on the provisioned CA Enterprise Log Manager server.

Deploy an OVF Template

You can specify the properties of virtual appliance in an OVF template. VMware uses this template to provision a CA Enterprise Log Manager server. Use the VMware vSphere Client to deploy the OVF template.

Note: The screenshots in the following procedures contain sample data for your reference. These sample screenshots are in reference to VMware vSphere Client 4.0.0. We recommend that you specify data appropriate to your environment.

To deploy an OVF template

1. Click Start, All Programs, VMware vSphere Client on the computer where VMware vSphere Client is installed.

The VMware vSphere Client dialog opens.

2. Enter the IP address or host name of the VMware vCenter Server you want to connect in the IP address/Name field.
3. Enter the login credentials in the User name and Password fields.
4. Click Logon.

The application window opens.

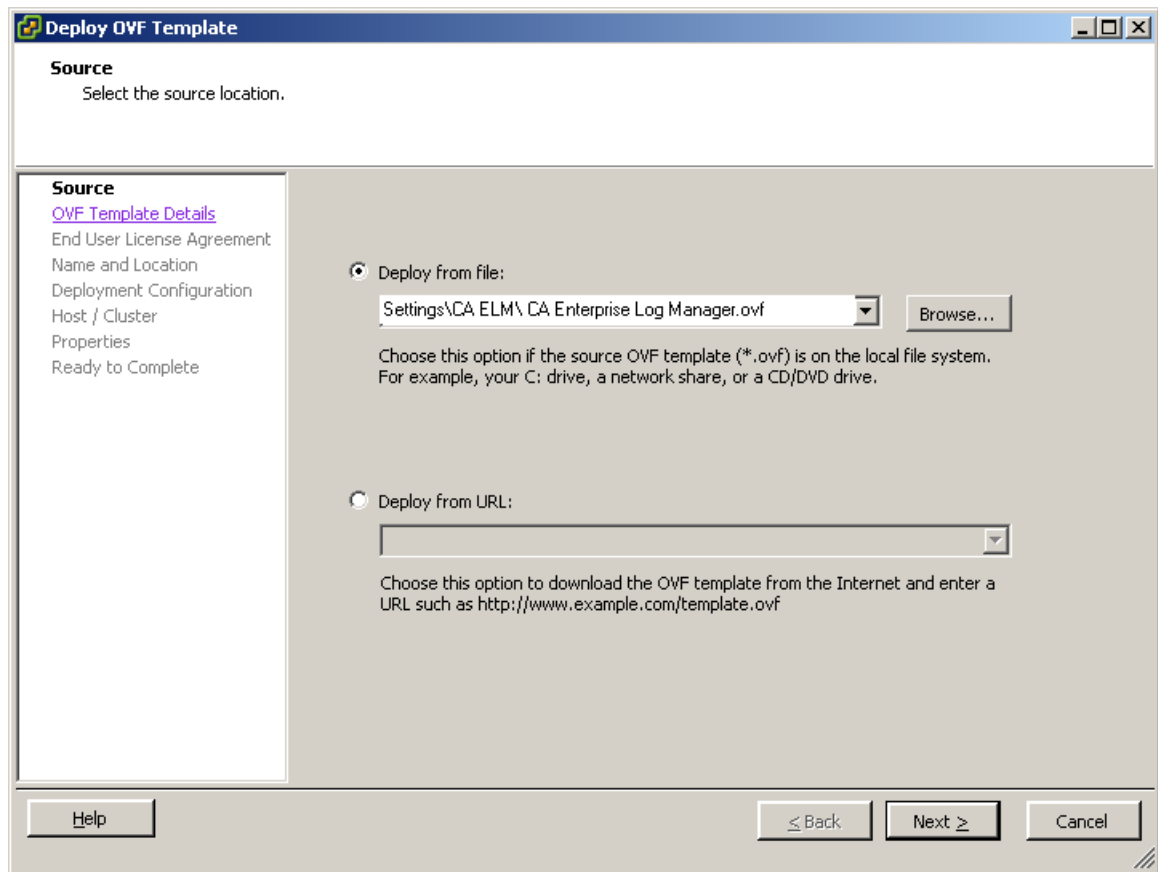
5. Select the location where you want to provision a CA Enterprise Log Manager server under a Datacenter in the left pane.
6. Click File, Deploy OVF Template.

The Deploy OVF Template window appears. By default, the Deploy OVF Template window displays the Source page. You must enter the location of the OVF template in this page.

Note: The pages displayed in the Deploy OVF Template window vary according to the VMware vSphere Client version and settings you are using. For more information about deploying a OVF template, go to www.vmware.com.

7. Choose the Deploy from file option, and click Browse to select the location of the OVF template.
8. Navigate to the OVF template location from the Open dialog, select the OVF template, and click Open.

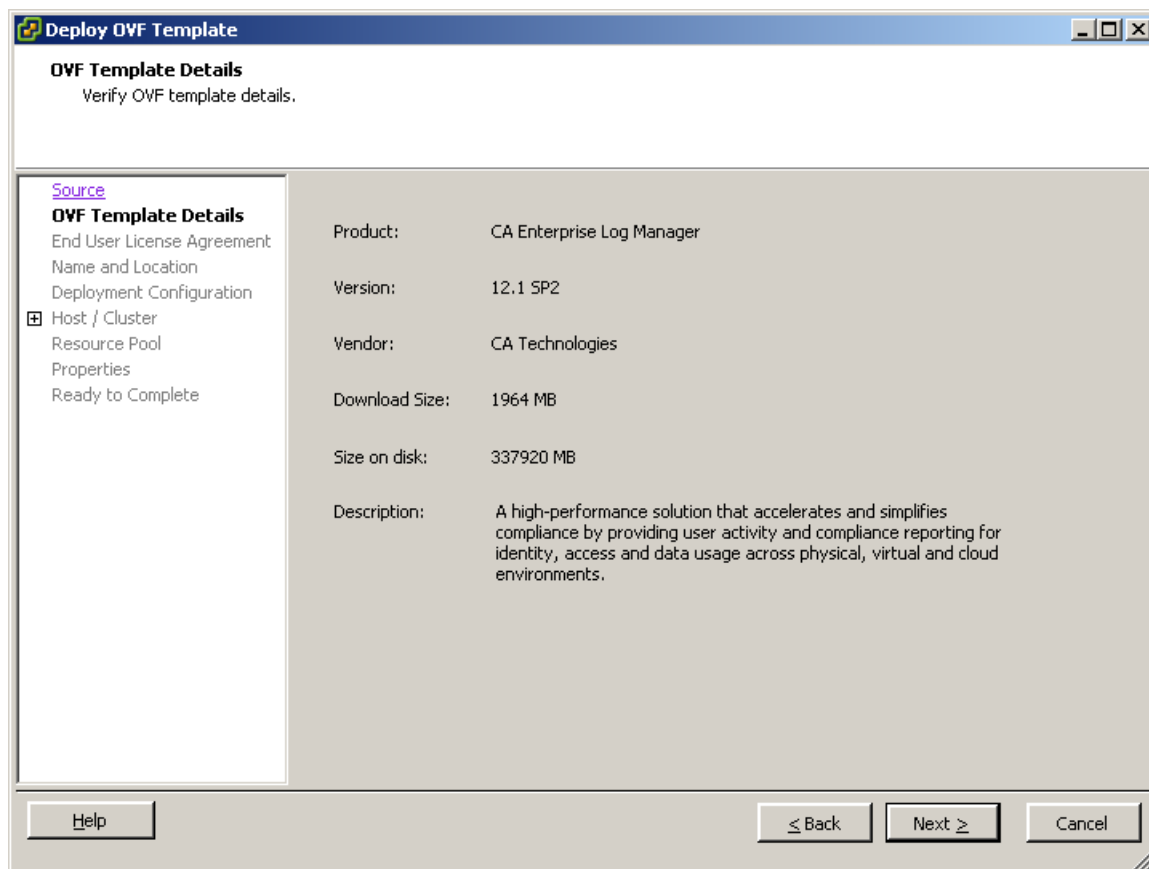
The path of the OVF template location is displayed in the Deploy from file field.



9. Click Next.

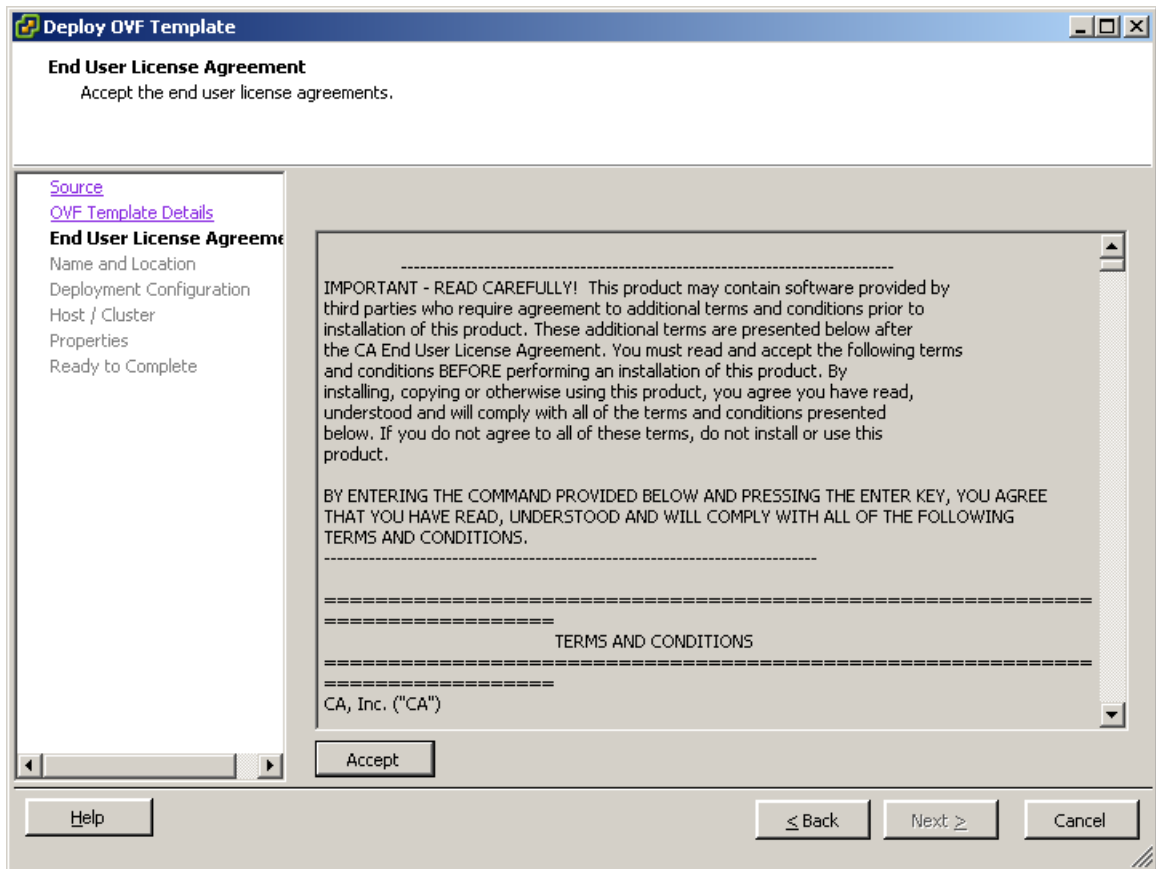
The OVF Template Details page opens. This page displays the details stored in the OVF template such as the download size, available disk size, and vendor name.

10. Verify that there is a minimum of 350 GB disk space on the VMware server, and then click Next.



The End User License Agreement page opens. This page displays the license agreement for third-party products. You must accept this license agreement to install CA Enterprise Log Manager.

11. Read the license text.



12. Click Accept, and click Next.

The Name and Location page opens. This page lets you add a name to identify the CA Enterprise Log Manager server, and specify the datacenter where you want to provision the CA Enterprise Log Manager server.

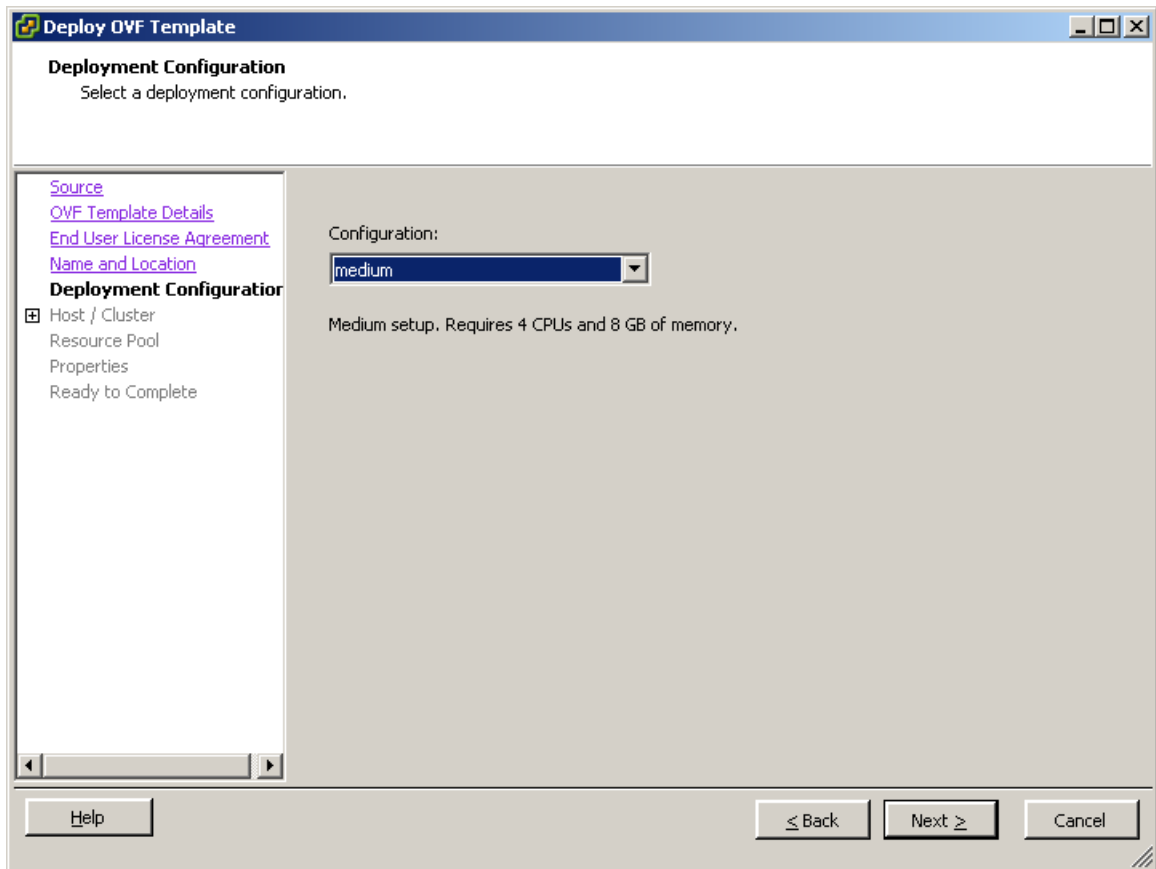
13. Enter the CA Enterprise Log Manager server name the Name field, select the Datacenter from Inventory Location, and then click Next.

Note: By default, the name specified in the OVF template is displayed in the Name field.

The screenshot shows a window titled "Deploy OVF Template" with a sub-header "Name and Location" and the instruction "Specify a name and location for the deployed template". On the left is a navigation pane with links: "Source", "OVF Template Details", "End User License Agreement", "Name and Location" (selected), "Deployment Configuration", "Host / Cluster", "Resource Pool", "Properties", and "Ready to Complete". The main area contains a "Name:" label and a text box with "Example CA Enterprise Log Manager". Below this is a note: "The name can contain up to 80 characters and it must be unique within the inventory folder." Under the "Inventory Location:" label is a tree view showing a folder "elmqa-vserver.ca.com" containing four items: "ELMQA Agents Datacenter", "ELMQA Persistent Lab (LC)", "ELMQA Persistent Lab (MC)", and "ELMQA SP2 vApp Datacenter" (which is selected). At the bottom are buttons for "Help", "< Back", "Next >", and "Cancel".

The Deployment Configuration page opens. The Deployment Configuration page lets you specify the configuration mode of the CA Enterprise Log Manager server you want to provision.

14. Select Medium or Large from the Configuration drop-down, and then click Next.

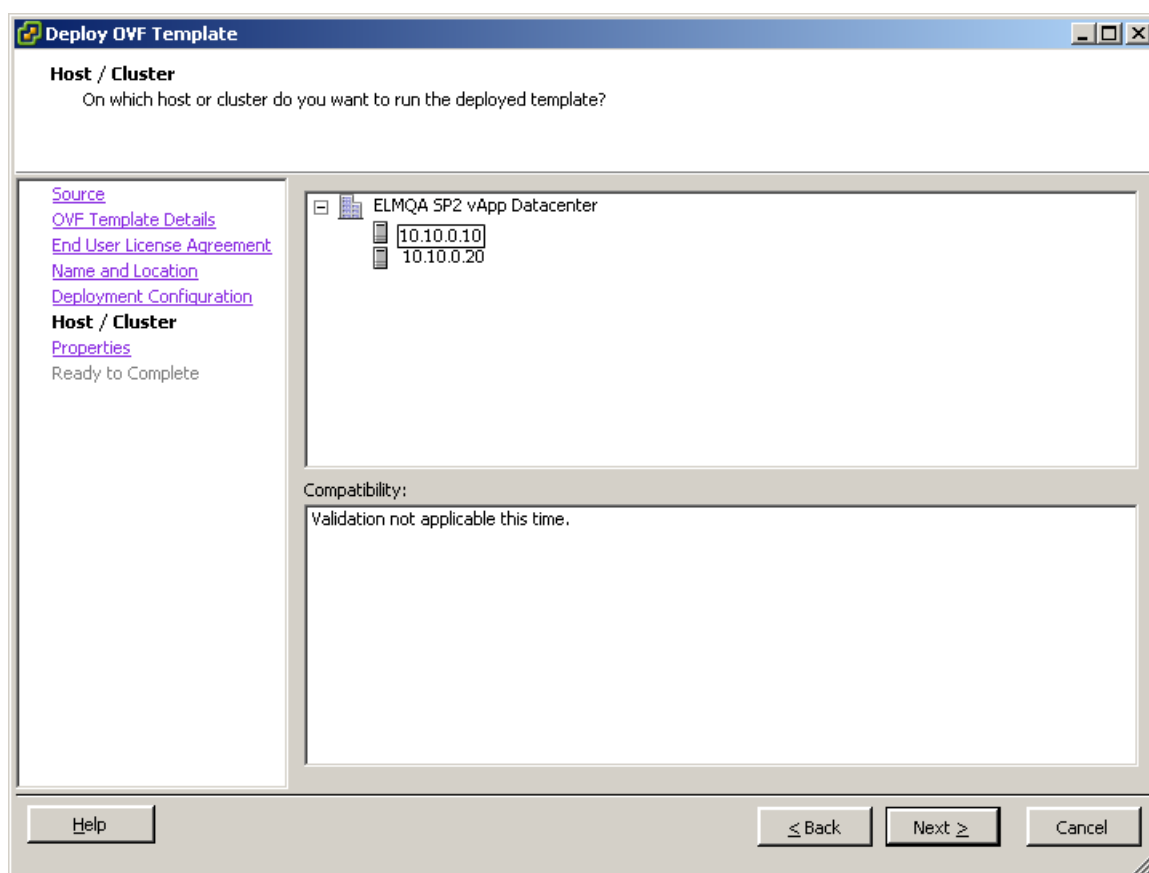


If you select medium, VMware provides four CPUs with 8 GB RAM for each CPU. If you select large, VMware provides eight CPUs with 8 GB RAM for each CPU.

Note: We highly recommend that you use a medium deployment configuration to provision a collection server, and a large deployment configuration to provision a management or reporting server.

The Host / Cluster page opens. This page appears only if you have not selected the resource pool before you start importing the OVF template. The Host / Cluster page displays the datacenter you selected and its available clusters. You must specify the cluster location under the datacenter where you want to provision the CA Enterprise Log Manager server.

15. Select a cluster under the datacenter, and then click Next.



The Properties page opens. This page contains the Host settings and CA Enterprise Log Manager settings.

16. Enter values for each field using the information you gathered in the Installation Worksheet, and then click Next.

Deploy OVF Template

Properties
Customize the software solution for this deployment.

[Source](#)
[OVF Template Details](#)
[End User License Agreement](#)
[Name and Location](#)
[Deployment Configuration](#)
[Host / Cluster](#)
[Datastore](#)
Properties
Ready to Complete

A. Host Settings

A. Host Name
Enter name of this host machine.
examplecaelm

B. Root Password
Enter root password of this machine.
examplerootpassword

C. IP Address
Enter IP address of this machine.
172 . 160 . 0 . 0

D. Subnet Mask
Enter the subnet mask.
10 . 0 . 0 . 0

E. Default Gateway
Enter the IP address of the default gateway.
198 . 168 . 0 . 0

F. DNS Servers
Enter a list of the IP addresses for your DNS servers. Use a comma to separate the IP addresses of the DNS servers.
198.168.10.20,198.168.10.25

G. Domain Name
Enter the domain name of this machine.
example.com

H. Time Zone
Choose the time zone.
Africa/Abidjan

I. NTP Server Location
Enter the NTP Server Location if you want to configure System Time through NTP.
198.168.10.30

Help ≤ Back Next > Cancel

The screenshot shows a window titled "Deploy OVF Template" with a "Properties" tab selected. The left sidebar contains links: "Source", "OVF Template Details", "End User License Agreement", "Name and Location", "Deployment Configuration", "Host / Cluster", "Resource Pool", and "Properties". The "Properties" section is labeled "Ready to Complete". The main content area is titled "B. CA Enterprise Log Manager Settings" and contains four sections: "A. Location of CA EEM Server" with a dropdown menu set to "Local"; "B. Host Name or IP Address of the Remote CA EEM Server" with a text field containing "none"; "C. Password for CA EEM Server" with a text field containing "exampleeiamadminpassword"; and "D. FIPS Mode" with a dropdown menu set to "NO". At the bottom are buttons for "Help", "≤ Back", "Next ≥", and "Cancel".

Deploy OVF Template

Properties
Customize the software solution for this deployment.

[Source](#)
[OVF Template Details](#)
[End User License Agreement](#)
[Name and Location](#)
[Deployment Configuration](#)
[Host / Cluster](#)
[Resource Pool](#)
Properties
Ready to Complete

B. CA Enterprise Log Manager Settings

A. Location of CA EEM Server
Select Local if the CA EEM server is to be installed on this host. Select Remote if this CA Enterprise Log Manager server must use a remote CA EEM server.
Local

B. Host Name or IP Address of the Remote CA EEM Server
Specify the IP address or the host name of the remote CA EEM server. Enter none to install a CA EEM server on this host.
none

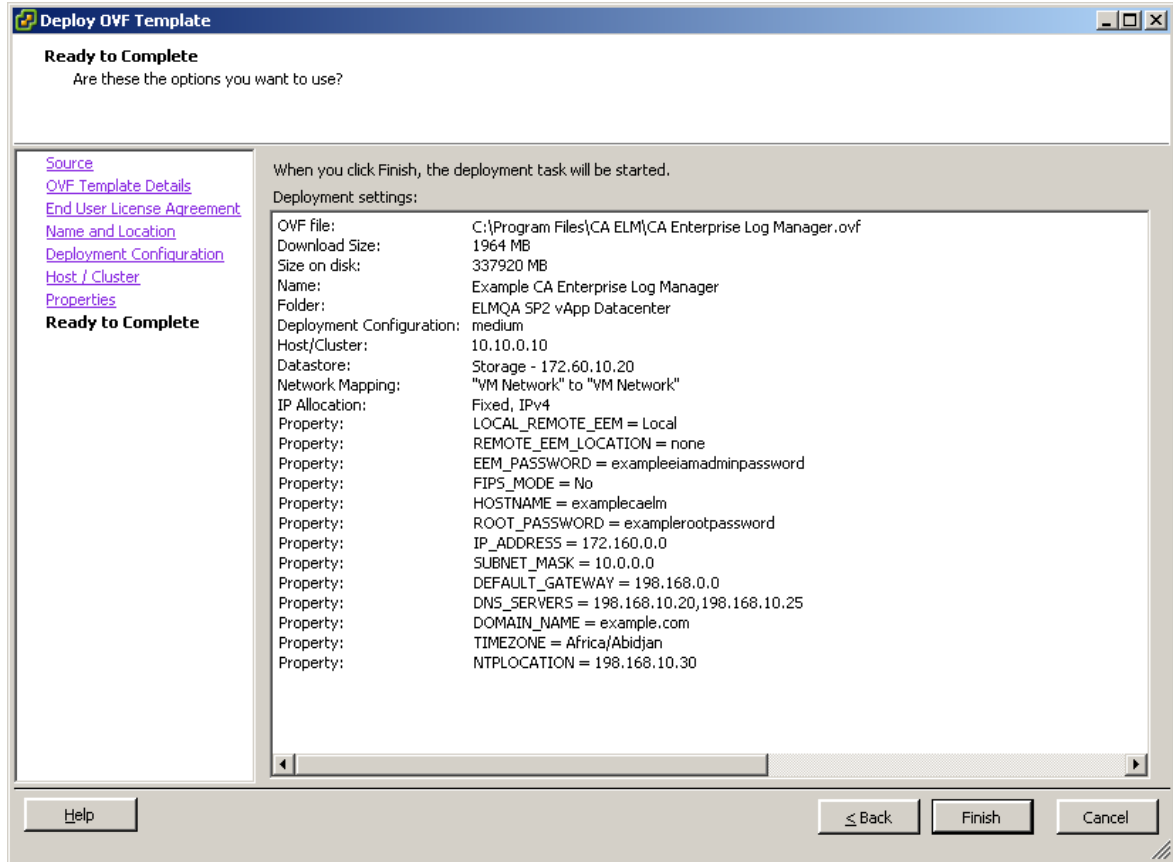
C. Password for CA EEM Server
Enter the password for the EEM server EiamAdmin user.
exampleeiamadminpassword

D. FIPS Mode
Do you want to run CA Enterprise Log Manager in FIPS mode? Choose Yes for FIPS mode or No for non-FIPS mode.
NO

Help ≤ Back Next ≥ Cancel

The Ready to Complete page opens. This page displays a summary of the details you have entered in the previous pages.

17. Verify the entered details, and then click Finish.



The message Opening VI target is displayed. The deployment status of the virtual appliance is displayed. If the installation is successful, the virtual appliance is listed under the datastore you selected in the left pane.

18. (Optional) If you want to make changes to the entered details, do the following:
- Click Back repeatedly in the Deploy OVF Template window until you navigate to the relevant page.
 - Make the necessary changes.
 - Click Next repeatedly in the Deploy OVF until you navigate to the Ready to Complete page.

More information:

[Virtual Appliance Installation Worksheet](#) (see page 284)

Set the Paravirtualization and Resource Settings

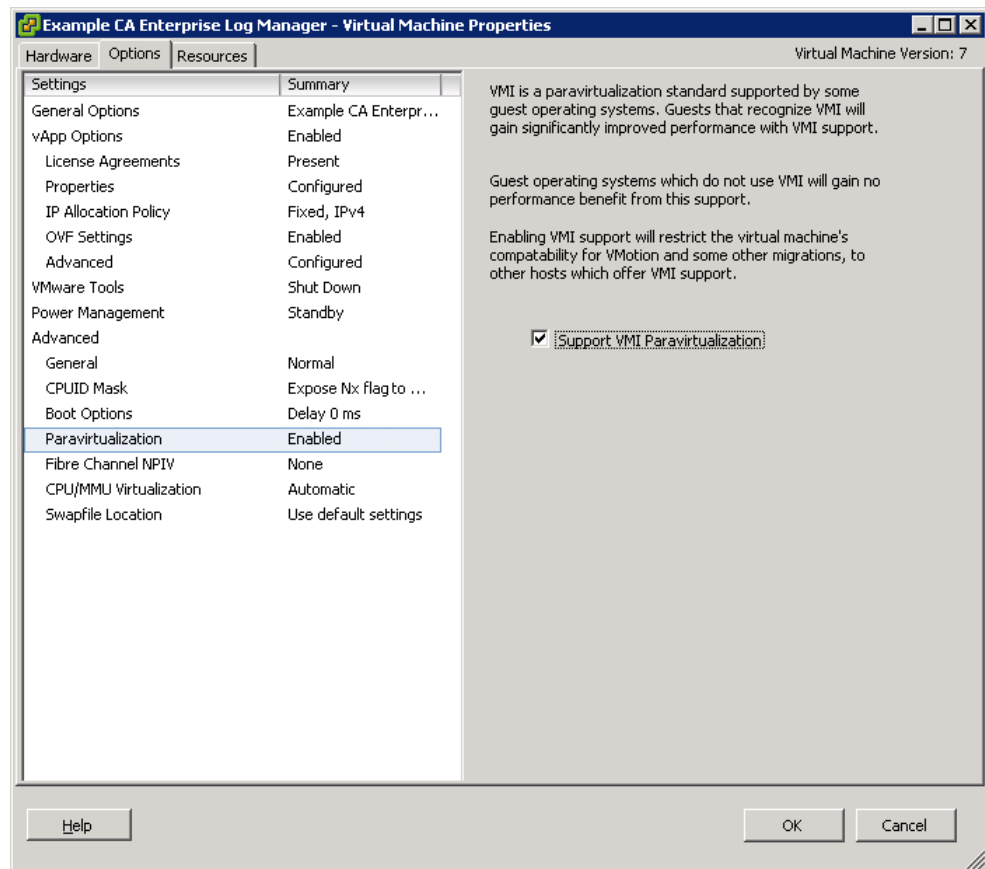
After you import the OVF template, you must manually set the paravirtualization and resource settings to improve the performance of the provisioned CA Enterprise Log Manager server.

Note: Verify that you set the CD/DVD Drive to Client Device.

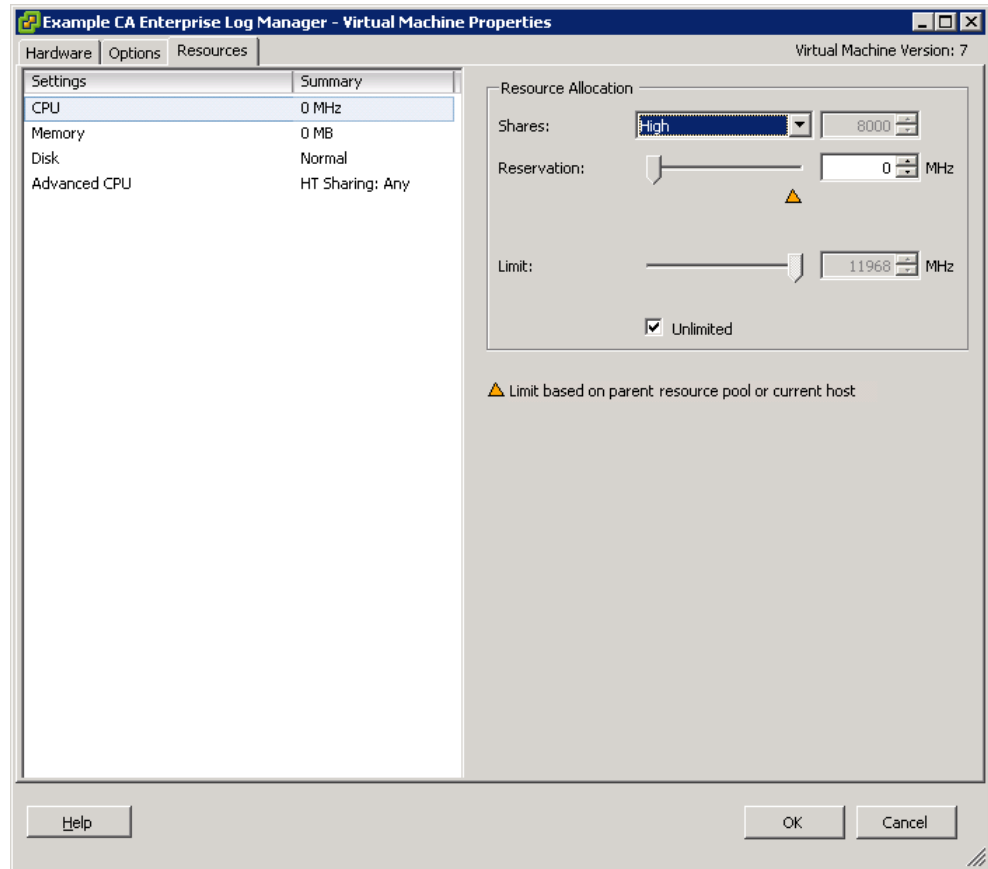
To set the paravirtualization and resource settings

1. Right-click the new CA Enterprise Log Manager Virtual Appliance in the left pane, and click Edit Settings.

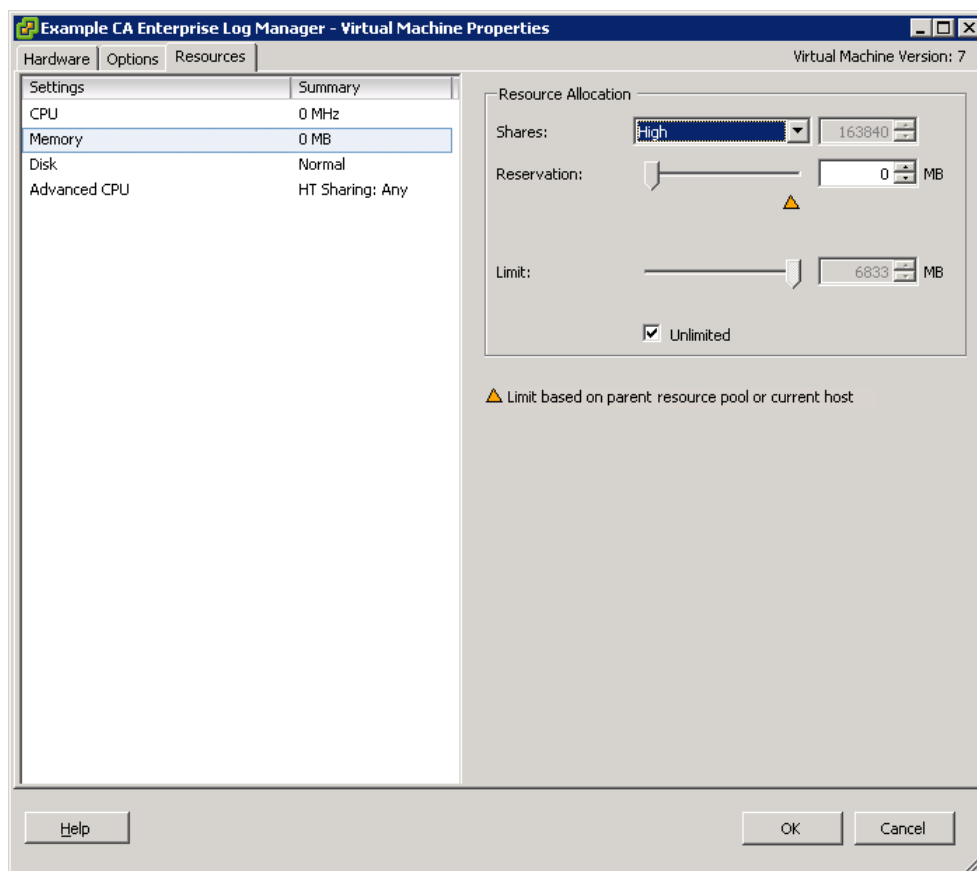
The *<CA Enterprise Log Manager Virtual Appliance name> - Virtual Machine Properties* window appears.
2. Click the Option tab in the window.
3. Select the Paravirtualization setting in the left pane, and select the Support VMI Paravirtualization option in the right pane.



4. Click the Resources tab in the window.
5. Select the CPU option under the Settings column, and select High from the Shares drop-down in the Resource Allocation section.



6. Select the Memory option under the Settings column, and select High from the Shares drop-down in the Resource Allocation section.



7. Click OK.
8. **Note:** For more information about Paravirtualization, go to www.vmware.com.

Power on the Provisioned CA Enterprise Log Manager Server

You must power on the CA Enterprise Log Manager server to start running it.

To power on a CA Enterprise Log Manager server

1. Select the new CA Enterprise Log Manager server in the left pane of the VMware application window.
2. Click the Power On option under Basic Tasks of the Getting Started tab in the right pane.

The CA Enterprise Log Manager server is powered on.

Note: Verify that a primary CA Enterprise Log Manager server is running before you power on a secondary CA Enterprise Log Manager server.

Install a CA Enterprise Log Manager Server Silently

When you install the virtual appliance silently, you must perform the following tasks:

1. Invoke the OVF Tool.
2. Set the Paravirtualization and Resource settings.
3. Power on the provisioned CA Enterprise Log Manager server.

The following table describes the parameters used to deploy CA Enterprise Log Manager using the OVF tool. You must specify these parameters as command line arguments in the command line.

Required information	Value	Comments
Host Specific Settings		
HOSTNAME	<i>hostname for this CA Enterprise Log Manager server</i> For example: CA-ELM1	Specify the host name for this server using only supported characters for hosts. Industry standards recommend A-Z (case-insensitive), 0-9, and hyphen, where the first character is a letter and the final character is alphanumeric. Do not use the underscore character in a host name, or append a domain name to this host. Note: The host name must not exceed 15 characters.
ROOT_PASSWORD	<i>new root password</i>	Create and confirm a new root password for this server.
IP_ADDRESS	<i>relevant IPv4 address</i>	Enter a valid IP address for this server.
SUBNET_MASK	<i>relevant IP address</i>	Enter a valid subnet mask for use with this server.
DEFAULT_GATEWAY	<i>relevant IP address</i>	Enter a valid subnet mask and default gateway for use with this server.
DNS_SERVERS	<i>relevant IPv4 addresses</i>	Enter one or more DNS server IP addresses in use in your network. The list is comma-separated with no spaces between entries. If your DNS servers use IPv6 addressing, enter these addresses in that format.

Required information	Value	Comments
DOMAIN_NAME	<i>your domain name</i>	Enter the qualified domain name in which this server operates, for example, mycompany.com. Note: The domain name must be registered with the Domain Name Server (DNS) server in your network to enable resolution of the hostname to IP address.
acceptAllEulas	Accept	Accept the CA license agreement to continue provisioning a CA Enterprise Log Manager server.
deploymentOption	medium or large	If you select medium, VMware provides four CPUs with 8 GB RAM for each CPU. If you select large, VMware provides eight CPUs with 8 GB RAM for each CPU.
TIMEZONE	<i>your desired time zone</i>	Select the time zone where this server resides.
NTPLOCATION	<i>relevant hostname or IP address</i>	Enter the host name or the valid IP address of the NTP server from which the CA Enterprise Log Manager server gets date and time information.
Application Specific Settings		
LOCAL_REMOTE_EEM	Local - for the first installed server (management server) Remote - for each additional server	Indicate whether you plan to use a local or a remote CA EEM server. For a management CA Enterprise Log Manager server, choose Local. The installation prompts you to create a password for the default EiamAdmin user account. For each additional server, choose Remote. The installation prompts you for the management server name. Regardless of whether you chose local or remote, you must use the EiamAdmin account ID and password to log on to each CA Enterprise Log Manager server the first-time.
REMOTE_EEM_LOCATION	<i>IP address or hostname</i>	Enter this value only if you select Remote in the Local or Remote server option. Enter the IP address or host name of the management CA Enterprise Log Manager server that you installed first. The host name must be registered with the DNS Server. If you want to use a local CA EEM server, the default value is none .

Required information	Value	Comments
EEM_PASSWORD	<i>EiamAdmin account password</i>	<p>Record the password for the default administrator account, EiamAdmin.</p> <p>Your CA Enterprise Log Manager server requires these account credentials for the initial login.</p> <p>If you are installing the management server, you are creating and confirming a new EiamAdmin password here.</p> <p>Make a note of this password as you must use it during the installations of other CA Enterprise Log Manager servers and agents.</p> <p>Note: The password you enter here is also the initial password for the default caelmadmin account that you use to access the CA Enterprise Log Manager server directly through ssh.</p> <p>You can create additional administrator accounts to access the CA EEM functions after installation, if desired.</p>
FIPS_MODE	Yes or No	<p>Specifies if the virtual appliance must run in FIPS mode or non-FIPS mode. If you choose to use a local CA EEM server, you can choose any mode. If you choose to use a remote CA EEM server, you must choose the mode that the remote CA EEM server uses.</p>

More information

[Adding Virtual Servers to Your Environment](#) (see page 286)
[Creating a Completely Virtual Environment](#) (see page 309)
[Deploying Virtual Servers Rapidly](#) (see page 332)

Invoke the OVF Tool from a Command Line

Note: You must install the OVF Tool 1.0.0.0 before you perform the silent installation. For more information about the OVF Tool, see VMware's *OVF Tool User Guide* or go to www.vmware.com.

You must pass the configuration parameters as command line arguments to invoke the OVF Tool.

Note: We highly recommend that you use a medium deployment configuration to provision a collection server, and a large deployment configuration to provision a reporting server. We also recommend that you use thick deployment method as outlined in the VMware documentation.

To invoke the OVF Tool from command line

1. Open the command prompt on the computer where VMware vSphere Client is installed.
2. Execute the following command to invoke the OVF Tool:

```
ovftool -dm=thick --acceptAllEulas --name=value --deploymentOption=value  
--prop:ROOT_PASSWORD=value --prop:LOCAL_REMOTE_EEM=value  
--prop:REMOTE_EEM_LOCATION=value --prop:EEM_PASSWORD=value  
--prop:FIPS_MODE=value --prop:IP_ADDRESS=value --prop:SUBNET_MASK=value  
--prop:HOSTNAME=value --prop:DEFAULT_GATEWAY=value --prop:DNS_SERVERS=value  
--prop:DOMAIN_NAME=value --prop:TIMEZONE=value --prop:NTPLOCATION=value  
<OVF_Name.ovf>  
vi://username:password@hostname_of_VMware_vSphere_Client/Datacenter/host/host  
name
```

The message Opening VI target is displayed. The deployment status of CA Enterprise Log Manager server is displayed. If the installation is successful, the CA Enterprise Log Manager server is listed under the datastore you selected in the left pane.

Note: If a property value contains space, enclose the property value in double quotes (""). For example, if the OVF name is CA ELM, enter the value as "CA ELM.ovf". For more information about the OVF Tool, see the *OVF Tool User Guide*.

Example


```
ovftool -dm=thick --acceptAllEulas --name="example_server"
--deploymentOption=medium --prop:ROOT_PASSWORD="example_password"
--prop:LOCAL_REMOTE_EEM=Local --prop:REMOTE_EEM_LOCATION=none
--prop:EEM_PASSWORD=calmr12 --prop:FIPS_MODE=Yes --prop:IP_ADDRESS=172.168.0.0
--prop:SUBNET_MASK=10.0.0.0 --prop:HOSTNAME="example_server1"
--prop:DEFAULT_GATEWAY=198.168.0.0 --prop:DNS_SERVERS=198.168.10.20,198.168.10.25
--prop:DOMAIN_NAME=example.com --prop:TIMEZONE=Asia/Kolkata
--prop:NTPLOCATION=198.168.10.30 "C:\Program Files\CA ELM\CA Enterprise Log
Manager.ovf"
"vi://administrator:password@examplevmwarehost/ELMQAvAppDatacenter/host/10.0.10.0
"
```

Set the Paravirtualization and Resource Settings

After you import the OVF template, you must manually set the paravirtualization and resource settings to improve the performance of the provisioned CA Enterprise Log Manager server.

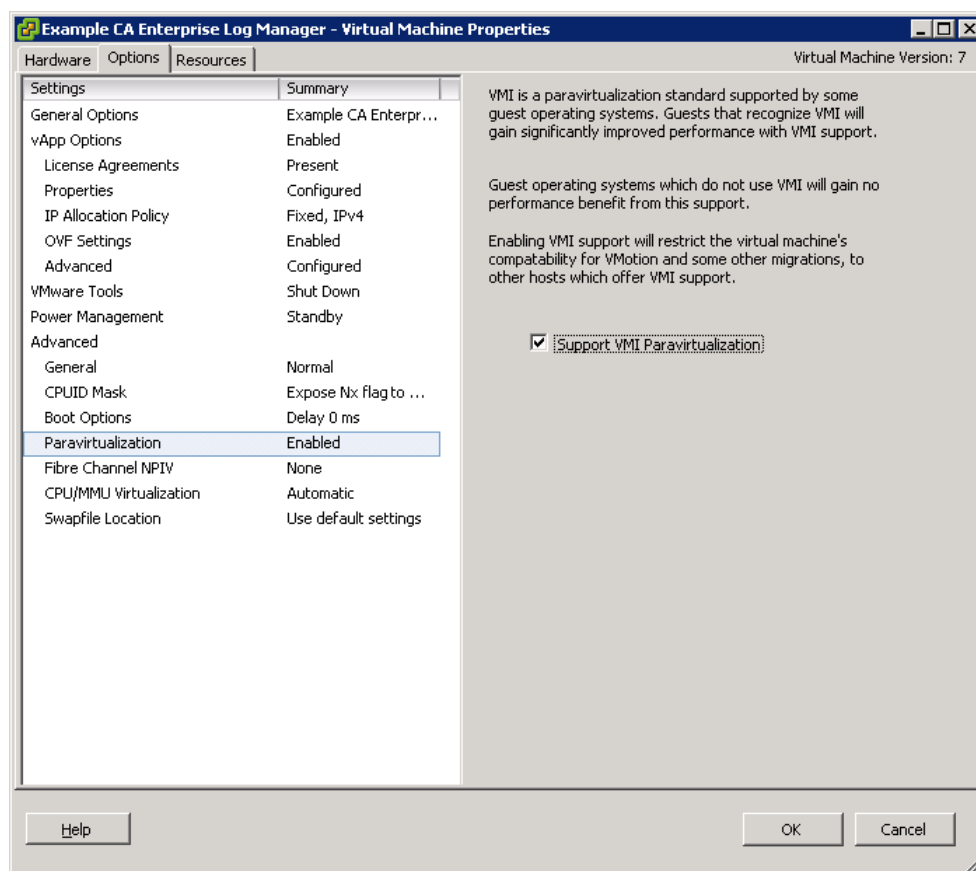
Note: Verify that you set the CD/DVD Drive to Client Device.

To set the paravirtualization and resource settings

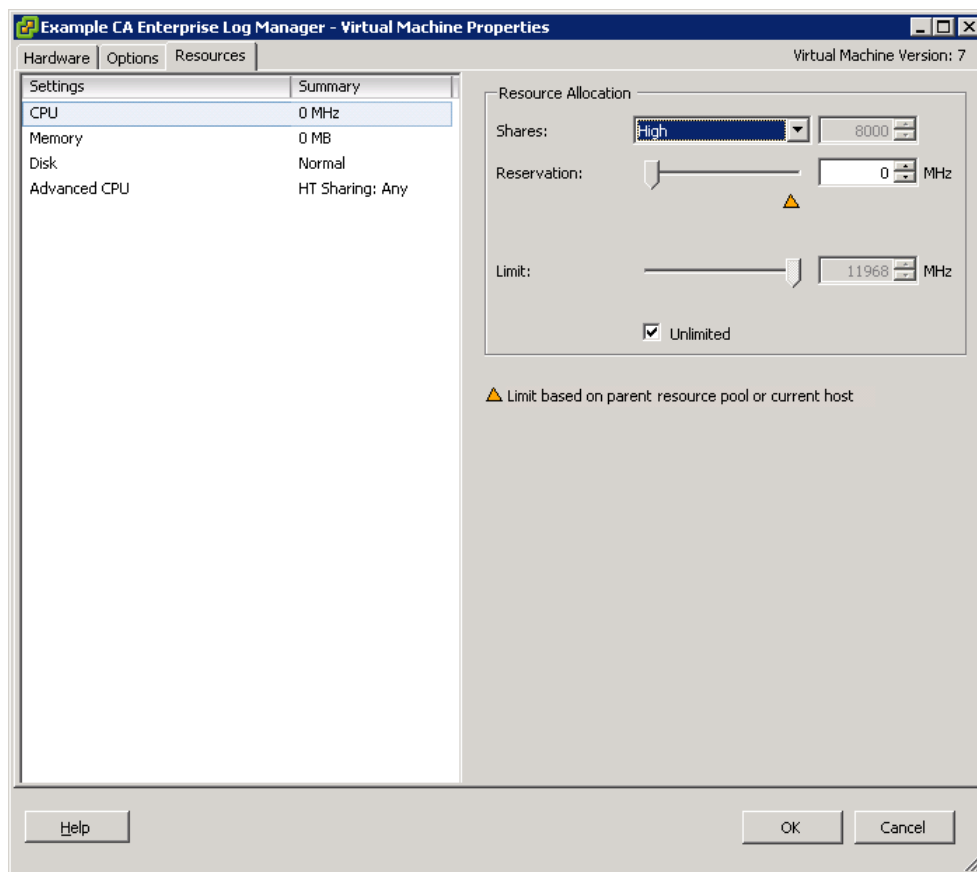
1. Right-click the new CA Enterprise Log Manager Virtual Appliance in the left pane, and click Edit Settings.

The *<CA Enterprise Log Manager Virtual Appliance name> - Virtual Machine Properties* window appears.

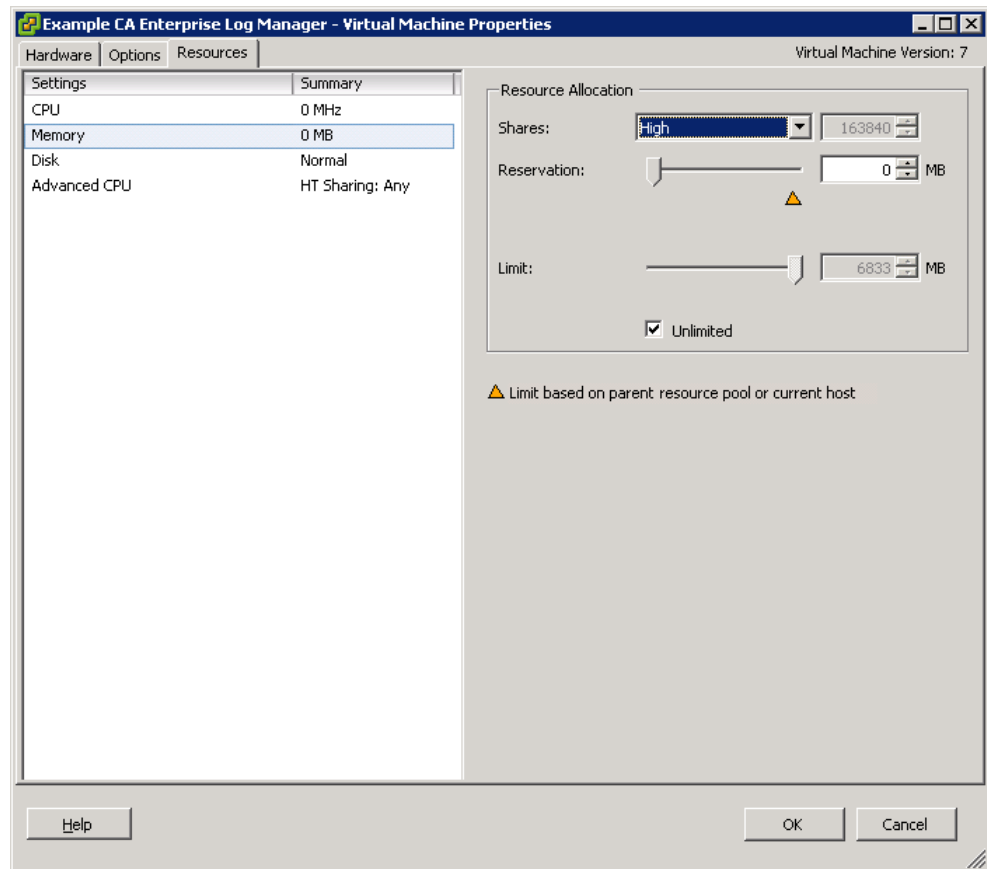
2. Click the Option tab in the window.
3. Select the Paravirtualization setting in the left pane, and select the Support VMI Paravirtualization option in the right pane.



4. Click the Resources tab in the window.
5. Select the CPU option under the Settings column, and select High from the Shares drop-down in the Resource Allocation section.



6. Select the Memory option under the Settings column, and select High from the Shares drop-down in the Resource Allocation section.



7. Click OK.
8. **Note:** For more information about Paravirtualization, go to www.vmware.com.

Power on the Provisioned CA Enterprise Log Manager Server

You must power on the CA Enterprise Log Manager server to start running it.

To power on a CA Enterprise Log Manager server

1. Select the new CA Enterprise Log Manager server in the left pane of the VMware application window.
2. Click the Power On option under Basic Tasks of the Getting Started tab in the right pane.

The CA Enterprise Log Manager server is powered on.

Note: Verify that a primary CA Enterprise Log Manager server is running before you power on a secondary CA Enterprise Log Manager server.

Verify the Installation of a Virtual CA Enterprise Log Manager Server

When you power on the provisioned CA Enterprise Log Manager server, a URL to access CA Enterprise Log Manager is displayed in the Console tab of the VMware vSphere Client window. Use this URL and the following default login credentials to access CA Enterprise Log Manager:

Default Username: EiamAdmin

Default Password: The password you entered during the CA Enterprise Log Manager server installation procedure

More information

[Adding Virtual Servers to Your Environment](#) (see page 286)

[Creating a Completely Virtual Environment](#) (see page 309)

[Deploying Virtual Servers Rapidly](#) (see page 332)

Creating a Completely Virtual Environment

If you do not yet have a CA Enterprise Log Manager environment implemented, you can create an all-virtual log collection environment. This scenario assumes that have a sufficient number of physical servers available, each with a group of at least four processors, to install each of the intended CA Enterprise Log Manager servers.

Install one CA Enterprise Log Manager server to act as a management server. During configuration, do not send event logs to this server or use this server to generate reports. Configuring your environment in this way maintains the event log collection throughput required for enterprise-level production.

Generally, you install two, four-processor CA Enterprise Log Manager servers in place of each of the appliance-class servers you would typically install when using certified hardware. (Appliance-class servers have a minimum of eight processors.)

The process you follow to create a virtual environment using virtual appliance includes the following procedures.

1. Download the virtual appliance package.
2. Install a CA Enterprise Log Manager virtual server for management functions.
3. Install two or more virtual appliance servers for collection and reporting.
4. Configure the virtual appliance servers as described in the section on installing a CA Enterprise Log Manager server.

Important! If you want to provision a CA Enterprise Log Manager server using the virtual appliance, the Application Instance Name of the primary CA Enterprise Log Manager server must be CAELM.

Download the Virtual Appliance Package

The distribution image for the CA Enterprise Log Manager virtual appliance is available from Support Online from the Downloads link. There are five files that you must download:

- The manifest file
- The .ovf file
- Three virtual disk files

Install a CA Enterprise Log Manager Server Manually

When you install the virtual appliance manually, perform the following tasks:

1. Deploy an OVF template.
2. Set the Paravirtualization and Resource settings.
3. Power on the provisioned CA Enterprise Log Manager server.

Deploy an OVF Template

You can specify the properties of virtual appliance in an OVF template. VMware uses this template to provision a CA Enterprise Log Manager server. Use the VMware vSphere Client to deploy the OVF template.

Note: The screenshots in the following procedures contain sample data for your reference. These sample screenshots are in reference to VMware vSphere Client 4.0.0. We recommend that you specify data appropriate to your environment.

To deploy an OVF template

1. Click Start, All Programs, VMware vSphere Client on the computer where VMware vSphere Client is installed.

The VMware vSphere Client dialog opens.

2. Enter the IP address or host name of the VMware vCenter Server you want to connect in the IP address/Name field.
3. Enter the login credentials in the User name and Password fields.
4. Click Logon.

The application window opens.

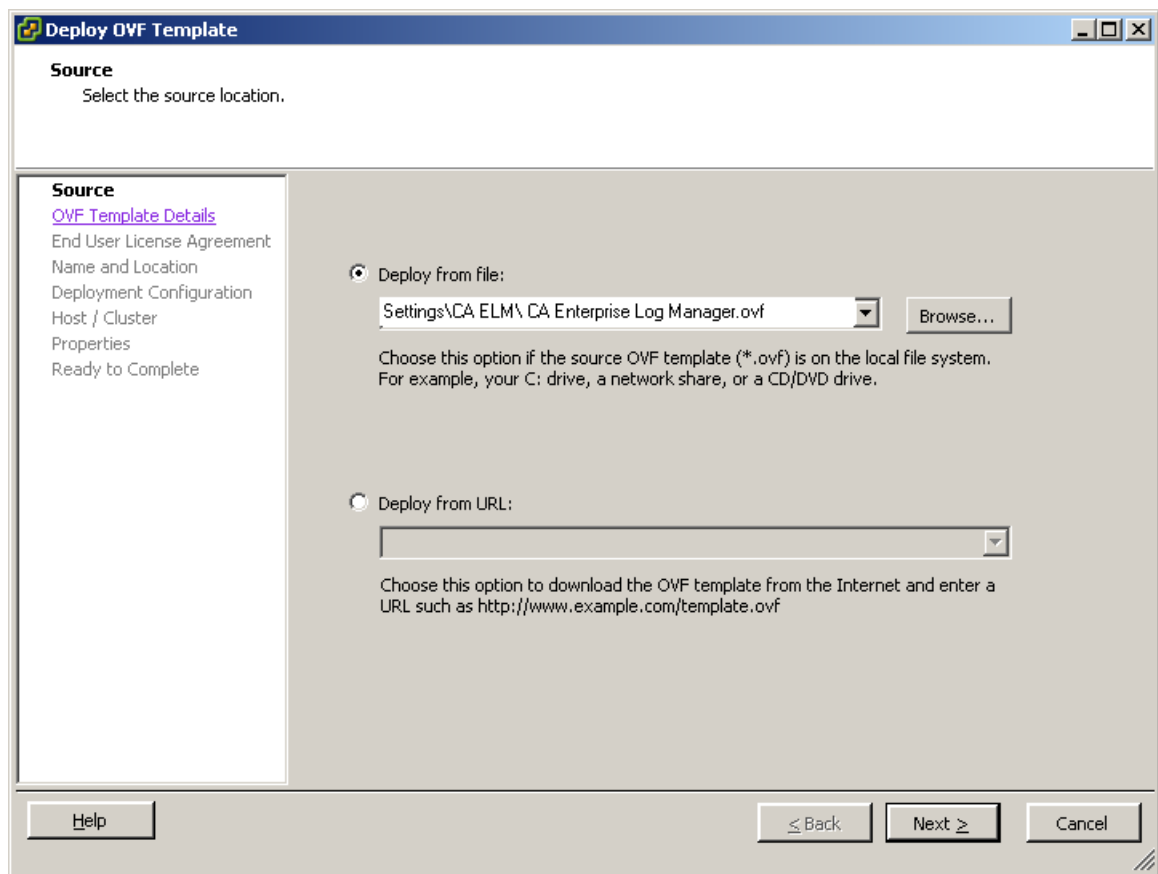
5. Select the location where you want to provision a CA Enterprise Log Manager server under a Datacenter in the left pane.
6. Click File, Deploy OVF Template.

The Deploy OVF Template window appears. By default, the Deploy OVF Template window displays the Source page. You must enter the location of the OVF template in this page.

Note: The pages displayed in the Deploy OVF Template window vary according to the VMware vSphere Client version and settings you are using. For more information about deploying a OVF template, go to www.vmware.com.

7. Choose the Deploy from file option, and click Browse to select the location of the OVF template.
8. Navigate to the OVF template location from the Open dialog, select the OVF template, and click Open.

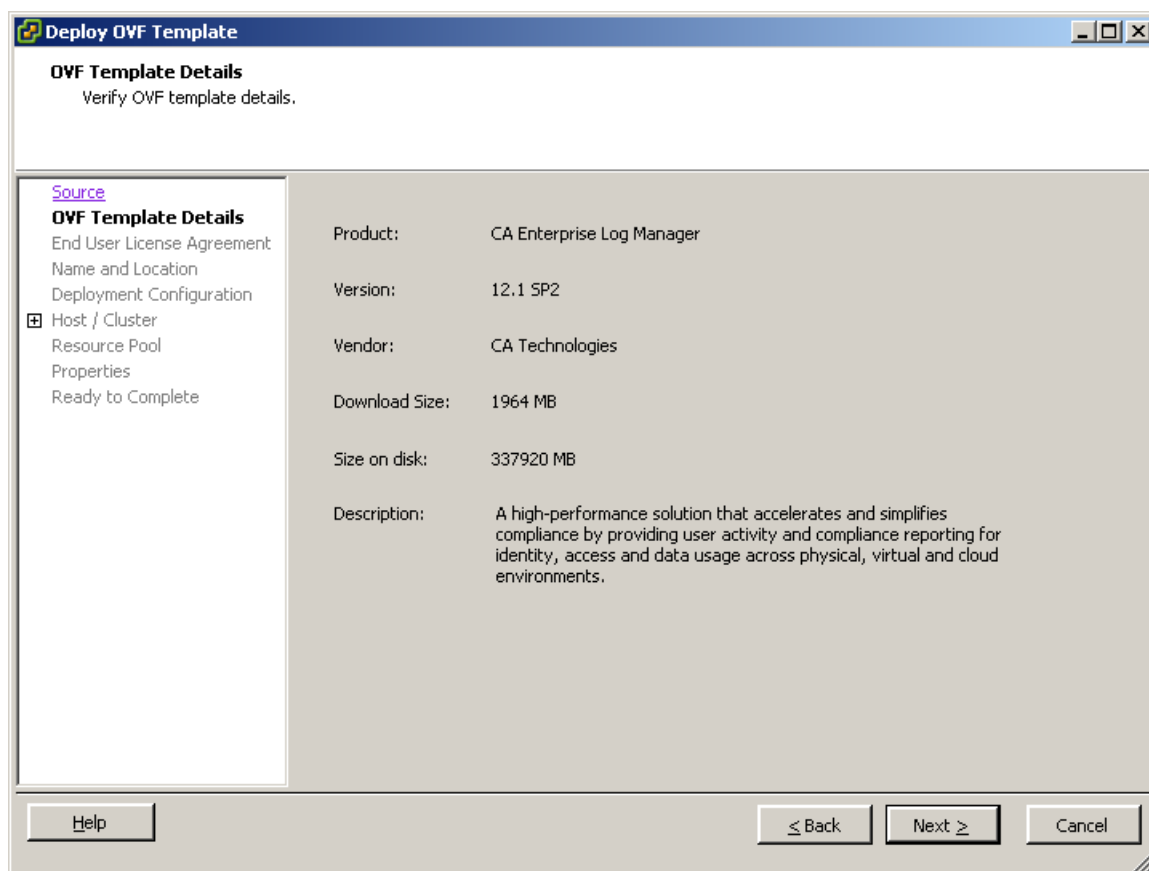
The path of the OVF template location is displayed in the Deploy from file field.



9. Click Next.

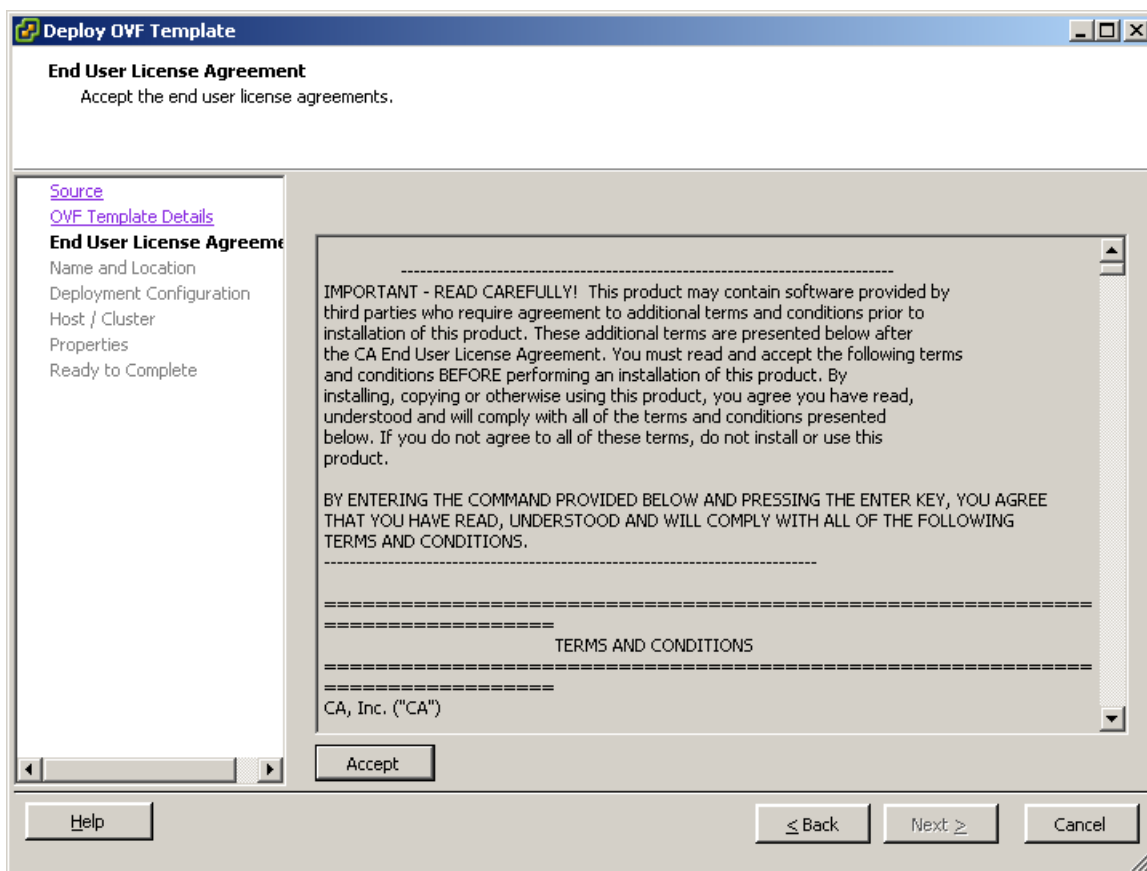
The OVF Template Details page opens. This page displays the details stored in the OVF template such as the download size, available disk size, and vendor name.

10. Verify that there is a minimum of 350 GB disk space on the VMware server, and then click Next.



The End User License Agreement page opens. This page displays the license agreement for third-party products. You must accept this license agreement to install CA Enterprise Log Manager.

11. Read the license text.



12. Click Accept, and click Next.

The Name and Location page opens. This page lets you add a name to identify the CA Enterprise Log Manager server, and specify the datacenter where you want to provision the CA Enterprise Log Manager server.

13. Enter the CA Enterprise Log Manager server name the Name field, select the Datacenter from Inventory Location, and then click Next.

Note: By default, the name specified in the OVF template is displayed in the Name field.

Deploy OVF Template

Name and Location
Specify a name and location for the deployed template

[Source](#)
[OVF Template Details](#)
[End User License Agreement](#)
Name and Location
 Deployment Configuration
 Host / Cluster
 Resource Pool
 Properties
 Ready to Complete

Name:
 Example CA Enterprise Log Manager
 The name can contain up to 80 characters and it must be unique within the inventory folder.

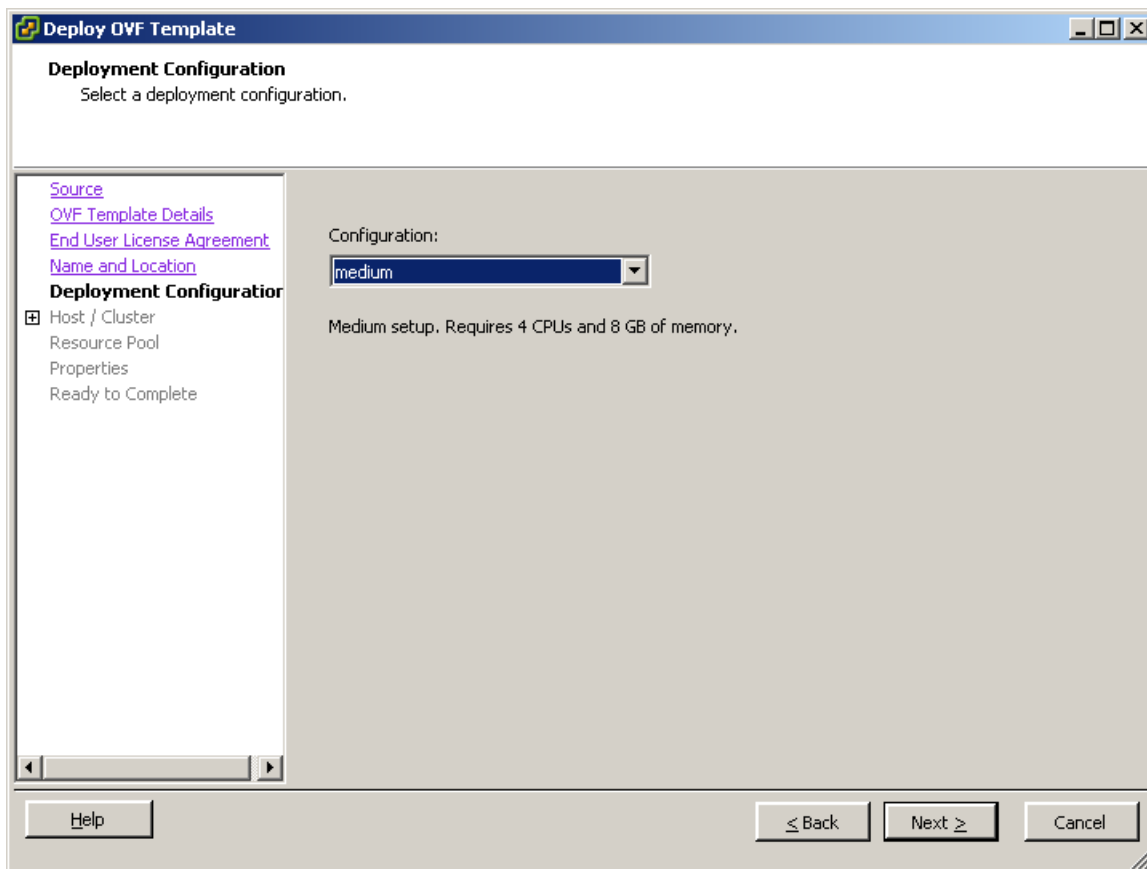
Inventory Location:

- elmqa-vserver.ca.com
 - ELMQA Agents Datacenter
 - ELMQA Persistent Lab (LC)
 - ELMQA Persistent Lab (MC)
 - ELMQA SP2 vApp Datacenter

Help < Back Next > Cancel

The Deployment Configuration page opens. The Deployment Configuration page lets you specify the configuration mode of the CA Enterprise Log Manager server you want to provision.

14. Select Medium or Large from the Configuration drop-down, and then click Next.

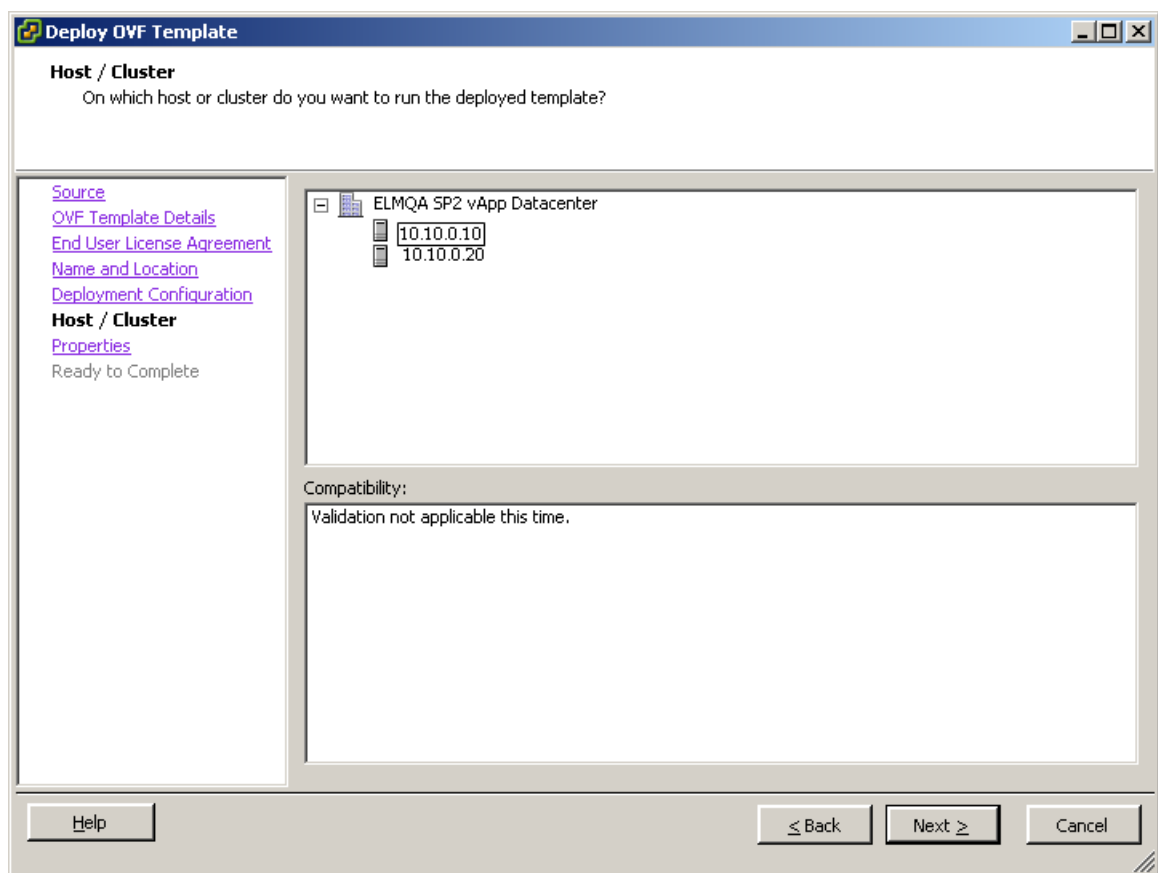


If you select medium, VMware provides four CPUs with 8 GB RAM for each CPU. If you select large, VMware provides eight CPUs with 8 GB RAM for each CPU.

Note: We highly recommend that you use a medium deployment configuration to provision a collection server, and a large deployment configuration to provision a management or reporting server.

The Host / Cluster page opens. This page appears only if you have not selected the resource pool before you start importing the OVF template. The Host / Cluster page displays the datacenter you selected and its available clusters. You must specify the cluster location under the datacenter where you want to provision the CA Enterprise Log Manager server.

15. Select a cluster under the datacenter, and then click Next.



The Properties page opens. This page contains the Host settings and CA Enterprise Log Manager settings.

16. Enter values for each field using the information you gathered in the Installation Worksheet, and then click Next.

Deploy OVF Template

Properties
Customize the software solution for this deployment.

[Source](#)
[OVF Template Details](#)
[End User License Agreement](#)
[Name and Location](#)
[Deployment Configuration](#)
[Host / Cluster](#)
[Datastore](#)
Properties
Ready to Complete

A. Host Settings

A. Host Name
Enter name of this host machine.
examplecaelm

B. Root Password
Enter root password of this machine.
examplerootpassword

C. IP Address
Enter IP address of this machine.
172 . 160 . 0 . 0

D. Subnet Mask
Enter the subnet mask.
10 . 0 . 0 . 0

E. Default Gateway
Enter the IP address of the default gateway.
198 . 168 . 0 . 0

F. DNS Servers
Enter a list of the IP addresses for your DNS servers. Use a comma to separate the IP addresses of the DNS servers.
198.168.10.20,198.168.10.25

G. Domain Name
Enter the domain name of this machine.
example.com

H. Time Zone
Choose the time zone.
Africa/Abidjan

I. NTP Server Location
Enter the NTP Server Location if you want to configure System Time through NTP.
198.168.10.30

Help ≤ Back Next > Cancel

Deploy OVF Template

Properties
Customize the software solution for this deployment.

[Source](#)
[OVF Template Details](#)
[End User License Agreement](#)
[Name and Location](#)
[Deployment Configuration](#)
[Host / Cluster](#)
[Resource Pool](#)
Properties
Ready to Complete

B. CA Enterprise Log Manager Settings

A. Location of CA EEM Server
Select Local if the CA EEM server is to be installed on this host. Select Remote if this CA Enterprise Log Manager server must use a remote CA EEM server.

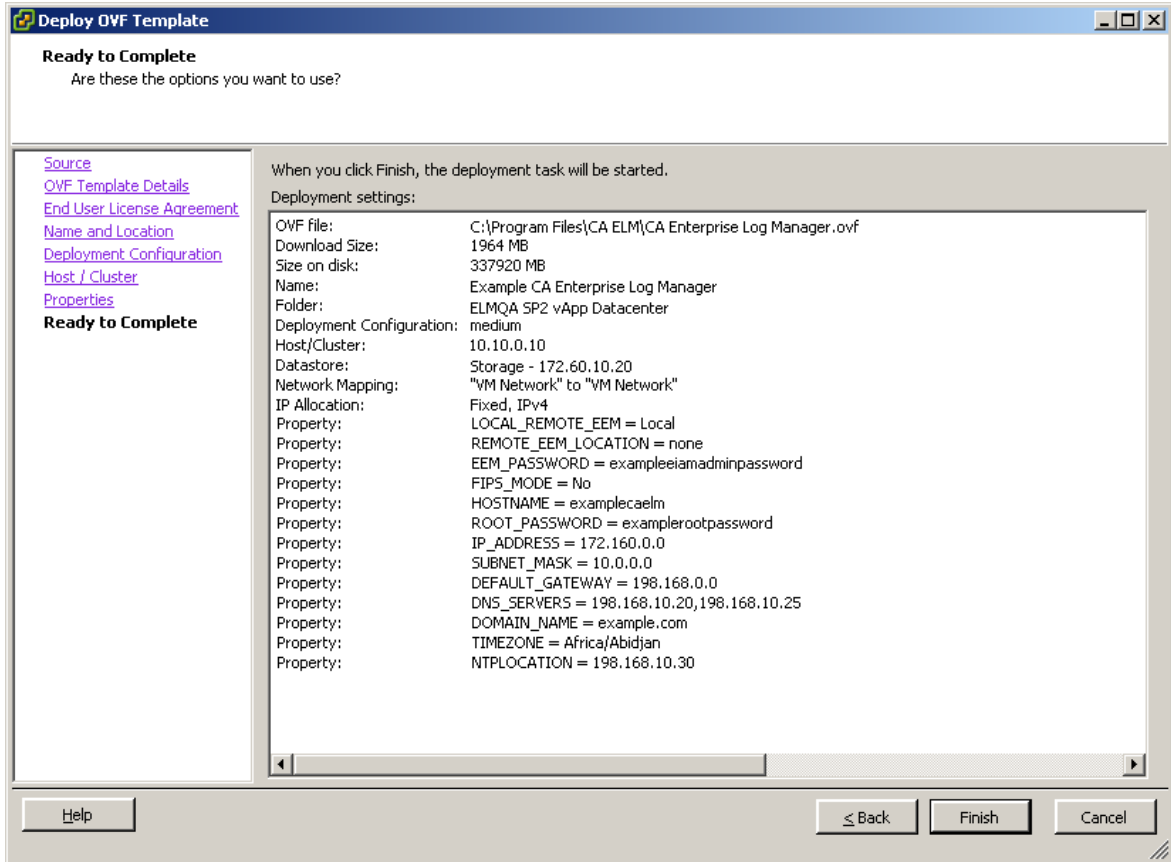
B. Host Name or IP Address of the Remote CA EEM Server
Specify the IP address or the host name of the remote CA EEM server. Enter none to install a CA EEM server on this host.

C. Password for CA EEM Server
Enter the password for the EEM server EiamAdmin user.

D. FIPS Mode
Do you want to run CA Enterprise Log Manager in FIPS mode? Choose Yes for FIPS mode or No for non-FIPS mode.

The Ready to Complete page opens. This page displays a summary of the details you have entered in the previous pages.

17. Verify the entered details, and then click Finish.



The message Opening VI target is displayed. The deployment status of the virtual appliance is displayed. If the installation is successful, the virtual appliance is listed under the datastore you selected in the left pane.

18. (Optional) If you want to make changes to the entered details, do the following:
 - a. Click Back repeatedly in the Deploy OVF Template window until you navigate to the relevant page.
 - b. Make the necessary changes.
 - c. Click Next repeatedly in the Deploy OVF until you navigate to the Ready to Complete page.

More information:

[Virtual Appliance Installation Worksheet](#) (see page 284)

Set the Paravirtualization and Resource Settings

After you import the OVF template, you must manually set the paravirtualization and resource settings to improve the performance of the provisioned CA Enterprise Log Manager server.

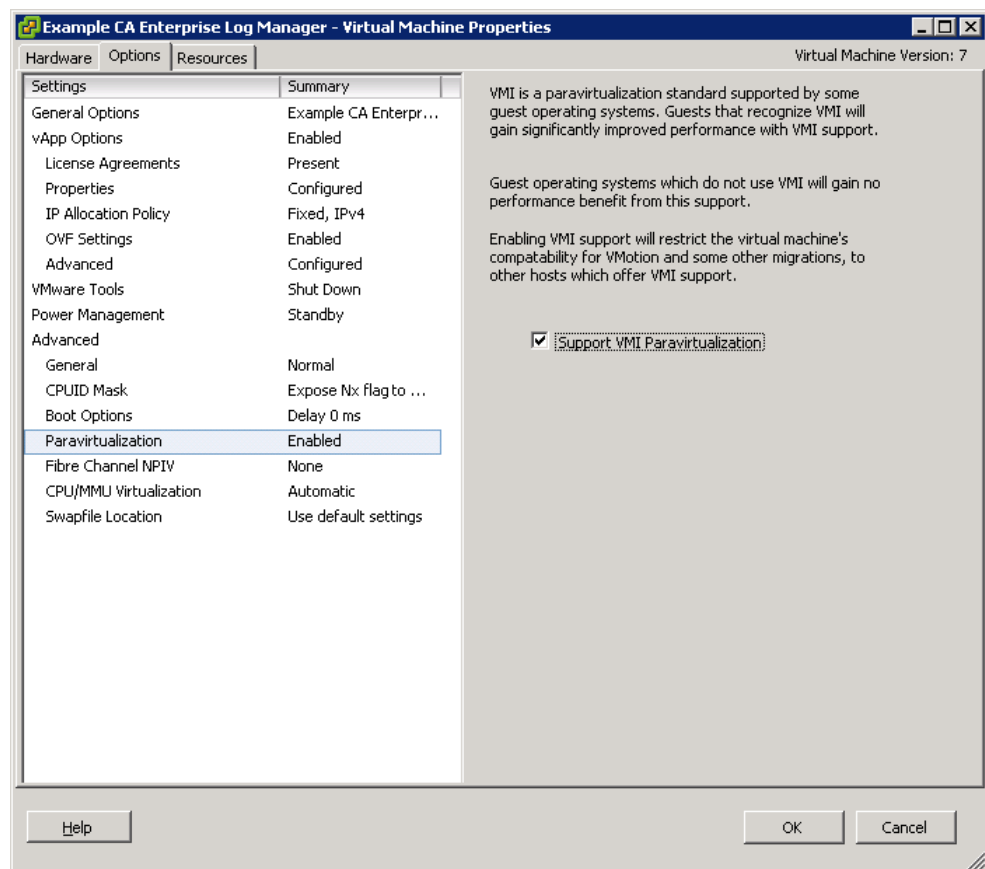
Note: Verify that you set the CD/DVD Drive to Client Device.

To set the paravirtualization and resource settings

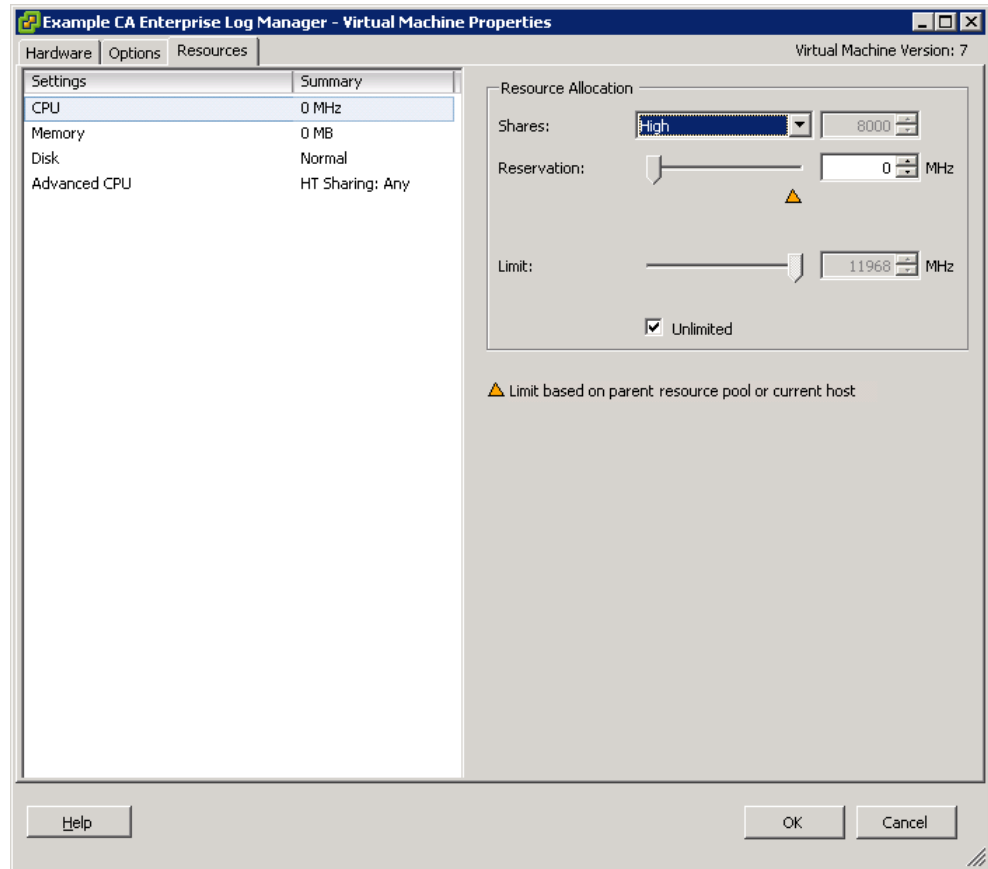
1. Right-click the new CA Enterprise Log Manager Virtual Appliance in the left pane, and click Edit Settings.

The *<CA Enterprise Log Manager Virtual Appliance name>* - Virtual Machine Properties window appears.

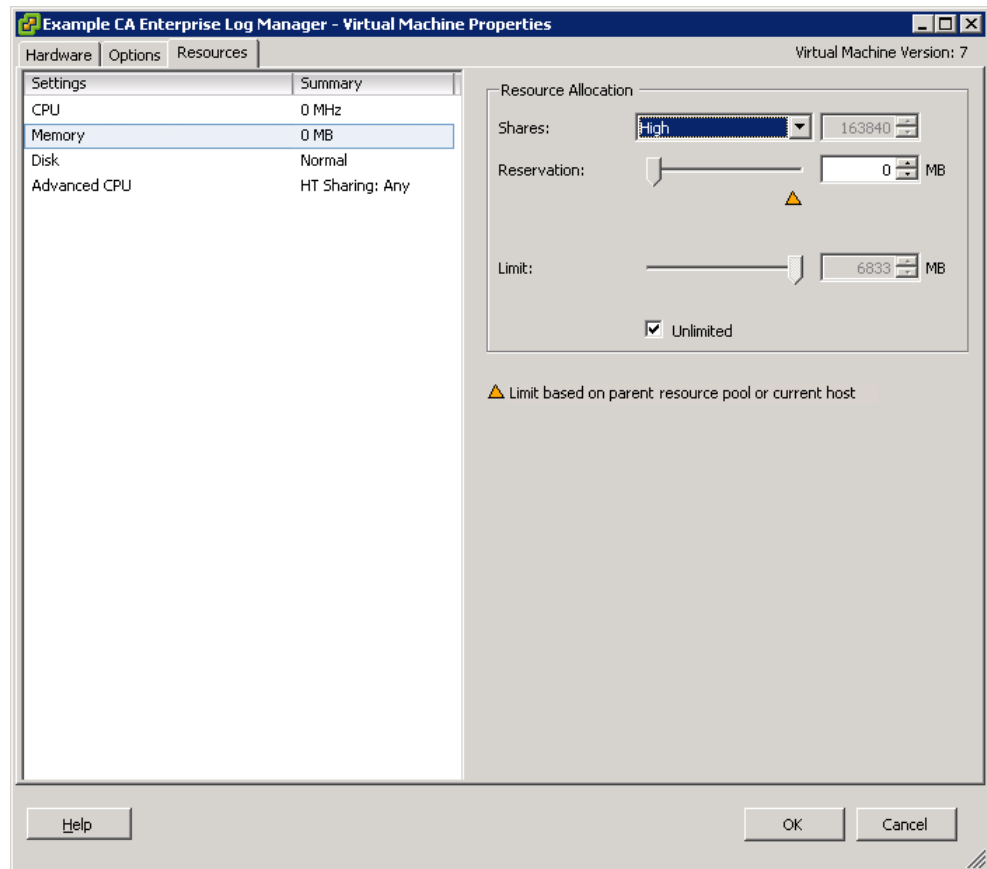
2. Click the Option tab in the window.
3. Select the Paravirtualization setting in the left pane, and select the Support VMI Paravirtualization option in the right pane.



4. Click the Resources tab in the window.
5. Select the CPU option under the Settings column, and select High from the Shares drop-down in the Resource Allocation section.



6. Select the Memory option under the Settings column, and select High from the Shares drop-down in the Resource Allocation section.



7. Click OK.
8. **Note:** For more information about Paravirtualization, go to www.vmware.com.

Power on the Provisioned CA Enterprise Log Manager Server

You must power on the CA Enterprise Log Manager server to start running it.

To power on a CA Enterprise Log Manager server

1. Select the new CA Enterprise Log Manager server in the left pane of the VMware application window.
2. Click the Power On option under Basic Tasks of the Getting Started tab in the right pane.

The CA Enterprise Log Manager server is powered on.

Note: Verify that a primary CA Enterprise Log Manager server is running before you power on a secondary CA Enterprise Log Manager server.

Install a CA Enterprise Log Manager Server Silently

When you install the virtual appliance silently, you must perform the following tasks:

1. Invoke the OVF Tool.
2. Set the Paravirtualization and Resource settings.
3. Power on the provisioned CA Enterprise Log Manager server.

The following table describes the parameters used to deploy CA Enterprise Log Manager using the OVF tool. You must specify these parameters as command line arguments in the command line.

Required information	Value	Comments
Host Specific Settings		
HOSTNAME	<i>hostname for this CA Enterprise Log Manager server</i> For example: CA-ELM1	Specify the host name for this server using only supported characters for hosts. Industry standards recommend A-Z (case-insensitive), 0-9, and hyphen, where the first character is a letter and the final character is alphanumeric. Do not use the underscore character in a host name, or append a domain name to this host. Note: The host name must not exceed 15 characters.
ROOT_PASSWORD	<i>new root password</i>	Create and confirm a new root password for this server.
IP_ADDRESS	<i>relevant IPv4 address</i>	Enter a valid IP address for this server.
SUBNET_MASK	<i>relevant IP address</i>	Enter a valid subnet mask for use with this server.
DEFAULT_GATEWAY	<i>relevant IP address</i>	Enter a valid subnet mask and default gateway for use with this server.
DNS_SERVERS	<i>relevant IPv4 addresses</i>	Enter one or more DNS server IP addresses in use in your network. The list is comma-separated with no spaces between entries. If your DNS servers use IPv6 addressing, enter these addresses in that format.

Required information	Value	Comments
DOMAIN_NAME	<i>your domain name</i>	Enter the qualified domain name in which this server operates, for example, mycompany.com. Note: The domain name must be registered with the Domain Name Server (DNS) server in your network to enable resolution of the hostname to IP address.
acceptAllEulas	Accept	Accept the CA license agreement to continue provisioning a CA Enterprise Log Manager server.
deploymentOption	medium or large	If you select medium, VMware provides four CPUs with 8 GB RAM for each CPU. If you select large, VMware provides eight CPUs with 8 GB RAM for each CPU.
TIMEZONE	<i>your desired time zone</i>	Select the time zone where this server resides.
NTPLOCATION	<i>relevant hostname or IP address</i>	Enter the host name or the valid IP address of the NTP server from which the CA Enterprise Log Manager server gets date and time information.
Application Specific Settings		
LOCAL_REMOTE_EEM	Local - for the first installed server (management server) Remote - for each additional server	Indicate whether you plan to use a local or a remote CA EEM server. For a management CA Enterprise Log Manager server, choose Local. The installation prompts you to create a password for the default EiamAdmin user account. For each additional server, choose Remote. The installation prompts you for the management server name. Regardless of whether you chose local or remote, you must use the EiamAdmin account ID and password to log on to each CA Enterprise Log Manager server the first-time.
REMOTE_EEM_LOCATION	<i>IP address or hostname</i>	Enter this value only if you select Remote in the Local or Remote server option. Enter the IP address or host name of the management CA Enterprise Log Manager server that you installed first. The host name must be registered with the DNS Server. If you want to use a local CA EEM server, the default value is none .

Required information	Value	Comments
EEM_PASSWORD	<i>EiamAdmin account password</i>	<p>Record the password for the default administrator account, EiamAdmin.</p> <p>Your CA Enterprise Log Manager server requires these account credentials for the initial login.</p> <p>If you are installing the management server, you are creating and confirming a new EiamAdmin password here.</p> <p>Make a note of this password as you must use it during the installations of other CA Enterprise Log Manager servers and agents.</p> <p>Note: The password you enter here is also the initial password for the default caelmadmin account that you use to access the CA Enterprise Log Manager server directly through ssh.</p> <p>You can create additional administrator accounts to access the CA EEM functions after installation, if desired.</p>
FIPS_MODE	Yes or No	<p>Specifies if the virtual appliance must run in FIPS mode or non-FIPS mode. If you choose to use a local CA EEM server, you can choose any mode. If you choose to use a remote CA EEM server, you must choose the mode that the remote CA EEM server uses.</p>

More information

[Adding Virtual Servers to Your Environment](#) (see page 286)
[Creating a Completely Virtual Environment](#) (see page 309)
[Deploying Virtual Servers Rapidly](#) (see page 332)

Invoke the OVF Tool from a Command Line

Note: You must install the OVF Tool 1.0.0.0 before you perform the silent installation. For more information about the OVF Tool, see VMware's *OVF Tool User Guide* or go to www.vmware.com.

You must pass the configuration parameters as command line arguments to invoke the OVF Tool.

Note: We highly recommend that you use a medium deployment configuration to provision a collection server, and a large deployment configuration to provision a reporting server. We also recommend that you use thick deployment method as outlined in the VMware documentation.

To invoke the OVF Tool from command line

1. Open the command prompt on the computer where VMware vSphere Client is installed.
2. Execute the following command to invoke the OVF Tool:

```
ovftool -dm=thick --acceptAllEulas --name=value --deploymentOption=value
--prop:ROOT_PASSWORD=value --prop:LOCAL_REMOTE_EEM=value
--prop:REMOTE_EEM_LOCATION=value --prop:EEM_PASSWORD=value
--prop:FIPS_MODE=value --prop:IP_ADDRESS=value --prop:SUBNET_MASK=value
--prop:HOSTNAME=value --prop:DEFAULT_GATEWAY=value --prop:DNS_SERVERS=value
--prop:DOMAIN_NAME=value --prop:TIMEZONE=value --prop:NTPLOCATION=value
<OVF_Name.ovf>
vi://username:password@hostname_of_VMware_vSphere_Client/Datacenter/host/host
name
```

The message Opening VI target is displayed. The deployment status of CA Enterprise Log Manager server is displayed. If the installation is successful, the CA Enterprise Log Manager server is listed under the datastore you selected in the left pane.

Note: If a property value contains space, enclose the property value in double quotes (""). For example, if the OVF name is CA ELM, enter the value as "CA ELM.ovf". For more information about the OVF Tool, see the *OVF Tool User Guide*.

Example

```
ovftool -dm=thick --acceptAllEulas --name="example_server"
--deploymentOption=medium --prop:ROOT_PASSWORD="example_password"
--prop:LOCAL_REMOTE_EEM=Local --prop:REMOTE_EEM_LOCATION=none
--prop:EEM_PASSWORD=calmr12 --prop:FIPS_MODE=Yes --prop:IP_ADDRESS=172.168.0.0
--prop:SUBNET_MASK=10.0.0.0 --prop:HOSTNAME="example_server1"
--prop:DEFAULT_GATEWAY=198.168.0.0 --prop:DNS_SERVERS=198.168.10.20,198.168.10.25
--prop:DOMAIN_NAME=example.com --prop:TIMEZONE=Asia/Kolkata
--prop:NTPLOCATION=198.168.10.30 "C:\Program Files\CA ELM\CA Enterprise Log
Manager.ovf"
"vi://administrator:password@examplevmwarehost/ELMQAvAppDatacenter/host/10.0.10.0
"
```


Set the Paravirtualization and Resource Settings

After you import the OVF template, you must manually set the paravirtualization and resource settings to improve the performance of the provisioned CA Enterprise Log Manager server.

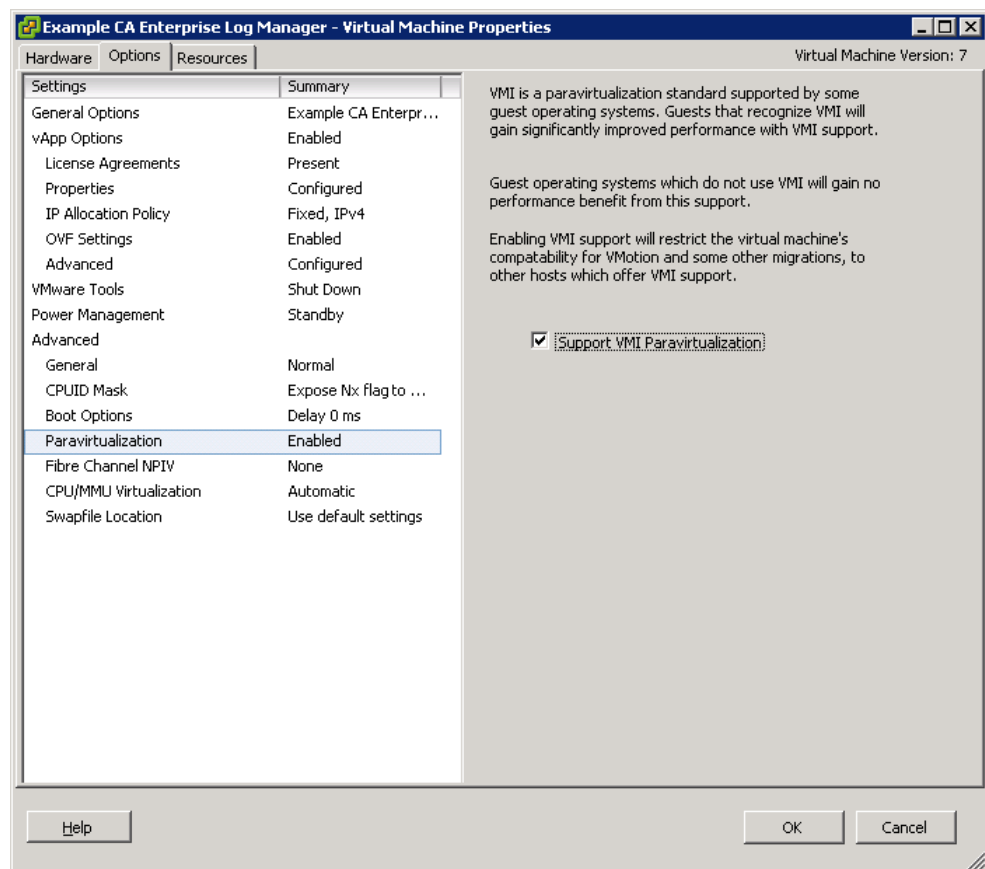
Note: Verify that you set the CD/DVD Drive to Client Device.

To set the paravirtualization and resource settings

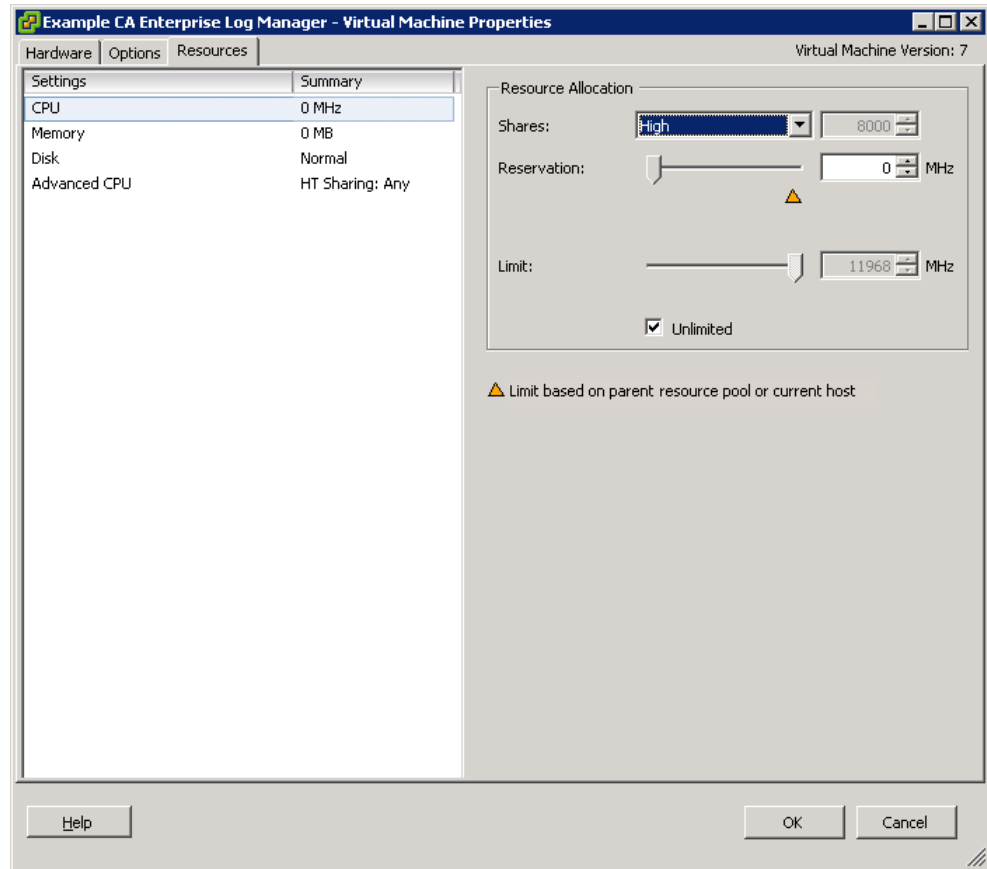
1. Right-click the new CA Enterprise Log Manager Virtual Appliance in the left pane, and click Edit Settings.

The *<CA Enterprise Log Manager Virtual Appliance name>* - Virtual Machine Properties window appears.

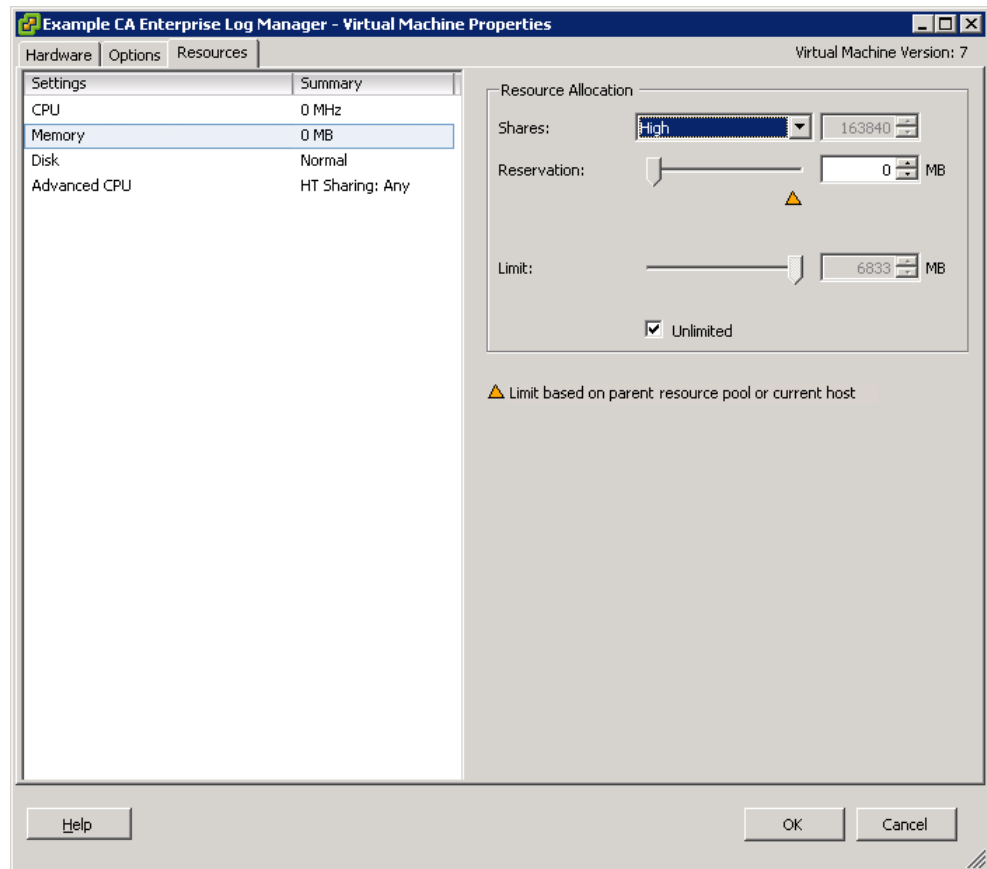
2. Click the Option tab in the window.
3. Select the Paravirtualization setting in the left pane, and select the Support VMI Paravirtualization option in the right pane.



4. Click the Resources tab in the window.
5. Select the CPU option under the Settings column, and select High from the Shares drop-down in the Resource Allocation section.



6. Select the Memory option under the Settings column, and select High from the Shares drop-down in the Resource Allocation section.



7. Click OK.
8. **Note:** For more information about Paravirtualization, go to www.vmware.com.

Power on the Provisioned CA Enterprise Log Manager Server

You must power on the CA Enterprise Log Manager server to start running it.

To power on a CA Enterprise Log Manager server

1. Select the new CA Enterprise Log Manager server in the left pane of the VMware application window.
2. Click the Power On option under Basic Tasks of the Getting Started tab in the right pane.

The CA Enterprise Log Manager server is powered on.

Note: Verify that a primary CA Enterprise Log Manager server is running before you power on a secondary CA Enterprise Log Manager server.

Verify the Installation of a Virtual CA Enterprise Log Manager Server

When you power on the provisioned CA Enterprise Log Manager server, a URL to access CA Enterprise Log Manager is displayed in the Console tab of the VMware vSphere Client window. Use this URL and the following default login credentials to access CA Enterprise Log Manager:

Default Username: EiamAdmin

Default Password: The password you entered during the CA Enterprise Log Manager server installation procedure

More information

[Adding Virtual Servers to Your Environment](#) (see page 286)

[Creating a Completely Virtual Environment](#) (see page 309)

[Deploying Virtual Servers Rapidly](#) (see page 332)

Deploying Virtual Servers Rapidly

The process you follow to rapidly deploy a virtual CA Enterprise Log Manager server for collection includes the following procedures:

1. Download the CA Enterprise Log Manager virtual appliance package.
2. Install a CA Enterprise Log Manager server silently.
3. Configure the virtual appliance servers as described in the section on installing a CA Enterprise Log Manager server.

Important! If you want to provision a CA Enterprise Log Manager server using the virtual appliance, the Application Instance Name of the primary CA Enterprise Log Manager server must be CAELM.

Download the Virtual Appliance Package

The distribution image for the CA Enterprise Log Manager virtual appliance is available from Support Online from the Downloads link. There are five files that you must download:

- The manifest file
- The .ovf file
- Three virtual disk files

Install a CA Enterprise Log Manager Server Silently

When you install the virtual appliance silently, you must perform the following tasks:

1. Invoke the OVF Tool.
2. Set the Paravirtualization and Resource settings.
3. Power on the provisioned CA Enterprise Log Manager server.

The following table describes the parameters used to deploy CA Enterprise Log Manager using the OVF tool. You must specify these parameters as command line arguments in the command line.

Required information	Value	Comments
Host Specific Settings		
HOSTNAME	<i>hostname for this CA Enterprise Log Manager server</i> For example: CA-ELM1	Specify the host name for this server using only supported characters for hosts. Industry standards recommend A-Z (case-insensitive), 0-9, and hyphen, where the first character is a letter and the final character is alphanumeric. Do not use the underscore character in a host name, or append a domain name to this host. Note: The host name must not exceed 15 characters.
ROOT_PASSWORD	<i>new root password</i>	Create and confirm a new root password for this server.
IP_ADDRESS	<i>relevant IPv4 address</i>	Enter a valid IP address for this server.
SUBNET_MASK	<i>relevant IP address</i>	Enter a valid subnet mask for use with this server.
DEFAULT_GATEWAY	<i>relevant IP address</i>	Enter a valid subnet mask and default gateway for use with this server.
DNS_SERVERS	<i>relevant IPv4 addresses</i>	Enter one or more DNS server IP addresses in use in your network. The list is comma-separated with no spaces between entries. If your DNS servers use IPv6 addressing, enter these addresses in that format.

Required information	Value	Comments
DOMAIN_NAME	<i>your domain name</i>	Enter the qualified domain name in which this server operates, for example, mycompany.com. Note: The domain name must be registered with the Domain Name Server (DNS) server in your network to enable resolution of the hostname to IP address.
acceptAllEulas	Accept	Accept the CA license agreement to continue provisioning a CA Enterprise Log Manager server.
deploymentOption	medium or large	If you select medium, VMware provides four CPUs with 8 GB RAM for each CPU. If you select large, VMware provides eight CPUs with 8 GB RAM for each CPU.
TIMEZONE	<i>your desired time zone</i>	Select the time zone where this server resides.
NTPLOCATION	<i>relevant hostname or IP address</i>	Enter the host name or the valid IP address of the NTP server from which the CA Enterprise Log Manager server gets date and time information.
Application Specific Settings		
LOCAL_REMOTE_EEM	Local - for the first installed server (management server) Remote - for each additional server	Indicate whether you plan to use a local or a remote CA EEM server. For a management CA Enterprise Log Manager server, choose Local. The installation prompts you to create a password for the default EiamAdmin user account. For each additional server, choose Remote. The installation prompts you for the management server name. Regardless of whether you chose local or remote, you must use the EiamAdmin account ID and password to log on to each CA Enterprise Log Manager server the first-time.
REMOTE_EEM_LOCATION	<i>IP address or hostname</i>	Enter this value only if you select Remote in the Local or Remote server option. Enter the IP address or host name of the management CA Enterprise Log Manager server that you installed first. The host name must be registered with the DNS Server. If you want to use a local CA EEM server, the default value is none .

Required information	Value	Comments
EEM_PASSWORD	<i>EiamAdmin account password</i>	<p>Record the password for the default administrator account, EiamAdmin.</p> <p>Your CA Enterprise Log Manager server requires these account credentials for the initial login.</p> <p>If you are installing the management server, you are creating and confirming a new EiamAdmin password here.</p> <p>Make a note of this password as you must use it during the installations of other CA Enterprise Log Manager servers and agents.</p> <p>Note: The password you enter here is also the initial password for the default caelmadmin account that you use to access the CA Enterprise Log Manager server directly through ssh.</p> <p>You can create additional administrator accounts to access the CA EEM functions after installation, if desired.</p>
FIPS_MODE	Yes or No	<p>Specifies if the virtual appliance must run in FIPS mode or non-FIPS mode. If you choose to use a local CA EEM server, you can choose any mode. If you choose to use a remote CA EEM server, you must choose the mode that the remote CA EEM server uses.</p>

More information

[Adding Virtual Servers to Your Environment](#) (see page 286)
[Creating a Completely Virtual Environment](#) (see page 309)
[Deploying Virtual Servers Rapidly](#) (see page 332)

Invoke the OVF Tool Using Scripts

Note: You must install the OVF Tool 4.0.0 before you perform the silent installation. For more information about the OVF Tool, see the *VMware's OVF Tool User Guide* or www.vmware.com.

You can install multiple CA Enterprise Log Manager servers simultaneously by creating and running scripts containing the commands that invoke the OVF tool. You can use any scripting language to create scripts.

To invoke OVF tool using scripts

1. Create a script for the invoking the OVF tool.
2. Open the command prompt on the computer where VMware vSphere Client is installed.
3. Navigate to the path where you stored your script.
4. Run the script.

The message Opening VI target is displayed. The deployment status of each CA Enterprise Log Manager server is displayed. If the installation is successful, a CA Enterprise Log Manager server is listed under the datastore you selected in the left pane.

Example 1: Batch Script for creating a primary CA Enterprise Log Manager server and a secondary CA Enterprise Log Manager server

```
REM Primary CA Enterprise Log Manager Server
ovftool -dm=thin --acceptAllEulas --name="example_primaryserver"
--deploymentOption=medium --prop:ROOT_PASSWORD="example_password"
--prop:LOCAL_REMOTE_EEM=Local --prop:REMOTE_EEM_LOCATION=none
--prop:EEM_PASSWORD=calmr12 --prop:FIPS_MODE=Yes --prop:IP_ADDRESS=172.162.0.0
--prop:SUBNET_MASK=10.0.0.0 --prop:HOSTNAME="example_primary_server"
--prop:DEFAULT_GATEWAY=198.168.0.0 --prop:DNS_SERVERS=198.168.10.20,198.168.10.25
--prop:DOMAIN_NAME=example.com --prop:TIMEZONE=Asia/Kolkata
--prop:NTPLOCATION=198.168.10.30 "C:\Program Files\CA ELM\CA Enterprise Log
Manager.ovf"
"vi://administrator:password@examplevmwarehost/ELMQAvAppDatacenter/host/10.0.10.0
"
```

```
REM Secondary CA Enterprise Log Manager Server
```



```
ovftool -dm=thin --acceptAllEulas --name="example_secondaryserver"
--deploymentOption=medium --prop:ROOT_PASSWORD="example_password1"
--prop:LOCAL_REMOTE_EEM="Remote"
--prop:REMOTE_EEM_LOCATION="example_primaryserver" --prop:EEM_PASSWORD="calmr12"
--prop:FIPS_MODE="Yes" --prop:IP_ADDRESS="172.168.10.10"
--prop:SUBNET_MASK="10.0.10.10" --prop:HOSTNAME="example_secondary_server"
--prop:DEFAULT_GATEWAY="198.168.10.30"
--prop:DNS_SERVERS="198.168.20.20,198.168.20.25" --prop:DOMAIN_NAME="example.com"
--prop:TIMEZONE="Asia/Kolkata" --prop:NTPLOCATION=198.168.10.30 "C:\Program
Files\CA ELM\CA Enterprise Log Manager.ovf"
"vi://administrator:password@examplevmwarehost/ELMQAvAppDatacenter/host/10.0.10.0
"
```

Example 2: Batch Script for creating a management server and two collection servers

```
REM CA Enterprise Log Manager Management Server
ovftool -dm=thin --acceptAllEulas --name="example_managementserver"
--deploymentOption=medium --prop:ROOT_PASSWORD="example_password"
--prop:LOCAL_REMOTE_EEM=Local --prop:REMOTE_EEM_LOCATION=none
--prop:EEM_PASSWORD=calmr12 --prop:FIPS_MODE=Yes --prop:IP_ADDRESS=172.168.0.0
--prop:SUBNET_MASK=10.0.0.0 --prop:HOSTNAME="example_management_server"
--prop:DEFAULT_GATEWAY=198.168.0.0 --prop:DNS_SERVERS=198.168.10.20,198.168.10.25
--prop:DOMAIN_NAME=example.com --prop:TIMEZONE=Asia/Kolkata
--prop:NTPLOCATION=198.168.10.30 "C:\Program Files\CA ELM\CA Enterprise Log
Manager.ovf"
"vi://administrator:password@examplevmwarehost/ELMQAvAppDatacenter/host/10.0.10.0
"
```

```
REM CA Enterprise Log Manager Collection Server 1
ovftool -dm=thin --acceptAllEulas --name="example_collectionserver1"
--deploymentOption=medium --prop:ROOT_PASSWORD="example_password1"
--prop:LOCAL_REMOTE_EEM=Remote
--prop:REMOTE_EEM_LOCATION="example_managementserver" --prop:EEM_PASSWORD=calmr12
--prop:FIPS_MODE=Yes --prop:IP_ADDRESS=172.168.10.10 --prop:SUBNET_MASK=10.0.10.10
--prop:HOSTNAME="example_collection_server1" --prop:DEFAULT_GATEWAY=198.168.10.30
--prop:DNS_SERVERS=198.168.20.20,198.168.20.25 --prop:DOMAIN_NAME=example.com
--prop:TIMEZONE=Asia/Kolkata --prop:NTPLOCATION=198.168.10.30 "C:\Program Files\CA
ELM\CA Enterprise Log Manager.ovf"
"vi://administrator:password@examplevmwarehost/ELMQAvAppDatacenter/host/10.0.10.0
"
```

```
REM CA Enterprise Log Manager Collection Server 2
```

```
ovftool -dm=thin --acceptAllEulas --name="example_collectionserver2"
--deploymentOption=medium --prop:ROOT_PASSWORD="example_password2"
--prop:LOCAL_REMOTE_EEM=Remote
--prop:REMOTE_EEM_LOCATION="example_managementserver" --prop:EEM_PASSWORD=calmr12
--prop:FIPS_MODE=Yes --prop:IP_ADDRESS=172.168.10.30 --prop:SUBNET_MASK=10.0.10.40
--prop:HOSTNAME="example_collection_server2" --prop:DEFAULT_GATEWAY=198.168.10.40
--prop:DNS_SERVERS=198.168.30.30,198.168.30.25 --prop:DOMAIN_NAME=example.com
--prop:TIMEZONE=Asia/Kolkata --prop:NTPLLOCATION=198.168.10.30 "C:\Program Files\CA
ELM\CA Enterprise Log Manager.ovf"
"vi://administrator:password@examplevmwarehost/ELMQAvAppDatacenter/host/10.0.10.0
"
```

Set the Paravirtualization and Resource Settings

After you import the OVF template, you must manually set the paravirtualization and resource settings to improve the performance of the provisioned CA Enterprise Log Manager server.

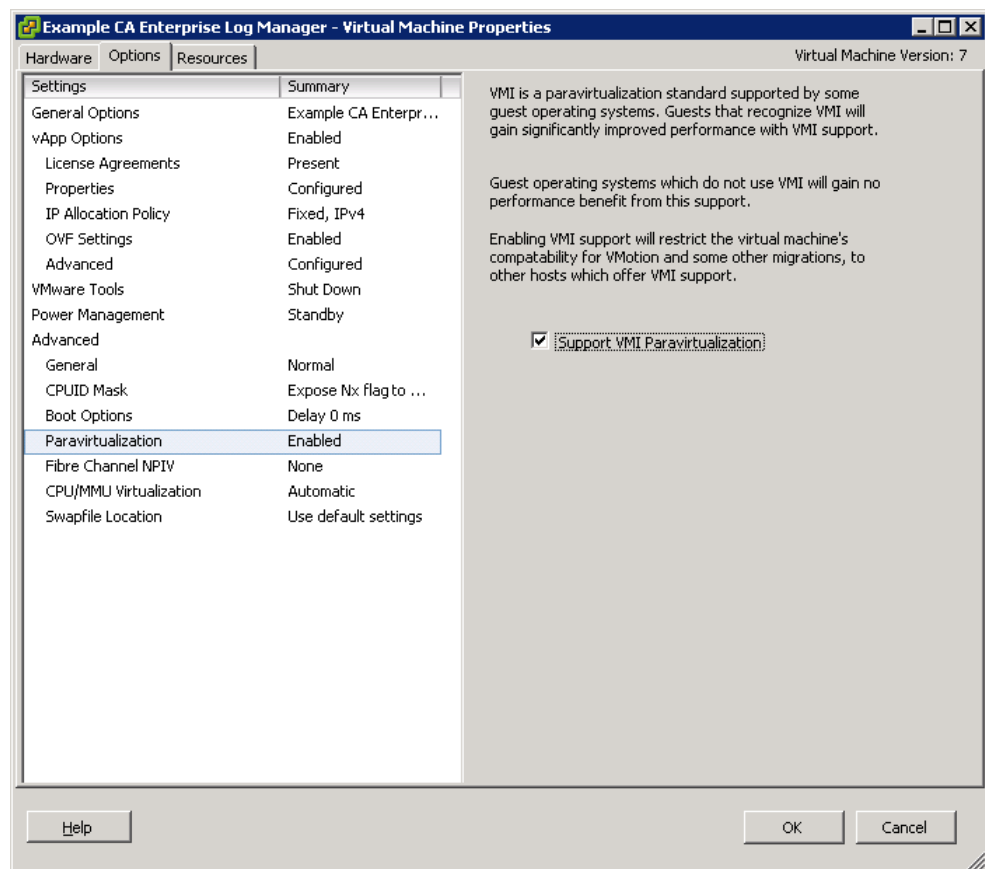
Note: Verify that you set the CD/DVD Drive to Client Device.

To set the paravirtualization and resource settings

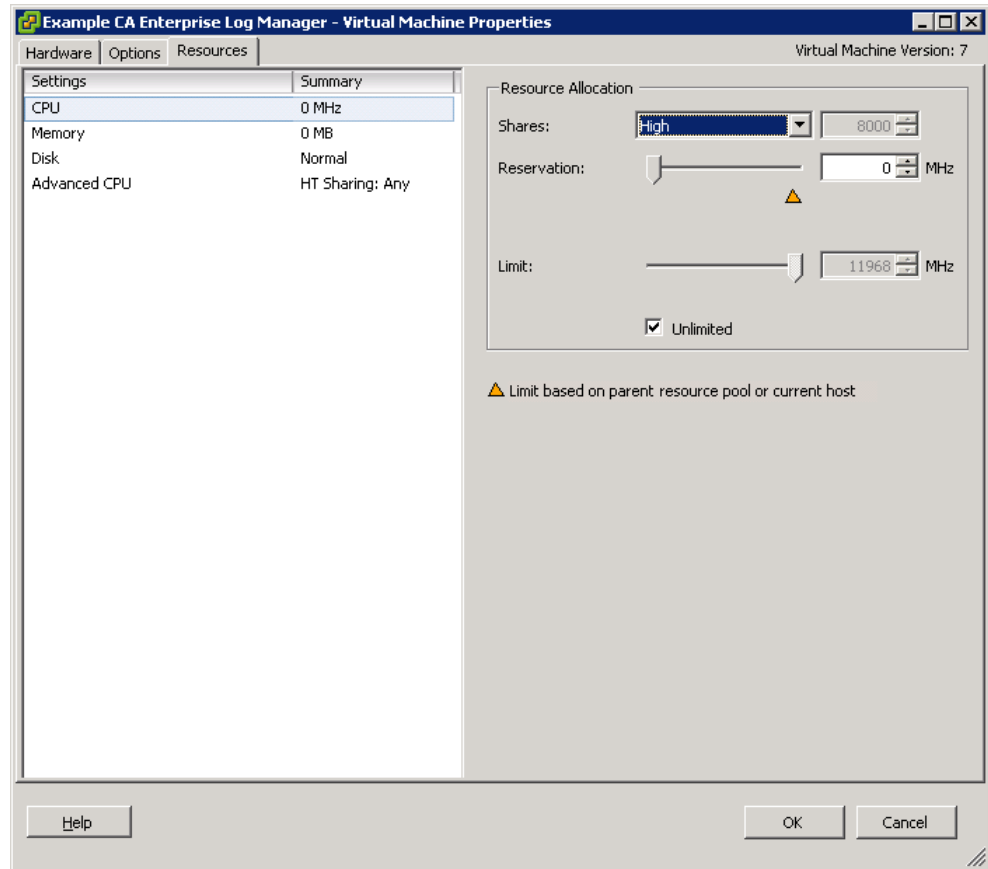
1. Right-click the new CA Enterprise Log Manager Virtual Appliance in the left pane, and click Edit Settings.

The *<CA Enterprise Log Manager Virtual Appliance name>* - Virtual Machine Properties window appears.

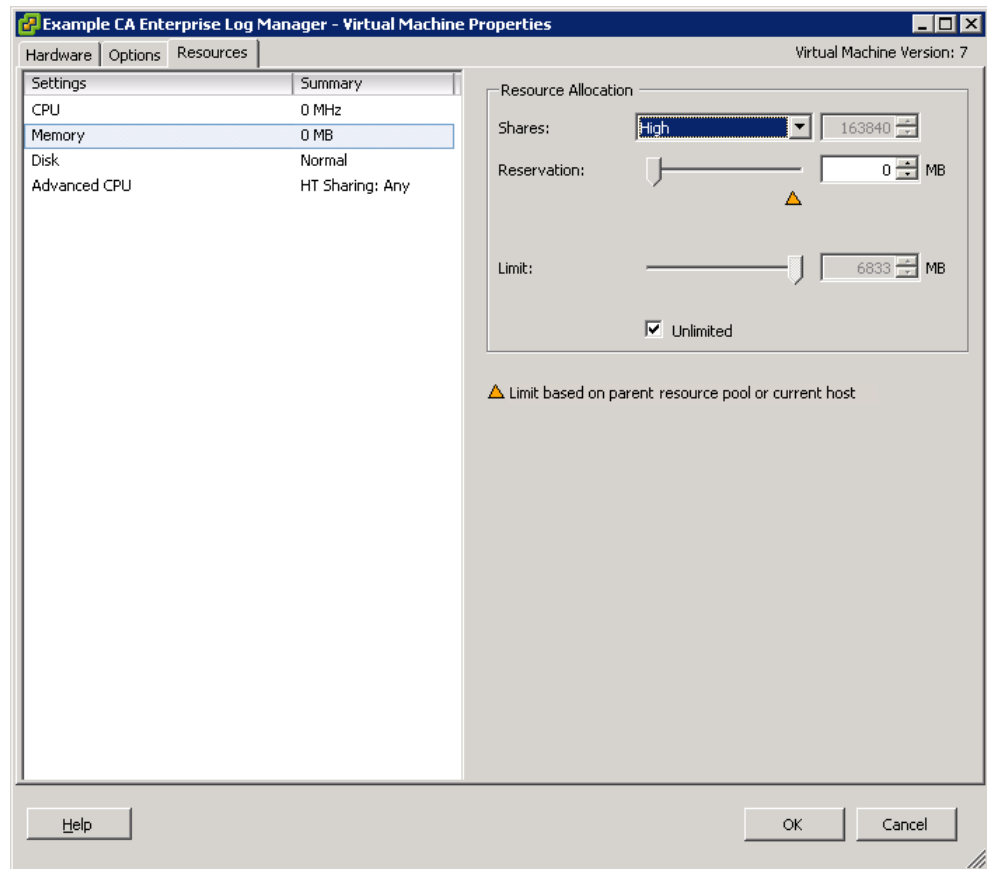
2. Click the Option tab in the window.
3. Select the Paravirtualization setting in the left pane, and select the Support VMI Paravirtualization option in the right pane.



4. Click the Resources tab in the window.
5. Select the CPU option under the Settings column, and select High from the Shares drop-down in the Resource Allocation section.



6. Select the Memory option under the Settings column, and select High from the Shares drop-down in the Resource Allocation section.



7. Click OK.
8. **Note:** For more information about Paravirtualization, go to www.vmware.com.

Power on the Provisioned CA Enterprise Log Manager Server

You must power on the CA Enterprise Log Manager server to start running it.

To power on a CA Enterprise Log Manager server

1. Select the new CA Enterprise Log Manager server in the left pane of the VMware application window.
2. Click the Power On option under Basic Tasks of the Getting Started tab in the right pane.

The CA Enterprise Log Manager server is powered on.

Note: Verify that a primary CA Enterprise Log Manager server is running before you power on a secondary CA Enterprise Log Manager server.

Verify the Installation of a Virtual CA Enterprise Log Manager Server

When you power on the provisioned CA Enterprise Log Manager server, a URL to access CA Enterprise Log Manager is displayed in the Console tab of the VMware vSphere Client window. Use this URL and the following default login credentials to access CA Enterprise Log Manager:

Default Username: EiamAdmin

Default Password: The password you entered during the CA Enterprise Log Manager server installation procedure

More information

[Adding Virtual Servers to Your Environment](#) (see page 286)

[Creating a Completely Virtual Environment](#) (see page 309)

[Deploying Virtual Servers Rapidly](#) (see page 332)

Post Installation Tasks

After you power on a CA Enterprise Log Manager server, you can do the following:

- Change the keyboard type
- Add an NTP server

Change the Keyboard Type

By default, a provisioned CA Enterprise Log Manager server uses the standard US keyboard. You can change the keyboard type you want to use by changing its national language setting.

To change the keyboard type

1. Login to the CA Enterprise Log Manager console as root user.
2. Execute the following command:

```
vi /etc/sysconfig/keyboard
```

The keyboard file opens in edit mode. The existing keyboard type details are displayed.
3. Replace US in the KEYTABLE value with the national language setting you want.
For example, to use a UK keyboard, enter KEYTABLE value as KEYTABLE="UK".
Note: For more information about the national language settings, see the RHEL installation documentation set.
4. Save and close the file.
5. Restart the computer.
The keyboard type is changed.

Add an NTP Server

We highly recommend that you add an NTP server to update the date and time of CA Enterprise Log Manager server.

To add an NTP server

1. Login to the CA Enterprise Log Manager console as root user.
2. Execute the following commands:

```
crontab -e
```

```
00 0 * * * /usr/sbin/ntpdate NTPserver_hostname
```

A cron job is added.
3. Save the changes, and exit the console.
The NTP server is added.

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

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.

custom MIB

A *custom MIB* is a MIB you create for an action alert sent to an SNMP trap destination, such as CA NSM. The custom trap ID specified in the action alert assumes the existence of an associated custom MIB that defines the selected CEG fields sent as a trap.

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 Technologies 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.

FIPS 140-2

FIPS 140-2 is the Federal Information Processing Standard. This federal standard specifies the security requirements for cryptographic modules used within a security system that protects sensitive but unclassified information. The standard provides four increasing, qualitative levels of security intended to cover a wide range of potential applications and environments.

FIPS 140-2 compatible

FIPS 140-2 compatible is a designation for a product that can *optionally* use FIPS-compliant cryptographic libraries and algorithms to encrypt and decrypt sensitive data. CA Enterprise Log Manager is a FIPS-compatible log collection product because you can select whether to run in FIPS mode or non-FIPS mode.

FIPS 140-2 compliant

FIPS 140-2 compliant is a designation for a product that by default uses *only* encryption algorithms certified by an accredited Cryptographic Module Testing (CMT) laboratory. CA Enterprise Log Manager can use cryptographic modules based on the certified RSA BSAFE Crypto-C ME and Crypto-J libraries in FIPS mode, but may not do so by default.

FIPS mode

FIPS mode is the setting that requires CA Enterprise Log Manager servers and agents to use FIPS-certified cryptographic modules from RSA for encryption. The alternative setting is non-FIPS mode.

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 Technologies 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.

non-FIPS mode

Non-FIPS mode is the default setting that permits CA Enterprise Log Manager servers and agents to use a combination of encryption techniques, some of which are not FIPS-compliant. The alternative setting is FIPS mode.

non-interactive ssh authentication

Non-interactive authentication enables files to move from one server to another without requiring the entry of a passphrase for authentication. Set non-interactive authentication from the source server to the destination server before configuring auto archiving or using the `restore-ca-elm.sh` script.

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 Technologies 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 Technologies 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 Technologies Audit before iTechnology. SAPI stands for Submit API (Application Programming Interface). CA Technologies 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

A *soft appliance* is a fully functional software package that contains the software as well as the underlying operating system and all dependant packages. It is installed onto end-user provided hardware by booting from the soft appliance installation media.

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 Technologies 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)

Subscription 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 Technologies 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 Technologies 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 updates refer to the binary and non-binary files that are made available by CA Technologies 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.

varbind

A *varbind* is an SNMP variable binding. Each varbind is made up of an OID, a type, and a value. You add varbinds to a custom MIB.

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

A

- administration tasks
 - user store • 114
- agents
 - about • 54
 - about agent groups • 55
 - default agent • 175
 - installing • 173
 - planning for • 52
 - user account privileges • 55
 - viewing status • 186

- archive
 - about archive files • 129
 - example • 141

C

- CA Adapters
 - configuring for use with CA Audit • 205, 208
- CA Audit
 - architecture differences • 199
 - configuring CA adapters • 205
 - considerations for users of • 199
 - modify existing r8 SP1 CR2 policy • 210
 - modify existing r8 SP2 policy • 212
 - sending events to CA Enterprise Log Manager • 209
 - when to import events • 213
- CA Embedded Entitlements Manager
 - defined • 28
- CA Enterprise Log Manager
 - federation • 30
 - installation • 67
 - planning the architecture • 59
 - processes • 90
- CA Management Database (CA-MDB)
 - user store • 114
- caelmadmin account
 - defined • 87
- configurations
 - initial server configurations • 86
- connectors
 - about log sensors • 56
 - stopping and restarting • 186
 - viewing status • 186

D

- default agent
 - configuring a connector with the ODBC log sensor • 177
 - configuring a connector with the WinRM log sensor • 182
- disaster recovery
 - back up a CA Enterprise Log Manager server • 262
 - back up CA Embedded Entitlements Manager server • 260
 - planning • 259
 - replace a CA Enterprise Log Manager server • 264
 - restore a CA Embedded Entitlements Manager server • 261
 - restore a CA Enterprise Log Manager server • 263
- disk space
 - planning • 28

E

- event log store
 - about • 129
 - about archive files • 129
 - basic settings • 146
 - configuring • 128, 148
- event plugin
 - iTechnology event plugin • 208
- event refinement library
 - about • 197
 - supporting new event sources • 197
- examples
 - auto-archiving across three servers • 141
 - direct collection of database logs • 177
 - direct collection of Windows logs • 182
 - subscription configuration with six servers • 50

F

- federation
 - about queries and reports in • 189
 - configuring • 193
 - federation map • 31

- federation map example for a large enterprise • 32
- federation map example for a mid-sized enterprise • 34
- heirarchical • 190
- meshed • 191
- planning • 30
- select federated queries • 127
- filters
 - global and local • 126

I

- iGateway process
 - controlling • 67
 - user account for controlling • 87
- importing
 - SEOSDATA events from CA Audit • 214, 220
- installation
 - CA IT PAM with shared CA EEM • 249
 - create DVDs for install • 61
 - customized operating system image • 88
 - default directory structure • 87
 - of CA Enterprise Log Manager • 67
 - on system with SAN drives • 79
 - troubleshooting • 102
 - verify CA Enterprise Log Manager server • 70
- integration with CA Audit
 - configuring CA Technologies Adapters • 205
 - importing SEOSDATA events • 214
 - sending CA Audit events to CA Enterprise Log Manager • 209
 - understanding architectures • 199
 - when to import events • 213
- integrations
 - about • 55
- iTechnology event listener
 - about • 208

L

- LMSeosImport utility
 - about the utility • 213
 - command line examples • 218
 - copy to Solaris Data Tools server • 215
 - copy to Windows Data Tools server • 215
 - import events from Windows Data Tools server • 220
 - import from Solaris Data Tools server • 220
 - import options • 216

- importing from a live SEOSDATA table • 214
- using the command line • 216
- when to import events • 213
- log collection
 - guidelines • 29
 - planning • 26
- log sensors
 - about • 56

N

- non-interactive authentication
 - configuring for auto archive • 132
 - hub and spoke example • 133
 - simplest use case example • 140

P

- password policies
 - configuring • 117
 - planning • 40
- planning
 - disaster recovery • 259
 - disk space • 28
 - federation • 30
 - integration with CA Audit • 199
 - password policies • 40
 - sizing • 57
 - user store • 36
- plugin
 - iTechnology event plugin • 208
- ports
 - firewall, for syslogs • 93
 - network adapter • 103

S

- SAN drives
 - install CA Enterprise Log Manager with disabled, • 79
 - install CA Enterprise Log Manager with enabled, • 85
- self-monitoring events
 - viewing • 71
- server roles
 - in federated reports • 32
- subscription management
 - example configuration • 50
- suppression rules
 - effects • 58
- syslog

collection defined • 52

U

user accounts

adding an application user group • 120

user and access management

configuring the user store • 114

user roles

assigning • 120

user store

CA SiteMinder worksheet • 39

configuring as CA-MDB • 114

external LDAP directory worksheet • 37

planning • 36

reference an LDAP directory • 115

referencing CA SiteMinder • 116

W

worksheets

CA SiteMinder • 39

external LDAP directory • 37