CA Virtual Assurance for Infrastructure Managers

Installation Guide

Release 12.7.1

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 © 2013 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 eHealth®
- CA Embedded Entitlements Manager (CA EEM)
- CA IT Asset Manager (CA ITAM)
- CA IT Client Manager (CA ITCM)
- CA Network and Systems Management (CA NSM)
- CA Patch Manager
- CA Server Automation
- CA Service Desk Manager (CA SDM)
- CA Spectrum®
- CA SystemEDGE
- CA Systems Performance for Infrastructure Managers
- CA Virtual Assurance for Infrastructure Managers
- CA Software Delivery

Contact CA Technologies

Contact CA Support

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

- 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

Providing Feedback About Product Documentation

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

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.

Contents

Chapter 1: Introduction 9

Scope 9
Audience 9
Related Publications 10
Conventions 10

Chapter 2: Installing CA Virtual Assurance 13

Installation Requirements and Considerations 13
- Install and Configure SQL Server Express 13
- Verify Requirements for Using SQL Server 14
- Security Considerations 15
- Optimize Windows Memory Management 15
- Comparison between SystemEDGE and CA Systems Performance LiteAgent 15

Installation of CA Virtual Assurance 17
- Prepare for the Installation 17
- Run the Installation 19
- Canceling the Installation 22
- Component Installation after Initial Installation 22

Silent Manager Installation 23
- Copy the Silent Installation Files from the Installation Media 23
- Edit the silent.properties File 24
- Perform a Silent Manager Installation 24

Installation on Multiple Servers 25
- Guidelines for an Installation on Multiple Servers 25
- Communication Ports 27

How to Adjust SQL Server User Permissions to the Required Minimum 30
- Review Requirements 31
- Create a Database User With the dbcreator Role 31
- Install the Product Using the New Database User 32
- Change the Owner of the aom2 and dpm Databases to sa 32
- Adjust the Permissions of the New Database User to the Required Minimum 33
- Log in the User Interface and Manage Your Environments 33

How to Update CA Virtual Assurance 34
- Check for Updates 34
- Download and Apply the Updates (PTFs) 35

Agent Deployment 36

Create a Deployment Job 37
Individual Agent Installations 39
Dependencies of SystemEDGE Components 39
SystemEDGE Installation Through CA Virtual Assurance Manager Installer 40
Installation on Windows Systems 41
Installation on UNIX and Linux Systems 53
Configure and Use a Response File 66
Install the Agent in Legacy Mode 67
Install AIMs 67
Install the CA Systems Performance LiteAgent 69

Chapter 3: Upgrading CA Virtual Assurance 71

Supported Upgrades 71
How to Upgrade CA Virtual Assurance 72
Review Upgrade Documentation 73
Prepare the Environment You Want to Upgrade 74
Establish a Maintenance Window 75
Apply Important Patches 75
Back up the Entire System 75
Revert Multiple Apache Configuration to Single Apache 76
Stop Services 77
Review Upgrade Limitations 77
Upgrade Remote CA EEM Manually 78
Run Manager Installation 78
Review Old Configurations Not Upgraded Automatically 80
Apply Old Configurations Manually 80
Upgrade Managed Nodes and AIM Servers 80
Agent and AIM Upgrades 81
Import SystemEDGE Monitors into a Policy 84
Verify the CA Virtual Assurance Upgrade in Your Environment 85

Chapter 4: Getting Started with User Interfaces 87

Start CA Virtual Assurance 87
Functional Overview 88
Start AutoShell 89
Valid AutoShell User 90
Start the CA Virtual Assurance Command Prompt 90
Start the Bookshelf and Online Help 91

Chapter 5: Uninstalling CA Virtual Assurance 93

Uninstallation Options 93
Uninstalling the Manager 93
Perform a Complete Uninstall 94
Uninstall the Manager from Command Prompt 95
Uninstall the Manager in Silent Mode 95
Uninstalling SystemEDGE 96
Uninstall SystemEDGE and the AIMs on Windows 96
Uninstall SystemEDGE and the AIMs on UNIX Systems 98

Chapter 6: Backup and Restore 101

Backup and Restore Overview 101
Back up the Entire System 102
Back up the Configuration and Data 103
Back up the Databases 103
Back up the Directories and Data 104
Restore the Entire System 107
Restore the Configuration and Data 107
Restore the Databases 108
Restore the Directories and Data 109

Chapter 7: Scalability Best Practices 111

Scalability Overview 111
Hardware Specifications 112
Database Considerations 112
Network Considerations 113
Remote Deployment and Policy Configuration Overview 113
Scalability Recommendations 115
vCenter AIM Monitoring Recommendations 115
CA Virtual Assurance vCenter Management Recommendations 116
LPAR AIM Monitoring Recommendations 118
Solaris Zones AIM Monitoring Recommendations 119
Remote Deployment and Policy Configuration Recommendations 120

Glossary 129

Index 131

Chapter 1: Introduction

CA Virtual Assurance is a policy-based product that manages the performance of virtual data center infrastructures.

Built on a Service Oriented Architecture, CA Virtual Assurance continuously analyzes these infrastructures to ensure that UNIX, Linux, and Windows servers are provisioned to perform required tasks and that changes are automatically detected.

CA Virtual Assurance improves operational efficiency and end-to-end data center automation by enhancing the performance and workload of virtual and dynamic environments.

This section contains the following topics:

Scope (see page 9)
Audience (see page 9)
Related Publications (see page 10)
Conventions (see page 10)

Scope

This guide explains how to install and implement CA Virtual Assurance and how to get started with this product. It provides a brief overview about the product architecture, its components, and requirements.

The guide describes step-by-step installations of CA Virtual Assurance in different modes and details post-installation tasks.

A glossary explains specific terminology used in virtualization technologies.

Audience

This guide is intended for administrators who install, configure, and use CA Virtual Assurance to manage virtual environments. It assumes that you are familiar with the operating systems used in your environment, virtualization technologies, and SNMP.

Related Publications

The CA Virtual Assurance documentation consists of the following deliverables:

Administration Guide

Explores how to administer and use CA Virtual Assurance to manage virtual resources in your environment.

Installation Guide

Contains brief architecture information, various installation methods, post-installation configuration information, and Getting Started instructions.

Online Help

Provides window details and procedural descriptions for using the CA Virtual Assurance user interface.

Reference Guide

Provides detailed information about AutoShell, CLI commands, MIB attributes, and performance metrics.

Release Notes

Provides information about operating system support, system requirements, published fixes, international support, known issues, and the documentation roadmap.

Service Response Monitoring User Guide

Provides installation and configuration details of SRM.

SystemEDGE User Guide

Provides installation and configuration details of SystemEDGE.

SystemEDGE Release Notes

Provides information about operating system support, system requirements, and features.

Conventions

This guide uses the following conventions:

Case-Sensitivity

All names of classes, commands, directives, environment parameters, functions, and properties mentioned in this guide are case-sensitive and you must spell them exactly as shown. System command and environment variable names *may* be case-sensitive, depending on your operating system's requirements.

Cross-References

References to information in other guides or in other sections in this guide appear in the following format:

Guide Name

Indicates the name of another guide.

"Chapter Name"

Indicates the name of a chapter in this or another guide.

Synonyms

Terms such as attribute, object, object identifier (OID) are synonymous to the term 'variable' in this document.

Terms such as SystemEDGE Agent, CA SystemEDGE are synonymous to SystemEDGE in this document.

Syntax

Syntax and user input use the following form:

Italic

Indicates a variable name or placeholder for which you must supply an actual value.

{a|b}

Indicates a choice of mandatory operands, a or b.

[ ] or [[ ]]

Indicates optional operands.

Syntax Example

The following example uses these conventions:

`modify -t ZONE [-m zoneserver] -p psetname {-min mincpu|-max maxcpu} pset -session ssh`

The operands -min and -max are mandatory, but you can only use one of them depending on what you want to define, the minimum number of CPUs in the processor set or the maximum number. The operand -m is not required for this command to function. All other parts of the command must be entered as shown.

Default Directory

CASYSEDGE used in path statements indicates the directory in which SystemEDGE is installed. **Default:** C:\Program Files\CA\SystemEDGE.

Installation Path

Install_Path used in path statements indicates the directory in which CA Virtual Assurance or components of CA Virtual Assurance are installed.

Defaults:

- Windows x86: C:\Program Files\CA
- Windows x64: C:\CA, C:\Program Files (x86)\CA, or C:\Program Files\CA
- UNIX, Linux: /opt/CA

Chapter 2: Installing CA Virtual Assurance

This section contains the following topics:

Installation Requirements and Considerations (see page 13)
Installation of CA Virtual Assurance (see page 17)
Silent Manager Installation (see page 23)
Installation on Multiple Servers (see page 25)
How to Adjust SQL Server User Permissions to the Required Minimum (see page 30)
How to Update CA Virtual Assurance (see page 34)
Agent Deployment (see page 36)
Individual Agent Installations (see page 39)

Installation Requirements and Considerations

This section provides information on requirements and considerations to install CA Virtual Assurance.

Install and Configure SQL Server Express

If you do not have SQL Server installed, install SQL Server Express from DVD1 alternatively.

Follow these steps:

1. Change to the Installers\Windows\External\MSSQLExpress directory on DVD1 and run setup.
2. After the installation, use SQL Server Configuration Manager to enable TCP/IP.
3. Determine the static TCP Port number from SQL Server Configuration Manager (Network Configuration/Protocols/TCP/IP Properties/IP Addresses).
4. Apply the port number and instance name (SQLEXPRESS per default) during CA Virtual Assurance installation to connect with SQL Server Express.

If you plan to access a *remote SQL Server*:

- Install SQL Server Client on the CA Virtual Assurance manager computer.
- Enable Remote Connections on the remote SQL Server.

More Information

Verify Requirements for Using SQL Server (see page 14)

Verify Requirements for Using SQL Server

CA Virtual Assurance requires SQL Server for Management Database and Performance Database. CA Virtual Assurance provides the following SQL Server support:

- Local or remote SQL Server
- Default SQL Server instance or named instances
- Static SQL Server TCP/IP port
- Windows authentication and SQL Server authentication

Follow these steps:

1. Verify SQL Server requirements
   - Verify that TCP/IP is enabled.
   - Verify that a static TCP/IP port is specified for the instance that you plan to use. Dynamic ports are not supported.
   - Verify that there is no IP address used as the server name for the local database.
   - Verify that Remote Connections are enabled if you want to connect from a remote computer.
   - Verify that the authentication mode that you require is specified (Mixed Mode or Windows authentication).
   - Verify that the instance that you plan to use for a new typical or custom installation does not contain databases named AOM2 or DPM. CA Virtual Assurance creates these databases during installation.
2. Verify SQL Server Client requirements

   Verify that the SQL Server Client is installed on the local CA Virtual Assurance manager system. CA Virtual Assurance manager requires the SQL Server Client to connect to a local or remote SQL Server. The CA Virtual Assurance manager installation program uses the available system PATH entries to access the SQL Server Client programs.

Security Considerations

CA Virtual Assurance is secured using the CA Embedded Entitlements Manager (CA EEM). When installing CA Virtual Assurance, you can select one of the following authentication methods.

Native Security

If you are the CA EEM administrator, you can create your own universe of users, user groups, and policies specifically for CA Virtual Assurance because all this information is kept in the local store. However, this requires you to define your own set of users and user groups manually, which can be inconsistent with what is currently available in your directory service.

Active Directory

When you integrate with an existing Active Directory configuration, all your users and user groups are predefined and remain consistent with your central repository of users. However, use Active Directory to create new users or modify existing ones; you cannot use CA Virtual Assurance or CA EEM to do so.

Evaluate your requirements and select the setting that best fits them.

Optimize Windows Memory Management

To optimize Windows Memory Management performance on the CA Virtual Assurance manager or on the CA Virtual Assurance AIM server, you can apply the settings described in the Microsoft Knowledge Base article:
http://support.microsoft.com/kb/Q315407

Comparison between SystemEDGE and CA Systems Performance LiteAgent

CA Virtual Assurance ships with two monitoring agents, SystemEDGE and CA Systems Performance LiteAgent.

SystemEDGE is an SNMP-compliant agent providing access to monitored elements using an industry standard MIB. SystemEDGE also provides an extensible plug-in (AIM) interface which allows additional monitoring, such as vCenter Server, Solaris Zones or Service Response monitoring. SystemEDGE provides status and performance data to the CA Virtual Assurance manager. SystemEDGE is mandatory to manage virtual environments and servers.

CA Systems Performance LiteAgent is a lightweight monitoring agent, providing access to many performance metrics on Windows, UNIX, and Linux. On Windows, including the ability to monitor virtually all metrics included in the Performance Registry. Monitoring is performed on-demand based on a request from a manager component. CA Systems Performance LiteAgent provides performance data to the CA Virtual Assurance manager.

For further details on the differences between SystemEDGE and CA Systems Performance LiteAgent, refer to the following table:

Feature	SystemEDGE Agent	CA Systems Performance LiteAgent
SNMP-compliant agent	Y	N
SNMP-based traps	Y	N
Zero configuration agent	N	Y
SNMP v1/v2 communications	Y	N
SNMP v3 communications	Y	N
Monitoring restriction by computer name/address	Y	N
CAM-based communications	Configuration operations only	Y
Support for multiple manager instances	Y	Y
Support for Spectrum IM	Y	N
Support for eHealth	Y	N
Support for NSM	Y	Y
Support for third Party Managers	Y	N
Support for the UI Resource tab	Y	N
Support for the UI Policy tab	Y	Y
Data stored in Performance DB	Y	Y
File based configuration	Y	n/a
Manager UI-based configuration	Y	n/a
Hierarchical object model	Y	N
Agent-based threshold monitoring	Y	N
Support for Host Resource MIB	Y	N
Windows performance metrics	Partial [1]	Y
Extensible performance monitoring	N	Y [2]
Wide breadth UNIX or Linux monitoring	Y	Y
True average performance monitoring	Y	N
Support for vCenter Server management	Y (AIM)	N

Feature	SystemEDGE Agent	CA Systems Performance LiteAgent
Support for Hyper-V management	Y (AIM)	N
Support for Solaris Zones management	Y (AIM)	N
Support for LPAR monitoring	Y (AIM)	Y
Support for UCS management	Y (AIM)	N
Support for Exchange Server and Active Directory	Y (AIM)	N
Support for IBM High Availability Cluster Multiprocessing AIM	Y (AIM)	N
Support for VMware vCloud AIM	Y (AIM)	N
Support for Citrix XenServer AIM	Y (AIM)	N
Support for KVM AIM	Y (AIM)	N

(1) SystemEDGE provides support for a limited set of performance metrics. See the *SystemEDGE User Guide*.

(2) CA Systems Performance LiteAgent can monitor Windows Performance Metrics dynamically.

Installation of CA Virtual Assurance

This section details the components, installation options, and procedures for installing CA Virtual Assurance in a Windows operating environment.

Prepare for the Installation

The installation lets you select which components to install or specify credentials. During the installation, the wizard displays only the dialogs necessary to install the selected components. Depending on your selections, the installation wizard requests the following environment-related data (default values in parentheses):

Component	Server	User	Password	Protocol	Port
Management DB (1)	X	X (sa)	X	-	X (1443)
Performance DB (1)	X	X (sa)	X	-	X (1443)
CA EEM Authentication (2)	X	EiamAdmin	X	-	-

Component	Server	User	Password	Protocol	Port
Apache Logon as Service User (3)	-	X	X	-	-
Tomcat Logon as Service User (4)	-	X	X	-	-
Native Security User (5)	-	X	X	-	-
Active Directory Security (5, 6)	X	X	X	-	-
System User	-	sys_service	X	-	-
Network Discovery Gateway	-	-	-	-	X (8082)
Apache HTTP Server	-	-	-	-	X (443)
Apache Tomcat Server	-	-	-	-	X (8443)
Apache Tomcat Shutdown	-	-	-	-	X (8005)
ActiveMQ	-	-	-	-	X (61616)

(1) Select Windows Authentication (default) or SQL Authentication. If SQL Authentication is selected, enter the name of the database administrator (sa) and password. Select the appropriate initial size of the Management Database:

Initial Size	Number of Systems	Disk Space
Small	1,000	1 GB - core components 500 MB - log files
Medium	5,000	5 GB - core components 1 GB - log files
Large	10,000	10 GB - core components 5 GB - log files

The SQL Server databases are set to Full Recovery Model by default, so the transaction log grows until it is backed up. Regularly schedule database backups.

The Performance database defaults to 500 MB and increases automatically as needed.

(2) CA EEM supports only one AIP instance. If an AIP instance exists in the specified EEM installation, do one of the following options:

- Specify a CA EEM installation without an AIP instance.
- Remove the AIP instance, if it is no longer required. Open <EMM> user interface, open the Configure tab, select AIP, click Unregister.
- Let CA Virtual Assurance install CA EEM on the local system.

(3) Enter the user name and password to grant Logon as Service permissions for Apache to a Windows administrative domain user. This user is required if you use Windows Authentication for a remote SQL Server. See also Installation on Multiple Servers (see page 25) in this chapter.

(4) Enter the user name and password to grant Logon as Service permissions for Tomcat to a Windows administrative domain user. This user is required if you use Windows Authentication for a remote SQL Server. You can specify the same user for Tomcat and Apache. See also Installation on Multiple Servers (see page 25) in this chapter.

(5) Select Active Directory Security or Native Security (default).

(6) Select Active Directory Security, provide the External Directory host name, user, and password.

Note: If the installation installs SystemEDGE on the same system as the Distribution Server, the Configuration Manager Host Name for SystemEDGE is set to localhost.

More Information

SystemEDGE Installation Through CA Virtual Assurance Manager Installer (see page 40)

Run the Installation

Perform this procedure after you determine that all prerequisites have been met.

Follow these steps:

1. Insert the installation media into the DVD drive.

   If autorun is enabled, the installation wizard starts automatically. If the installation wizard does not start, double-click setup.hta or navigate to the *DVDdrive*\Installers\Windows directory on the installation media and double-click install.exe.

   The Preinstall Checks dialog appears.

2. Verify that the Preinstall Check items are passed.

   If an item fails, fix the requirement and restart the installation.

3. Click Continue.

   The License Agreement dialog appears.

4. Read and scroll to the bottom of the agreement until the *I accept the terms of the License Agreement* option is active. Select this option and click Next.

   The Choose Features To Install dialog appears.

5. Select the CA Virtual Assurance component to install and click Next.

   The Required Configuration dialog appears.

6. Review the items with a green checkmark and items with red x icon.

   - Installation Paths

     Note: The following characters are not supported in the destination path: exclamation point (!), left square bracket ([), right square bracket (]), left parenthesis '(', right parenthesis ')', and semicolon (;).

   - Database

     Verify the Management and Performance Database settings and change the database server name, instance, authentication type, or port number (1433) if necessary. Click OK.

     Default: Windows Authentication

     If you select SQL Authentication, enter the name of the database administrator (sa) and password.

     Note: If the database login credentials, server name, or port is not valid, an error message appears and you can enter the correct information. If the error cannot be resolved, the installation program exits and no changes are made to your computer. For more information, see the Verify Requirements for Using SQL Server (see page 14) section.

   - CA EEM

     If you do not refer to an existing CA EEM installation, CA Virtual Assurance installs CA EEM on the local system. CA Virtual Assurance creates an AIP instance in CA EEM during installation. CA EEM supports only one AIP instance.

     If you refer to an existing CA EEM installation, the installation program checks CA EEM for a registered AIP instance. If the installation program discovers an AIP instance, the installation process stops. If the AIP instance is no longer used, you can unregister it. To remove an AIP instance from CA EEM: Open CA EEM user interface, open the Configure tab, select AIP, click Unregister.

- Network Ports

  You can specify the network ports for the listed components or accept the following default values:

  - Network Discovery Gateway Port: 8082
  - Apache Port: 443
  - Tomcat Server Port: 8443
  - Tomcat Shutdown Port: 8005
  - Apache ActiveMQ Message Broker Port: 61616

- Additional Runtime Locale

  If necessary, specify *one* additional locale to activate, and click Ok.

  Default: English (United States)

- SNMP Management

  In addition to the default communities public and admin and their associated SNMP ports 161, 1691, and 6665, you can specify your own read-only and read-write community and port.

  Default: public, snmp_admin

  All communities which are specified during installation, are used as global (default) SNMP Settings in the installed product. If necessary, you can specify further SNMP settings in the CA Virtual Assurance user interface. See the *Administration Guide*, section How to Configure SNMP and Access Control Lists.

7. Enter the necessary information and click Next.

   The Pre-installation Summary dialog opens with the list of components to install.

8. Click Install to start the installation.

   The installation progress dialog appears.

   Note: If the installation is successful, the installation program creates log files for each installed component in the *Install_Path**productname*\log\install directory.

9. Click Done.

   The Product Status Checks dialog appears.

10. Verify that the Product Status Check items are passed.

    If an item fails, verify which action to take. For example, install available patches.

    Note:

    - To install the updates for CA Virtual Assurance, see How to Update CA Virtual Assurance (see page 34) section.
    - If the installation is not successful, the Installation Complete with Errors dialog appears. See the installation log (Install_Path*productname*\log\install\install.log) and the error list (Install_Path*productname*\log\install\install_error_detected.log) for details.

11. Navigate to Start, Programs, CA, CA Virtual Assurance, Launch CA Virtual Assurance and log in using the credentials that you have specified during the installation.

More Information

Prepare for the Installation (see page 17)
Verify Requirements for Using SQL Server (see page 14)

Canceling the Installation

When you run the CA Virtual Assurance installation program, a progress bar appears while the program unpacks product files to a temporary directory on your system. If you cancel the installation process before the first installation dialog appears, the progress bar disappears and the product is not installed. However, because the unpacking process cannot be interrupted, the installation program continues unpacking files until complete. The program then deletes the temporary directory and leaves the system unchanged. The unpacking of files and the deletion of the temporary directory can cause a temporary decrease in CPU performance.

Component Installation after Initial Installation

If you did not install all components during the initial installation, you can rerun the installation program to install missing components.

Silent Manager Installation

This section describes how to perform a silent manager installation. Complete one or more procedures in each section.

Note: Before you start a silent installation, verify that the target computer meets the prerequisites specified in the *Release Notes*.

More Information

Copy the Silent Installation Files from the Installation Media (see page 23)
Perform a Silent Manager Installation (see page 24)

Copy the Silent Installation Files from the Installation Media

Before editing the response files and running the actual installation program, copy them and the other support files from the installation media to the supported server where the Manager or agents reside.

DVD1 is required for a complete Manager installation on Windows, including SystemEDGE and SystemEDGE AIMs.

DVD2 is required for a CA Virtual Assurance managed node installation on AIX, HP-UX, Linux, or Solaris (SPARC, x86).

Follow these steps:

1. Copy the DVD1 Installers directory to the target computer.
2. Navigate to the root directory of the downloaded installation media and change to the *ResponseFileTemplates* directory.

   The silent.properties file appears in the list.
3. Copy the silent.properties file to the \Installers\Windows directory on the target computer.

   You can edit the silent.properties file on the host server as per your requirements.

Edit the silent.properties File

The silent installation program uses the silent.properties file to get information about your preferences for installing the Manager components on a supported Windows computer. Edit this file to perform a silent installation.

Important! We only support UTF-8 character encoding for silent.property file. For more information about UTF-8 character support and internationalization, see the *Release Notes*.

Follow these steps:

1. Navigate to the \Installers\Windows directory on the target computer and open the silent.properties file in a text editor.

   The contents of the file appear.

2. Follow the instructions contained in the file for specifying the installation options section in the comments. For example:
   `USER_INSTALL_DIR=C:\\Program Files\\CA\\productname`

   Use double backslashes (\\) to define a path.

   Note: Update the necessary sections, but do not remove sections of the file, even if they are not used.

3. Save and close the file.

When you run the silent installation program, it uses your settings to install the specified Manager components.

Perform a Silent Manager Installation

Use files from DVD1 to perform a silent Manager installation on a Windows system.

Follow these steps:

1. Open a command prompt on the target system.

   The command prompt window appears.

2. Change to the \Installers\Windows\ directory, and enter the following command:

   `install.exe -i silent -f path_to_silent.properties_file\silent.properties`

   The installation begins and installs the Manager on your system.

3. Check the files in the *install_path**productname*\log\install directory for errors and warnings after the installation is complete.

   Note: In a distributed silent installation, the Service Controller must be running before other components are installed so that they can be validated.

More Information

Copy the Silent Installation Files from the Installation Media (see page 23)
Edit the silent.properties File (see page 24)

Installation on Multiple Servers

The installation that is based on the default settings results in a centralized installation. All CA Virtual Assurance Manager components, databases, SystemEDGE, and all AIMs run on a single Windows server. However, you can install all required CA Virtual Assurance components on separate servers.

This section describes installation scenarios with multiple servers involved.

More Information

Guidelines for an Installation on Multiple Servers (see page 25)
Individual Agent Installations (see page 39)

Guidelines for an Installation on Multiple Servers

To install CA Virtual Assurance components on different servers you must run the installation on each server. Select the appropriate components from the components tree during installation respectively. Due to dependencies between components, consider the following guidelines:

- If an installation ranges across firewalls, open the corresponding communication ports between the affected components.
- For seamless timezone operation, verify that your distributed computing environment is synchronized to a common time source (for example, NTP server, GPS).
- Verify that the SQL Management Tools (OSQL, BCP) are available on the server on which the Automation Management Framework runs. The SQL Management Tools (OSQL, BCP) are part of the SQL Server installation and required to access a local or remote SQL Server. The Automation Management Framework and all CA Virtual Assurance manager components which access the Management Database and Performance Database reside on one server.
- Verify that TCP is enabled for SQL Server and a static port (default: 1433) has been set. If you connect to a remote SQL Server, allow Remote Access in SQL Server. CA Virtual Assurance allows Windows or SQL Server authentication to access the Management Database and the Performance Database.

- If you use Windows authentication for a remote SQL Server, verify the following requirements: CA SM Domain Server, Apache HTTP Server, and Apache Tomcat services have to run under a nonlocal system account. The nonlocal system account (domain user account) must have the required access privileges for the manager server and the database server. If you use Windows authentication for a remote SQL Server, the installation program automatically prompts you for that user.

  These conditions are not required for SQL Server authentication.

- When you install the Distribution Server on a remote system, configure the Distribution Server to connect to the associated CA SM Domain Server.

Follow these steps:

1. Open the Services dialog from the Control Panel, Administrative Tools.

   The list of available services appears.

2. Open the Properties dialog for the CA SM Distribution Server.
3. Stop the service
4. Add the following parameter into the Start parameters field:

   -m <*name of the system on which the CA SM Domain Server service runs*>

5. Start the service and click OK.

Scenario: Maximal Distributed Installation

This scenario lists all those CA Virtual Assurance components that you can install on separate servers.

Server 1

CA Virtual Assurance manager components
SQL Server Management Tools (OSQL, BCP)

Server 2

CA EEM

Server 3

Management Database

Server 4

Performance Database

Server 5

Distribution Server

Server 6

SystemEDGE and AIMs

Depending on your implementation, a smaller number of servers can be sufficient.

Example

Remote databases on one server, remote Distribution Server, local CA EEM, SystemEDGE, and AIMs:

Server 1

CA Virtual Assurance manager components
SQL Server Management Tools (OSQL, BCP)
CA EEM
SystemEDGE and AIMs

Server 2

Management Database
Performance Database

Server 3

Distribution Server

More Information

Communication Ports (see page 27)

Communication Ports

CA Virtual Assurance requires that multiple ports are open to function properly. If a distributed manager installation ranges across firewalls, you can use this list to verify that the required communication ports are open.

Active Directory and Exchange Server (ADES)

PowerShell Ports: 80, 443, 5985, and 5986

ADSI Ports: 3268, 389

Apache Server

HTTPS Port: 443

CA EEM Server

iGateway Port: 5250

SystemEDGE

UDP Port: 161 (SNMP Get/Set Requests); alternative port: 1691

UDP Trap Port: 162 (Outbound)

SystemEDGE in Managed Mode uses CAM:

CAM UDP Port: 4104

CAM TCP Port: 4105

CA Systems Performance LiteAgent

CAM UDP Port: 4104

CAM TCP Port: 4105

Cisco UCS

HTTP Port: 80

HTTPS Port: 443

Citrix XenServer

HTTPS Port: 443

SNMP Port: 161

Huawei Galax

HTTP Port: 8773

Hyper-V and SCVMM

WMI Port: 135

IBM HACMP

Secure Shell TCP Port: 22

IBM PowerVM

Secure Shell TCP Port: 22

Kernel-based Virtual Machines (KVM)

REST API Port: 8443

Microsoft SQL Server

Management DB TCP Port: 1433

Performance DB TCP Port: 1433

MSCS AIM

Windows RPC Endpoint Mapper Port: 135

DCOM/WMI Port: dynamically assigned during RPC Endpoint negotiation

Oracle Solaris Zones

Secure Shell TCP Port: 22

Policy Configuration

CAM UDP Port: 4104 (Inbound/Outbound)

CAM TCP Port: 4105 (Inbound)

Remote Deployment (Windows)

CIFS UDP Port: 137 (Inbound/Outbound)

CIFS UDP Port: 138 (Inbound/Outbound)

TCP Port: 135 (Inbound)

CIFS TCP Port: 139 (Inbound/Outbound)

CIFS TCP Port: 445 (Inbound/Outbound)

CAM UDP Port: 4104 (Inbound/Outbound)

CAM TCP Port: 4105 (Configurable)

Remote Deployment (UNIX, Linux)

CAM UDP Port: 4104 (Inbound/Outbound)

Secure Shell TCP Port: 22 (Inbound)

TCP Port: 135 (Inbound)

CAM TCP Port: 4105 (Configurable)

Remote Monitoring AIM

Windows RPC Endpoint Mapper Port: 135

DCOM/WMI Port: dynamically assigned during RPC Endpoint negotiation

SNMP Stack

UDP Ports: 161, 1691, 162 (Trap, Inbound)

Tomcat (User Interface)

HTTPS Port: 8443

Shutdown Port: 8005

VMware vCenter

HTTPS Port: 443

VMware vCloud

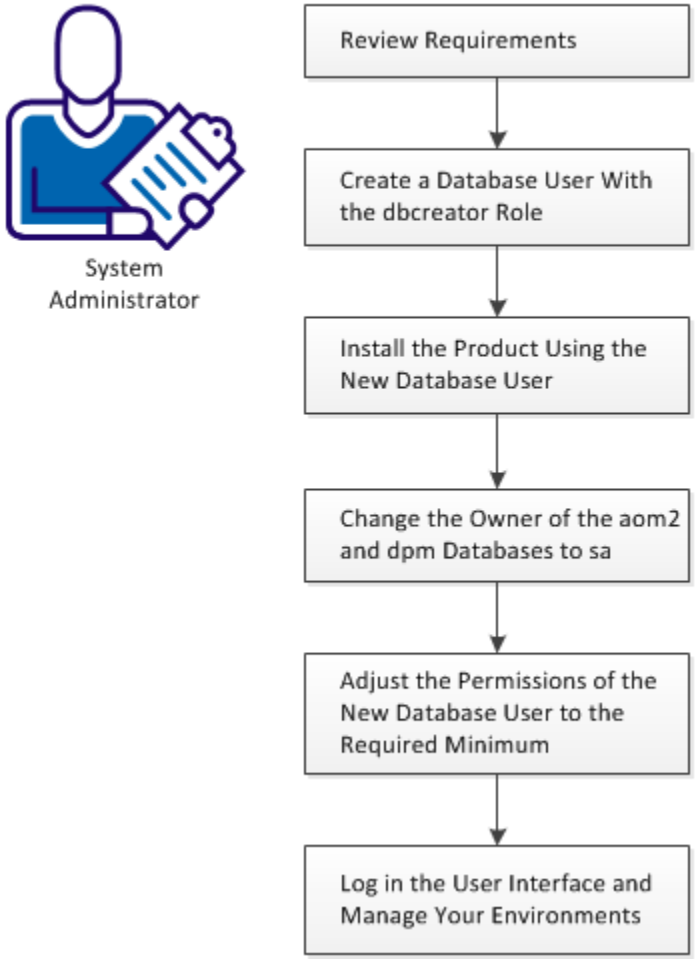
REST API Port: 8443

How to Adjust SQL Server User Permissions to the Required Minimum

As a System Administrator you want to minimize the permissions required by CA Virtual Assurance to access its SQL Server databases.

The following diagram illustrates the required steps to adjust the permissions.

How to Adjust SQL Server User Permissions to the Required Minimum



Follow these steps:

Review Requirements (see page 31)
Create a Database User With the dbcreator Role (see page 31)
Install the Product Using the New Database User (see page 32)
Change the Owner of the aom2 and dpm Databases to sa (see page 32)
Adjust the Permissions of the New Database User to the Required Minimum (see page 33)
Log in the User Interface and Manage Your Environments (see page 33)

Review Requirements

Review the following requirements before you start changing user pemissions of the database user of CA Virtual Assurance:

- SQL Server is installed according to the requirements specified in the Installation Guide.
- SQL Authentication (sa user) is enabled.

Create a Database User With the dbcreator Role

Create a database user for CA Virtual Assurance with the dbcreator role which you want to use during the installation of the product. After the installation, CA Virtual Assurance can use the same user with different permissions during runtime.

Follow these steps:

1. Login the SQL Server with administrator (sa) permissions.
2. Expand the Security folder in the navigation tree.
3. Right-click the Logins folder and select New Login ...

   The New Login dialog opens.
4. Under the General section, specify the following settings:
   - Enter a login name, for example, causer.
   - Select SQL Server authentication and enter the password for this user.
   - Uncheck "User must change password at next login".
5. Change to the Server Roles section, add the dbcreator role, and click OK.

   The new database user has sufficient privileges to install the product.

Install the Product Using the New Database User

You can install the product using the new database user.

Follow these steps:

1. Start the product installer of CA Virtual Assurance and start the installation wizard.
2. In the Required Configuration dialog click the Database entry.

   The database configuration dialog appears.
3. Select SQL Server authentication, enter the new user name (causer) and password, and click OK.
4. Start the installation.
5. After a successful installation, click Start (Windows), Administrative Tools, Services.

   The Services window opens.
6. Scroll down to CAAIPApache and CAAIPTomcat and stop the services.

Change the Owner of the aom2 and dpm Databases to sa

During the installation process, two databases for CA Virtual Assurance are created: dpm and aom2. Change the ownership of these databases to the sa user.

Follow these steps:

1. Log into SQL Server using the sa user.
2. Click New Query.

   The SQL console opens.
3. Enter the following SQL commands:

```
use dpm
exec sp_changedbowner 'sa', 'true'
use aom2
exec sp_changedbowner 'sa', 'true'
```

4. Click Execute.

   The sa user owns the aom2 and dpm databases.

Adjust the Permissions of the New Database User to the Required Minimum

CA Virtual Assurance requires a database user with sufficient permissions to use the aom2 and dpm databases. This procedure describes how to adjust these permissions to a minimum.

Follow these steps:

1. In the SQL Server Management Studio, expand Security, Logins in the Object Explorer.
2. Right-click the new user (for example, causer) and open Properties, User Mappings.

   The User Mapping dialog appears.
3. Select the aom2 and dpm databases in the dialog and assign db_datareader and db_datawriter role memberships to both databases. Click OK.
4. Click New Query.

   The SQL console opens.
5. Enter the following SQL commands to allow the new database user (causer) the execution of stored procedures:

   ```
   use dpm
   GRANT EXECUTE TO causer
   use aom2
   GRANT EXECUTE TO causer
   ```
6. Right-click the new user (causer) in the Object Explorer and open Properties, Server Roles.

   The Server Roles dialog appears.
7. Remove the db_creator role and click OK.

   The new database user provides sufficient permissions to CA Virtual Assurance to use the aom2 and dpm databases.

Log in the User Interface and Manage Your Environments

Before you can use CA Virtual Assurance user interface, start the CAAIPApache and CAAIPTomcat services.

Follow these steps:

1. Click Start (Windows), Administrative Tools, Services.

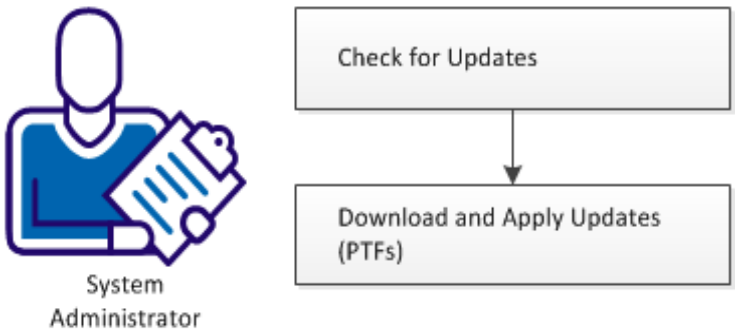
   The Services window opens.
2. Scroll down to CAAIPApache and CAAIPTomcat and start the services.

   After a successful start of the services, CA Virtual Assurance is ready to use.
3. Start the CA Virtual Assurance user interface and manage your environment.

How to Update CA Virtual Assurance

As a System Administrator, your job includes applying the PTFs (program temporary fix) for CA Virtual Assurance on manager systems. Applying the PTFs includes downloading and installing the PTFs that you can handle through one application.

How to Apply Updates (PTFs)



Follow these steps:

1. Check for Updates (see page 34).
2. Download and Apply the Updates (PTFs) (see page 35).

Check for Updates

Before you download and apply updates, verify if appropriate updates for this release are available.

Follow these steps:

1. Right-click the icon in the system tray and click "Check for updates".

   The tooltip displays the result.

Additionally, you can specify the settings when to check for updates automatically.

Follow these steps:

1. Right-click the icon in the system tray and click "Settings".

   The Settings dialog appears.
2. Specify the fields in the dialog and click OK.

   The "Check for updates" schedule is set.

Download and Apply the Updates (PTFs)

Download and apply the PTFs to keep the CA Virtual Assurance up-to-date on the manager system.

Follow these steps:

1. Go to Start, All Programs, CA, CA Virtual Assurance, and click CA Virtual Assurance Update.

   The "Updates for CA Virtual Assurance" window is displayed.

2. Open the Applicable page.

   The applicable PTFs for this release are listed.

3. Select the PTFs that you require, click Download selected updates, and then click Apply all downloaded updates.

   The update utility downloads the PTFs to the %INSTALL_PATH%*productname*\CAPTFS directory and starts the application process. The application progress dialog displays the status.

4. After the PTFs are applied successfully, exit the application progress dialog.

   The applied PTFs are listed in the Applied page of the "Updates for CA Virtual Assurance" window.

5. Click Exit.

Agent Deployment

CA Virtual Assurance provides a comprehensive solution for remotely deploying the SystemEDGE agent to all managed systems. You can create deployment templates that are based on the provided packages that contain customized installation parameters and simultaneously deploy these templates to numerous managed systems. This automated deployment solution provides one location from which to deploy and configure the agents throughout your enterprise.

CA Virtual Assurance provides the following base deployment packages:

- SystemEDGE Agent Core
- SystemEDGE Advanced Encryption
- CA Citrix XenServer AIM
- SystemEDGE Remote Monitoring AIM
- SystemEDGE Service Response Monitor AIM
- CA Systems Performance LiteAgent
- CA IBM LPAR AIM
- CA IBM High Availability Cluster Multiprocessing AIM
- CA KVM AIM (not applicable to CA Server Automation)
- CA Cisco UCS AIM
- CA Microsoft Hyper-V AIM
- CA Microsoft Cluster Service Support AIM
- CA Solaris Zones AIM
- CA VMware vCenter Server AIM
- CA VMware vCloud AIM
- CA Exchange Server and Active Directory AIM (not applicable to CA Server Automation)

CA Virtual Assurance supports the following SystemEDGE deployment scenarios:

- You can deploy a SystemEDGE Release 5.7.1 agent to systems with no pre-existing SystemEDGE agent.
- You can deploy a SystemEDGE Release 5.7.1 agent to systems with a pre-existing SystemEDGE 4.3 agent. The deployment automatically upgrades the existing agent to Release 5.7.1.
- You can make configuration changes to individual systems or through a configuration template. The latter option allows you to apply changes to an existing managed SystemEDGE agent or a group of managed SystemEDGE agents.

Note: For more information about how deployment works, see the *CA Virtual Assurance Online Help* and the *Administration Guide*.

CA Virtual Assurance does *not* support the following SystemEDGE deployment scenarios:

- You cannot deploy a version of the agent earlier than SystemEDGE 5.0.0.
- You cannot deploy the SystemEDGE agent on the CA Virtual Assurance manager system. The agent is automatically installed through the CA Virtual Assurance manager installation.

Note: For more information about deployment support, see the C*A Virtual Assurance Administration Guide*.

Create a Deployment Job

You can install SystemEDGE and AIMs on AIX, HP-UX, Linux, Solaris, or Windows systems that they support from the CA Virtual Assurance Manager through Remote Deployment.

To deploy agents to systems, create a deployment job. Deployment jobs contain the details that are required for CA Virtual Assurance to deliver the deployment packages to the appropriate systems at the appropriate time.

Follow these steps:

1. Select Resources, Deploy.

   The Deployment pane displays the Packages, Templates, and Jobs.

2. Right-click the Jobs folder in the Manage Resource pane and select Create New Job. You can also select the Jobs folder and Click + (New) on the Job Status toolbar.

   The Jobs Setup page appears.

3. Enter a name in the Job Name pane and optionally base the job on an existing template, and click Next.

   The Package Selection page appears.

4. Select a platform and the packages you want to deploy.
5. (Optional) Click the Details tab.

   The Package Wrapper Details dialog appears and lets you edit the package properties in-line. If the package wrappers are in an incomplete or invalid state, and the fields can be modified through in-line editing.

   a. Click Edit and modify the package wrapper properties.

   b. Click Save, and then click OK.

      The package wrapper properties are updated.
6. Click the down arrow to add the package wrappers to the job, and click Next.

   The Machine Selection page appears.
7. Select the systems to deploy to and click Next. If you have many servers in your environment, multiple pages with some entries can be required to list all servers. When you select servers on a page and scroll to the next page, any selections that are made on previous pages remain valid.

   The Machines Selected page appears.
8. Click Set Credentials, set the system credentials that are required to establish a connection and click Next.

   Note: Deployment to Windows target systems using domain credentials must be in the form of DOMAIN\username.

   The Advanced page appears.
9. (Optional) Set the distribution server to manage the deployment. If not set, it is automatically chosen.
10. Select the scheduling options for the job:

    Immediate Delivery

    Starts the job immediately after creating new deployment job. The immediate delivery is the default option.

    Staggered Delivery

    Delivers the packages over a specific time period.

    Scheduled Delivery

    Schedules the deployment for a specific time in the future.
11. (Optional) If a package has previously been successfully deployed to a system using this deployment infrastructure, you can force it to run again.
12. Click Next.

    The Summary page appears.

13. Review the details of the job and click Deploy.

    The deployment job is created.

Note: You can save the job as a template after you create it. A template saves the package and machine selections so that you can easily reuse them for subsequent jobs.

For more information about Remote Deployment, see the *CA Virtual Assurance Administration Guide*.

Individual Agent Installations

This section details the components and procedures for installing CA Virtual Assurance agents on Managed Nodes.

Dependencies of SystemEDGE Components

CA Virtual Assurance uses the SystemEDGE with appropriate Application Insight Modules (AIMs) to manage physical and virtualized environments. An AIM is a SystemEDGE plug-in that extends the functional scope of this agent.

The following AIMs are available:

- AIM for Remote Monitoring (Windows)
- AIM for Service Response Monitoring (Windows, UNIX, Linux)
- AIM for IBM LPAR (Windows)
- AIM for IBM High Availability Cluster Multiprocessing (Windows)
- AIM for KVM (Windows, Linux)
- AIM for Microsoft Hyper-V (Windows)
- AIM for Microsoft Cluster Service Support (Windows)
- AIM for Solaris Zones (Windows)
- AIM for Cisco UCS (Windows)
- AIM for Citrix XenServer (Windows)
- AIM for VMware vCenter Server to manage VMware Infrastructure or vSphere (Windows)
- AIM for VMware vCloud (Windows)
- AIM for Exchange Server and Active Directory (Windows)
- AIM for HUAWEI GalaX8800

Note: For more information about platform details, see the *Release Notes*.

Use these AIMs only on systems that have SystemEDGE and Advanced Encryption installed. CA Virtual Assurance discovers such systems and manages them according to the functional scope of the installed components.

SystemEDGE runs on the following operating systems:

- AIX
- HP-UX
- Linux
- Solaris x86
- Solaris SPARC
- Windows

Note: The agent does not function correctly, when you specify community strings with space characters or semicolon (;) during installation with graphical user interfaces.

SystemEDGE Installation Through CA Virtual Assurance Manager Installer

The CA Virtual Assurance Manager Installer lets you install SystemEDGE without the necessity to run the individual SystemEDGE setup program. Consider the following default behavior regarding the Configuration Manager Host Name when you use the CA Virtual Assurance Manager Installer for SystemEDGE:

- Typical Installation sets the Configuration Manager Host Name for SystemEDGE to localhost.
- If the Custom Installation installs SystemEDGE on the same system as the Distribution Server, the Configuration Manager Host Name for SystemEDGE is set to localhost.
- If the Custom Installation installs SystemEDGE on a system without a Distribution Server, the Configuration Manager Host Name for SystemEDGE is set to asterisk (*). The asterisk specifies that the first CA Virtual Assurance manager that discovers this system is the Configuration Manager Host for SystemEDGE.

If you want to set up and manage remote servers with SystemEDGE and AIMs, it is recommended to use Remote Deployment and Policy Configuration. Remote Deployment guides you through the deployment package creation process. You can specify a schedule and a list of servers (Windows, Linux, UNIX) to which the package is being deployed. Based on the Configuration Manager Host Name settings, Policy Configuration lets you manage the configurations of the SystemEDGE agents in your network. For details, see the *Administration Guide* and *Online Help*.

The following situations require you to install the agent manually, instead of using the recommended CA Virtual Assurance Remote Deployment method:

- You are installing the agent on a system, which does not support Remote Deployment.
- You want to install the agent in legacy mode.
- You want to specify the Configuration Manager Host Name and all other settings manually during setup.

For a list of supported versions, see the *Release Notes*.

More Information

Install the Agent in Legacy Mode (see page 67)

Installation on Windows Systems

This section describes how to manually install SystemEDGE on Windows systems. You can install using an interactive wizard or silently using the command line. Separate packages are available for all supported hardware architectures. The installer detects your hardware architecture and runs the appropriate installation package.

The following situations require you to install the agent manually, instead of using the recommended CA Virtual Assurance deployment method:

- You are installing the agent on a system, which does not support Remote Deployment.
- You want to install the agent in legacy mode.

Throughout this guide, the term *Windows* encompasses supported versions of Windows. For a list of supported versions, see the *SystemEDGE Release Notes*.

More Information

Install the Agent in Legacy Mode (see page 67)

Install the Agent on Windows

You can use an interactive wizard to install the SystemEDGE agent for Windows manually.

Follow these steps:

1. Log in to the Windows system as an Administrator and do one of the following:
   - Double-click setup.hta from DVD1 of the CA Virtual Assurance installation image and click Install SystemEDGE Agent on the CA Virtual Assurance dialog.
   - Open the DVD1\Installers\Windows\Agent\SysMan\CA_SystemEDGE_Core folder and double-click ca-setup.exe.

   Note: For systems running Windows Vista or later, you can install as a non-administrator. The operating system prompts you to authorize the installation with Administrator credentials.

   The installation wizard opens. The installer detects the hardware architecture of a system and runs the appropriate version of the installation package.

2. Click Next.

   The License Agreement page opens.

3. Read the License agreement and scroll down to the bottom. Select I accept the terms of the License Agreement option and click Next.

   The Installation Type page opens.

4. Select Typical or Custom and click Next.

   Note: The following procedure describes a custom installation. If you select Typical, the Review Settings page opens when you click Next.

   The Destination Location dialog appears.

5. Accept the default or Browse to select the locations for the installation and data directories, click Next, and continue with Step 9. If you want to specify different locations, click Advanced and continue with Step 8.

   Destination Location

   Specifies the location at which to install the agent. By default, the installation directory is *Install_Path*\SystemEDGE and the runtime program data is stored in the config subdirectory. To specify more parameters, click Advanced.

   Note: When installing the agent on a system with a previous version of the agent already installed, the installer selects the installation directory of the existing agent.

   If you skip the Advanced dialog, the Configuration Manager Settings dialog appears.

6. Complete the following fields in the Advanced Destination Locations dialog and click Next.

   SystemEDGE binary path

   Specifies the directory for program binaries and documentation.

   SystemEDGE data path

   Specifies the directory for run-time program data.

   CA Shared Components path

   Specifies the directory for CA Shared Components. Once set by any CA software, this directory cannot be changed and the corresponding field in the user interface is disabled.

   The Configuration Manager Settings dialog appears.

7. Complete the following fields and click Next.

   Configuration Manager Host Name

   Specifies the host name of the configuration manager from which you want to manage this agent. Enter a value for this parameter to configure this agent from the system on which CA Virtual Assurance runs. Enter an asterisk (*) to accept the first manager that discovers the agent system.

   Default Configuration Policy Name

   Specifies the name of the configuration policy file (maintained by the CA Virtual Assurance manager) for the agent to use. Enter a value for this parameter to set the SystemEDGE configuration according to an existing configuration file from the manager.

   If the installer detects the native Microsoft SNMP agent running on the system, the following Native SNMP Options dialog appears.

8. If Simple Network Management Protocol (SNMP) is installed on your system, select one of the following options and click Next.

   Default from existing SNMP agent

   Specifies whether to use the default settings from the native SNMP agent. Leave this check box cleared to use different community strings and trap destinations than the native SNMP agent.

   Disable native SNMP agent

   Specifies whether to stop and disable the native SNMP agent. If you leave the native SNMP agent enabled, run SystemEDGE on a different port.

9. Complete the following fields and click Next.

   SNMP port number

   Specifies the port on which to run the SystemEDGE agent.

   Default: 161

   Important! Dedicate this port number to SystemEDGE agent. The installation fails if other application uses this port number. If the native SNMP agent already uses the default port, specify a different port, for example, 1691 or 6665.

   The SNMP System Information dialog appears.

10. Complete the following fields and click Next.

    System Description

    Specifies information about the system (such as a system name) that populates the sysDescr MIB-II object.

    System Location

    Specifies the system location that populates the sysLocation MIB-II object.

    System Contact

    Specifies system contact information that populates the sysContact MIB-II object.

    The SNMP Community Settings dialog appears.

11. Complete the following fields, click Next, and continue with Step 13. If you want to specify multiple community strings, click Advanced and continue with Step 12.

    Read-only Community

    Specifies the SNMP read-only community string.

    Default: public

    Read-write community

    Specifies the SNMP read-write community string.

    If you skip the Advanced dialog, the SNMP Trap Settings dialog appears.

12. Complete the following fields in the SNMP Community Settings - Advanced dialog and click Next.

    Read-only Community

    Specifies the SNMP read-only community string. You can specify multiple communities by separating each with a semicolon (for example, public1; public2). You can also include an IP address list for each community to restrict access (for example, public 1.2.3.4).

    Default: public

    Read-write community

    Specifies the SNMP read-write community string. You can specify multiple communities by separating each with a semicolon (for example, rwcomm1; rwcomm2). You can also include a space delimited IP address list for each community to restrict access (for example, rwcomm1 1.2.3.4). A read-write community is required for correct operation of some AIMs (for example, RM) and for some remote uses (for example, creating monitors).

    The SNMP Trap Settings dialog appears.

13. Complete the following fields, click Next, and continue with Step 15. If you want to specify multiple trap destinations, click Advanced and continue with Step 14.

    Trap community string

    Specifies the SNMP community encoded in sent trap messages.

    Default: public

    Destination host

    Specifies the destination of the trap messages.

    Default: The *configuration manager host name* set in Configuration Manager Settings dialog.

    Port number

    Specifies the port trap messages are sent to.

    Default: 162.

    If you skip the Advanced dialog, the Miscellaneous Settings dialog appears.

14. Complete the following field in the SNMP Trap Settings - Advanced dialog and click Next.

    Trap Configuration

    Specifies one or more trap destinations. You can specify multiple entries by separating each with a semicolon (for example, public server1; public server2 1162).

    The Miscellaneous Settings dialog appears.

15. Complete the following fields and click Next:

    Start After Install

    Specifies whether the agent is started at the end of installation.

    Install Documentation

    Specifies whether to install the documentation.

    The Review Settings page appears.

16. Review the installation settings and click Install.

    The Installation Completed page appears after the installation finishes.

17. Click Finish.

    The installation is complete.

Install the Agent on Windows from the Command Line

You can install the SystemEDGE Windows package using a command line version of the installer. When installing from the command line, you use parameters to set various installation properties. You can do the following from the command line:

- Start the installation wizard, with or without prefilled installation parameters
- Specify installation parameters and run the installer without the interactive wizard

This procedure covers the second scenario: running an unattended installation from the command line.

Follow these steps:

1. Log on to the Windows system as an Administrator.

   Note: For systems running Windows Vista and later, you can install as a non-administrator, and the operating system prompts you to authorize the installation with Administrator credentials.

2. Open a command prompt, navigate to the DVD1\Installers\Windows\Agent\SysMan\CA_SystemEDGE_Core folder, and enter the following required parameters (do **not** run the command until you complete Step 3):

   ```
   ca-setup CA_SETUP_MODE=UNATTENDED EULA_ACCEPTED="YES" [parameter]
   ```

   Note: For help with installation parameters, enter ca-setup -? at the command prompt.

   CA_SETUP_MODE

   Specifies the installation mode. Set this parameter to UNATTENDED to run the installation in silent mode. If you omit this parameter, the installation wizard opens with specified parameter values prefilled after you run the command.

   EULA_ACCEPTED

   Read the license agreement and specify whether to accept the license agreement. If you omit this parameter or set it to anything other than **YES** when you set the installation mode to UNATTENDED, the installation fails. This parameter is not required in an interactive installation.

3. Add optional parameters as appropriate and run the command.

   Note: The following optional parameters do not require a value if you omit them:

   CA_SETUP_LOG_FILE
   CA_SETUP_VERBOSE
   CASE_INSTALLDIR
   CASE_PUBDATADIR
   CASE_SNMP_PORT
   CASE_SNMP_SYS_DESC
   CASE_SNMP_SYS_LOC
   CASE_SNMP_SYS_CONTACT
   CASE_SNMP_READ_COMMUNITY
   CASE_SNMP_READ_ALLOWED_MANAGERS
   CASE_SNMP_WRITE_COMMUNITY
   CASE_SNMP_WRITE_ALLOWED_MANAGERS
   CASE_SNMP_TRAP_COMMUNITY
   CASE_SNMP_TRAP_DESTINATION
   CASE_SNMP_TRAP_PORT
   CASE_DISABLE_NATIVE_SNMP
   CASE_DEFAULT_FROM_NATIVE_SNMP
   CASE_MANAGER_HOSTNAME
   CASE_MANAGER_POLICY_NAME
   CASE_START_AFTER_INSTALL
   CASE_INSTALL_DOCS
   CASE_LEGACY_MODE

   CA_SETUP_LOG_FILE

   Specifies a location and file name in which to log installation messages.

   CA_SETUP_VERBOSE

   Turns on verbose installation mode when set to "yes". Verbose mode logs more information to the installation log file.

CASE_INSTALLDIR

Specifies the SystemEDGE installation directory. This directory contains everything SystemEDGE-related, such as AIMs and Advanced Encryption, and is never modified after being set by the Core installer.

Note: If you define a non-default installation directory, the installer installs agent files directly to the specified directory without creating a SystemEDGE subfolder.

Default: C:\Program Files\CA\SystemEDGE

CASE_PUBDATADIR

Specifies the SystemEDGE data directory, where all configurations take place and dynamic data is stored (referred to in this document as the variable CASYSEDGE_DATA). The configuration files of the agent are located in a port-specific subdirectory which is based on the SNMP_PORT parameter value.

Defaults: C:\Documents and Settings\All Users\Application Data\CA\SystemEDGE (Windows XP and 2003), C:\Users\Public\CA\SystemEDGE (Windows Vista and 2008)

CASE_SNMP_PORT

Specifies the port used by SystemEDGE. This value can also be inherited from the native SNMP agent using the CASE_DEFAULT_FROM_NATIVE_SNMP parameter. If you specify a port using the CASE_SNMP_PORT parameter, it overrides the inherited value. This port must be unique, or the installation fails. If the default port of 161 is already in use by the native SNMP agent (and you do not plan on disabling this agent), you must specify a different unique port, for example, 1691 or 6665.

Default: 161

CASE_SNMP_SYS_DESC

Specifies information about the system (such as a system name) that populates the sysDescr MIB-II object. This value can also be inherited from the native SNMP agent using the CASE_DEFAULT_FROM_NATIVE_SNMP parameter. If you specify a description using the CASE_SNMP_SYS_DESC parameter, it overrides the inherited value.

CASE_SNMP_SYS_LOC

Specifies the system location that populates the sysLocation MIB-II object. This value can also be inherited from the native SNMP agent using the CASE_DEFAULT_FROM_NATIVE_SNMP parameter. If you specify a location using the CASE_SNMP_SYS_LOC parameter, it overrides the inherited value.

CASE_SNMP_SYS_CONTACT

Specifies system contact information that populates the sysContact MIB-II object. This value can also be inherited from the native SNMP agent using the CASE_DEFAULT_FROM_NATIVE_SNMP parameter. If you specify a contact using the CASE_SNMP_SYS_CONTACT parameter, it overrides the inherited value.

CASE_SNMP_READ_COMMUNITY

Specifies the name of the SNMP read community that can send GET requests to the agent. You can specify multiple communities by separating them with a semicolon (for example, public1;public2), and you can include a space delimited IP address list for each community to restrict access (for example, public 1.2.3.4). This value can also be inherited from the native SNMP agent using the CASE_DEFAULT_FROM_NATIVE_SNMP parameter. If you specify a read community using the CASE_SNMP_READ_COMMUNITY parameter, it overrides the inherited value.

Default: snmp_public (valid for a new installation only (no upgrade) and if no read-write community is specified)

CASE_SNMP_READ_ALLOWED_MANAGERS

Specifies the space-separated list of IP addresses/hostnames of SNMP managers allowed to query the agent with SNMP_READ_COMMUNITY. When this is specified, SNMP_READ_COMMUNITY must only contain a single word, the SNMP community.

CASE_SNMP_WRITE_COMMUNITY

Specifies the name of the SNMP write community that can send GET and SET requests to the agent. You can specify multiple communities by separating them with a semicolon (for example, rwcomm1;rwcomm2), and you can include a space delimited IP address list for each community to restrict access (for example, rwcomm1 1.2.3.4). This value can also be inherited from the native SNMP agent using the CASE_DEFAULT_FROM_NATIVE_SNMP parameter. If you specify a write community using the CASE_SNMP_WRITE_COMMUNITY parameter, it overrides the inherited value.

CASE_SNMP_WRITE_ALLOWED_MANAGERS

Specifies the space-separated list of IP addresses/hostnames of SNMP managers allowed to query the agent with SNMP_WRITE_COMMUNITY. When this is specified, SNMP_WRITE_COMMUNITY must only contain a single word, the SNMP community.

CASE_SNMP_TRAP_COMMUNITY

Specifies the SNMP trap community and the trap destination address. You can specify multiple trap community settings by separating them with a semicolon (;). The value for this parameter can also be inherited from the native SNMP agent using the CASE_DEFAULT_FROM_NATIVE_SNMP parameter. If you specify a trap community using the CASE_SNMP_TRAP_COMMUNITY parameter, it overrides the inherited value. The following values are required for this parameter:

- Community name
- Destination address to which to send traps

The following values are optional for this parameter:

- Port number to which to send traps
- Trap source encoding options
- Trap source host name

Syntax of a trap community setting:

community-string {*ip-address*|*hostname*} [*port* [*encoding* [*source*]]]

Example:

public 1.2.3.4;public 2.3.4.5 1162;trapcom 3.4.5.6 1162 100 4.5.6.7

CASE_SNMP_TRAP_DESTINATION

Specifies the hostname or IP address to which to send traps. When this is specified, SNMP_TRAP_COMMUNITY must only contain a single word, the SNMP community and SNMP_TRAP_PORT must also be specified.

CASE_SNMP_TRAP_PORT

Specifies the destination port number to which to send traps. When this is specified, SNMP_TRAP_COMMUNITY must only contain a single word, the SNMP community and SNMP_TRAP_DESTINATION must also be specified.

CASE_DISABLE_NATIVE_SNMP

Specifies whether to stop and disable the native SNMP agent.

Default: no

CASE_DEFAULT_FROM_NATIVE_SNMP

Specifies whether to use the default SNMP settings from the native SNMP agent.

Default: no

CASE_MANAGER_HOSTNAME

Specifies the host name of the configuration manager from which you want to manage this agent. Entering a value for this parameter lets you configure this agent from the specified manager. Entering an asterisk (*) accepts the first manager that discovers the agent system. This manager will have full control over the agent's configuration. By default, no manager host is entered (used), and the agent runs in unmanaged mode.

CASE_MANAGER_POLICY_NAME

Specifies the name of the configuration manager policy file that the agent should use. Entering a value for this parameter sets the SystemEDGE configuration according to an existing configuration file from the manager. By default, the agent uses the installed policy file.

CASE_START_AFTER_INSTALL

Specifies whether to start the agent automatically after the installation completes.

Default: yes

CASE_INSTALL_DOCS

Specifies whether to install the SystemEDGE documentation with the agent.

Default: yes

CASE_LEGACY_MODE

Specifies whether to install the agent in legacy mode, which installs the base agent only while omitting all materials that facilitate usage with CA Virtual Assurance. Install using legacy mode if you do not want to use the agent with CA Virtual Assurance.

You can turn the agent into managed mode by reinstalling or upgrading and specifying CASE_LEGACY_MODE=no.

Default: no

Enter the command and all required parameters and values in the command line. Press Enter to start the installation. The installer detects the hardware architecture of the operating system and runs the appropriate version of the installer.

Note: If you do not accept the installation agreement, the installation fails.

To verify the installation, confirm the existence of the CA SystemEDGE service in the Windows Services dialog, the SystemEDGE files in the installation directory, or the presence of CA SystemEDGE Core in the Add or Remove Programs dialog. You can also check the installation log file if you specified one to confirm a successful installation.

Note: The SystemEDGE installer automatically installs "Microsoft Visual C++ 2005 Redistributable Package" if you are installing on a system running Windows Vista or later. SystemEDGE will not function without this package installed. To install "Microsoft Visual C++ 2005 Redistributable Package" you must accept the license agreement that is displayed. The license agreement for "Microsoft Visual C++ 2005 Redistributable Package" is suppressed in the interactive version of the SystemEDGE installer.

Installation on UNIX and Linux Systems

This section describes how to manually install the SystemEDGE agent on UNIX and Linux systems. You can install using an interactive wizard or silently using the command line. The interactive wizard displays in text mode on the console or as a graphical application if Xserver is available and the DISPLAY environment correctly set.

The following situations require you to install the agent manually, instead of using the recommended CA Virtual Assurance deployment method:

- You are installing the agent on a system, which does not support Remote Deployment.
- You want to install the agent in legacy mode.

For more information about the supported UNIX and Linux platforms and versions, see the *SystemEDGE Release Notes*.

More Information

Install the Agent in Legacy Mode (see page 67)

Install the Agent on UNIX and Linux Systems

You can use an interactive wizard to install the SystemEDGE agent manually for UNIX and Linux.

Notes:

- This document refers to the installation directory as CASYSEDGE and to the data directory as CASYSEDGE_DATA.
- The installation program does not modify the system environment settings in /etc/profile.

Follow these steps:

1. Log in to the system as the root user and mount DVD2.
2. Open a terminal console and change to Installers/*platform*/Agent/SysMan/CA_SystemEDGE_Core directory, selecting the *platform* directory that corresponds to your operating system.
3. Run the installer from this directory as follows:

   ```
   sh ca-setup.sh
   ```

   The Introduction page of the installer appears.
4. Click Next.

   The License Agreement page appears.
5. Read the license agreement and select I accept the terms of the License Agreement. Click Next.

   The Installation Type page appears.
6. Select Typical or Custom and click Next.

   Note: This procedure describes a custom installation. If you select Typical, the Review Settings page appears when you click Next.

   The Destination Location dialog appears.
7. Accept the default or Browse to select the locations for the installation and data directories, click Next, and continue with Step 9. If you want to specify different locations click Advanced and continue with Step 8.

   Destination Location

   Specifies the location at which to install the agent. By default, the installation directory is /opt/CA/SystemEDGE and the runtime program data is stored in the config subdirectory. To specify more parameters, click Advanced.

   Note: If you are installing the agent on a system with a previous version of the agent already installed, the installer automatically selects the installation directory of the existing agent.

   If you skip the Advanced dialog, the Configuration Manager Settings dialog appears.

8. Complete the following fields in the Advanced Destination Locations dialog and click Next.

   SystemEDGE binary path

   Specifies the directory for program binaries and documentation.

   SystemEDGE data path

   Specifies the directory for run-time program data.

   CA Shared Components path

   Specifies the directory for CA Shared Components. Once set by any CA software, this directory cannot be changed and the corresponding field in the user interface is disabled.

   The Configuration Manager Settings dialog appears.

9. Complete the following fields and click Next.

   Configuration Manager Host Name

   Specifies the host name of the configuration manager from which you want to manage this agent. Enter a value for this parameter to configure this agent from the system on which CA Virtual Assurance runs. Enter an asterisk (*) to accept the first manager that discovers the agent system.

   Default Configuration Policy Name

   Specifies the name of the policy file (maintained by the CA Virtual Assurance manager) for the agent to use. Enter a value for this parameter to set the SystemEDGE configuration according to an existing configuration file from the manager.

   If the installer detects the native SNMP agent running on the system, the Native SNMP Options dialog appears.

10. Complete the following fields and click Next.

    Default from existing SNMP agent

    Specifies whether to use the default settings from the native SNMP agent. Leave this check box cleared to use different community strings and trap destinations than the native SNMP agent.

    Disable native SNMP agent

    Specifies whether to stop and disable the native SNMP agent. If you leave the native SNMP agent enabled, run SystemEDGE on a different port.

11. Complete the following fields and click Next.

    SNMP port number

    Specifies the port on which to run the SystemEDGE agent. This port must be not be used by any other application or the installation fails. If the native SNMP agent already uses the default port, specify a different port, for example, 1691 or 6665.

    Default: 161

    The SNMP System Information dialog appears.

12. Complete the following fields and click Next.

    System Description

    Specifies information about the system (such as a system name) that populates the sysDescr MIB-II object.

    System Location

    Specifies the system location that populates the sysLocation MIB-II object.

    System Contact

    Specifies system contact information that populates the sysContact MIB-II object.

    The SNMP Community Settings dialog appears.

13. Complete the following fields, click Next, and continue with Step 15. If you want to specify multiple community strings, click Advanced and continue with Step 14.

    Read-only Community

    Specifies the SNMP read-only community string.

    Default: public

    Read-write community

    Specifies the SNMP read-write community string.

    If you skip the Advanced dialog, the SNMP Trap Settings dialog appears.

14. Complete the following fields in the SNMP Community Settings - Advanced dialog and click Next.

    Read-only Community

    Specifies the SNMP read-only community string. You can specify multiple communities by separating each with a semicolon (for example, public1;public2). You can also include an IP address list for each community to restrict access (for example, public 1.2.3.4).

    Default: public

    Read-write community

    Specifies the SNMP read-write community string. You can specify multiple communities by separating each with a semicolon (for example, rwcomm1;rwcomm2). You can also include a space delimited IP address list for each community to restrict access (for example, rwcomm1 1.2.3.4). A read-write community is required for correct operation of some AIMs (for example, RM) and for some remote uses (for example, creating monitors).

    The SNMP Trap Settings dialog appears.

15. Complete the following fields, click Next, and continue with Step 17. If you want to specify multiple trap destinations, click Advanced and continue with Step 16.

    Trap community string

    Specifies the SNMP community encoded in sent trap messages.

    Default: public

    Destination host

    Specifies the destination of the trap messages.

    Default: The *configuration manager host name* set in Configuration Manager Settings dialog.

    Port number

    Specifies the port trap messages are sent to.

    Default: 162.

    If you skip the Advanced dialog, the Privilege Separation User dialog appears.

16. Complete the following field in the SNMP Trap Settings - Advanced dialog and click Next.

    Trap Configuration

    Specifies one or more trap destinations. You can specify multiple entries by separating each with a semicolon (for example, public server1;public server2 1162).

    The Privilege Separation User dialog appears.

17. Complete the following field and click Next:

    User Name

    Specifies the user name under which credentials the agent run during SNMP communication.

    This entry instructs the agent (UNIX only) to run SNMP communication under another user account. The agent also uses this user's default group as an effective group.

    Default: The agent operates using root account.

    The Miscellaneous Settings dialog appears.

18. Complete the following fields and click Next:

    Start After Install

    Specifies whether the agent is started at the end of installation.

    Install Documentation

    Specifies whether to install the documentation.

    The Review Settings page appears.

19. Review the installation settings and click Install.

    The Installation Completed page appears after the installation finishes.

20. Click Finish.

    The installation is complete.

SystemEDGE Installation on 64-bit Linux Releases Fails

Symptom:

When I install SystemEDGE on a 64-bit Linux release, the installation fails.

Solution:

To run and install SystemEDGE on a 64-bit Linux release, install the required 32-bit libraries:

- Valid on Redhat or SuSE distributions:

  ```
  yum install glibc.i686
  ```

- Valid on Debian distribution:

  ```
  apt-get install ia32-libs
  ```

Install the Agent on UNIX from the Command Line

You can install the SystemEDGE UNIX package using a command line version of the installer. When installing from the command line, you use parameters to set various installation properties. You can do the following from the command line:

- Start the installation wizard, with or without prefilled installation parameters
- Specify installation parameters and run the installer without the interactive wizard

Notes:

- UNIX does not support the automatic creation of a response file to run a silent installation. However, you can create a response file manually and use it for an unattended installation.
- The installation program does not modify the system environment settings in /etc/profile.

This procedure covers the second scenario: running an unattended installation from the command line.

Follow these steps:

1. Log on to the system as root.
2. Navigate to the DVD2/Installers/*platform*/Agent/SysMan/CA_SystemEDGE_Core folder (specifying the platform folder that corresponds to your operating system), and enter the following required parameters (do **not** run the command until you complete Step 3):

   ```
   sh ca-setup.sh CA_SETUP_MODE="UNATTENDED" EULA_ACCEPTED="yes" [parameter]
   ```

   Note: For help with installation parameters, enter ca-setup -? at the command prompt.

   CA_SETUP_MODE

   Specifies the installation mode. Set this parameter to UNATTENDED to run the installation without displaying the installation wizard. If you omit this parameter, the installation wizard opens with specified parameter values prefilled after you run the command.

   EULA_ACCEPTED

   Read the license agreement and specify whether to accept the license agreement. If you omit this parameter or set it to anything other than **YES** when you set the installation mode to UNATTENDED, the installation fails. This parameter is not required in an interactive installation.

3. Add optional parameters as appropriate, and run the command.

   Note: The following optional parameters do not require a value if you omit them:

   CA_SETUP_LOG_FILE
   CA_SETUP_VERBOSE
   CASE_INSTALLDIR
   CASE_PUBDATADIR
   CASE_SNMP_PORT
   CASE_SNMP_SYS_DESC
   CASE_SNMP_SYS_LOC
   CASE_SNMP_SYS_CONTACT
   CASE_SNMP_READ_COMMUNITY
   CASE_SNMP_READ_ALLOWED_MANAGERS
   CASE_SNMP_WRITE_COMMUNITY
   CASE_SNMP_WRITE_ALLOWED_MANAGERS
   CASE_SNMP_TRAP_COMMUNITY
   CASE_SNMP_TRAP_DESTINATION
   CASE_SNMP_TRAP_PORT
   CASE_DISABLE_NATIVE_SNMP
   CASE_DEFAULT_FROM_NATIVE_SNMP
   CASE_MANAGER_HOSTNAME
   CASE_MANAGER_POLICY_NAME
   CASE_PRIVSEP_USER
   CASE_START_AFTER_INSTALL
   CASE_INSTALL_DOCS
   CASE_LEGACY_MODE

   CA_SETUP_LOG_FILE

   Specifies a location and file name in which to log installation messages. By default, messages are logged to /opt/CA/installer/log/CA_SETUP_*PACKAGE_NAME*.log.

   CA_SETUP_VERBOSE

   Turns on verbose installation mode when set to "yes". Verbose mode logs more information to the installation log file.

   CASE_INSTALLDIR

   Specifies the SystemEDGE installation directory. This directory contains everything SystemEDGE-related, such as AIMs and Advanced Encryption, and is never modified after being set by the Core installer.

   Note: If you define a non-default installation directory, the installer installs agent files directly to the specified directory without creating a SystemEDGE subfolder.

   Default: /opt/CA/SystemEDGE

CASE_PUBDATADIR

Specifies the SystemEDGE data directory, where all configurations take place and dynamic data is stored (referred to in this document as the variable CASYSEDGE_DATA). The configuration files of the agent are located in a port-specific subdirectory which is based on the SNMP_PORT parameter value.

Default: /opt/CA/SystemEDGE/config

CASE_SNMP_PORT

Specifies the port used by SystemEDGE. This value can also be inherited from the native SNMP agent using the CASE_DEFAULT_FROM_NATIVE_SNMP parameter. If you specify a port using the CASE_SNMP_PORT parameter, it overrides the inherited value. This port must be unique, or the installation fails. If the default port of 161 is already in use by the native SNMP agent (and you do not plan on disabling this agent), you must specify a different unique port, for example, 1691 or 6665.

Default: 161

CASE_SNMP_SYS_DESC

Specifies information about the system (such as a system name) that populates the sysDescr MIB-II object. This value can also be inherited from the native SNMP agent using the CASE_DEFAULT_FROM_NATIVE_SNMP parameter. If you specify a description using the CASE_SNMP_SYS_DESC parameter, it overrides the inherited value.

CASE_SNMP_SYS_LOC

Specifies the system location that populates the sysLocation MIB-II object. This value can also be inherited from the native SNMP agent using the CASE_DEFAULT_FROM_NATIVE_SNMP parameter. If you specify a location using the CASE_SNMP_SYS_LOC parameter, it overrides the inherited value.

CASE_SNMP_SYS_CONTACT

Specifies system contact information that populates the sysContact MIB-II object. This value can also be inherited from the native SNMP agent using the CASE_DEFAULT_FROM_NATIVE_SNMP parameter. If you specify a contact using the CASE_SNMP_SYS_CONTACT parameter, it overrides the inherited value.

CASE_SNMP_READ_COMMUNITY

Specifies the name of the SNMP read community that can send GET requests to the agent. You can specify multiple communities by separating them with a semicolon (for example, public1;public2), and you can include a space delimited IP address list for each community to restrict access (for example, public 1.2.3.4). This value can also be inherited from the native SNMP agent using the CASE_DEFAULT_FROM_NATIVE_SNMP parameter. If you specify a read community using the CASE_SNMP_READ_COMMUNITY parameter, it overrides the inherited value.

Default: snmp_public (valid for a new installation only (no upgrade) and if no read-write community is specified)

CASE_SNMP_READ_ALLOWED_MANAGERS

Specifies the space-separated list of IP addresses/hostnames of SNMP managers allowed to query the Agent with CASE_SNMP_READ_COMMUNITY. When this is specified, CASE_SNMP_READ_COMMUNITY must only contain a single word, the SNMP community.

CASE_SNMP_WRITE_COMMUNITY

Specifies the name of the SNMP write community that can send GET and SET requests to the agent. You can specify multiple communities by separating them with a semicolon (for example, rwcomm1;rwcomm2), and you can include a space delimited IP address list for each community to restrict access (for example, rwcomm1 1.2.3.4). This value can also be inherited from the native SNMP agent using the CASE_DEFAULT_FROM_NATIVE_SNMP parameter. If you specify a write community using the CASE_SNMP_WRITE_COMMUNITY parameter, it overrides the inherited value.

CASE_SNMP_WRITE_ALLOWED_MANAGERS

Specifies the space-separated list of IP addresses/hostnames of SNMP managers allowed to query the agent with CASE_SNMP_WRITE_COMMUNITY. When this is specified, CASE_SNMP_WRITE_COMMUNITY must only contain a single word, the SNMP community.

CASE_SNMP_TRAP_COMMUNITY

Specifies the SNMP trap community and the trap destination address. You can specify multiple trap community settings by separating them with a semicolon (;). The value for this parameter can also be inherited from the native SNMP agent using the CASE_DEFAULT_FROM_NATIVE_SNMP parameter. If you specify a trap community using the CASE_SNMP_TRAP_COMMUNITY parameter, it overrides the inherited value. The following values are required for this parameter:

- Community name
- Destination address to which to send traps

The following values are optional for this parameter:

- Port number to which to send traps
- Trap source encoding options
- Trap source host name

Syntax of a trap community setting:

community-string {*ip-address*|*hostname*} [*port* [*encoding* [*source*]]]

Example:

public 1.2.3.4;public 2.3.4.5 1162;trapcom 3.4.5.6 1162 100 4.5.6.7

CASE_SNMP_TRAP_DESTINATION

Specifies the hostname or IP address to which to send traps. When this is specified, CASE_SNMP_TRAP_COMMUNITY must only contain a single word, the SNMP community and CASE_SNMP_TRAP_PORT must also be specified.

CASE_SNMP_TRAP_PORT

Specifies the destination port number to which to send traps. When this is specified, CASE_SNMP_TRAP_COMMUNITY must only contain a single word, the SNMP community and CASE_SNMP_TRAP_DESTINATION must also be specified.

CASE_DISABLE_NATIVE_SNMP

Specifies whether to stop and disable the native SNMP agent.

Default: no

CASE_DEFAULT_FROM_NATIVE_SNMP

Specifies whether to use the default SNMP settings from the native SNMP agent.

Default: no

CASE_MANAGER_HOSTNAME

Specifies the host name of the configuration manager from which you want to manage this agent. Entering a value for this parameter lets you configure this agent from the specified manager. Entering an asterisk (*) accepts the first manager that discovers the agent system. This manager will have full control over the agent's configuration. By default, no manager host is entered (used), and the agent runs in unmanaged mode.

CASE_MANAGER_POLICY_NAME

Specifies the name of the configuration manager policy file that the agent should use. Entering a value for this parameter sets the SystemEDGE configuration according to an existing configuration file from the manager. By default, the agent uses the installed policy file.

CASE_START_AFTER_INSTALL

Specifies whether to start the agent automatically after the installation completes. Valid values are: Yes, No, PRESERVE. PRESERVE can be used when upgrading to only start the agent when it was running at the time when the installation started.

Default: PRESERVE

CASE_PRIVSEP_USER

Specifies the user name under which credentials the agent run during SNMP communication.

This entry instructs the agent (UNIX only) to run SNMP communication under another user account. The agent also uses this user's default group as an effective group.

Default: The agent operates using root account.

CASE_INSTALL_DOCS

Specifies whether to install the SystemEDGE documentation with the agent.

Default: yes

CASE_LEGACY_MODE

Specifies whether to install the agent in legacy mode, which installs the base agent only while omitting all materials that facilitate usage with CA Virtual Assurance. Install using legacy mode if you do not want to use the agent with CA Virtual Assurance.

You can turn the agent into managed mode by reinstalling or upgrading and specifying CASE_LEGACY_MODE=no.

Default: no

The installation begins. If you did not accept the license agreement, the installation fails.

There is always the lsm installer log file in /opt/CA/installer/log/$CA_SETUP_PACKAGE_NAME.log that you can use to check if the installation was successful.

If you want to verify the installation, confirm the existence of the SystemEDGE files in the installation directory.

Legacy Support of the $CASYSEDGE Variable

The installation program on Linux/UNIX does not modify the system environment settings in /etc/profile. As a result the $CASYSEDGE variable is no longer available.

If you have to support $CASYSEDGE in your environment, do one of the following options:

- Create $CASYSEDGE in a shell.

  Run the following command in a sh, ksh, or bash shell:

  ```
  ./etc/profile.CA
  ```

  If you use csh, run the following command:

  ```
  source /etc/csh_login.CA
  ```

- Force the installation program to modify /etc/profile and create $CASYSEDGE.

  Open a shell and enter the following commands:

  ```
  Update_Profile=1;export Update_Profile
  sh ca-setup.sh
  ```

  If you use csh, run the following commands:

  ```
  setenv Update_Profile 1
  sh ca-setup.sh
  ```

  The installation program installs SystemEDGE and creates $CASYSEDGE in the environment.

During an upgrade to Release 5.7.1, the SystemEDGE installation program does not change the existing environment. The previously created $CASYSEDGE variable remains in the environment.

Configure and Use a Response File

You can create a response file for running a silent installation with no user interaction. Using a response file has the same effect as specifying CA_SETUP_MODE=UNATTENDED in the command line. A response file turns the installation into the silent, unattended mode.

The installer uses the properties in the response file to install the agent without prompting for user input.

Follow these steps:

1. Log on to the computer system as administrator or root.
2. Create a response file based on the parameters specified in the Install the Agent from Command Line sections. A response file is a text file that consists of parameter settings like the following:

   ```
   parameter1=value1
   parameter2=value2
   ...
   ```

3. Navigate to the *DVDdrive*\Installers*OperatingSystem*\Agent\SysMan\CA_SystemEDGE_Core directory, and enter one of the following commands according to your operating system:

   ```
   ca-setup CA_SETUP_RESPONSE_FILE="<name of the response file>" (Windows)
   ```

   ```
   sh ca-setup.sh CA_SETUP_RESPONSE_FILE="<name of the response file>" (UNIX, Linux)
   ```

   CA_SETUP_RESPONSE_FILE

   Specifies the path and name of the response file.

   The installation uses the settings in the response file to run silently.

Install the Agent in Legacy Mode

You can install SystemEDGE in legacy mode to acquire all base agent functionality while omitting the following components that facilitate use with CA Virtual Assurance:

- CAM, which enables remote configuration from CA Virtual Assurance.
- IDPrimer, which enables remote deployment from CA Virtual Assurance.

Install SystemEDGE in legacy mode *only* if you do not plan to manage it with CA Virtual Assurance or a similar management application. If you install an agent in legacy mode and want to manage it with CA Virtual Assurance later, you can upgrade the agent.

Note: When you upgrade a previous version of SystemEDGE, it automatically upgrades to the full agent unless you specify otherwise.

Follow these steps:

1. Copy the CA_SystemEDGE_Core directory from the installation media to the harddisk.
2. Change to the CA_SystemEDGE_Core directory and open ca-setup.dat with an ASCII editor.
3. Edit ca-setup.dat to set CASE_LEGACY_MODE=yes.
4. Save ca-setup.dat.
5. Run the installation as described in Install the Agent on Windows (see page 42) or Install the Agent on UNIX (see page 53).
6. Complete the installation.

To install the agent in legacy mode from the command line, include the following parameter in the ca-setup command:

```
CASE_LEGACY_MODE="yes"
```

Install AIMs

When you install AIMs on top of SystemEDGE, consider the following guidelines:

- The SRM AIM, RM AIM, MSCS AIM, or AIMs for managing virtual environments depend on Advanced Encryption and SystemEDGE.
- Advanced Encryption depends on SystemEDGE.

Based on these dependencies, the installation sequence is as follows:

1. SystemEDGE Core
2. Advanced Encryption
3. SRM AIM, RM AIM, MSCS AIM, or AIMs for managing virtual environments

The installer does not allow any other sequence. For example, when you try to install SRM before Advanced Encryption, it displays an error message and the installation does not start.

To install an AIM on Windows using ca-setup.exe

1. Navigate to the DVD1\Installers\Windows\Agent\SysMan directory that contains the following subdirectories:
   - CA_SystemEDGE_CXEN
   - CA_SystemEDGE_GALAX
   - CA_SystemEDGE_HACMP
   - CA_SystemEDGE_HYPERV
   - CA_SystemEDGE_KVM
   - CA_SystemEDGE_LPAR
   - CA_SystemEDGE_MSCS
   - CA_SystemEDGE_RM
   - CA_SystemEDGE_SOLZONES
   - CA_SystemEDGE_SRM
   - CA_SystemEDGE_UCS
   - CA_SystemEDGE_VC
   - CA_SystemEDGE_VCLOUD
2. For the SRM or RM AIM, change to the appropriate directory and run the following command:

   ```
   ca-setup
   ```

   Follow the instructions on the screen and complete the installation.
3. For the Hyper-V, LPAR, MSCS, Zones, UCS, vCenter, HACMP, vCloud, CXEN, or KVM AIM open a command prompt, change to the appropriate directory and run the following command:

   ```
   ca-setup EULA_ACCEPTED="YES"
   ```

   The ca-setup program completes the installation silently.

Note: You can also use the CA Virtual Assurance manager custom installation to install the SystemEDGE components on a Windows server.

To install an AIM on UNIX using ca-setup.sh

1. Open a terminal console and change to the DVD2/Installers/*Platform*/Agent/SysMan directory that contains the following subdirectories:
   - CA_SystemEDGE_SRM
2. Change to the appropriate directory and run the following command:

   ```
   sh ca-setup.sh
   ```

   Follow the instructions on the screen and complete the installation.

During the SRM installation, you can specify the following parameters:

Allow Running Scripts

Specifies if you want to allow running custom scripts. These scripts run with superuser privileges.

Default: No (typical installation)

Allow FileIO Tests

Allows running FileIO tests. Since the tests run with superuser privileges, they can access any file on the system when this parameter is enabled.

Default: No (typical installation)

Allows untrusted SSL certificates

Allows HTTPS tests to access sites with invalid certificates (untrusted or when the website does not match the name in the certificate).

Default: No (typical installation)

Miscellaneous

Installs the SRM documentation component.

Default: Yes

Install the CA Systems Performance LiteAgent

You can install the CA Systems Performance LiteAgent on Windows and UNIX or Linux systems.

Note: The CA Systems Performance LiteAgent runs on 32-bit and 64-bit operating systems.

To install the CA Systems Performance LiteAgent on Windows Systems

Run a custom installation from DVD1 to install the CA Systems Performance LiteAgent.

To install the CA Systems Performance LiteAgent on AIX, HP-UX, Linux, Solaris SPARC, or Solaris x86 Systems

Use Remote Deployment to install the CA Systems Performance LiteAgent on UNIX or Linux.

Note: For more information about Remote Deployment, see the Administration Guide.

Chapter 3: Upgrading CA Virtual Assurance

This section contains the following topics:

Supported Upgrades (see page 71)
How to Upgrade CA Virtual Assurance (see page 72)
Review Upgrade Documentation (see page 73)
Prepare the Environment You Want to Upgrade (see page 74)
Upgrade Remote CA EEM Manually (see page 78)
Run Manager Installation (see page 78)
Review Old Configurations Not Upgraded Automatically (see page 80)
Apply Old Configurations Manually (see page 80)
Upgrade Managed Nodes and AIM Servers (see page 80)
Verify the CA Virtual Assurance Upgrade in Your Environment (see page 85)

Supported Upgrades

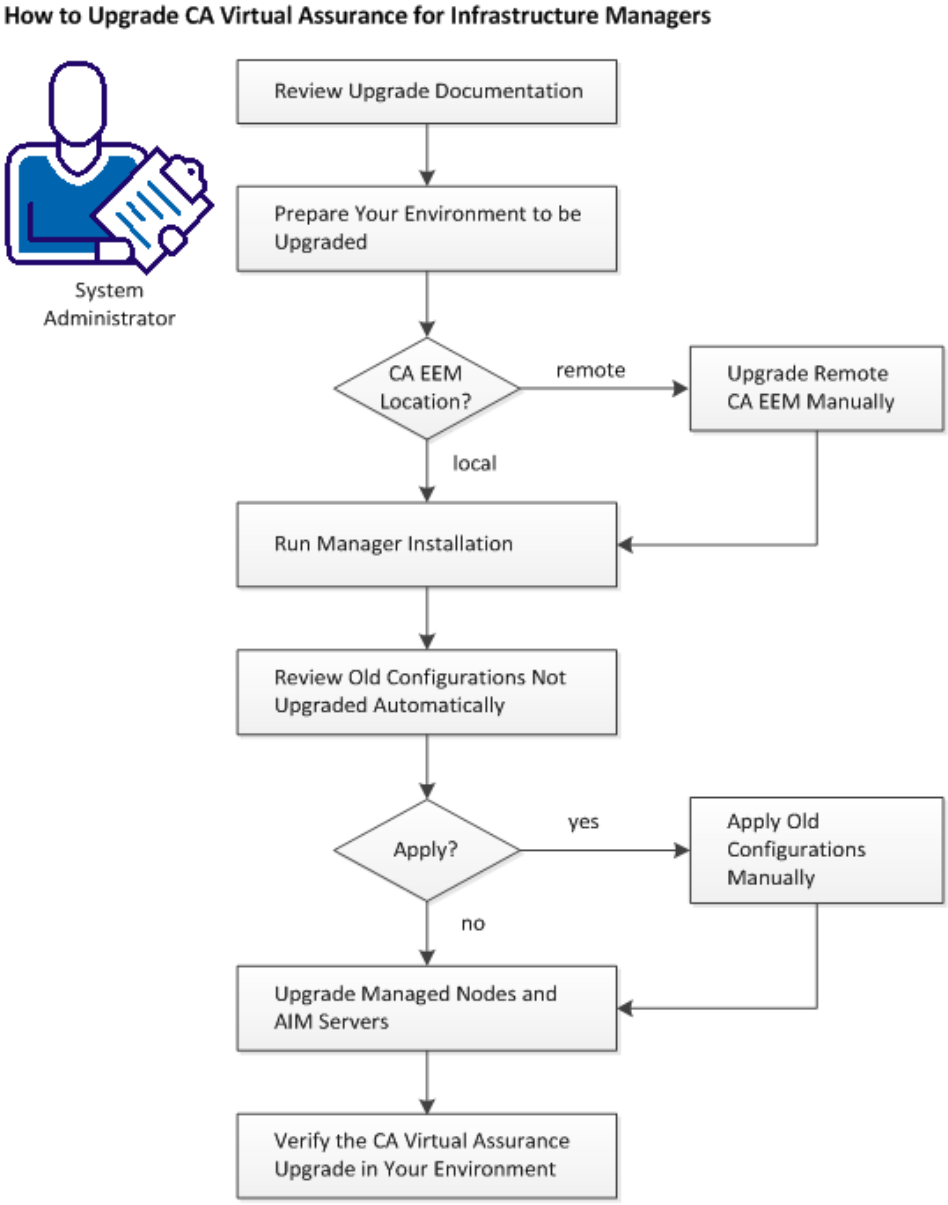
You can upgrade the following CA Virtual Assurance releases to Release 12.7.1:

- CA Virtual Assurance Release 12.6 and 12.7

Note: See the most recent Release Notes and Solutions and Patches on CA Support Online for important patches before you upgrade.

How to Upgrade CA Virtual Assurance

The following diagram provides an overview about the upgrade process.



Follow these steps:

Review Upgrade Documentation (see page 73)
Prepare the Environment You Want to Upgrade (see page 74)
Upgrade Remote CA EEM Manually (see page 78)
Run Manager Installation (see page 78)
Review Old Configurations Not Upgraded Automatically (see page 80)
Apply Old Configurations Manually (see page 80)
Upgrade Managed Nodes and AIM Servers (see page 80)
Verify the CA Virtual Assurance Upgrade in Your Environment (see page 85)

Review Upgrade Documentation

Read the upgrade information in this chapter before you start the Upgrading CA Virtual Assurance process. This chapter contains critical information about the steps required to prepare and perform an upgrade.

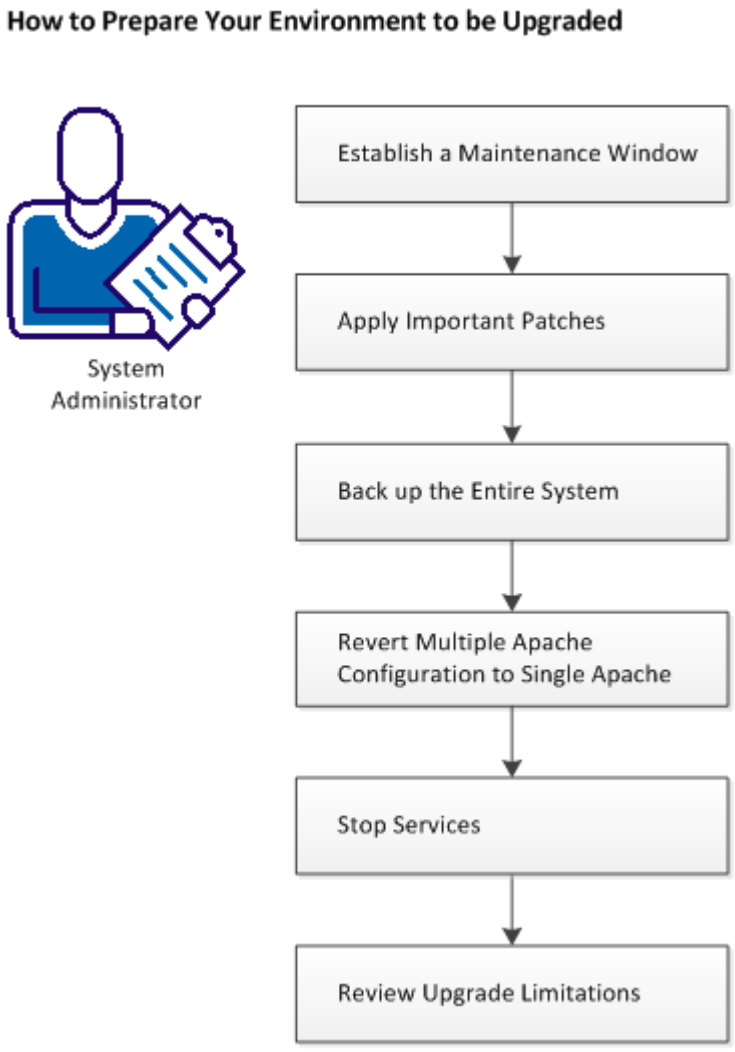
In addition to this chapter, verify the hardware and software requirements in the Release Notes and read Prepare a Custom Installation (see page 17) in this guide.

If you are using a remote CA EEM installation for authentication, read the upgrade instructions in the CA EEM documentation.

If you use Remote Deployment for upgrading the Managed Nodes or AIM Servers in your network, see the Remote Deployment documentation in the Administration Guide and Online Help for details.

Prepare the Environment You Want to Upgrade

This section describes how you can prepare your environment before you start the upgrade process.



Follow these steps:

Establish a Maintenance Window (see page 75)
Apply Important Patches (see page 75)
Back up the Entire System (see page 102)
Revert Multiple Apache Configuration to Single Apache (see page 76)
Stop Services (see page 77)
Review Upgrade Limitations (see page 77)

Establish a Maintenance Window

Establish a maintenance window in advance with your affected users. Verify that no administrative user is attempting an operation during that maintenance window.

Apply Important Patches

See the most recent Release Notes and Solutions and Patches on CA Support Online for updates.

If you had CA Virtual Assurance release 12.0.2 (SP2) that you upgraded to release 12.5, apply the following fix to your Domain Server manager 12.5 before you upgrade to Release 12.7.1:

- RO36999 (VDEPIN - upgrade deployment)

If you upgrade from release 12.6 to Release 12.7.1, apply one of the following patches to release 12.6:

- RO48212 (LPARAIM - 32 BIT - CUMULATIVE FIX 12162)
- RO48213 (LPARAIM - 64 BIT - CUMULATIVE FIX 12162)

Back up the Entire System

Perform the entire system (full) backup for the manager nodes. A manager node is any server that has the following components:

- Domain Server
- Distribution Server
- Databases
- EEM server

Back up the manager nodes using an industry standard tool (for example, ARCserve for Physical servers or Snapshots for Virtual Machines). If you have more than one manager node, verify that the backup is performed at the same time on all the servers.

We recommend that the backup is done offline when there is no user activity. Verify that any active jobs for Remote Deployment are complete before you start the backup.

Note: As Disaster Recovery is for an entire system, consult other product owners who have software on the systems.

Follow these steps:

1. Navigate to Resources, Deploy pane, Jobs and verify that all jobs are 100 percent complete.
2. Stop the following services using *one* of the options:
   - The command-line interface:
     ```
     net stop CASMDmnSrvr
     net stop CASMDstrbnSrvr
     ```
   - Windows Service Control Manager:
     - CA SM Domain Server
     - CA SM Distribution Server
3. Do *one* of the following:
   - Take a snapshot of the entire manager system.
   - Take a ghost image of the entire manager system.
4. Restart the services that were stopped using *one* of the options:
   - The command-line interface:
     ```
     net start CASMDmnSrvr
     net start CASMDstrbnSrvr
     ```
   - Windows Service Control Manager.
     - CA SM Domain Server
     - CA SM Distribution Server

Note: If the backup is not performed on the manager node with the Domain Server, stop and start only the Distribution Service.

Revert Multiple Apache Configuration to Single Apache

If you have configured your installation to run in a multiple Apache configuration, change to a single Apache configuration before you perform an in-place upgrade. After the upgrade, you can revert to the multiple Apache configuration.

Contact CA Support (see page 4) for Multiple Apache documentation and instructions on how to revert the configuration.

Stop Services

Stop the following services before starting the upgrade.

Follow these steps:

1. Log out CA Virtual Assurance user interfaces.
2. Stop the following Windows services:
   - CAAIPTomcat
   - CAAIPApache
   - CA Message Queuing Server (ActiveMQ)

Review Upgrade Limitations

Several component directories are renamed as follows during the product upgrade:

<product root>\component is renamed to <product root>\component-old

These “old” directories remain after upgrade is complete, for reference. If any modifications or additions are made to these directory trees before the upgrade, they are included in that “old” directory. Those alterations are not automatically merged with the new running product that takes over <product root>\component. If such alterations are desired to be in effect for the new product, reapply the customized settings manually.

The following list provides the components that have this limitation and their directory names:

- Apache HTTP Server: <product root>\apache
- Apache ActiveMQ: <product root>\activeMQ
- Apache Tomcat: <product root>\tomcat, including \tomcat\UI

  Note: While this limitation is true for Tomcat itself, some configuration data under Tomcat is in fact carried forward automatically during the upgrade.

Upgrade Remote CA EEM Manually

If you run CA EEM on the same server as the CA Virtual Assurance manager, you can skip this section. The CA Virtual Assurance upgrade procedure automatically upgrades a locally installed CA EEM.

If you run CA EEM on a separate server, see the Release Notes for supported CA EEM versions. If you have to upgrade CA EEM, perform the following procedure:

Follow these steps:

1. Open the CA EEM documentation bookshelf on the CA EEM server from the Windows Start menu.
2. Read the upgrade sections in the Getting Started Guide.
3. Insert the CA Virtual Assurance installation media (DVD1) into the DVD drive.
4. Open Windows Explorer and change to the \Installers\Windows\External\CAEEMServer directory.
5. Start EEMServer_win32.exe to upgrade CA EEM and follow the instructions of the CA EEM upgrade documentation.

Run Manager Installation

All previously installed components are upgraded. Upgrading the previously installed components is mandatory and all existing configurations are maintained. You can also select new components that you want to install with the upgrade. Newly selected components can be configured during the installation.

Perform this procedure after you determine that all prerequisites have been met. If you decide to skip a component configuration during installation, configure this component after the installation using the Administration tab of the graphical user interface.

Note: For more information about configuration of components, see the *Administration Guide*.

Follow these steps:

1. Insert the installation media into the DVD drive.

   If autorun is enabled, the installation wizard starts automatically. If the installation wizard does not start, double-click setup.hta or navigate to the *DVDdrive*:\Installers\Windows directory on the installation media and double-click install.exe.

   The Upgrade Detected dialog appears.

2. Click Continue.

   The Introduction dialog appears.

3. Click Next.

   The License Agreement dialog appears.

4. Read and scroll to the bottom of the agreement until the *I accept the terms of the License Agreement* option becomes active. Select this option and click Next.

   The Choose Features To Install dialog appears. All the installed components are upgraded.

5. (Optional) Select additional components you want to install and click Next.

6. The Upgrade procedure requests you to provide credentials or other additional information for CA EEM, Network Discovery Gateway, and any additional components.

   The installation wizard finally displays the Installation Summary dialog, listing the components to install.

7. Click Install to start the upgrade.

   If the installation is successful, the installation program creates log files for each installed component in the following directory:

   Install_Path\log\install

   The Installation Complete dialog appears.

8. Read the information provided in the dialog before you quit the installer.

9. Navigate to Start, Programs, CA, CA Virtual Assurance, Launch CA Virtual Assurance and log in the user interface.

10. If the upgrade is not successful, see the installation log (*Install_Path*\log\install\install.log) and the error list (*Install_Path*\log\install\install_error_detected.log) for details.

    The Installation Complete with Errors dialog appears. Contact CA Support to resolve issues with upgrade failure.

Review Old Configurations Not Upgraded Automatically

You can use the following directories to verify whether you need configurations from the previous release that have not been carried forward.

- Apache HTTP Server: <product root>\apache-old
- Apache ActiveMQ: <product root>\activeMQ-old
- Apache Tomcat: <product root>\tomcat-old, including \tomcat\UI

  Note: Some configuration data under Tomcat is carried forward automatically during the upgrade.

Apply Old Configurations Manually

If you have configuration data that you want to use in the upgraded CA Virtual Assurance installation and that has not been carried forward, use the following guideline.

Follow these steps:

1. Read the Apache, Tomcat, or ActiveMQ configuration documentation.
2. Log out CA Virtual Assurance.
3. Change the appropriate Apache, Tomcat, or ActiveMQ configuration file.
4. Restart the service for which you have changed the configuration file.
5. Log in CA Virtual Assurance.

Upgrade Managed Nodes and AIM Servers

The recommended method is Remote Deployment to upgrade managed nodes and remote AIM servers. Remote Deployment allows you to upgrade SystemEDGE, Advanced Encryption, and AIMs.

If your system does not support Managed Mode for SystemEDGE, you cannot use Remote Deployment. We recommend using *one* of the following options:

- Manual installation from the installation media
- Remote installation of SystemEDGE, Advanced Encryption, and SRM AIM using, for example, SSH

Follow these steps:

Agent and AIM Upgrades (see page 81)
Import SystemEDGE Monitors into a Policy (see page 84)

Agent and AIM Upgrades

You can upgrade to SystemEDGE release 5.7.1 from any upgrade-eligible release of SystemEDGE:

- 4.3.4 and above (4.3.x)
- 5.1.0 and above (5.1.x)
- 5.6.0 and above (5.6.x)
- 5.7.0 and above (5.7.x)

The installer creates an upgraded directory at the root of the original installation path and copies configuration files from the previous release to it. When the agent starts for the first time, it migrates the configuration data to the newly created data directory. When upgrading SystemEDGE to Release 5.7.1, upgrade Advanced Encryption and all the corresponding AIMs to the latest versions.

Note: SystemEDGE Release 5.7.1 does not load AIMs of previous CA Virtual Assurance releases.

You can upgrade SystemEDGE in either of the following ways:

- Remote Deployment through CA Virtual Assurance to a system with an upgrade-eligible agent installed.

  Note: If you want to upgrade SystemEDGE, Advanced Encryption, and AIMs, use a single Remote Deployment job for the upgrade. Add SystemEDGE, Advanced Encryption, and all required AIMs to the Remote Deployment job. SystemEDGE loads only AIMs which are at 5.7.1 level or which are legacy AIMs like iddmod. That is, AIMs at 5.7 level or below are quarantined.

  For more information about Remote Deployment, see the Remote Deployment chapter in the *Administration Guide*.

- Custom Manager installation on Windows. This option upgrades all the installed components. Select any additional agents and AIMs you want to install.

- Manual installation on a system with an upgrade-eligible agent installed.

  To perform an upgrade, install the agent as described in Install the Agent on Windows (see page 42) or Install the Agent on UNIX (see page 53).

If an upgrade of an older agent release is not supported, do the following steps:

- For earlier releases of SystemEDGE, uninstall the agent and then install SystemEDGE Release 5.7.1. You can save all configuration data before uninstalling and then apply this data to SystemEDGE Release 5.7.1.

More Information:

Agent Upgrade from SystemEDGE 4.3.4 (see page 82)

Agent Upgrade from SystemEDGE 4.3.4

The installer does the following when upgrading configuration files from a previous 4.3.4 release.

- The installer detects and copies previous versions of the following files to the CASYSEDGE\upgraded directory:
  - system32\sysedge.cf (Windows) and /etc/syedge.cf (UNIX)
  - CASYSEDGE\config\sysedgeV3.cf (Windows and UNIX)
  - system32\sysedge.mon (Windows) and /etc/sysedge.mon (UNIX)
  - system32\sysedge.lic (Windows) and /etc/sysedge.lic (UNIX)
  - CASYSEDGE\plugins\monwin\monwin.cf (Windows and UNIX)
- When the agent starts for the first time, it copies the following files directly into the CASYSEDGE_DATADIR directory:
  - CASYSEDGE\config\sysedge.cf (Windows and UNIX)
  - CASYSEDGE\config\sysedgeV3.cf (Windows and UNIX)
- As part of the sysedge.cf copy operation, the agent migrates the configuration data in the sysedge.cf, sysedge.mon, and monwin.cf files in the upgraded directory into the new sysedge.cf file in the data directory.
- As part of the sysedgeV3.cf copy operation, the agent migrates the configuration data in the sysedgeV3.cf file in the upgraded directory into the new sysedgeV3.cf file in the data directory.

Note: The data directory stores the version of the sysedge.cf file used for runtime configuration changes.

The agent automatically makes the following changes to configuration file settings when upgrading from a previous release:

- The procAlive process monitor syntax has changed to adhere to the threshold process monitor syntax. The agent automatically converts any existing procAlive entries into the new format.

  Note: For more information about the syntax for procAlive entries, see *Process and Service Monitoring* chapter.

- Disabling the no_process_sets and no_remoteshell_group parameters would allow critical access to the agent system with only an SNMP write community. Consequently, the agent does not migrate previous settings for those parameters and always enables them.

- The sysedge_memory parameter no longer exists and is removed in the upgraded sysedge.cf file. Outstanding alarms are now handled by storing the current state of any monitor in the sysedge.mon file. Existing entries are migrated to the new alarm handling configuration.

- The tc_publish parameter is renamed no_trapcommunity_table (with reverse logic) and is enabled by default.

- When you upgrade from SystemEDGE Release 4.3.4 to SystemEDGE Release 5.7.1 using Remote Deployment, the migrated monitors are stored in the sysedge.cf.bak file.

- Depending on your deployment strategy, you can use Policy Configuration to apply migrated monitors in your environment.

  Note: For more information, see the CA Virtual Assurance Bookshelf.

- When you upgrade from SystemEDGE Release 4.3.4 to SystemEDGE Release 5.7.1 on the local system, the installation program migrates monitors and provides them in the new configuration.

All previous syntax is compatible with the new version of the agent. However, many new options are available that enhance agent capabilities. We recommend that you examine older monitor entries and edit the syntax to contain additional options.

Note: When you upgrade SystemEDGE from Release 4.3.4 or above (4.3.x), the installer uses the following parameters only:

CASE_PUBDATADIR
CASE_MANAGER_HOSTNAME
CASE_MANAGER_POLICY_NAME
CASE_START_AFTER_INSTALL
CASE_LEGACY_MODE
CASE_SNMP_PORT
CASE_INSTALL_DOCS
CASE_SNMP_TRAP_COMMUNITY (1)
CASE_SNMP_TRAP_DESTINATION (1)
CASE_SNMP_TRAP_PORT (1)
CASE_SNMP_READ_COMMUNITY (1)
CASE_SNMP_WRITE_COMMUNITY (1)
CASE_SNMP_READ_ALLOWED_MANAGERS (1)
CASE_SNMP_WRITE_ALLOWED_MANAGERS (1)

Other parameters are ignored.

(1) These parameters are special. Their settings are appended to the existing SystemEDGE 4.x settings allowing both the SystemEDGE 4.x manager and SystemEDGE 5.x manager to function.

Import SystemEDGE Monitors into a Policy

Before you upgrade the agent, verify the SNMP community strings used in the SystemEDGE agent are specified under the Administration tab, SNMP. Community strings can also be specified on a computer by computer basis under Policy, *computer,* Metrics, SNMP. The SystemEDGE installer moves SystemEDGE files to the 'upgraded' directory, which the agent reads after the upgrade. The OIDs are preserved. Policy Configuration only reads the entries from the existing sysedge.cf file. The sysedge.mon file is not imported.

Remote Deployment imports the raw OIDs of the monitors into the instance.

Follow these steps:

1. Verify that the SystemEDGE agent community strings are included under the Administration tab, SNMP for the port of the agent.
2. Upgrade SystemEDGE to Release 5.7.1.
3. Verify that SystemEDGE Release 5.7.1 is discovered correctly (Resources tab) and has a policy.

4. Click the Resources tab, open the Configuration pane, expand Policies, and click SystemEDGE.

   The SystemEDGE pane appears.

5. Click + (New) on the Available Policies toolbar.

   The New SystemEDGE Policy dialog appears.

6. Enter a name for the policy and click 'Import...'.

   The SystemEDGE Agent Machine dialog appears.

7. Select the server that was upgraded and click OK.

   The SystemEDGE Agent Machine dialog closes.

8. Click OK on the New SystemEDGE dialog.

   CA Virtual Assurance creates a policy that contains the imported monitors.

You can edit or update the monitors and use the SystemEDGE Release 5.7.1 state model.

Verify the CA Virtual Assurance Upgrade in Your Environment

After all CA Virtual Assurance components have been upgraded sucessfully, verify if CA Virtual Assurance as a whole works as expected.

Chapter 4: Getting Started with User Interfaces

This chapter provides a brief introduction to the CA Virtual Assurance graphical user interface, AutoShell, and Bookshelf. These components are available after a typical installation on the Manager under the Windows Start menu entry CA, CA Virtual Assurance.

For further concepts, details, and specific tasks to manage virtual environments, see the *Administration Guide*, *Online Help*, or *Reference Guide*.

This section contains the following topics:

Start CA Virtual Assurance (see page 87)
Start AutoShell (see page 89)
Start the CA Virtual Assurance Command Prompt (see page 90)
Start the Bookshelf and Online Help (see page 91)

Start CA Virtual Assurance

After a successful installation and post-installation configuration, you can start CA Virtual Assurance.

Follow these steps:

1. Select CA, CA Virtual Assurance, and start CA Virtual Assurance.

   The CA Virtual Assurance login page appears.

   Note: When you start the CA Virtual Assurance user interface for the first time, the browser displays an SSL certificate warning. The browser displays this warning when it connects to secure sites that do not have a signed SSL certificate. The SSL certificate must be created for the specific server and certificate authority and cannot be automatically generated and installed. When the warning appears, click OK to proceed.

2. Enter the user name and password that you have defined during the installation and click Log In.

   The product Dashboard appears.

CA Virtual Assurance can only display diagrams or charts if you installed the Flash Plug-in for your web browser. If the Flash Plug-in is not available, plug-in download links appear instead of diagrams or charts. By default, the Dashboard displays Systems Status, Utilization History, Services, CA Virtual Assurance Status, and Events. Configure the dashboard by dragging modules from the left pane to the right pane.

Functional Overview

The CA Virtual Assurance graphical user interface consists of a navigation pane on the left and a data pane on the right. Use the tabs at the top of the panes to switch between the following functional areas:

Dashboard

Provides a high-level view at the current status of your virtual environment and associated physical resources. Drag modules from the navigation pane to the data pane to configure the Dashboard.

Resources

Provides details about the resources discovered in your environment. For detailed information about a monitored resource, click it in the navigation tree. To discover new resources, select Data Center from the navigation tree and open the Quick Start tab.

You can use the following features from the Resources tab:

- Configure monitoring and management capabilities.
- Provision VMs and Solaris Zones.
- Remotely deploy SystemEDGE and AIMs.
- Create and manage SystemEDGE and AIM configurations.
- Manage actions and rules that cause the action to run.

Reporting

Lets you create reports about specific aspects or characteristics of the environment. You can select predefined or custom reports from the left pane.

Administration

Lets you configure CA Virtual Assurance components, administer user groups, or access management.

Note: For more information, see the *Administration Guide* and the *Online Help* for further details.

Start AutoShell

AutoShell is a command line and scripting environment that automates complex recurring and management tasks. It is a combination of a scripting language (JavaScript) and a command line shell. It allows you to use JavaScript syntax with AutoShell commands, functions, and classes directly in the AutoShell, or run the scripts in .js files.

Note: For more information about the AutoShell, see the *Reference Guide*.

Follow these steps:

1. Open the Windows Explorer and navigate to the following directory:
   C:\Program Files\CA\SC\AutoShellManager
2. Double-click caaipaomautoshell.exe.

   The AutoShell login dialog appears.
3. Enter the user name and password that you have defined during the installation.

   The AutoShell command prompt appears.

   ```
   CA AutoShell v1.5.0.1
   Based on Mozilla SpiderMonkey 1.7
   User name: ca
   Password : *********
   VASU::->
   ```
4. Enter AutoShell expressions or commands as appropriate.
5. Enter **exit** to exit AutoShell.

Examples

Display Hello World!:

```
? "Hello World!"
Hello World
```

Display the numbers from 1 to 10:

```
for(i=1;i<11;i++)qout(i);
1
2
3
4
5
6
7
8
9
10
```

Display the current date and time:

```
? "Today is", new Date
Today is Tue Jun 02 2009 14:17:05 GMT-0400 (Eastern Daylight Time)
```

More Information

Valid AutoShell User (see page 90)

Valid AutoShell User

During the CA Virtual Assurance installation, you define a CA Embedded Entitlements Manager (CA EEM) user identity and password in the Native Security User Information screen of the installation wizard. The credentials are stored in the CA EEM database. The user is assigned to the CA Virtual Assurance administrator group and can be used to log in to the CA Virtual Assurance User Interface and AutoShell manager.

If CA Virtual Assurance components that use CA EEM are installed on a local or remote system, the AutoShell manager always validates the login credentials against the CA EEM data. If not, the AutoShell manager validates the login credentials against Windows authentication.

Start the CA Virtual Assurance Command Prompt

Start the CA Virtual Assurance Command Prompt if you want to use the CLI commands described in the *Reference Guide*.

Follow these steps:

1. Select CA, CA Virtual Assurance, CA Virtual Assurance Command Prompt.

   The CA Virtual Assurance Command Prompt dialog appears and opens the *Install_Path**productname*\bin directory.

2. Enter CLI commands.

Start the Bookshelf and Online Help

The Bookshelf contains the entire CA Virtual Assurance documentation set. All guides are available in HTML and PDF formats; the online help and the readme are only available in HTML format. The bookshelf supports full-text search across all deliverables. The online help system is context-sensitive regarding the high-level tabs in the user interface.

To start the online help

1. Open the CA Virtual Assurance user interface and click Help in the upper right corner of the window.

   A tab-related topic appears.

2. If necessary, use the navigation pane with Table of Contents, Index, or Search.

To open the Bookshelf from the online help

1. Open the CA Virtual Assurance user interface and click Help in the upper right corner of the window.

   A tab-related topic appears.

2. Change to the Table of Contents in the navigation pane.
3. Scroll up to the top and click Back to Bookshelf.

   The Bookshelf appears.

To start the Bookshelf from the start menu

1. Select CA, CA Virtual Assurance, Bookshelf from the Windows Start menu.

   The Bookshelf window appears.

2. Do one of the following:

   - Click the appropriate link on the Bookshelf window to open a document or online help system.
   - Type a word in the field in the upper right corner of the Bookshelf window and click Search to perform a full-text search across all deliverables.

Chapter 5: Uninstalling CA Virtual Assurance

This section contains the following topics:

Uninstallation Options (see page 93)
Uninstalling the Manager (see page 93)
Uninstalling SystemEDGE (see page 96)

Uninstallation Options

CA Virtual Assurance provides the following uninstallation options:

- Complete Uninstall
- Uninstall Specific Features (Manager only)
- Uninstall in Silent Mode

Uninstalling the Manager

The Complete Uninstall option removes all components and features of CA Virtual Assurance and provides the option to remove the following embedded components:

- CA EEM
- Apache
- Tomcat
- Management Database
- Performance Database

The uninstall wizard lets you remove an embedded component only if it was initially installed during the CA Virtual Assurance installation process. Shared components that existed on the system prior to the installation of this product will not be removed by the uninstallation of this product.

Note: The uninstallation process may stop Apache and Tomcat services, even if you have not chosen to uninstall these applications.

More Information

Perform a Complete Uninstall (see page 94)
Uninstall the Manager from Command Prompt (see page 95)
Uninstall the Manager in Silent Mode (see page 95)

Perform a Complete Uninstall

Use the Complete Uninstall option when you want to remove all CA Virtual Assurance features and components. This option also gives you the option to retain or remove embedded components.

Follow these steps:

1. Click Start, Settings, Control Panel, Add or Remove Programs from the Windows Start menu.

   The Add or Remove Programs window appears.

2. Select CA Virtual Assurance and click Change/Remove.

   The Uninstall CA Virtual Assurance dialog appears.

3. Click Next.

   The Uninstall Options dialog appears.

4. Select if you want to keep the Management Database, and click Next.

   The uninstallation begins. CA Virtual Assurance and all selected components are removed from your system.

   Notes: If the embedded component was not installed during the CA Virtual Assurance installation, the component is not uninstalled.

Uninstall the Manager from Command Prompt

Use this procedure to uninstall CA Virtual Assurance from the Windows command prompt.

Follow these steps:

Note: The quotation marks in the command syntax in this procedure are required, because the command names contain spaces.

1. Log in as Administrator and open a command prompt.

   The command prompt window appears.

2. Change to the *install_path**productname*\Uninstall directory, and enter the following command:

   ```
   Uninstall.exe
   ```

   The uninstallation begins.

3. Select one of the following options, and follow the on-screen instructions to complete the uninstallation:

   - Complete Uninstall
   - Uninstall Selected Features

More Information

Uninstall the Manager in Silent Mode (see page 95)

Uninstall the Manager in Silent Mode

Use this procedure to remove the Manager silently from a Windows server.

Follow these steps:

1. Log in as Administrator and open a command prompt.

   The Command Prompt window appears.

2. Change to the *install_path**productname*\Uninstall directory, and enter the following command to uninstall the Manager:

   ```
   Uninstall.exe -i silent
   ```

   The uninstallation begins. CA Virtual Assurance is removed from your system.

More Information

Uninstall the Manager from Command Prompt (see page 95)

Uninstalling SystemEDGE

This section explains how to remove the files and subdirectories associated with the SystemEDGE agent.

Uninstall SystemEDGE and the AIMs on Windows

The uninstaller removes SystemEDGE from your system. You can specify whether to remove the configuration data from the data directory. You can uninstall the agent and the AIMs from the Windows Add or Remove Programs window or from the command line.

Consider the following dependencies when you uninstall:

- AIMs for virtual environments, RM AIM and the SRM AIM depend on Advanced Encryption and SystemEDGE.
- Advanced Encryption depends on SystemEDGE.

Based on these dependencies, the uninstallation sequence is as follows:

1. RM AIM, SRM AIM, or AIMs for virtual environments
2. Advanced Encryption
3. SystemEDGE Core

The uninstallation is not possible if you use any other sequence. In case of removing components that were originally installed through Remote Deployment, Idprimer and CAM are not uninstalled.

To uninstall SystemEDGE or an AIM from the Windows Add or Remove Programs Window

1. Select Start, Settings, Control Panel, Add or Remove Programs.

   The Add or Remove Programs window appears and lists the following components:

   - AIMs for virtual environments
   - CA SystemEDGE Core
   - CA SystemEDGE AdvancedEncryption
   - CA SystemEDGE RM
   - CA SystemEDGE SRM

2. According to the uninstallation sequence, right-click the appropriate component and select Uninstall.

   In case of SystemEDGE, a dialog prompts you to specify whether to preserve the configuration files.

3. Click Yes or No.

   A dialog charts the uninstallation process. When the uninstallation completes, the dialog closes.

To uninstall SystemEDGE or an AIM from the command line

1. Open a command prompt and change to the DVD1\Installers\Windows\Agent\SysMan directory. It contains the following subdirectories:

   - CA_SystemEDGE_SRM
   - CA_SystemEDGE_RM
   - CA_SystemEDGE_AdvancedEncryption
   - CA_SystemEDGE_Core

2. Run the following command:

   ```
   ca-setup -x
   ```

   In case of SystemEDGE, a dialog prompts you to specify whether to preserve the configuration files.

3. Click Yes or No.

   A dialog charts the uninstallation process. When the uninstallation completes, the dialog closes.

To uninstall SystemEDGE or an AIM Silently

- Perform the following steps to uninstall SystemEDGE:

  a. Open a Command Prompt window and change to the following directory path:

     DVD1\Installers\Windows\Agent\SysMan\CA_SystemEDGE_Core

  b. Run the following command:

     ```
     ca-setup.exe CA_SETUP_MODE=UNINSTALL CASE_KEEP_DATA=[YES|NO]
     ```

     The SystemEDGE is uninstalled from the computer.

  Note: To verify, go to the control panel and see that the SystemEDGE is deleted from the control panel items.

- Perform the following steps to delete an AIM:

  a. Open a Command Prompt window and change to the appropriate AIM directory path:

     DVD1\Installers\Windows\Agent\SysMan*AIM*

b. Run the following command:

```
ca-setup.exe CA_SETUP_MODE=UNINSTALL
```

AIM is uninstalled from the computer.

Note: Navigate to Program Files, CA, SystemEDGE, plugins and verify that the AIM folder is deleted.

Uninstall SystemEDGE and the AIMs on UNIX Systems

The uninstaller removes SystemEDGE or the AIMs from your system. You can specify for SystemEDGE whether to remove the configuration data from the data directory.

Consider the following dependencies when you uninstall:

- The SRM AIM depends on Advanced Encryption and SystemEDGE.
- Advanced Encryption depends on SystemEDGE.

Based on these dependencies, the uninstallation sequence is as follows:

1. SRM AIM
2. Advanced Encryption
3. SystemEDGE Core

The uninstallation is not possible if you use any other sequence. It case of removing components that were originally installed through Remote Deployment, Idprimer and CAM are not uninstalled.

To uninstall the agent or an AIM using ca-setup.sh

1. Open a terminal console and log in as root (su).
2. Change to the DVD2/Installers/<*Platform*>/Agent/SysMan directory. It contains the following subdirectories:
   - CA_SystemEDGE_SRM
   - CA_SystemEDGE_AdvancedEncryption
   - CA_SystemEDGE_Core
3. Change to the appropriate directory and run the following command:

   ```
   sh ca-setup.sh -x
   ```

   A dialog prompts you to specify whether to preserve the configuration files.
4. Click Yes or No.

   A dialog charts the uninstallation process. When the uninstallation completes, the dialog closes.

To uninstall the agent or an AIM using lsm

1. Open a terminal console and log in as root (su).
2. Run the appropriate command from the following list:

   ```
   lsm -e CA_SystemEDGE_SRM
   lsm -e CA_SystemEDGE_AdvancedEncryption
   lsm -e CA_SystemEDGE_Core
   ```

   In case of SystemEDGE, you are prompted to specify whether to preserve the configuration files.
3. Click Yes or No.

   The uninstallation completes.

To uninstall the agent or an AIM Silently

- Perform the following steps to uninstall agent:
  a. Open a terminal console and log in as root (su). Change to the following directory path:

     DVD2/Installers/*Platform*/Agent/SysMan/CA_SystemEDGE_Core

  b. Run the following command:

     ```
     sh ca-setup.sh CA_SETUP_MODE=UNATTENDED_UNINSTALL CASE_KEEP_DATA=[YES|NO]
     ```

     The agent is uninstalled on the computer.
- Perform the following steps to uninstall an AIM:
  a. Open a terminal console and log in as root (su). Change to the appropriate AIM directory path:

     DVD2/Installers/*Platform*/Agent/SysMan/*AIM*

  b. Run the following command:

     ```
     sh ca-setup.sh CA_SETUP_MODE=UNATTENDED_UNINSTALL
     ```

     AIM is uninstalled from the computer.

Chapter 6: Backup and Restore

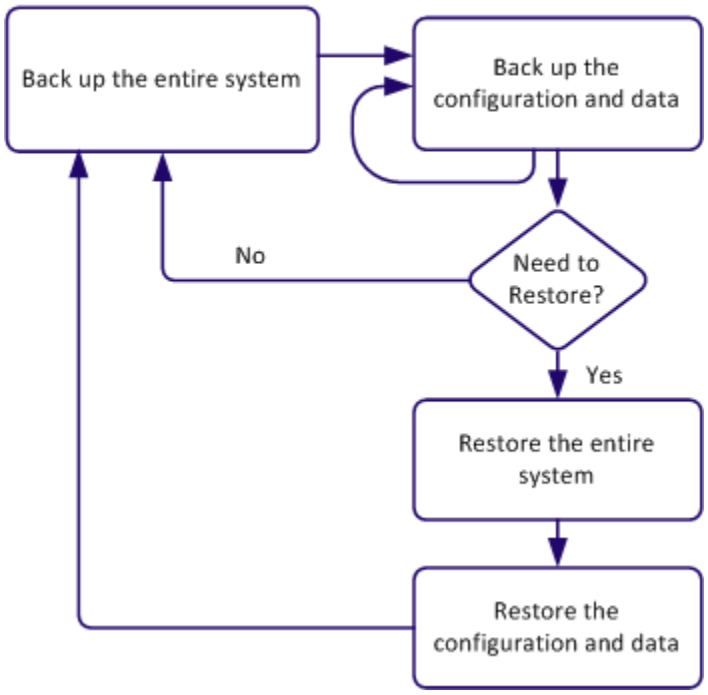
This section contains the following topics:

Backup and Restore Overview (see page 101)
Back up the Entire System (see page 102)
Back up the Configuration and Data (see page 103)
Restore the Entire System (see page 107)
Restore the Configuration and Data (see page 107)

Backup and Restore Overview

The following sections provide information about the two modes of backup and their corresponding restore processes. The diagram illustrates the procedures required to restore your environments.

Backup and Restore Process



To back up and recover your systems, do the following:

1. Back up the entire system (see page 102) according to your needs.
2. Back up the configuration and data. (see page 103)
3. If you want to restore your system:
   a. Restore the entire system. (see page 107)
   b. Restore the configuration and data. (see page 107)

Back up the Entire System

We recommend performing the entire system (full) backup for disaster recovery at least once a week for the manager nodes. A manager node is any server that has the following components:

- Domain Server
- Distribution Server
- Databases
- EEM server

Back up the manager nodes using an industry standard tool (for example, ARCserve for Physical servers or Snapshots for Virtual Machines). If you have more than one manager node, verify that the backup is performed at the same time on all the servers.

We recommend that the backup is done offline when there is no user activity. Verify that any active jobs for Remote Deployment are complete before you start the backup.

Note: As Disaster Recovery is for an entire system, consult other product owners who have software on the systems.

Follow these steps:

1. Navigate to Resources, Deploy pane, Jobs and verify that all jobs are 100 percent complete.
2. Stop the following services using *one* of the options:
   - The command-line interface:
     ```
     net stop CASMDmnSrvr
     net stop CASMDstrbnSrvr
     ```
   - Windows Service Control Manager:
     - CA SM Domain Server
     - CA SM Distribution Server

3. Do *one* of the following:
   - Take a snapshot of the entire manager system.
   - Take a ghost image of the entire manager system.
4. Restart the services that were stopped using *one* of the options:
   - The command-line interface:
     ```
     net start CASMDmnSrvr
     net start CASMDstrbnSrvr
     ```
   - Windows Service Control Manager.
     - CA SM Domain Server
     - CA SM Distribution Server

Note: If the backup is not performed on the manager node with the Domain Server, stop and start only the Distribution Service.

Back up the Configuration and Data

This section provides the recommendation for incremental backup of the databases, key configuration files, and other data. We recommend that the differential backup is performed at least once a day when the usage is off-peak or the system can be offline.

This section describes the following procedures:

- Back up the Databases (see page 103)
- Back up the Directories and Data (see page 104)

Back up the Databases

SQL Management Studio enables you to back up the Management and Performance Databases.

Follow these steps:

1. Launch the SQL Server Management Studio.
2. Expand the registered SQL Server where AOM2 and DPM databases reside.
3. Expand Databases.
4. Right-click the database, click Tasks, then Back Up.
5. Verify that the Backup type is set to Full and identify the path to where the backup is made.
6. Click OK.

The following table presents the recommendations for the Performance and Management Databases:

Database	Description	Recommendation
AOM2	Management Database	Incremental backup
DPM	Performance Database	The Performance Database contains performance metrics collected by the agents. Unless this data is deemed critical from a historical point of view, it is not recommended to back up this database.

Back up the Directories and Data

We recommend backing up Remote Deployment and Configuration data on a daily basis or according to your company backup policies.

The following table presents the list of key directories, their locations, and the corresponding abbreviations.

Directory	Locating the Directory	Abbreviation
Product Installation Directory* (valid for 32-bit systems)	REG QUERY "HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\DynamicProvisioningManager" /v InstallDirectory	<INSTALLDIR>
Product Installation Directory* (valid for 64-bit systems)	REG QUERY "HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ComputerAssociates\DynamicProvisioningManager"/v InstallDirectory	<INSTALLDIR>
Deployment and Configuration Private Data Directory	Findstr /i "CAISM_PRIVATE_DATA" "<INSTALLDIR>\bin\smglobals.ini"	<PRIVATEDATADIR>

Directory	Locating the Directory	Abbreviation
Deployment and Configuration Public Data Directory	Findstr /i "CAISM_PUBLIC_DATA" "<InstallDir>\bin\smglobals.ini"	<PUBLICDATADIR>
IDManager Install Directory * (valid for 32-bit systems)	REG QUERY "HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\InfrastructureDeployment" /v MgrApiPath	<IDDIR>
IDManager Install Directory * (valid for 64-bit systems)	REG QUERY "HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ComputerAssociates\InfrastructureDeployment"/v MgrApiPath	<IDDIR>

(*) Note: Use the 32-bit command prompt on 64-bit systems.

The backup recommendations are summarized in the following table:

Description	Directory	Recommendation
Installer configuration file	<INSTALLDIR>\bin\ smglobals.ini	This file defines the <CAVPM> directory settings. Recommended for an incremental backup set.
Domain Server Data	<PRIVATEDATADIR>\ domainserver	Directory and below required for incremental backup except for deployment packages in <PRIVATEDATADIR>\domainserver\Deployment\Packages\SM
Deployment packages	<PRIVATEDATADIR>\ domainserver\ Deployment\ Packages\SM	No need to back up. Can be obtained from installation media.
Distribution Server Data	<PRIVATEDATADIR>\ distributionserver\	No need to back up if backup is done when Domain Server and Distribution Services are stopped.

Description	Directory	Recommendation
IDManager Configuration on the Distribution server	<IDDIR>\config\SM	Required for incremental backup. If this information cannot be backed up on remote distribution servers and the distribution server is reinstalled, reenter credentials during the next deployment using this distribution server.
Web Service Data	<PRIVATEDATADIR>\ caismwebservice	No need to back up. Will be propagated from the domain server.
CA Virtual Assurance Log files	<PUBLICDATADIR>\log	Back up if needed for reference.
ID Log files	<IDDIR>\logs	Back up if needed for reference.

Follow these steps:

1. Verify that all active Remote Deployment jobs are complete.
2. Stop the following services using *one* of the options:
   - The command-line interface:
     ```
     net stop CASMDmnSrvr
     net stop CASMDstrbnSrvr
     ```
   - Windows Service Control Manager:
     - CA SM Domain Server
     - CA SM Distribution Server
3. Back up the recommended directories.
4. Restart the services that were stopped using *one* of the options:
   - The command-line interface:
     ```
     net start CASMDmnSrvr
     net start CASMDstrbnSrvr
     ```
   - Windows Service Control Manager.
     - CA SM Domain Server
     - CA SM Distribution Server

Restore the Entire System

Follow these steps:

1. Stop the following services using *one* of the options:
   - The command-line interface:
     ```
     net stop CASMDmnSrvr
     net stop CASMDstrbnSrvr
     ```
   - Windows Service Control Manager:
     - CA SM Domain Server
     - CA SM Distribution Server
2. Perform the restore using the same backup tool on the same machine that was backed up.

   Important! If you have restored multiple manager nodes, restore all systems to the same backup level to avoid inconsistent data. Restore the manager node with the Domain Server last.
3. Restart the services that were stopped using *one* of the options:
   - The command-line interface:
     ```
     net start CASMDmnSrvr
     net start CASMDstrbnSrvr
     ```
   - Windows Service Control Manager.
     - CA SM Domain Server
     - CA SM Distribution Server

Note: If the backup is not performed on the manager node with the Domain Server, stop and start only the Distribution Service.

More Information

Restore the Configuration and Data (see page 107)

Restore the Configuration and Data

After performing the restore of the entire system, restore the differential backup data.

This section describes the following procedures:

- Restore the Databases (see page 108)
- Restore the Directories and Data (see page 109)

More Information

Restore the Entire System (see page 107)

Restore the Databases

When you restore the databases, use SQL Management Studio.

Follow these steps:

1. Shut down the services: CAAIPApache, CAAIPTomcat, CA SM Distribution Server, CA SM Domain Server
2. Launch the SQL Server Management Studio.
3. Expand the registered SQL Server where the database resides.
4. Expand Databases.
5. Right-click the database, click Tasks, then Restore Database.
6. Select the database.
7. Identify the device path from where the restore is made.
8. Click OK.
9. Restart the services: CAAIPApache, CAAIPTomcat, CA SM Distribution Server, CA SM Domain Server

Restore the Directories and Data

Restore the configuration and data files from the same backup media on to the same machine that was backed up.

Follow these steps:

1. Go to Resources, Deploy, Jobs to verify that there are no active Deployment jobs in progress.
2. Stop the following services using *one* of the options:
   - The command-line interface:
     ```
     net stop CASMDmnSrvr
     net stop CASMDstrbnSrvr
     ```
   - Windows Service Control Manager:
     - CA SM Domain Server
     - CA SM Distribution Server
3. Restore the configuration and data files from the same backup media.

   Note: The restore operation gets the information back to the same state as at the time of the last backup. Any changes made after the last backup are lost.
4. If multiple manager nodes were backed up, continue to restore other manager nodes.
5. Restart the services that were stopped using *one* of the options:
   - The command-line interface:
     ```
     net start CASMDmnSrvr
     net start CASMDstrbnSrvr
     ```
   - Windows Service Control Manager.
     - CA SM Domain Server
     - CA SM Distribution Server

Note: If the backup is not performed on the manager node with the Domain Server, stop and start only the Distribution Service.

Chapter 7: Scalability Best Practices

This section contains the following topics:

Scalability Overview (see page 111)
Hardware Specifications (see page 112)
Database Considerations (see page 112)
Network Considerations (see page 113)
Remote Deployment and Policy Configuration Overview (see page 113)
Scalability Recommendations (see page 115)

Scalability Overview

This section provides best practices and recommendations for the deployment of CA Virtual Assurance. The purpose of the document is to assist with the planning of a roll out of CA Virtual Assurance within a production environment, with particular focus on:

- Monitoring and CA Virtual Assurance Management of VMware Environments
- Monitoring of IBM LPAR Environments
- Monitoring of Oracle Solaris Zones Environments
- Deployment of SystemEDGE and other Monitoring Software
- Initial and on-going configuration of SystemEDGE

The following sections are included:

1. Remote Deployment and Policy Configuration Overview (see page 113)
2. Hardware Specifications (see page 112)
3. Database Considerations (see page 112)
4. Network Considerations (see page 113)
5. Scalability Recommendations and Limitations (see page 115)
6. Scalability Use Cases (see page 122)

Hardware Specifications

This section lists the minimum hardware specifications for large-scale implementation of CA Virtual Assurance. For larger scale implementations, consider increasing the specification of the management servers.

- Domain Server: 2.6-GHz Dual-core Processor, 4-GB RAM, 100-GB disk.
- Distribution Server: 1-GHz Single Core/Processor/Virtual Processor, 2-GB RAM, 100-GB disk, 100-Mb/sec Ethernet.
- VC AIM Monitoring Server: Dual Core Processor: 2.6-GHz CPU, 4-GB RAM, 100-GB disk.
- LPAR AIM Monitoring Server: Dual Core Processor: 2.6-GHz CPU, 4-GB RAM, 100-GB disk.
- Solaris Zones AIM Monitoring Server: Dual Core Processor: 2.6-GHz CPU, 4-GB RAM, 100-GB disk.
- Target System: 1-GHz Single Core/Processor/Virtual Processor, 512-MB RAM, 2-GB disk, Single 100-Mb/sec Ethernet.

Note: 50 percent is the maximum usage allowed for CPU and memory.

Database Considerations

As the managed environment grows larger, more database activity can be expected. The product databases grow in size based on product usage, potentially consuming 30 GB or more, depending on the maintenance that is being done. We recommend the following general rule for data retention: for every 1000 machines in your monitored environment, increase the poll interval by 300 seconds.

Note: Using a dedicated standalone system for the database can improve its performance. Keep the database close to other CA Virtual Assurance components on the network, for example, on the same subnet, to improve response times.

Network Considerations

When planning the roll out of CA Virtual Assurance, consider the quality of the network connections to decide where to locate management components. The following items influence the scalability and effectiveness of the solution:

- Network quality: Poor quality results in data loss, causing slow response, or failures.
- Network bandwidth: Lower bandwidth limits the rate at which data can be sent between the components.
- Network latency: Higher latency (delay) limits the rate of data transfer, in a similar way to low bandwidth.
- DNS: Badly configured DNS hinders the deployment and ongoing configuration of the monitoring agents.

We recommend using at least 100-Mb/sec Network Links between management components, especially when using a remote DB. If the network speed is less than 100Mb/sec, consider introducing additional Distribution Servers that are collocated with the target systems.

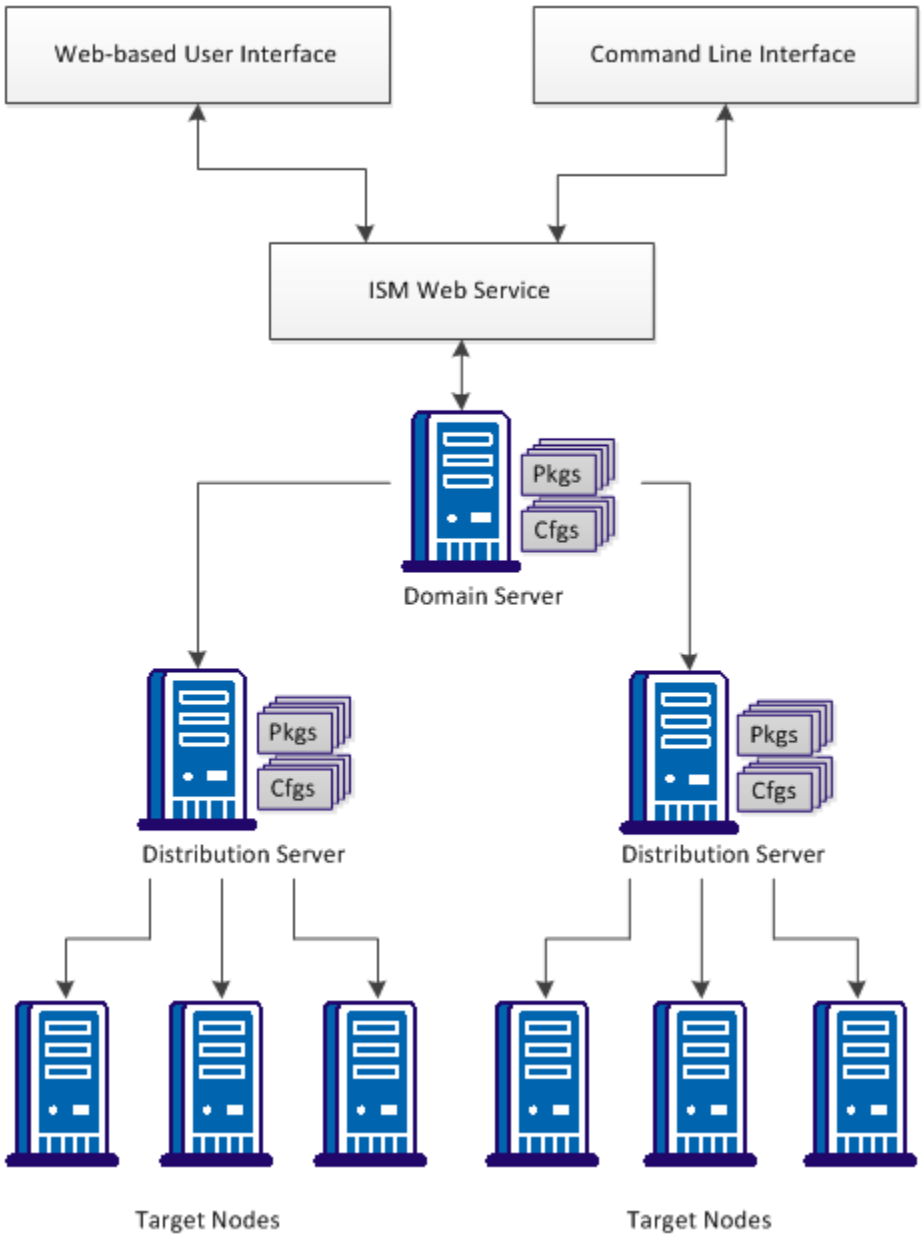
Remote Deployment and Policy Configuration Overview

CA Virtual Assurance provides a comprehensive solution for remotely deploying the SystemEDGE agent to all managed systems. You can create deployment templates that are based on packages that contain customized installation parameters and simultaneously deploy these templates to numerous managed systems.

In addition CA Virtual Assurance provides a comprehensive solution for the ongoing configuration of the SystemEDGE agents running on all managed systems. Policy Configuration allows a library of Policies to be created. These policies are applied to one or more systems running SystemEDGE and SRM AIM. When an agent managed by Policy Configuration is installed, it automatically requests a policy. As a result, the agent runs a controlled and consistent set of Policies. Each agent can then be updated individually, based on the Policy the agent is running, or the service the agent is a member of.

Remote Deployment and Policy Configuration share the Domain Server and Distribution Server technology. This technology provides a solution that is both scalable and able to be distributed across multiple data centers.

The diagram illustrates the basic architecture of the Remote Deployment and Policy Configuration components.



Scalability Recommendations

This section provides information about scalability recommendations and limitations.

Consider the following information:

- Monitoring of VMware Environments (see page 115)
- CA Virtual Assurance Management of VMware Environments (see page 116)
- Remote Deployment and Policy Configuration Recommendations (see page 120)
- Domain Server Recommendations (see page 122)
- Distribution Server Recommendations (see page 122)
- Scalability Use Cases (see page 122)

vCenter AIM Monitoring Recommendations

The SystemEDGE agent provides a plug-in architecture through which it can load optional *application insight modules (AIMs)* when it initializes. AIMs are functional extensions to the SystemEDGE agent. For example, the vCenter AIM enables SystemEDGE to manage vSphere environments through VMware vCenter Servers.

The vCenter AIM (Application Insight Module) is a pluggable component implemented within the SystemEDGE framework. As such, the data that it publishes is available to multiple SNMP Managers. Products such as CA Virtual Assurance Manager, eHealth, and Spectrum IM can leverage this data.

Due to the possibility of this component being utilized outside of the CA Virtual Assurance Manager, scalability recommendations are specified separately. Two main scalability considerations are discussed:

General Recommendation for vCenter AIM Monitoring

The general recommendation for scalability limitations for vCenter AIM Monitoring is as follows:

- Maximum Number of VMs is approximately 240,000 / (x + 6)
- Maximum Number of Objects is approximately 2,000,000 / (x + 6)

  where x is the number of SNMP polls against AIM per hour.

Scalability Limitations in Terms of Monitored Objects

In general, CPU usage is the primary concern when scalability limitations are considered. For vCenter AIM monitoring, consider the three main factors that influence CPU usage:

- The dynamic nature of the vCenter Servers being monitored.

  The level of activity of vCenter Servers influences CPU consumption. The following scalability recommendations assume an average level of activity of the vCenter Server being monitored.

- The number of SNMP Managers, and polling intervals of those SNMP Managers.

  Large numbers of SNMP Managers polling the vCenter AIM, or short poll intervals, result in increased CPU consumption.

- The ratio of object count in relation to the VM count.

  An *object* is any element of vSphere that is monitored by the vCenter AIM. For example, vCenter AIM monitors Datastores, Virtual Disks, Physical Network Interface Controllers, Virtual Switches, SCSI Controllers, ESX Host Hardware Sensors, and so on. The number of objects directly impacts CPU consumption. Due to the need to maintain the vCenter AIM cache and the additional overhead that is required for publishing this data. In real-world systems, there are typically from 6 through 11 times as many objects as there are Virtual Machines within a given vCenter.

Based on the preceding factors, a single SNMP Manager monitoring vCenter AIM with a 10-minute poll interval has a limitation of approximately 20,000 VMs.

Scalability Limitation in Terms of Monitored Servers

The vCenter AIM functions in a multiple vCenter Server environment. The vCenter AIM framework results in a slight CPU usage reduction with fewer VMs per vCenter Server. For example, CPU usage is lower for three vCenter Servers, each with 2,000 VMs, than for a single vCenter Server with 6,000 VMs.

Sometimes the responsiveness of the vCenter AIM becomes the scalability limit. In general, vCenter AIM is able to monitor up to ten vCenter Servers.

CA Virtual Assurance vCenter Management Recommendations

The CA Virtual Assurance manager does far more than simply monitor and publish vCenter data. The manager stores and manages historical data, performs active operations against the vCenter, runs automation policy, reporting, and so on. As such, it often requires more resources than the vCenter AIM, which it uses as its main data collection mechanism.

vCenter Management Limitations in Terms of Virtual Machines

Because most of the CA Virtual Assurance manager resides within a single process space, Operating System limitations tend to be the primary culprit in scalability. Consider the following limiting factors:

- Available Memory: As the number of objects being managed increases, the amount of memory that is required to cache the data and handle messaging increases rapidly. We recommend increasing the memory of the manager to at least 8 GB.
- Available CPU: The CA Virtual Assurance manager requires significant CPU resources, especially in times of rapid environmental change, or during initial startup. We recommend supplying an additional CPU (3.2 GHz or larger) for moderately large managed environments to improve the responsiveness of automated processes.
- Operating System Limitations: Most of the CA Virtual Assurance Manager resides within a single process space. As a result, the memory addressing space of a 32-bit operating system can become exhausted, even when system memory is not exhausted. To avoid this issue, we recommend using a 64-bit processor and an operating system for a moderately large managed environment.

Examples:

The following examples provide requirements and scalability limit recommendations for the CA Virtual Assurance manager:

- Minimum Requirements (32-bit, 2.6-GHz CPU, 4-GB RAM, 100-GB disk)

  Scalability limit: 2,500 Computer Systems (that is, VMs and ESX Hosts).
- Recommended System (64-bit processor and Operating System, 3.2-GHz CPU, 8-GB RAM, 100-GB disk)

  Scalability limit: 8,000 Computer Systems (that is, VMs and ESX Hosts).

Performance Considerations during Initial Discovery

Performing the initial discovery and database load of the vCenter environment you want to manage can be a time consuming process. During this process, the following actions take place:

1. The vCenter AIM parses the entire vCenter environment and publishes the results for the managers.
2. The CA Virtual Assurance manager retrieves the published data from the vCenter AIM and creates an internal cache for processing.
3. The internal cache is synchronized with the current CA Virtual Assurance manager database contents, with discoveries performed for Computer Systems not currently within the database.

During initial management of the vCenter server, the database has no Computer Systems in the database, so all of these objects are discovered and created. Consider the estimated time to complete the initial discovery. Based upon baseline testing, the average throughput is: from eight to nine Computer Systems per minute.

Examples:

The following examples provide the sizes of environments and corresponding estimated times to complete initial discovery:

- 2,500 Computer Systems - approximately five hours
- 8,000 Computer Systems - approximately 15 hours

During this initial population, CPU usage may be high for extended periods.

Note: The initial discovery process takes the vast majority of this time. However, the initial discovery is done once for the lifetime of the product. The vCenter AIM and CA Virtual Assurance internal caching processes, are considerably quicker. For example, 2,500 Computer Systems are typically published through vCenter AIM and the CA Virtual Assurance manager caches them in approximately 5 minutes.

LPAR AIM Monitoring Recommendations

The LPAR AIM (Application Insight Module) is a pluggable component that is implemented within the SystemEDGE framework. As such, the data that it publishes is available to multiple SNMP Managers. Products such as CA Virtual Assurance, eHealth, and Spectrum IM can leverage this data.

The following section specifies the scalability recommendations for LPAR AIM monitoring.

Scalability Recommendation for LPAR AIM Monitoring

One LPAR AIM can handle P systems environment configurations in the following range:

- Number of HMC Servers: 1 to 4
- Number of Power Systems per HMC Server: 2 to 10
- Number of Virtual I/O Servers per Power System: 1 to 2
- Number of LPARs per Power System: 10 to 100

General recommendations for LPAR AIM monitoring present a typical configuration of LPAR environment:

- Monitored Power Systems: up to 20
- Monitored VIO Servers: up to 30
- Monitored LPARs: up to 300

The AIM consumes CPU and Memory which is roughly a function of the number of LPARs. With a maximum of 300 LPARs the CPU consumption of the sysedge process would be less than 10 percent.

Note: The presented CPU consumption is valid for a dedicated SystemEDGE agent not running any other AIM.

With 300 LPARs added to the LPAR AIM, the sysedge process memory consumption increases by approximately 8 MB.

Solaris Zones AIM Monitoring Recommendations

The Solaris Zones AIM (Application Insight Module) is a pluggable component that is implemented within the SystemEDGE framework. As such, the data that it publishes is available to multiple SNMP Managers. Products such as CA Virtual Assurance, eHealth, and Spectrum IM can leverage this data.

The following section specifies the scalability recommendations for Solaris Zones AIM monitoring.

Scalability Recommendation for Solaris Zones AIM Monitoring

General recommendations are to have one Zones AIM monitor the following configuration:

- Monitored Zones Servers: Up to 20
- Monitored Zones: Up to 1000

The AIM consumes CPU and Memory proportionally to the number of Zones. However the initial consumption of memory for the first couple of zones is higher and decreases with more zones being added.

With 1000 Zones the CPU consumption of the sysedge process is less than 5 percent.

Note: The presented CPU consumption is valid for a dedicated SystemEDGE agent not running any other AIM.

With 1000 Zones being added to the Zone AIM, the memory consumption of the sysedge process increases by approximately 20 MB.

Remote Deployment and Policy Configuration Recommendations

Consider the following aspects and recommendations to improve remote deployment and policy operations:

- Number of target machines

  For optimal performance, limit the deployment job size to 500 target machines in a batch.

- Number of Distribution Servers

  Deployment throughput is better when multiple distribution servers are used.

- Deployment package size

  The smaller the deployment software package, the better the throughput. The numbers recommended assume that all of the managed servers are required to have SystemEDGE and Advanced Encryption.

  Note: A typical package size ranges from 10MB through 20MB.

- Quality and speed of the network

  Low bandwidth, high packet loss and high latency between the Distribution server and the target affect the rate and reliability of Deployment and Configuration operations.

- The timescale for the rollout of Monitoring Software to the target systems

  Stagger the deployment of monitoring software using collocated deployment servers. Staggering reduces the load on the network infrastructure. This load reduction can be achieved by creating a number of jobs, or by using the Staggering capability that is built into the solution.

  If the monitoring software must be deployed in a short time, we recommend deploying more Distribution Servers in the environment.

- Frequency of agents reconfiguration (by Policy Configuration)

  Reconfiguration of SystemEDGE Agents is expected to take around 30 seconds plus from 2 through 10 seconds per agent in a typical network environment. If agents must be reconfigured frequently, we recommend deploying additional Distribution Server in the environment.

- Geographical distribution of the target systems across multiple sites

  Where the target systems are distributed across multiple sites, we recommend deploying a Distribution Server at each location. This recommendation is especially true if the remote data centers use a slow (slower than 100Mb/sec) or unreliable link. Deploying a local Distribution Server allows all Deployment and Configuration requests to be directed through the on-site Distribution Server. This action limits the network traffic between the central and remote site.

- Communication ports

  Remote Deployment and Policy Configuration rely on communications by CA-Messaging for Domain Server to Distribution Server and Distribution Server to Agent communications. CA-Messaging communicates over ports 4104(UDP) and 4105(TCP). For remote sites that are firewall protected, placing a Distribution Server on site allows all CA-Messaging communications to be set up as point-to-point.

  Note: For agent discovery and ongoing monitoring, SNMP communications (typically port 161) are used. Open this port for direct communication from the managed systems to the manager.

- Management of Policy Configuration Policies and Templates

  We recommend organizing the monitoring requirements into templates based on the different workloads in your environment. Use a maximum of 1000 monitors per policy or template. Any number of templates can be applied to a system, but we recommend limiting the number of templates to 100 per system.

- Service Membership

  To ease configuration operations, we recommend organizing servers into Services, with an upper limit of around 500 servers per Service. A server can be a member of multiple Services, and therefore we suggest creating services to represent different workloads. A template can then be applied directly to a Service.

- Test Deployment

Domain Server Recommendations

A *deployment and configuration domain server* (domain server) manages and controls all deployment and policy configuration operations.

If the number of target systems exceeds 10,000, we recommend running multiple instances of CA Virtual Assurance.

Distribution Server Recommendations

A *deployment and configuration distribution (scalability) server* ensures that deployment and policy configuration operations are carried out in an efficient and timely manner.

Once the CA Virtual Assurance manager is installed, the next step in the rollout of Remote Deployment and Policy Configuration is to consider the number of Distribution Servers.

For Deployment operations, we recommend using one Distribution Server per 2,000 target systems for a typical 100-Mb/sec network environment.

Note: If you use Policy Configuration and you do not use Remote Deployment, each Distribution Server can scale up to 3,000 servers.

Important! We recommend performing a test deployment to at least one system for each distribution server before large deployment operations. We recommend deploying all possible packages using the distribution server to verify that there are no failures with the larger scale deployments.

Scalability Use Cases

This section provides use cases that aim to represent typical production environments. We suggest comparing these cases with your own environment and following the recommendations that best matches your environment.

Departmental Data Center

In this use case, monitoring is required for 1,000 systems, all contained within one data center. All systems are in one location, within a firewall, and fast links exist between the computers.

Recommendations for this environment are:

- Component Installation

  All CA Virtual Assurance manager components can be installed on the same system.

- Initial Deployment

  Two jobs could be created to deploy the monitoring software to all target nodes. Depending on network load, the initial deployment of SystemEDGE (and Advanced Encryption if necessary), would be expected to complete in 8 to 12 hours.

  Once deployment to remote systems completes, the CA Virtual Assurance Manager discovers SystemEDGE. Policy Configuration delivers an initial policy to each agent. We expect the initial policy delivery to complete approximately eight hours after the completion of the job.

- Service membership

  For ease of maintenance, we suggest aligning the monitored servers into Services, with approximately 200 servers per Service. You can align services to business function, network topology, or other categorization as desired.

- Applying Policies

  If necessary, applying policies to all monitored systems can be performed in a single operation.

Multiple Data Centers

In this use case, 10,000 systems, spread across multiple Data Centers, are being managed. The number of systems per data center varies from 500 through 2,500. The Data Centers are geographically distributed across multiple locations. The links between the Data Centers include leased lines of less than 100Mb/sec. The systems run various workloads, and are managed by a number of different departments (application owners).

Recommendations for this environment are:

- Component Installation

  Install the CA Virtual Assurance manager components on a dedicated server. This server must meet the minimum supported specification, but a quad-core server with at least 8-GB RAM is recommended.

  We recommend installing the Database on a separate dedicated server with an increased specification of quad-core processor and 8-GB RAM.

  To support the remote data centers, we recommend installing one Distribution Server in each data center. For a data center that contains more than 2,000 servers, we recommend installing a second Distribution Server.

  Note: If you use Policy Configuration and you do not use Remote Deployment, each Distribution Server can scale up to 3,000 servers.

- Initial Deployment

  The following are relevant factors to consider while planning to deploy using multiple distribution servers:

  - If possible, limit a single deployment job size to a maximum of 500 target systems.
  - Verify that the nearest distribution server is chosen for the deployment operation.
  - Although concurrent deployments are supported within a single distribution server, it is advised to only use concurrent deployments across multiple distribution servers. If you have 4 distribution servers, you could start a job to deploy to 500 machines for every distribution server.
  - When you perform concurrent deployment using the same distribution server, verify that the second job does not deploy to the same set of target machines as the previous one.
  - Where multiple packages are being delivered to many systems, consider splitting the package deliver to multiple jobs. For example, by deploying SystemEDGE and Advanced Encryption first.

- If you do see failures during a large-scale deployment, verify all prerequisites then use “resubmit job” to retry the deployment.
- To help with future deployments, we recommend saving the deployments as templates.

- Service membership

  For ease of maintenance, we suggest aligning the monitored servers into Services, with a maximum of 500 servers per Service. For remote data centers, we recommend creating one or more Services (depending on data center size) to represent data center.

  Where multiple departments use particular systems, the systems can be added to multiple services for ease of management by each department.

- Applying Policies

  In this use case, the servers run various workloads. We therefore recommend that the base policy contains only the control settings. Hold your monitoring configuration in templates based on different monitoring requirements. These templates can then be applied to the required systems, either by manually selecting systems, or by applying templates to a service.

  Splitting the monitoring requirements into templates allows the templates to be applied to the required systems, independently of each other. Select the systems manually, or apply templates to a service. We recommend applying templates in batches of 2,000 to 2,500 systems.

  If the base policy is required to be changed, we recommend applying the policy to systems in batches of 2,000 to 2,500 systems.

  Note: When templates are used, each delivery of a template or policy involves merging of all assigned templates with the base policy. The next step is delivering the resultant configuration to the agent. Therefore, where multiple templates are applied to a system, the time for delivery may be slightly increased.

Large Environments

In this use case, approximately 21,000 Agents are being managed. These agents are spread across three data centers, with each data center containing from 2,000 through 10,000 targets. The data centers are distributed, but have fast links between them. The managed systems are largely virtualized, run various workloads, and are reprovisioned at times.

Recommendations for this environment would be:

- Component Installation

  We strongly recommend running an instance of CA Virtual Assurance in each data center, so that each instance manages up to 10,000 systems.

  Within each data center, we recommend installing the CA Virtual Assurance manager components on a dedicated server. This server must meet the minimum supported specification, but we recommend an increased 8-GB RAM.

  We suggest installing the Database on a separate, dedicated server with 8-GB RAM.

  If a single instance of CA Virtual Assurance is required, we recommend using Manager and Database Servers with quad-core processors with 16-GB RAM.

  To support Remote Deployment and Policy Configuration operations, we recommend installing a Distribution Server in each Data Center and one being installed on the Manager system.

- Initial Deployment

  In this use case, we have one additional distribution server in the datacenter. Apart from that one difference in the setup, all the factors that were highlighted in the previous scenario apply equally to this scenario.

- Service membership

  For ease of maintenance, we suggest splitting the monitored servers into multiple Services, with a maximum of 500 servers per Service.

- Applying Policies

  We suggest limiting the base policy to control settings and 'base OS' monitors. Where different images are being used as the basis for virtual machines, a base policy can be created for each OS image. Verify that the SystemEDGE is configured to request this policy on registration.

  For application-specific monitors, create templates that are based on individual monitoring requirements. To avoid index conflicts across templates, we suggest defining 'index ranges' up-front for each application. Alternatively, the base policy can be configured to "Automatically Resolve Indexes" under the 'Control settings' section.

  Splitting the monitoring requirements into templates allows the templates to be applied to the required systems, independently of each other. You can either manually select systems, or apply templates to a service. We recommend applying templates in batches of 2,000 to 2,500 systems.

  If the base policy is required to be changed, we recommend applying the policy to systems in batches of 2,000 to 2,500 systems.

  Note: When templates are used, each delivery of a template or policy involves merging of all assigned templates with the base policy. The next step is delivering the resultant configuration to the agent. Therefore, where multiple templates are applied to a system, the time for delivery may be slightly increased.

  Important! Contact CA Support if multiple instances of CA Virtual Assurance are deployed and if you want to share the created policies between the different instances. CA Support can assist with the export and import of policies and templates between CA Virtual Assurance instances.

Glossary

application insight module, AIM

The SystemEDGE agent provides a plug-in architecture through which it can load optional *application insight modules (AIMs)* when it initializes. AIMs are functional extensions to the SystemEDGE agent. For example, the vCenter AIM enables SystemEDGE to manage vSphere environments through VMware vCenter Servers.

dynamic reconfiguration connector index, DRC-index (LPAR)

Each slot in a physical system unit has a *DRC-index* assigned to it. The deploy process requires this number to perform the actual creation of the LPARs. The management console (HMC) and the system uses this index to identify uniquely each slot on the system. The DRC-index is not assigned to a slot until the unit is powered up.

Hyper-V

Hyper-V is the Microsoft hypervisor-based server virtualization technology for Windows Server 2008 R2. Separate virtual machines (VMs) run on a single physical server and can run multiple different operating systems, such as Windows or Linux.

internet Small Computer Systems Interface, iSCSI

iSCSI is used to facilitate data transfers over intranets and to manage storage over large distances. iSCSI encapsulates SCSI commands in IP packets, which are routed just like any other IP packet on the network. When the IP packet reaches its destination, the iSCSI device removes the encapsulation and interprets the SCSI command.

logical partition, LPAR

A *Logical Partition (LPAR)* is a subset of hardware resources, virtualized as a separate system. A physical system can be partitioned into multiple LPARs, each providing a separate operating system and applications. The number of logical partitions depends on the hardware configuration of the system. LPARs are typically used for different environments, such as databases, web servers, and so on. LPARs communicate as separate systems in the network.

platform management module, PMM

A *Platform Management Module (PMM)* is a web service which is responsible for providing connection and operational support for the corresponding environment. Supported environments are for example: VMware vSphere, Microsoft Hyper-V, IBM PowerVM, Solaris Zones, Cisco UCS, or Microsoft Cluster Service. A PMM manages connections with the servers of these environments, performs environment-related operations, retrieves data from the corresponding AIM, and populates the CA Virtual Assurance Management Database.

poll interval

The *poll interval* is the length of time between consecutive polls of a resource group.

POWER processors (LPAR)

POWER processors are RISC-based and used as the CPU in many of IBM servers, mini-computers, workstations, and supercomputers.

regular expressions

Regular expressions are text patterns used for matching. Regular expressions are strings that include a mix of plain text and special characters to indicate the kind of matching required.

VA--ADES AIM

Active Directory and Exchange Server AIM lets you monitor Active Directory and Exchange Server environments on both off-premise and on-premise infrastructure. This AIM enables configuration of AD and ES environments, and monitoring of the key performance indicators.

Virtual I/O Server, VIOS (LPAR)

A *Virtual I/O Server (VIOS)* is a special logical partition that is configured to own all physical I/O resources and provides its virtualization capabilities to other LPARs. LPARs access disk, network, and optical devices through the Virtual I/O Servers as virtual devices. Each PowerVM system with virtualized input output devices has one or more Virtual I/O Servers.

Index

A

Adjust the Permissions of the New Database User to the Required Minimum • 33
Agent and AIM Upgrades • 81
Agent Deployment • 36
Agent Upgrade from SystemEDGE 4.3.4 • 82
application insight module, AIM • 129
Apply Important Patches • 75
Apply Old Configurations Manually • 80
Audience • 9

B

Back up the Configuration and Data • 103
Back up the Databases • 103
Back up the Directories and Data • 104
Back up the Entire System • 75, 102
Backup and Restore • 101
Backup and Restore Overview • 101

C

CA Technologies Product References • 3
CA Virtual Assurance vCenter Management Recommendations • 116
Canceling the Installation • 22
Change the Owner of the aom2 and dpm Databases to sa • 32
Check for Updates • 34
Communication Ports • 27
Comparison between SystemEDGE and CA Systems Performance LiteAgent • 15
Component Installation after Initial Installation • 22
Configure and Use a Response File • 66
Contact CA Technologies • 4
Conventions • 10
Copy the Silent Installation Files from the Installation Media • 23
Create a Database User With the dbcreator Role • 31
Create a Deployment Job • 37

D

Database Considerations • 112
Departmental Data Center • 123
Dependencies of SystemEDGE Components • 39
Distribution Server Recommendations • 122
Domain Server Recommendations • 122
Download and Apply the Updates (PTFs) • 35
dynamic reconfiguration connector index, DRC-index (LPAR) • 129

E

Edit the silent.properties File • 24
Establish a Maintenance Window • 75

F

Functional Overview • 88

G

General Recommendation for vCenter AIM Monitoring • 115
Getting Started with User Interfaces • 87
Guidelines for an Installation on Multiple Servers • 25

H

Hardware Specifications • 112
How to Adjust SQL Server User Permissions to the Required Minimum • 30
How to Update CA Virtual Assurance • 34
How to Upgrade CA Virtual Assurance • 72
Hyper-V • 129

I

Import SystemEDGE Monitors into a Policy • 84
Individual Agent Installations • 39
Install AIMs • 67
Install and Configure SQL Server Express • 13
Install the Agent in Legacy Mode • 67
Install the Agent on UNIX and Linux Systems • 53
Install the Agent on UNIX from the Command Line • 59
Install the Agent on Windows • 42
Install the Agent on Windows from the Command Line • 47
Install the CA Systems Performance LiteAgent • 69
Install the Product Using the New Database User • 32
Installation of CA Virtual Assurance • 17
Installation on Multiple Servers • 25

Installation on UNIX and Linux Systems • 53
Installation on Windows Systems • 41
Installation Requirements and Considerations • 13
Installing CA Virtual Assurance • 13
internet Small Computer Systems Interface, iSCSI • 129
Introduction • 9

L

Large Environments • 126
Legacy Support of the $CASYSEDGE Variable • 65
Log in the User Interface and Manage Your Environments • 33
logical partition, LPAR • 129
LPAR AIM Monitoring Recommendations • 118

M

Multiple Data Centers • 124

N

Network Considerations • 113

O

Optimize Windows Memory Management • 15

P

Perform a Complete Uninstall • 94
Perform a Silent Manager Installation • 24
Performance Considerations during Initial Discovery • 118
platform management module, PMM • 129
poll interval • 129
POWER processors (LPAR) • 130
Prepare for the Installation • 17
Prepare the Environment You Want to Upgrade • 74

R

regular expressions • 130
Related Publications • 10
Remote Deployment and Policy Configuration Overview • 113
Remote Deployment and Policy Configuration Recommendations • 120
Restore the Configuration and Data • 107
Restore the Databases • 108
Restore the Directories and Data • 109
Restore the Entire System • 107
Revert Multiple Apache Configuration to Single Apache • 76
Review Old Configurations Not Upgraded Automatically • 80
Review Requirements • 31
Review Upgrade Documentation • 73
Review Upgrade Limitations • 77
Run Manager Installation • 78
Run the Installation • 19

S

Scalability Best Practices • 111
Scalability Limitation in Terms of Monitored Servers • 116
Scalability Limitations in Terms of Monitored Objects • 116
Scalability Overview • 111
Scalability Recommendation for LPAR AIM Monitoring • 119
Scalability Recommendation for Solaris Zones AIM Monitoring • 120
Scalability Recommendations • 115
Scalability Use Cases • 122
Scope • 9
Security Considerations • 15
Silent Manager Installation • 23
Solaris Zones AIM Monitoring Recommendations • 119
Start AutoShell • 89
Start CA Virtual Assurance • 87
Start the Bookshelf and Online Help • 91
Start the CA Virtual Assurance Command Prompt • 90
Stop Services • 77
Supported Upgrades • 71
SystemEDGE Installation on 64-bit Linux Releases Fails • 58
SystemEDGE Installation Through CA Virtual Assurance Manager Installer • 40

U

Uninstall SystemEDGE and the AIMs on UNIX Systems • 98
Uninstall SystemEDGE and the AIMs on Windows • 96
Uninstall the Manager from Command Prompt • 95
Uninstall the Manager in Silent Mode • 95
Uninstallation Options • 93

Uninstalling CA Virtual Assurance • 93
Uninstalling SystemEDGE • 96
Uninstalling the Manager • 93
Upgrade Managed Nodes and AIM Servers • 80
Upgrade Remote CA EEM Manually • 78
Upgrading CA Virtual Assurance • 71

V

VA--ADES AIM • 130
Valid AutoShell User • 90
vCenter AIM Monitoring Recommendations • 115
vCenter Management Limitations in Terms of Virtual Machines • 117
Verify Requirements for Using SQL Server • 14
Verify the CA Virtual Assurance Upgrade in Your Environment • 85
Virtual I/O Server, VIOS (LPAR) • 130