CA Virtual Assurance for Infrastructure Managers

Release Notes

Release 12.7.1

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

The CA Virtual Assurance Release Notes provide you details about new and enhanced features of this release, the prerequisites of the product installation, and integration with Third-party tools.

For the most recent CA Virtual Assurance Release Notes, see the bookshelf at CA Support Online.

For details about installing CA Virtual Assurance, see the *Installation Guide*. For a brief description of the entire documentation set, see chapter *Related Publications* in this guide.

Chapter 2: System Requirements

Your system must meet or exceed the requirements in this section for successful installation and operation of CA Virtual Assurance.

This product relies on TCP/IP, SNMP, Domain Name Service (DNS) and other networking technologies. If these technologies are not available, failing, slow, or have incorrect or out-of-date information, product functionality can be adversely affected.

This section contains the following topics:

Manager Requirements

This section provides details on the hardware and software requirements for a manager installation of CA Virtual Assurance Release 12.7.1.

Hardware Requirements

The following hardware is required to implement distributed and nondistributed CA Virtual Assurance component implementations.

- CPU: Intel Xeon 51xx 2.6 GHz or equivalent, or Intel Core 2 Duo 2.6 GHz or equivalent

  Note: The CPU requirements also apply to client desktops/workstations running the CA Virtual Assurance web browser-based UI.

- RAM:
  - 4 GB for deployments managing up to 1,000 systems
  - 8 GB on a 64-bit operating system for deployments managing up to 5,000 systems
  - 16 GB on a 64-bit operating system for deployments managing more than 5,000 systems
- Network Interface Controller (NIC): 100 Mbps or more
- Free disk space for main installation drive: 30 GB
- Free disk space for drive with databases: 30 GB

  Note: The disk space for the drive holding the databases is required wherever you have configured Microsoft SQL Server to store the databases for this product. The drive can be anywhere: on the same drive that is used for the product installation, on a different drive, or on a different system. If the drive is on the same drive as the product installation, the required free disk space is the sum of the two values. The product databases grow in size depending on the product usage, potentially consuming 30 GB or more, depending on the maintenance that is being done.

Important! To avoid unlimited growth of your transaction log, see the Microsoft KB Article 873235 for Microsoft SQL Server configuration instructions.

Important! To ensure continued optimal performance, see the Microsoft KB Article 189858 for information on detecting and resolving database fragmentation.

Important! If you install CA Virtual Assurance with other CA products, consider the combined impact and adjust the hardware specifications accordingly. For example, if you install CA Virtual Assurance (4-GB RAM) and CA Service Desk Manager (3-GB RAM) on one server, use a server with minimum 7-GB RAM. Review integration product Release Notes on the CA Support Online website: http://supportconnect.ca.com.

Note: The CPU requirements also apply to client desktops/workstations running the CA Virtual Assurance web browser-based UI.

Software Requirements

This section provides information about the software required to implement distributed and non-distributed components.

Manager on Windows

The CA Virtual Assurance manager supports and is certified for the following operating systems:

- Windows Server 2008 Standard, Enterprise, and Datacenter Edition (x86, x64), SP2 optional
- Windows Server 2008 R2 Standard, Enterprise, and Datacenter Edition (x86, x64), SP1 optional

CA Virtual Assurance supports the following Windows versions only for new SystemEDGE installations or for the CA Virtual Assurance manager upgrades from release 12.6 or 12.7:

- Windows Server 2003 SP2 and 2003 R2 SP2 Standard, Enterprise, and Datacenter Edition (x86, x64)

The compatibility matrix on the CA Support Online website provides the most current list of supported operating environments.

Note: For seamless time zone operation, verify that your distributed computing environment is synchronized to a common time source (for example, NTP server, GPS).

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

Database Requirements

CA Virtual Assurance uses Microsoft SQL Server as its database. Because CA Virtual Assurance integrates with other CA products, review the database requirements for integration products.

This release supports and is certified for the following versions:

- 2008 SP2 (32 bit, 64 bit), Standard and Enterprise Editions, SP3 optional
- 2008 R2 (32 bit, 64 bit), Standard and Enterprise Editions, SP1 optional
- 2008 R2 Express (32 bit, 64 bit), Database with Management Tools, and Database with Advanced Services Editions, SP1 optional
- 2012 (32 bit, 64 bit), Standard and Enterprise Editions
- 2012 Express (32 bit, 64 bit), Database with Management Tools, and Database with Advanced Services Editions

SQL Server Tools (OSQL.EXE) are required on the manager system to connect to a local or remote SQL Server database.

Important! If you are upgrading an existing 12.6 or 12.7 installation that uses SQL Server 2005: first upgrade the SQL Server to a supported version, verify that the 12.6 or 12.7 product is still operational, then upgrade to CA Virtual Assurance Release 12.7.1.

Note the following considerations:

- For your convenience, SQL Server 2008 R2 Express Edition (32 bit) is available on the CA Virtual Assurance installation media at the following location: DVD1\Installers\Windows\External\MSSQLExpress\setup.exe.
- Named instances and SQL Server clusters are supported. Enable TCP/IP and use static port assignments for each instance. Dynamic ports are not supported.
- The system that is installed with the manager components must also have the SQL client (server tools) installed.
- After the installation of SQL Server Tools, check to see that OSQL.EXE is properly installed to this location (if using the default install path):
  - MS SQL 2008: C:\Program Files\Microsoft SQL Server\100\Tools\Binn

Important! To ensure continued optimal performance, see the Microsoft KB Article 189858 for information on detecting and resolving database fragmentation.

Remote Databases

If you are using a remote database, the local system must have an appropriate matching version of the SQL Server Native Client.

Examples

- A remote 2008 SP2, R2, or R2 Express database requires a local 2008 SP2 or 2008 R2 Native Client, either is acceptable. A remote 2012 database requires a local 2012 Native Client.

The SQL Server Native Client is available from the Microsoft Download Center by searching, “Feature Pack for Microsoft SQL Server.” Based on your *remote* database and operating environment, complete these steps:

1. Select the most recent appropriate version.
2. Download and install the appropriate module for your operating environment on your *local* system.

   Example: ENU\<*x86 or x64*>\sqlncli.msi

Browser Requirements

CA Virtual Assurance supports the following browsers for the user interfaces. These web browsers are supported for the duration of their lifecycles (as determined by the manufacturer), or until CA Technologies ends support.

- Microsoft Internet Explorer 8.0, 9.0

  Note: If you get the message, “A script on this page is causing Internet Explorer to run slowly," review Microsoft KB Article 175500.

- Mozilla Firefox 16.0, including all minor versions

CA Virtual Assurance requires a supported browser with the Adobe Flash Player plug-in to display diagrams and charts. The following versions are supported:

- Adobe Flash Player versions 10.0, 11.1, 11.4

  Note: CA Virtual Assurance supports the major versions of the Adobe Flash Player. The minor versions can also work, but they are not certified.

Additional CA Software

CA Virtual Assurance requires the following software shipped with the installation media:

CA Embedded Entitlements Manager (CA EEM)

CA Virtual Assurance distributes, supports, and is certified to work with CA EEM version 8.4 SP4 CR14 (8.4.414).

CA Virtual Assurance also supports:

- All “CA EEM 8.4” subversions – from CA EEM 8.4 SP4 (8.4.244), up to and including the version we distribute, up to and including new “CA EEM 8.4” SP.
- CR subversions that ship after the release of this product.

If an insufficient version of CA EEM is detected during installation, the installation program displays the minimum and you can upgrade to a supported version.

To request support, or to certify this product with other versions of CA EEM, contact your CA representative.

Note: If your site has multiple instances of CA Server Automation or CA Virtual Assurance, the CA EEM server cannot be shared.

Note: If this product installs CA EEM, the "Use Transport Layer Security” option is not enabled by default. For additional security, log in to the CA EEM interface and select the TLS option on the Configuration tab.

CA Network Discovery Gateway

This software is required for system and network discovery.

SystemEDGE

Release 5.x.y corresponds to CA Virtual Assurance release 12.x.y.
Example: SystemEDGE 5.7.1 for CA Virtual Assurance 12.7.1

Note: If latest version of SystemEDGE is not already on your system, the installation program installs it. SystemEDGE is required for the CA Virtual Assurance AIMs. AIMs are functional extensions to the SystemEDGE agent.

SystemEDGE Releases 4.3.4, 4.3.5, 4.3.6, 5.1.0, 5.6.0, and 5.7.0 are supported for managing remote servers in your environment.

Optional CA Software for CA Virtual Assurance

You can install the following optional CA software and configure CA Virtual Assurance accordingly to enable specific integration functionality:

CA Service Desk Manager

Version 12.5 or higher is required to open help desk tickets.

Internationalization (i18n)

CA Virtual Assurance is an internationalized product (i18n) that uses UTF-8 character encoding to display language-specific characters. For example, the German ü (umlaut), the French è (grave accent), or Japanese characters in input and output data are displayed.

The UTF-8-encoded character support includes, but is not limited to, the following areas:

- Textual descriptions of objects or resources
- Messages
- User names and passwords to connect to manageable resources
- Regular expressions (SystemEDGE)

The installation of this product is supported on English, French, German, and Japanese versions of the supported operating systems. Also, for Windows, you can use a supported version of SQL Server that is either English, or the appropriate localized version for that operating system.

Important! If you edit a product file that uses UTF-8 encoding, be sure to save it with UTF-8 encoding. Operating systems that are not English and have multibyte characters must be saved with UTF-8 encoding. Windows Notepad can save with UTF-8 encoding.

General Limitations

Because CA Virtual Assurance integrates with other CA products, review the international support statements for integration products.

CA Virtual Assurance supports only host or cluster names with the characters 'a - z', 'A - Z', '0 - 9' and '-'. A host or cluster name cannot start with a hyphen ('-') or be all numeric. The NetBIOS name of a Windows system must match its DNS host name.

CA Virtual Assurance supports only ASCII characters in:

- SQL Server host names (subject to host name limitations), instance names, user names, and passwords
- CA EEM/Security host names (subject to host name limitations), user names, and passwords
- All CA SystemEDGE parameters with the exception of policy names
- SystemEDGE Privilege Separation User (UNIX and Linux only)
- SNMP read, read/write, and trap community strings
- %TEMP% environment variable
- Installation target paths of all CA Virtual Assurance components

Customize Console Display

If you want to display console data that contains language-specific characters, verify the following prerequisites for CLI commands and the NodeCfgUtil utility:

- Verify that the appropriate language support is available on your operating system.
- Enable the Lucida Console font in the Windows Command Prompt for running commands or NodeCfgUtil utility.
- Enable UTF-8 character encoding in the UNIX or Linux console that you want to use to run your commands. Enter the following command in the terminal console to display the current language setting:

  ```
  echo $LANG
  ```

  If UTF-8 is not enabled, enter, for example, the following command in a console window (use the appropriate character encoding: en_US.UTF-8, ja_JP.UTF-8, fr_BE.UTF-8, de_DE.UTF-8, and so on):

  ```
  LANG=en_US.UTF-8; export LANG
  ```

AutoShell and CA Virtual Assurance CLI Commands

AutoShell and CA Virtual Assurance CLI commands support the -locale switch that allows you to specify a locale based on an IS0 639_3166 combination (for example: fr_FR for French). See the *Invoking AutoShell* section and *CLI Commands* in the *Reference Guide*.

Solaris Zones Uptime

The Solaris Zone Uptime MIB attribute (zoneAimStatZoneUpTime) is specified as DisplayString that supports ASCII characters only. The corresponding fields in the user interface do not display UTF-8 characters.

Default Package Wrapper Name

The default package wrapper name is not localized and reads 'default' in all supported languages. Custom package wrapper names support UTF-8 characters.

Service Response Monitoring AIM Configuration File

When you modify the svcrsp.cf configuration file to add language-specific characters, verify that the text editor you use supports UTF-8 as a storage format. If your text editor inserts a UTF-8 Byte Order Mark when saving the file, SystemEDGE ignores the Byte Order Mark when reading the configuration file.

SRM CLI Commands

The svcwatch CLI supports localized output and console-help information.

If you use the optional –L switch, the utility detects the current locale of the console and language catalog if available. If a language catalog is not found, the utility falls back to English as a default language.

Cisco UCS Limitations

The Cisco Unified Computing System (Cisco UCS) only supports English language characters. Because the UCS Manager treats non-English characters as invalid, CA Virtual Assurance disallows unsupported characters in UCS fields for service profile, pools, and so on.

Business Objects Reports

Business Object reports require Microsoft SQL Server, English, or Japanese versions; no other languages are supported.

Installation Limitations

You can specify the language for a silent installation by using the parameter, –L *locale* (for example, Install.exe –L fr). The following locales are supported: en (English), ja (Japanese), de (German), and fr (French). If you do not specify a locale, the installer chooses the best fit (system locale or English (en)).

The DVD install path that you specify cannot contain Chinese characters, unless it is a Chinese system. If you specify Chinese characters on a non-Chinese system, the installer fails with the following message:

```
Unable to extract the compressed file. Please get another copy of the installer and try again.
```

CA Virtual Assurance AIM Server and Managed Node Requirements

This section provides details on the hardware requirements and operating systems supported by an AIM Server or a Managed Node.

Hardware Requirements for Managed Nodes and AIM Servers

The hardware requirements for SystemEDGE and AIMs are as follows:

Minimum

CPU: Same as OS vendor

RAM: Same as OS vendor

Free disk space: 50 MB (Managed Node, SystemEDGE only *)
Free disk space: 250 MB (AIM Server with all CA Virtual Assurance AIMs installed)

Network Interface Controller (NIC): 100 Mbps

Recommended

CPU: Same as OS vendor

RAM: Same as OS vendor

Free disk space: 150 MB or more (Managed Node, SystemEDGE only **)
Free disk space: 500 MB (AIM Server with all CA Virtual Assurance AIMs installed)

Network Interface Controller (NIC): 100 Mbps or more

(*) The disk space requirement varies for UNIX and Windows platforms. For Windows installations, MSI installer requires the disk space to install SystemEDGE.

(**) Disk space requirements for runtime files increase when diagnostic traces are enabled. By default, the size of diagnostic trace is limited to 10 MB.

SystemEDGE Operating System Support

A system running SystemEDGE Release 5.7.1 requires one of the following operating systems:

Windows

- Windows Server 2003 SP2 Standard, Enterprise, Data Center, and Small Business Server Edition (32 bit, x86)
- Windows Server 2003 R2 SP2 Standard, Enterprise, and Data Center Edition (32 bit, x86)
- Windows Server 2003 SP2 Standard, Enterprise, Data Center (64 bit, x64)
- Windows Server 2003 R2 SP2 Standard, Enterprise, and Data Center Edition (64 bit, x64)
- Windows Server 2003 SP2 x64 Edition (64 bit)
- Windows Server 2008 Standard, Enterprise and Data Center Edition (32 bit, x86)
- Windows Server 2008 Standard, Enterprise and Data Center Edition (64 bit, x64)

- Windows Server 2008 R2 Standard, Enterprise and Data Center Edition (64 bit, x64)
- Windows XP Professional SP3 (32 bit, x86)
- Windows Vista SP1 Business, Enterprise, and Ultimate Edition (32 bit, x86)
- Windows Vista SP1 Business, Enterprise, and Ultimate Edition (64 bit, x64)
- Windows 7 Professional, Ultimate Edition (32 bit, x86)
- Windows 7 Professional, Ultimate Edition (64 bit, x64)

HP

- HP-UX 11.11 PA-RISC (64 bit)
- HP-UX 11.23 PA-RISC (64 bit)
- HP-UX 11.23 ia64 (64 bit)
- HP-UX 11.31 PA-RISC (64 bit)
- HP-UX 11.31 ia64 (64 bit)

IBM AIX

- IBM AIX Version 6.1 (64 bit)
- IBM AIX Version 7.1 (64 bit)

Linux

- Red Hat Linux Web Server, Advanced Server, and Enterprise Server 5.0 (32 bit, x86)
- Red Hat Linux Web Server, Advanced Server, and Enterprise Server 5.0 (64 bit, x64)
- Red Hat Enterprise Linux 6.0 (32 bit, x86)
- Red Hat Enterprise Linux 6.0 (64 bit, x64)
- SUSE Linux Enterprise Server 10.0 (32 bit, x86)
- SUSE Linux Enterprise Server 10.0 (64 bit, x64)
- SUSE Linux Enterprise Server 10.0 (64 bit, ia_64)
- SUSE Linux Enterprise Server 11 (32 bit, x86)
- SUSE Linux Enterprise Server 11 (64 bit, x64)
- Debian Linux Version 5.0 (Lenny) (32 bit, x86)
- Debian Linux Version 5.0 (Lenny) (64 bit, x64) - Legacy Mode Only
- Debian Linux Version 5.0 (Lenny) (64 bit, ia_64) - Legacy Mode Only

zLinux

- SUSE Linux Enterprise Server 10 (zSeries) - Legacy Mode Only
- SUSE Linux Enterprise Server 11 (zSeries) - Legacy Mode Only
- Red Hat Enterprise Server 5.0 (zSeries) - Legacy Mode Only

Linux on pSeries

- Red Hat Enterprise Server 5.0
- Red Hat Enterprise Server 6.0

Solaris

Note: SystemEDGE supports all Solaris Zone configurations for the Solaris 10 operating system.

- Solaris UltraSPARC 9 (64 bit)
- Solaris UltraSPARC 10 (64 bit)
- Solaris 9 (32 bit, x86)
- Solaris 10 (32 bit, x86)
- Solaris 10 (64 bit, x64)

Note: CA Virtual Assurance-specific features such as deployment and configuration is not supported on all platforms.

CA Virtual Assurance AIM Operating System Support

The SystemEDGE AIMs and Advanced Encryption shipped with CA Virtual Assurance run on the following operating systems:

Windows: Advanced Encryption

- Windows XP Professional SP3 (32 bit, x86)
- Windows Vista SP1 Business, Enterprise, and Ultimate Edition (32 bit, x86)
- Windows Vista SP1 Business, Enterprise, and Ultimate Edition (64 bit, x64)
- Windows 7 Professional, Ultimate Edition (32 bit, x86)
- Windows 7 Professional, Ultimate Edition (64 bit, x64)

- Windows Server 2003 SP2 Standard, Enterprise, Data Center, and Small Business Server Edition (32 bit, x86)
- Windows Server 2003 R2 SP2 Standard, Enterprise, and Data Center Edition (32 bit, x86)
- Windows Server 2003 R2 SP2 Standard, Enterprise, and Data Center Edition (64 bit, x64)
- Windows Server 2003 SP2 x64 Edition (64 bit)
- Windows Server 2008 Standard, Enterprise and Data Center Edition (32 bit, x86)
- Windows Server 2008 Standard, Enterprise and Data Center Edition (64 bit, x64)
- Windows Server 2008 R2 Standard, Enterprise and Data Center Edition (64 bit, x64)

Windows: Service Response Monitoring AIM

- Windows Server 2003 SP2 Standard, Enterprise, Data Center, and Small Business Server Edition (32 bit, x86)
- Windows Server 2003 SP2 x64 Edition (64 bit)
- Windows Server 2003 R2 SP2 Standard, Enterprise, and Data Center Edition (32 bit, x86)
- Windows Server 2003 R2 SP2 Standard, Enterprise, and Data Center Edition (64 bit, x64)
- Windows Server 2008 Standard, Enterprise and Data Center Edition (32 bit, x86)
- Windows Server 2008 Standard, Enterprise and Data Center Edition (64 bit, x64)
- Windows Server 2008 R2 Standard, Enterprise and Data Center Edition (64 bit, x64)

Windows: LPAR AIM, UCS AIM, VC AIM, Zones AIM, XenServer AIM, Response Monitoring AIM

- Windows Server 2008 Standard, Enterprise and Data Center Edition (32 bit, x86)
- Windows Server 2008 Standard, Enterprise and Data Center Edition (64 bit, x64)
- Windows Server 2008 R2 Standard, Enterprise and Data Center Edition (64 bit, x64)

Windows: Hyper-V AIM

- Windows Server 2008 R2 Standard, Enterprise and Data Center Edition (64 bit, x64)

HP: Advanced Encryption, Service Response Monitoring AIM

- HP-UX 11.11 PA-RISC (64 bit)
- HP-UX 11.23 PA-RISC (64 bit)
- HP-UX 11.23 ia64 (64 bit)
- HP-UX 11.31 PA-RISC (64 bit)
- HP-UX 11.31 ia64 (64 bit)

IBM AIX: Advanced Encryption, Service Response Monitoring AIM

- IBM AIX Version 6.1 (64 bit)
- IBM AIX Version 7.1 (64 bit)

Note: JRE is shipped with the SRM AIM for AIX.

Linux: Advanced Encryption, Service Response Monitoring AIM

- Red Hat Linux Web Server, Advanced Server, and Enterprise Server 5.0 (32 bit, x86)
- Red Hat Linux Web Server, Advanced Server, and Enterprise Server 5.0 (64 bit, x64)
- Red Hat Enterprise Linux 6.0 (32 bit, x86)
- Red Hat Enterprise Linux 6.0 (64 bit, x64)
- SUSE Linux Enterprise Server 10.0 (32 bit, x86)
- SUSE Linux Enterprise Server 10.0 (64 bit, x64)
- SUSE Linux Enterprise Server 10.0 (64 bit, ia_64)
- SUSE Linux Enterprise Server 11 (32 bit, x86)
- SUSE Linux Enterprise Server 11 (64 bit, x64)
- Debian Linux Version 5.0 (Lenny) (32 bit, x86)
- Debian Linux Version 5.0 (Lenny) (64 bit, x64) - Legacy Mode Only
- Debian Linux Version 5.0 (Lenny) (64 bit, ia_64) - Legacy Mode Only

  Note: Service Response Monitoring AIM does not support Debian Linux 5.0 (64 bit, ia_64).

Solaris: Advanced Encryption, Service Response Monitoring AIM

Note: SystemEDGE supports all Solaris Zone configurations for the Solaris 10 operating system.

- Solaris UltraSPARC 9 (64 bit)
- Solaris UltraSPARC 10 (64 bit)

- Solaris 9 (32 bit, x86)
- Solaris 10 (32 bit, x86)
- Solaris 10 (64 bit, x64)

zLinux: Advanced Encryption

- SUSE Linux Enterprise Server 10 (zSeries) - Legacy Mode Only
- SUSE Linux Enterprise Server 11 (zSeries) - Legacy Mode Only
- Red Hat Enterprise Server 5.0 (zSeries) - Legacy Mode Only

Linux on pSeries: Advanced Encryption

- Red Hat Enterprise Server 5.0
- Red Hat Enterprise Server 6.0

CA Systems Performance LiteAgent Operating System Support

A computer running CA Systems Performance LiteAgent requires one of the following operating systems:

Windows

Note: The following Windows 2003 operating systems are supported only when upgrading from CA Virtual Assurance 12.6.

- Windows Server 2008 (32 bit, x86)
- Windows Server 2008 (64 bit, x64)
- Windows Server 2008 R2 (64 bit, x64)
- Windows Server 2003 Standard, Enterprise, Data Center, and Small Business Server Edition (32 bit, x86)
- Windows Server 2003 (64 bit, x64)
- Windows Server 2003 R2 Standard, Enterprise, and Data Center Edition (32 bit, x86)
- Windows Server 2003 R2 (64 bit, x64)
- Windows XP Professional SP3+ (32 bit, x86)
- Windows XP Professional SP2+ (64 bit, x64)
- Windows Vista Business, Enterprise, Ultimate (32 bit, x86)
- Windows Vista Business, Enterprise, Ultimate (64 bit, x64)

Linux

- Red Hat Linux Enterprise Server 5.0 (32 bit, x86)
- Red Hat Linux Enterprise Server 5.0 (64 bit, x64)
- SUSE Linux Enterprise Server 10.0 (32 bit, x86)
- SUSE Linux Enterprise Server 10.0 (64 bit, x64)

Solaris

Note: CA Virtual Assurance-specific features such as deployment and configuration is not supported on all platforms.

- Solaris UltraSPARC 9 (32 bit)
- Solaris UltraSPARC 9 (64 bit)
- Solaris UltraSPARC 10 (64 bit)
- Solaris 10 (32 bit, x86)
- Solaris 10 (64 bit, x64)

HP

- HP-UX 11.23 PA-RISC (64 bit)
- HP-UX 11.23 IA64 (64 bit)
- HP-UX 11.31 PA-RISC (64 bit)
- HP-UX 11.31 IA64 (64 bit)

Note: For HP-UX 11, we recommend PHNE 27063 s700 800 11 cumulative ARPA Transport patch or later. This patch fixes memory issues with HP-UX libraries.

IBM AIX

- IBM AIX Version 5.3 (32 bit, 64 bit)
- IBM AIX Version 6.1 (64 bit)
- IBM AIX Version 7.1 (64 bit)
- IBM AIX Version 7 (64 bit)

Supported Integration Platforms

CA Virtual Assurance integrates with virtual and physical platforms in your environment. To manage these platforms, install and configure the appropriate SystemEDGE AIMs on the CA Virtual Assurance manager server or on separate AIM servers.

Note: For Microsoft Hyper-V, install SystemEDGE and the Microsoft Hyper-V AIM on each physical Microsoft Hyper-V Server that you want to manage.

Supported Platforms

Active Directory and Exchange Server

To enable monitoring for Active Directory and Exchange Server, verify that you have the following product installed in your environment:

- .Net 3.5 or higher versions
- Power shell v2.0
- Exchange Management Tools SP3 on the AIM host to monitor Exchange Server 2007.

Note: Exchange Management Tools SP3 is not required for monitoring Exchange Server 2010.

Cisco Unified Computing System (UCS)

To enable management for Cisco UCS, verify that you have the following product installed in your environment:

- Cisco UCS 1.3, 1.4, and 2.0

Citrix XenServer

To enable virtual management for Citrix XenServer, verify that you have the following component installed in your environment:

- Citrix XenServer version 6.0

Huawei GalaX

To enable monitoring and management for Huawei GalaX, verify that you have the following component installed in your environment:

- Huawei GalaX8800 version 1.0

IBM HACMP for AIX

To enable monitoring for IBM HACMP for AIX, verify that you have the following component installed in your environment:

IBM HACMP 6.1

IBM HACMP for AIX version 6.1 platforms let you monitor clusters, nodes, and network interfaces status.

IBM Power VM (Logical Partitions, LPAR)

To enable virtual management for IBM LPAR, verify that you have the following components installed in your environment:

IBM AIX LPAR

IBM LPAR POWER5, POWER6, or POWER7 platforms let you manage logical partitions on AIX and their managed systems.

IBM Hardware Management Console (HMC)

To manage logical partitions of IBM POWER5, POWER6, or POWER7 platforms, install HMC V7R3.5, V7R7.1, V7R7.2.

Note: HMC V7R7.1 is the minimum level for POWER7 support.

IBM Integrated Virtualization Manager (IVM)

Alternative to HMC for managing logical partitions. Runs on the Virtual I/O Server (VIOS).

IBM Virtual I/O Server (VIOS)

IBM Virtual I/O Server (VIOS) lets you configure IBM AIX POWER5, POWER6, and POWER7 logical partitions.

Note: VIOS versions 1.5, 2.1, and 2.2 are supported.

Microsoft Cluster (MSCS)

To enable management for Microsoft Clusters, verify that you have the following component installed in your environment:

- Microsoft Clusters based on Windows Server 2003 and Windows Server 2008

Microsoft Hyper-V Server

To enable virtual management for Microsoft Hyper-V Server, verify that you have at least one of the following products installed in your environment:

- Hyper-V Server 2008 R2 (64 bit, x64)

Note: Reservation Manager supports Hyper-V provisioning of Windows Server 2003 and Windows Server 2008 operating systems.

Oracle Solaris Zones

To enable virtual management for Oracle Solaris Zones server, verify that you have the following component installed in your environment:

- Solaris 10 with zones compatibility to manage Solaris Zones.

Red Hat Enterprise Virtualization

To enable virtual management for Red Hat Enterprise Virtualization, verify that you have the following component installed in your environment:

- RHEV 3.0

VMware vCenter Server

To enable virtual management for VMware vCenter Server, verify that you have one of the following components installed in your environment:

VMware ESX Server/VMware ESXi Server

Version 4.0, 4.1, 5.0, or 5.1 is required to create VM sessions.

Note: ESX and ESXi Server support require that a vCenter Server is configured to manage the ESX or ESXi servers.

VMware vCenter Server

VMware vCenter Server version 4.0, 4.1, 5.0, or 5.1 is required to clone and migrate virtual machines and to manage the VMware vSphere environment.

Note: VMware Tools optimize the virtualization of VMs and it is strongly recommended that they are installed on each VM in your VMware environment. Some features of this product will not be available or may not function correctly for VMs that do not have VMware Tools installed. For this reason, VMs that do not have VMware tools installed are not supported.

VMware vCloud

To enable virtual management for VMware vCloud, verify that you have the following component installed in your environment:

- VMware vCloud Director version 1.5 and 5.1

Chapter 3: New Features and Enhancements

This section contains the following topics:

Huawei GalaX

In this release, the following new features or changes are available:

Huawei GalaX Monitoring

CA Virtual Assurance monitors Huawei GalaX environments.

Huawei GalaX Management

CA Virtual Assurance manages Huawei GalaX environments.

Multi-instances

The SystemEDGE GalaX AIM can manage multiple Huawei GalaX environments.

Remote Deployment

In this release, CA Virtual Assurance supports the following feature:

Support for Deploying AIMs

Provides a default package wrapper that allows deployment of the Huawei GalaX AIM.

User Interface

In this release, the following new features or changes are available:

Localized User Interface

The user interface is available in English and Japanese.

Product Banner

The top section of the user interface contains the following changes:

- Search can be used to find service templates and applications.
- The Help drop-down list provides a link to CA Support channels, which replaces the Get Satisfaction link.

Documentation

In this release, the documentation includes an End-to-End bookshelf with links to scenarios and auxiliary information, such as product details, support materials, and education.

You can open the bookshelf directly from the Start menu or click Back to Bookshelf in the navigation pane of the Online Help or Local Help.

The following scenarios and use cases have been added to the documentation and can be accessed directly from the bookshelf:

- How to Configure Huawei GalaX Management Components
- How to Create Virtual Private Clouds
- How to Manage Huawei SingleCLOUD Environments
- How to Adjust SQL Server User Permissions to the Minimum Necessary

Chapter 4: New Features and Enhancements of the Previous Release 12.7

This section contains the following topics:

Active Directory and Exchange Server AIM

This release provides:

Active Directory and Exchange Server 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 release supports the following:

- Microsoft Exchange Server 2007
- Microsoft Exchange Server 2010
- Microsoft Active Directory 2008

Supported Operating Systems

- Windows Server 2008 Standard, Enterprise and Data Center Edition
- Windows Server 2008 R2 Standard, Enterprise and Data Center Edition

Note: This release of Active Directory and Exchange Server AIM does not support internationalization.

Citrix XenServer

In this release, the following new features or changes are available:

Citrix XenServer Management and Monitoring

CA Virtual Assurance monitors and manages Citrix XenServer 6.0 environments.

Multi-instances

The XenServer AIM can manage multiple XenServers.

Customized XenServer Provisioning

CA Virtual Assurance supports customized provisioning of new virtual machines (VM) running Windows 2003 R2 Server (32 bit and 64 bit), Windows 2008 (32 bit and 64 bit) or Windows 2008 R2 Server (64 bit). Customization options include a number of settings. For example, changing the built-in Administrator account password, computer name, and the network configuration.

Documentation

In this release, the documentation includes an End-to-End bookshelf with links to scenarios and auxiliary information, such as product details, support materials, and education.

You can open the bookshelf directly from the Start menu or click Back to Bookshelf in the navigation pane of the Online Help or Local Help.

The following scenarios and use cases are available in the documentation and can be accessed directly from the bookshelf:

- How to Apply Policy and Layered Templates to Servers
- How to Backup Manager Servers
- How to Change the Configuration Mode for SystemEDGE (Managed Mode, Unmanaged Mode)
- How to Change SystemEDGE from Unmanaged Mode to Managed Mode
- How to Configure an Active Directory and Exchange Server AIM
- How to Configure Management Components for each Supported Virtual Environment (vCenter, vCloud, PowerVM, Cisco UCS, Hyper-V, Red Hat Enterprise Virtualization, Solaris Zones, XenServer)
- How to Configure Microsoft Cluster Service Management
- How to Configure SNMPv1/v2 Settings and Access Control Lists
- How to Configure SNMPv3

- How to Configure the Active Directory and Exchange Server AIM
- How to Create and Apply Autowatchers to Monitor Resources Dynamically
- How to Integrate with eHealth
- How to Integrate with CA Spectrum IM
- How to Prepare Windows Templates for KVM Provisioning
- How to Prepare Windows Templates for XenServer Provisioning
- How to Manage Server-level SNMP Settings
- How to Update CA Virtual Assurance
- How to Upgrade CA Virtual Assurance
- How to Use Policy Actions to Identify Performance Issues
- Scalability Best Practices
- User Permissions and Access Requirements Best Practices

IBM HACMP

In this release, the following new features or changes are available:

HACMP monitoring

HACMP AIM provides performance metrics for HACMP monitoring.

IBM LPAR

In this release, the following new features or changes are available:

Unified Administration Panel

The IBM PowerVM configuration has been unified with other platforms like VC or Zones. All Power servers that are managed by the HMC that is configured are managed automatically. CA Virtual Assurance discovers new Power servers that are added later to the HMC are automatically.

Multiple Shared Processor Pools

Enables creation of multiple processor pools for flexible allocation of resources. The Processor Pools Pane was added to the Summary tab for a selected Managed Power System.

Dual HMC

CA Virtual Assurance supports dual HMC. A *dual HMC* is a redundant Hardware Management Console (HMC) management system that provides high availability. When two HMCs manage one system, they are peers. Each HMC can be used to control the managed system. One HMC can manage multiple managed systems, and each managed system can have two HMCs.

Preferred AIM

The HMC/IVM Server Configuration in the Administration tab of the user interface has been enhanced to specify preferred AIM.

Management Status

The HMC/IVM Server Configuration allows enabling or disabling management of the HMC/IVM server.

Virtual I/O Server (VIOS) Default Credentials

The VIOS default credentials apply to VIOS that are discovered for a particular HMC server.

Multiple Virtual I/O Servers

CA Virtual Assurance supports multiple Virtual I/O servers (VIOS). *Multiple Virtual I/O servers* offer capability that increase application availability by enabling Virtual I/O server maintenance without a downtime for the client partitions. CA Virtual Assurance discovers all VIOS attached to a Power server and allows configuring VIOS access credentials.

Deferred Load of Unconfigured Components

This functionality provides a warning status  (*Not configured)* for registered components that are not configured.

Fibre Channel Support

The CA Virtual Assurance provides important information about the status of Fibre Channel virtualization and availability of worldwide port names (WWPN). *Fibre Channel* is a standardized gigabit-speed technology for transmitting data between computer devices. Fibre Channel is especially suited for connecting computer servers to shared storage devices and for interconnecting storage controllers and drives.

Oracle Solaris Zones

In this release, the following new feature or features are available:

Whole Root Zone Provisioning

Lets users specify the 'whole root Zone' type when creating a Zone. A whole root zone is a self-contained zone that does not inherit packages and is independent of the Global Zone OS.

Policy Configuration

In this release, the following new features or changes are available:

Enhanced Search Results of a Machine

Provides policy configuration information in search results of the CA Virtual Assurance user interface.

Multiple Monitor Deletion

Enables you to delete multiple monitors from a policy or a template in a single action to facilitate easy configuration monitoring.

ACL Association with Global SNMP Objects

Supports Access Control Lists in global SNMP objects to be applied to systems through policies.

Server-specific SNMP Settings

Supports Access Control Lists and SNMP settings at the server level. You can decide whether to apply these settings to systems through policies.

Autowatchers

Supports dynamic resource monitoring through generic, service, and process autowatchers.

Discover Agent

Allows Policy Configuration to detect an agent that is not yet registered with Policy Configuration, using all available names and addresses.

Reindex Monitors and Autowatchers

Allows the index of monitors and autowatchers to be reassigned in a single operation.

Import and Export of Policies or Templates

Allows Policies and templates to be exported from a CA Virtual Assurance instance, and imported into another CA Virtual Assurance instance.

Change Manager Support

Allows an existing manager to reconfigure remote SystemEDGE agents, so that they register with a different manager.

In this release, CA Virtual Assurance provides the following Policy Configuration reports:

Agent List by Distribution Server Report

Shows SystemEDGE agents managed by each of the distribution servers and indicates whether the configuration is up-to-date.

Agent List by Policy Report

Shows SystemEDGE agents managed by policy and indicates whether the configuration is up-to-date.

Configuration Exceptions by System Report

Shows the report of Systems, where the configuration has been modified through SNMP, since a policy or a template was last applied.

Managed Agent List Report

Lists the SystemEDGE agents in managed mode.

Out-of-Date Configurations by Policy/Template Report

Shows the out-of-date policies and templates currently on agents by each Policy and Template.

Out-of-Date Configurations by System Report

Shows the out-of-date policies and templates currently on agents by each Machine.

Policy and Policy Template Details Report

Shows the report of a selected Policy or Template.

System Configuration Details Report

Shows the report of the configuration that was applied to a selected System.

Systems not Configured Report

Shows the systems which are not registered in Policy Configuration.

Red Hat Enterprise Virtualization

In this release, the following new features or changes are available:

Red Hat Enterprise Virtualization monitoring

CA Virtual Assurance monitors RHEV 3.0 environments.

Customized RHEV Provisioning

CA Virtual Assurance supports customized provisioning of new virtual machines (VM) running Windows 2003 R2 Server (32 bit and 64 bit), Windows 2008 (32 bit and 64 bit) or Windows 2008 R2 Server (64 bit). Customization options include a number of settings. For example, changing the built-in Administrator account password, computer name, and the network configuration.

Remote Deployment

In this release, CA Virtual Assurance supports the following features:

New Platform Support

SystemEDGE support for RedHat Linux on IBM Power PC using Remote Deployment.

Deployment Reports

Provides a new report to get Deployment Job Status for a given distribution server over a timespan. Report Component Selection and Jobs Selection provide various report generation options.

Deployment to Managed Nodes through Context Menu

Lets you open the remote deployment job wizard. The job wizard deploys only to the selected node as the target.

Updates to Jobs Panel

Provides paging, filtering, sorting and other customizing support for the job detail.

Support for Deploying the AIMs

Provides a default package wrapper that allows deployment of the following AIMs:

- High Availability Cluster Multiprocessing (HACMP) AIM
- Citrix Xen Server (XEN) AIM
- VMware vCloud (VCLOUD) AIM
- Active Directory and Exchange Server (ADES) AIM
- Red Hat Enterprise Virtualization (KVM) AIM

Common Job Tracking Portlet

Provides enhanced job tracking of Remote Deployment jobs.

Enhanced Search Results

Provides swift access to Remote Deployment operations under search results.

Updates to Deployment Job Wizard

Removal of EULA in the Job wizard

Updates to SystemEDGE Package Wrapper

Updates to validate SNMP community strings in wrappers

Update Utilities

In this release, the following new features or changes are available:

CA Virtual Assurance Update

From the Start menu, you can run the CA Virtual Assurance Update utility to select and download available PTFs (program temporary fixes) for CA Virtual Assurance. You can install the patches through dpminstapplyptfs.exe which is located in the product bin directory.

User Interface

In this release, the following new features or changes are available:

Product Banner

The top section of the user interface contains the following new controls:

- Self-Service Portal link accesses the Liferay-based portal interface.
- Management/Dashboard link toggles between the Dashboard and operational pages.
- Help drop-down menu provides:
  - Online Help (latest documentation at support.ca.com)
  - Local Help (for systems without Web access)
  - CA Support (support.ca.com - requires registered login)
  - Get Satisfaction (online feedback discussion)
  - About (product information)

Dashboard

The Dashboard is larger and more streamlined in this release and provides:

- First Step Dashboard for operational choices in an interview format.
- Service Dashboard for access to service provisioning functions.
- Estimated Savings Dashboard for savings calculations based on operational environment.
- Jobs/Events/Alarms console with grouping and root cause correlation.

At lower right corner, a Configure menu accesses:

- Dashboard (Properties and Library for dashboards and portlets)
- User Preference... (Refresh and Events settings)

Management

Added features:

- Jobs table in bottom panel
- Drag and drop: servers to services and service profiles to UCS blades

VMware vCloud

In this release, the following new features or changes are available:

VMware vCloud management and monitoring

CA Virtual Assurance monitors and manages VMware vCloud Director 1.0, 1.0.1, or 1.5 environments.

Multi-instances

The vCloud AIM can manage multiple VMware vCloud Director servers.

Chapter 5: Patches and Published Fixes

Patches and published fixes may be available for this version of the product. Go to the CA Support Online website http://supportconnect.ca.com to download patches or view published fixes before proceeding with the product installation or upgrade. Patches and published fixes are available from the Download Center, Published Solutions pane.

This section contains the following topics:

SNMPv3 Trap Forwarding Issue (see page 41)

SNMPv3 Trap Forwarding Issue

The CA NSM Event Manager must be configured in a specific manner to successfully receive CA Virtual Assurance SNMPv3 traps. If the CA NSM Event Manager is not configured properly, trap processing terminates.

Important! CA NSM 11.1: You must apply CA fix QO99777 and Microsoft fix 931565.

For more information about the CA NSM issue, see fix number QO99777 on CA Support Online at http://ca.com/support. Click Technical Support, then Download Center, and enter fix number QO99777 in the Quick Search field to locate the Product Information Bulletin.

You should also search the Microsoft Support website for Knowledge Base article 931565, which discusses the situation in which a WinSNMP application stops responding when you run third-party security scanning software on a Windows Server 2003-based computer.

Chapter 6: Documentation

This section contains the following topics:

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.

Chapter 7: Known Issues

The *CA Virtual Assurance Release Notes* on CA Support Online contain issues and other information discovered after publication.

For the latest version of the Release Notes, visit http://ca.com/support.

1. Log in to CA Support Online.
2. Select Enterprise/Small and Medium Business.
3. Select Documentation.
4. Select the CA Virtual Assurance Bookshelf from the Bookshelf drop-down list, and click Go.
5. Open the Release Notes from the Bookshelf window.

This section contains the following topics:

Localized Service Desk Template Name is Truncated

Symptom:

When CA Virtual Assurance is integrated with CA Service Desk (CA Service Desk Manager) and the Service Desk template name is localized, template names might be truncated. CA Service Desk Manager cannot handle template names that exceed the maximum length. The maximum template name length is 30 single-byte or 15 double-byte characters.

Solution:

Open a Technical Support issue, and request a test fix patch. Report problem number USRD 2248.

Login Process is Slow

Symptom:

If the user management connects to Active Directory, the login process can take a long time.

Solution:

CA EEM can bind with Active Directory using the default LDAP port 389. If the login process takes a long time, change to the Global Catalog port 3268.

Follow these steps:

1. Start CA EEM.

   The login page appears.

2. Select AIP as application, EiamAdmin as user, and log in.

   The user interface appears.

3. Select Configure, EEM Server.

   The EEM Server pane appears.

4. Select Global Users/Global Groups.

   The user interface displays Global Users/Global Groups properties.

5. Change the Port number to 3268, and click Save.

   The change takes effect immediately. You do not have to recycle any services after this change.

Mozilla Firefox Automatic Upgrade

Symptom:

After Mozilla Firefox browser upgrade, you may face page rendering issues when using the CA Server Automation web application.

Solution:

Mozilla Firefox could be automatically upgraded. If you encounter page rendering issues, check if your browser was upgraded and perform browser cache cleanup.

Appendix A: Acknowledgements

This appendix contains copyright and licensing agreement information for third-party software used in CA Virtual Assurance.

This section contains the following topics:

Third-Party Software Acknowledgments (see page 47)

Third-Party Software Acknowledgments

This section provides information about third-party software acknowledgments. The third-party license agreements are available in the \Bookshelf Files\TXT folder in the CA Bookshelf.

- Adobe Flex SDK
- AIX JRE
- Apache Axis2 1.5.2
- Apache HTTP Web Server 2.2.23
- Apache Software Foundation
- Apache Solr 1.4.1
- Apache Tomcat 6.0.35
- base64 0.00.00B
- Boost 1.42
- bzip2 1.0.2
- Castor 0.9.5.4
- concurrent utilities 1.3.4
- curl 7.25.0
- Eclipse BIRT Runtime v. 2.3.2.2
- Expat 2.0.1
- Hibernate 3.2.2
- HP-UX JRE 6.0.14 PA-RISC
- HSQLDB 1.8
- ICU4C 3.4

- ipmitool 1.8.10
- JAXB 2.1
- JAXP 1.4.2
- JGoodies Looks 2.2.0
- JRE v1.6
- JSMin
- json-lib 2.4
- JSW v.3.2.3
- JXTA 2.3.6
- libarchive 3.0.2
- libcurl 7.21.0 and libcurl 7.21.1
- libssh2 1.2.6
- libtorrent 0.15.7
- Libxml2 2.7.7, Libxml2 2.7.8, Libxml2 2.8.0, and Libxml2 2.9.0
- Libxslt 1.1.24 (../../TXT/Libxslt1.1.24.txt)
- MIT Kerberos v5 release 1.4
- Mod_gsoap 0.7
- NetApp NMSDK 4.0
- Netscape Portable Runtime 4.7.1
- netx 0.5
- node.js 0.4.12
- NUNIT 2.2.8
- OpenFire 3.7.1
- OpenLDAP 2.1
- openSSH for Windows CE 0.0.2 Alpha
- OpenSSL 0.9.8g, 0.9.8h, 0.9.8j, and 0.9.8o
- OpenSSL 0.9.8r and OpenSSL 0.9.8u
- OpenSSL 0.9.8x
- openwsman 2.0
- Oracle JDBC Driver 10G Release 2
- Oracle JDK 1.6.0_32 (../../TXT/OracleJDK1.6.0_32.txt)

- PCRE 8.1 and PCRE Library 8.12
- Pegasus 2.7
- Perl 5.12.2
- PHP 5.3.13 (../../TXT/PHP5.3.13.txt)
- POCO 1.3.2
- PuTTY 0.60
- py2exe for Python 2.6.x 0.6.9
- Python 2.6
- Rhino 1.6R4
- Sun JDK 1.6.0
- Sun JRE v.1.6
- swfobject 2.1
- Ubuntu 10.04
- VIX API
- Windows Installer XML (WiX)
- Zlib 1.2.3 and Zlib 1.2.5