CA Server Automation

Release Notes

Release 12.8.2

CA Technologies Product References

This document may reference the following CA Technologies products and components or third-party components:

- 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 Process Automation, formerly CA IT Process Automation Manager (CA IT PAM)
- CA Server Automation
- CA Service Desk Manager (CA SDM)
- CA Software Delivery, a component of CA IT Client Manager
- CA Spectrum® Infrastructure Manager (CA Spectrum)
- CA SystemEDGE

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 *Release Notes* provides the new and enhanced features in this release, product requirements, and known issues.

For the most recent CA Server Automation Release Notes, see the bookshelf at CA Support Online.

This section contains the following topics:

Chapter 2: System Requirements

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

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 If these technologies are not available, failing, slow, or have incorrect or out-of-date information, product functionality can be adversely affected.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 CA Server Automation Release 12.8.2 installation.

Hardware Requirements

The following hardware is required to implement distributed and nondistributed CA Server Automation 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 Server Automation 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: In addition, the Performance Chart data collection can require up to 3.5 GB of disk space and 2 GB of RAM on the manager, depending on the number of machines and metrics being monitored.

- Free disk space for upgrade: >30 GB, depending on the size of the existing database

  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! If you install CA Server Automation with other CA products, consider the combined impact and adjust the hardware specifications accordingly. For example, if you install CA Server Automation (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.

Software Requirements

This section provides information about the software that is required to implement distributed and nondistributed components.

Manager on Windows

The CA Server Automation 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
- Windows Server 2012 Standard and Datacenter Edition (x64)

CA Server Automation supports the following Windows versions only for new SystemEDGE installations:

- 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).

Database Requirements

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

This release supports and is certified for the following versions:

- 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. 12.7, or 12.7.1 installation with SQL Server 2005 or SQL Server 2008, upgrade the SQL Server to a supported version. Then verify that the 12.6, 12.7, or 12.7.1 product is still operational and upgrade to CA Server Automation Release 12.8.2.

Note the following:

- For your convenience, SQL Server 2012 Express Edition (32 bit) is available on the CA Server Automation installation media at the following location: DVD1\Installers\Windows\External\MSSQLExpress\SQLEXPRWT_x86_ENU.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 also must have the SQL client (server tools) installed.
- After SQL Server Tools installation, verify that OSQL.EXE is installed properly to this location (if using the default install path):
  - MS SQL 2012 C:\Program Files\Microsoft SQL Server\110\Tools\Binn

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 R2, or R2 Express database requires a local 2008 R2 Native Client. 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 Server Automation 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 9.0, 10.0

  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 Server Automation 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 Server Automation supports the major versions of the Adobe Flash Player. The minor versions can also work, but they are not certified.

Required CA Software

CA Server Automation requires the following software shipped with the installation media:

CA Embedded Entitlements Manager (CA EEM)

CA Server Automation supports and is certified to work with the following CA EEM releases:

- CA EEM version 12.0 CR 07 (12.0.7.57 and later)
- CA EEM release 12.5 (12.5.0.7)

Note: If you use CA EEM version 12.0, the following functionality is not supported: CA EEM installation, CA EEM user creation using Native Security, and CA EEM configuration of LDAP service. To complete the mentioned actions, perform those procedures from the CA EEM UI and follow the CA EEM procedures.

Note: CA Server Automation currently does not support "Multiple Microsoft Active Directory" and "Microsoft Active Directory Forest" external LDAP Directory configuration. You must use "Basic LDAP Directory".

Note: CA EEM FIPS mode is not supported.

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

CA Server Automation Release 12.8.2 distributes with SystemEDGE Release 5.8.1.

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

Note: If the latest version of SystemEDGE is not already on your system, the installation program installs it. SystemEDGE is required for the CA Server Automation 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, 5.7.0, 5.7.1, and 5.8 are supported for managing remote servers in your environment.

Optional Software Requirements

You can use the following optional software with CA Server Automation:

CA AppLogic

Versions 3.0, 3.1, and 3.5 are supported.

CA ITCM

Version 12.8 CP01 is required for all server and software provisioning.

CA Process Automation

CA Server Automation Release 12.8.2 is certified for:

- CA Process Automation Version 4.1
- CA Process Automation Version 4.2 SP01

A 64-bit operating system is required.

Note: After installation, locate the file <PAM_Home>\server\c2o\bin\c2osvcw.conf, and increase its wrapper.java.maxmemory (heap) size from 1024 to 2048. Restart the PAM service and proceed to load CA Server Automation connectors. For more information about CA Process Automation requirements, see the *CA Process Automation Release Notes*.

CA SDM

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

Storage Management Support

CA Server Automation supports the following storage systems:

- EMC CLARiiON CX3 and CX4 Series Servers
- EMC Symmetrix VMAX 10K
- HP InForm OS 3.1.1
- IBM Storwize V7000 Version 6.3
- NetApp Data Fabric Manager (DMF) versions 4.0 and 4.0.2
- NetApp OnCommand Unified Management Core 5.1

More Information:

Deprecated Software (see page 30).

Solaris Systems for JumpStart Provisioning

CA Server Automation supports JumpStart provisioning of the following Solaris systems:

For SPARC-based systems:

- Solaris 8 Release 0204 (additional user configuration is required on the server)
- Solaris 9 (any release)
- Solaris 10 (any release)
- Flash Archives comprised of Solaris 8 0204, 9, or 10

For x86-based systems:

- Solaris 10 Release 1106 or newer
- Flash Archives comprised of Solaris 10 1106 or newer

CA Server Automation 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 Server Automation 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 Server Automation 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 5.8.1 requires one of the following operating systems:

Windows

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

- Windows Server 2012 Standard and Datacenter Edition (64 bit, x64)
- Windows Server 2012 R2
- 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 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 6.0 (Squeeze) (32 bit, x86)
- Debian Linux Version 6.0 (Squeeze) (64 bit, x64) - 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
- Red Hat Enterprise Server 6.0 (zSeries) - Legacy Mode Only

Linux on pSeries

- SUSE Linux Enterprise Server 10
- SUSE Linux Enterprise Server 11
- Red Hat Enterprise Server 5.0
- Red Hat Enterprise Server 6.0

Solaris

Note: SystemEDGE supports all Solaris Zone configurations for the Solaris 10 and Solaris 11 operating systems.

- Solaris UltraSPARC 9 (64 bit)
- Solaris UltraSPARC 10 (64 bit)
- Solaris UltraSPARC 11 (64 bit)
- Solaris 9 (32 bit, x86)
- Solaris 10 (32 bit, x86)
- Solaris 10 (64 bit, x64)
- Solaris 11 (32bit, x86)
- Solaris 11 (64bit, x64)

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

CA Server Automation AIM Operating System Support

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

Windows: Advanced Encryption

- Windows XP Professional SP3 (32 bit, x86)
- Windows Vista Business, Enterprise, Ultimate SP1 (32 bit, x86)
- Windows Vista Business, Enterprise, Ultimate SP1 (64 bit, x64)
- Windows 7 Professional, Ultimate (32 bit, x86)
- Windows 7 Professional, Ultimate (64 bit, x64)
- Windows Server 2003 SP2 Standard, Enterprise, Datacenter, and Small Business Server Edition (32 bit, x86)
- Windows Server 2003 SP2 x64 Edition (64 bit)
- Windows Server 2003 R2 SP2 Standard, Enterprise, and Datacenter Edition (32 bit, x86)
- Windows Server 2003 R2 SP2 Standard, Enterprise, and Datacenter Edition (64 bit, x64)
- Windows Server 2008 Standard, Enterprise, and Datacenter Edition (32 bit, x86)
- Windows Server 2008 Standard, Enterprise, and Datacenter Edition (64 bit, x64)
- Windows Server 2008 R2 Standard, Enterprise, and Datacenter Edition (64 bit, x64)
- Windows Server 2012 Standard and Datacenter Edition (64 bit, x64)
- Windows Server 2012 R2

Windows: Cisco UCS AIM, Huawei GalaX AIM, IBM LPAR AIM, IBM PowerHA AIM, KVM AIM, Remote Monitoring AIM, Solaris Zones AIM, vCenter Server AIM, vCloud AIM, XenServer AIM, XenDesktop AIM

- Windows Server 2008 Standard, Enterprise, and Datacenter Edition (32 bit, x86)
- Windows Server 2008 Standard, Enterprise, and Datacenter Edition (64 bit, x64)
- Windows Server 2008 R2 Standard, Enterprise, and Datacenter Edition (64 bit, x64)
- Windows Server 2012 Standard and Datacenter Edition (64 bit, x64)
- Windows Server 2012 R2

Windows: Hyper-V AIM

- Windows Server 2008 R2 Standard, Enterprise, and Datacenter 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 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 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 6.0 (Squeeze) (32 bit, x86)
- Debian Linux Version 6.0 (Squeeze) (64 bit, x64) - Legacy Mode Only

Linux: 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 11 (32 bit, x86)
- SUSE Linux Enterprise Server 11 (64 bit, x64)
- Debian Linux Version 5.0 (Lenny) (32 bit, x86)
- Debian Linux Version 6.0 (Squeeze) (32 bit, x86)
- Debian Linux Version 6.0 (Squeeze) (64 bit, x64) - Legacy Mode Only

Solaris: Advanced Encryption, Service Response Monitoring AIM

Note: SystemEDGE supports all Solaris Zone configurations for the Solaris 10 and Solaris 11 operating systems.

- Solaris UltraSPARC 9 (64 bit)
- Solaris UltraSPARC 10 (64 bit)
- Solaris UltraSPARC 11 (64 bit)
- Solaris 9 (32 bit, x86)
- Solaris 10 (32 bit, x86)
- Solaris 10 (64 bit, x64)
- Solaris 11 (32bit, x86)
- Solaris 11 (64bit, x64)

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 Server Automation 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, Datacenter, and Small Business Server Edition (32 bit, x86)
- Windows Server 2003 (64 bit, x64)
- Windows Server 2003 R2 Standard, Enterprise, and Datacenter 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 Server Automation-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 Platforms

Cisco Unified Computing System (UCS)

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

- Cisco UCS 1.4 and 2.1

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 PowerVM (Logical Partitions, LPAR)

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

IBM AIX LPAR

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

IBM AIX Network Installation Manager (NIM) server

To enable imaging functionality for computers running AIX operating systems, install NIM server on AIX 5.3, 6.1, or 7.1. NIM adapter component installations are supported on AIX 5.3 (TL11 or higher), AIX 6.1 (TL4 or higher), and AIX 7.1.

Note: To image NIM clients, NIM server must be running with equal or higher operating system version than that of the NIM client.

IBM AIX Network Installation Manager (NIM) client

NIM clients are supported on AIX 5.3 and 6.1.

IBM Hardware Management Console (HMC)

To manage logical partitions of IBM POWER5, POWER6, or POWER7 platforms, install HMC V7R3.5, V7R7.1, V7R7.2, V7R7.3, or V7R7.4.

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. Versions 1.5, 2.1, and 2.2 are supported.

IBM Virtual I/O Server

IBM Virtual I/O Server (VIOS) lets you configure IBM AIX POWER5, POWER6, and POWER7 logical partitions. VIOS versions 1.5, 2.1, and 2.2 are supported.

Oracle Solaris Zones

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

- Solaris 10 or 11 with zones compatibility to manage Solaris Zones.

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 4.1, 5.0, 5.1 or 5.5 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 4.1, 5.0, 5.1 or 5.5 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 5.1, 5.5

Internationalization (i18n)

CA Server Automation 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, Japanese, and Simplified Chinese versions of the supported Microsoft Windows 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 Server Automation integrates with other CA products, review the international support statements for integration products.

CA Server Automation 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 Server Automation supports non-ASCII Virtual Machine names, but only if they are provisioned using the virtualization vendor software directly. When cloning or provisioning a new Virtual Machine from within CA Server Automation, the Virtual Machine name must be ASCII.

CA Server Automation 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 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 Server Automation 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 for running commands in the Windows Command Prompt 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 Server Automation CLI Commands

AutoShell and CA Server Automation 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.

Service Response Monitoring 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 Server Automation disallows unsupported characters in UCS fields for service profile, pools, and so on.

Reservation Manager Requirement for a Common Windows Administrator Account Name

The Reservation Manager requires that all Windows systems that are provisioned, to have a common administrator account name. Because the default administrator account name can differ based on the language of the Windows OS, consider creating a common account name on all systems.

Reservation Manager Limitations

The names of virtual machines deployed by Reservation Manager contain only these characters: 'a - z', 'A - Z', '0 - 9' and '-'. This limitation is enforced to restrict the host names for virtual machines to characters supported by the product.

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.
```

The product installer accepts non-ASCII characters for the configuration of LPAR, vCenter, Solaris Zones, Microsoft Cluster Service, Hyper-V, SCVMM, Remote Monitoring, and UCS components. However, if non-ASCII characters are entered, the configuration of the associated AIMs can silently fail. If you have to configure an AIM using non-ASCII characters, then configure the AIM post-install using the UI Administration tab or CLI.

Chapter 3: New Features and Enhancements

This section contains the following topics:

Reservation Manager New Features and Enhancements

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

Direct access to VMWare VM Console

As a reservation manager end user, you can access the VMWare VM Console through a URL instead of through remote desktop (RDP) access. This feature is useful when there is a network connectivity issue in the RDP.

Enhanced Automatic VM Name generation by allowing 6 digit Reservation ID.

Earlier VM name allowed only five (5) digit Reservation ID, now CA Server Automation allows you to create more reservations by allowing six (6) digit Reservation ID.

IBM LPAR Provisioning - allowing NIM boot from Different Subnet

Network boot installation of an LPAR in a NIM environment is supported even if the NIM clients and NIM master are in different subnets.

Add AD group to local administrator group

You can now add a group as local administrator of a provisioned virtual machine.

Add AD Groups as secondary owners to a reservation

You can now add a group as secondary owners of a provisioned virtual machine.

Pre-System Release event to handle automated steps

An event is generated before the expiry of a VM allowing administrator to run any automated scripts when the event gets triggered.

Allow CPU & Memory selections based on administrator configuration

Allows administrator to configure options to be displayed to the end user for selection of desired CPU and Memory values when reserving a virtual machine.

Display all users and groups assigned to an existing reservation as secondary owners.

Allows the end user to view secondary owners (whether individual user or group) associated with the reservation.

Product Certifications:

- vCenter 5.5
- CA ITCM 12.8 C1
- CA Process Automation 4.2 SP01
- CA EEM r12.5 CR01

API updates to reservation manager web services

API updates to reservation manager web services to bypass organization unit while querying any data, and changing retention period when returning the reservation.

Deprecated Software

In this release, the integration support to the following components are removed/deprecated:

- Amazon EC2
- Microsoft Hyper-V 2008
- Citrix Xen server
- Red Hat Enterprise Virtualization
- VMware vCenter Server version 4.0
- VMware vCloud Director 1.0, 1.0.1, 1.5
- VMware ESX Server/VMware ESXi Server Version 4.0

Chapter 4: 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.

Chapter 5: Documentation

This section contains the following topics:

Related Publications

The CA Bookshelf provides the following CA Server Automation publications:

Administration Guide

Describes product architecture, troubleshooting, concepts, and configuration tasks for administrators.

Installation Guide

Describes installation prerequisites, best practices, and procedures for CA Server Automation.

Reference Guide

Provides detailed information about AutoShell, CLI scripting commands, and log files.

Performance Metrics Reference

Describes the performance metrics that are available for monitoring the systems performance of the supported platforms.

Online Help

Provides information to help you complete tasks using the CA Server Automation user interface.

Reservation Manager Help

Provides information to help users and administrators complete tasks using the Reservation Manager user interface.

Release Notes

Provides information about new and changed features and product implementation information including operating system support, system requirements, and how to contact Technical Support.

Service Response Monitoring User Guide

Provides installation and configuration details of SRM.

SystemEDGE User Guide

Provides end-user information about the SystemEDGE agent.

SystemEDGE Release Notes

Provides information about new and changed features and agent implementation information including operating system support, system requirements, and how to contact Technical Support.

To view PDF guides, download and install Adobe Reader from the Adobe website if it is not already installed on your computer.

Chapter 6: Known Issues

The *CA Server Automation 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 Server Automation 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:

CA Process Automation Security Vulnerability

Symptom:

CA Process Automation contains a high-risk vulnerability that can allow a remote attacker to execute arbitrary code. The vulnerability occurs in the JBoss Seam component. An attacker can potentially execute arbitrary JBoss EL (Unified Expression Language extension) and fully compromise the server.

To test for this vulnerability, replace <HOST> with the hostname of the CA Process Automation installation in the following URL:

```
http://<HOST>:8080/admin-console/login.seam?actionOutcome=/test.xhtml%3ftested%3d
%23{expressions.getClass().forName('java.lang.Runtime')}
```

This is the expected output if the JBoss EL command is successfully evaluated showing that the installation is vulnerable:

```
http://<HOST>:8080/admin-console/test.seam;jsessionid=0792523D29AE7A237D1CE5329C2
7A46F.?tested=class+java.lang.Runtime&conversationId=11
```

See the in-depth vulnerability details for further exploitation techniques.

Affected Products:

- CA Process Automation 4.0
- CA Process Automation 4.0 SP1
- CA Process Automation 4.1
- Potentially any CA product using CA Process Automation 4.0 and later.

Unaffected Products:

- CA Process Automation releases before Version 4.0

Solution:

A fix is planned for a future release of CA Process Automation. In the meantime, use the following instructions to manually remove the vulnerable JBoss Seam component from the CA PAM installation. These instructions also disable the JBoss Admin Console.

1. Stop the PAM service.
2. Delete the contents of the following directories:
   - <PAM_Home>\server\c2o\.tmp
   - <PAM_Home>\server\c2o\temp
   - <PAM_Home>\server\c2o\tmp
   - <PAM_Home>\server\c2o\work

3. Move the following folders from <PAM_Home>\server\c2o\deployers to a location outside the PAM directory tree to keep as a backup:
   - seam.deployer
   - webbeans.deployer
4. Move the following folder from <PAM_Home>\server\c2o\ to a location outside the PAM directory tree to keep as a backup:
   - admin-console.war
5. Start the PAM service.

Note: If the Admin Console is needed temporarily, stop the PAM service, revert the changes in Step 4 above, and restart the PAM service. Repeat Step 4 when the Admin Console is no longer needed.

"Field Set detected" Warning When Selecting Start Request Form

Symptom:

When creating a CA Process Automation action, a user can get an empty form (no fields) after selecting from a list of Start Request forms. The system displays the following message:

"Field Set detected in one of the pages of this form. Proceed only if this information is not required."

Solution:

In CA Process Automation 4.0 and higher, a new data type (Field Set) can be used to group related fields together. For example, text field, text area, multiline text, and so on. However, when using the CA Server Automation user interface, ensure that only valid fields (not Field Sets) are used.

CA Process Automation Action Does Not Support Environment Variable Substitution By Default

Symptom:

CA Process Automation actions in an *Application* for *Service Provisioning* do not support environment variable substitution by default.

Solution:

To ensure successful command execution, place **cmd.exe /c** in front of the command directive.

Example:

The following command executes successfully when executed as an installation action of *Execute Program* type in an *Application*.

```
%CD%\..\ORCDAgent\InstallMSI.cmd /i %CD%\httpd-2.2.22-win32-x86-openssl-0.9.8t.msi
/qn INSTALLDIR=C:\Apache SERVERADMIN="admin@localhost.com" SERVERNAME=%LOCALHOST%
AgreeToLicense=1 ALLUSERS=1 RebootYESNo=No
```

However, the same command fails if used in an installation action of *Process Automation Process* type. To correct this problem, you must append **cmd.exe /c** in front of the original command as follows:

```
cmd.exe /c  %CD%\..\ORCDAgent\InstallMSI.cmd /i
%CD%\httpd-2.2.22-win32-x86-openssl-0.9.8t.msi /qn INSTALLDIR=C:\Apache
SERVERADMIN="admin@localhost.com" SERVERNAME=%LOCALHOST% AgreeToLicense=1
ALLUSERS=1 RebootYESNo=No
```

Localized Service Desk Stack Name is Truncated

Symptom:

When CA Server Automation is integrated with CA Service Desk (CA SDM) and the Service Desk stack name is localized, stack names might be truncated. CA SDM cannot handle stack names that exceed the maximum length. The maximum stack 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.

Mozilla Firefox Automatic Upgrade

Symptom:

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

Solution:

Mozilla Firefox could have been upgraded automatically. If you encounter page rendering issues, verify that your browser was upgraded and perform browser cache cleanup.

Transfer of reservation is not working for users even in the same organization unit

Symptom:

Transfer of reservation from one user to another user is not working even if both the users are in the same organization unit.

Solution:

This issue currently has no known solution.

“Org Unit not specified” popup while reserving a VM through tenant user

Symptom:

An error message "Org Unit not specified" pops when reserving a VM as a tenant user.

Solution:

The message appears only for tenant user who is also the administrator of the tenant. You can click OK to ignore the message and continue reserving a VM.

Modify VM for “Linux template”, machine is getting rebooted even if we enable Memory/CPU plugin for the template

Symptom:

When modifying a VM for “Linux template”, machine is rebooted even if Memory/CPU plugin for the template is enabled.

Solution:

The machine reboots even if the memory/CPU plugin is enabled. The changes are applied on the VM after reboot. This scenario is noticed only in VM based on Linux template.

VM Snapshot level is not displaying correctly in Manage Snapshot page

Symptom:

VM Snapshot level is not displaying correctly in the Manage Snapshots page under System Details section.

Solution:

This issue currently has no known solution. Modification to the snapshots successfully applied and can be verified in the VCenter. The expected snapshot level is not displayed in the user interface, The VCenter administrator can verify the snapshot level from the VCenter.

The users of AD group are not able to manage reservation when isvmuseronly tag is set to false

Symptom:

The users of AD group are not able to manage reservation when isvmuseronly tag is set to false.

Solution:

This issue currently has no known solution.

Appendix A: Acknowledgements

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

This section contains the following topics:

Third-Party Software Acknowledgments

The following links provide information about third-party software acknowledgments.

- ActiveMQ 5.4.2
- 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 6.0.36
- Apache Tuscany SDO 1.1.1
- base64 0.00.00B
- Beanshell v.2.0b4
- 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
- GNUPlot 6.4
- 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
- JBoss Application Server 4.2.3
- JGoodies Looks 2.2.0
- 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
- Liferay 6.0.6 CE
- Linux Penguin Logo (Tux) 2.0
- Microsoft Cabinet File Software Development Kit (CAB SDK) 1
- 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_43
- Oracle JRE v.1.6
- PCRE 8.1 and PCRE Library 8.12
- Pegasus 2.7
- Perl 5.12.2
- PHP 5.3.13
- POCO 1.3.2
- PuTTY 0.60
- py2exe for Python 2.6.x 0.6.9
- Python 2.6
- Rhino 1.6R4
- swfobject 2.1
- Ubuntu 10.04
- VIX API
- Windows Installer XML (WiX)
- Zlib 1.2.3 and Zlib 1.2.5