CA IT Client Manager

Release Notes and Known Issues

r12 SP1

CA Product References

This document references the following CA products:

- CA IT Client Manager (CA ITCM)
- CA Service Desk
- CA Desktop and Server Management
- CA Desktop Migration Manager (CA DMM)
- CA Asset Management
- CA Asset Intelligence
- CA Software Delivery
- CA Remote Control
- CA Asset Portfolio Management (CA APM)
- CA Patch Manager
- CA Workflow
- CA Embedded Entitlements Manager (CA EEM), formerly CA eTrust® Identity and Access Management
- CA Network and Systems Management (CA NSM)
- CA Advantage™ Data Transport®
- CA WorldView™
- CleverPath™ Reporter

Contact CA

Contact Technical Support

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

- Online and telephone contact information for technical assistance and customer services
- Information about user communities and forums
- Product and documentation downloads
- CA Support policies and guidelines
- Other helpful resources appropriate for your product

Provide Feedback

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

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

Contents

Chapter 1: Introduction

CA ITCM r12 SP1 delivers improvements to existing features and functions found in CA ITCM r12. In addition, it provides consistency for supported languages and environments.

This document provides details of the new features and enhancements that were made to CA ITCM r12, information required to upgrade, known issues, and fixes related to this release.

The changes made to CA ITCM, including the asset management component, CA Asset Intelligence, and CA Patch Manager are covered in the following chapters.

Before you install CA ITCM or any of its components, we recommend that you read the *r12 Implementation Guide* in conjunction with the contents of this *Release Notes*. Both documents contain important pre-installation and post-installation considerations.

This section contains the following topics:

Changes and Enhancements

CA ITCM and all its components now support the following:

- Installation in the following languages:
  - English
  - French
  - German
  - Japanese

  For a complete list of supported languages, see Language Certification (see page 21).
- Oracle 10g Release 2 SP4, Microsoft SQL Server 2005, or Microsoft SQL Server 2008 as the database

  For a complete list of supported databases, see Supported Databases for the MDB (see page 13).
- Installation on computers running Microsoft Cluster
- Windows Server 2008 SP2 (Enterprise, Standard) 32- and 64-bit

  For a complete list of supported Windows environments, see Microsoft Windows Operating Environments (see page 13).

CA Workflow for CA ITCM

CA Workflow for CA ITCM, as a part of this release, supports the following:

- Installation in the following languages:
  - English
  - French
  - German
  - Japanese
- Installation in both compatible and non-compatible mode of MDB
- Port configuration for Apache Tomcat application server
- Windows Server 2008 SP2 (Enterprise Edition, Standard Edition, Datacenter Edition) 32- and 64-bit

  Important! To install CA Workflow for CA ITCM on Windows Server 2008, install CA EEM on another computer that is not running Windows Server 2008 because CA EEM does not support Windows Server 2008.

CA Workflow for CA ITCM requires JRE Version 1.5 Update 11 as an installation prerequisite.

Supported Operating Environments

The following sections contain the operating environments, databases, web servers, and web browsers supported by CA ITCM r12 SP1.

Microsoft Windows Operating Environments

CA ITCM r12 SP1 supports the following Windows operating environments.

Note: 64-bit support includes AMD64 and Intel EM64T chips.

Manager Operating Environments (Manager, Engine, Web Console, Web Services, and SQL Server MDB)

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

Scalability Server Operating Environments

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

ENC Gateway Operating Environments

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

DSM Explorer Operating Environments

- Windows Server 2003 R2 SP2 (Enterprise, Standard) 32- and 64-bit
- Windows Server 2003 SP2 (Enterprise, Standard, Web) 32- and 64-bit
- Windows XP Professional SP2 32- and 64-bit
- Windows Vista SP1 (Enterprise, Business, Ultimate) 32- and 64-bit
- Windows Server 2008 SP2 (Enterprise Edition, Standard Edition, Datacenter Edition) 32- and 64-bit

Agent, ENC Client, and Packager Operating Environments

- Windows Server 2003 R2 SP2 (Enterprise, Standard) 32- and 64-bit
- Windows Server 2003 SP2 (Enterprise, Standard, Web) 32- and 64-bit
- Windows 2000 SP4 (Professional, Server, Advanced Server) 32-bit
- Windows XP Professional SP2 32- and 64-bit
- Windows XP Professional SP3 32-bit
- Windows Server 2008 Itanium (IA-64)
- Windows Server 2008 SP2 (Enterprise Edition, Standard Edition, Datacenter Edition) 32- and 64-bit
- Windows Server 2008 SP2 Server Core (Enterprise Edition, Standard Edition, Datacenter Edition) 32- and 64-bit
- Windows XP Embedded SP2 32-bit
- Windows Vista SP1 (Enterprise, Business, Ultimate) 32- and 64-bit
- Windows Vista SP2 (Enterprise, Business, Ultimate) 32- and 64-bit
- Windows 7 (Enterprise, Ultimate, Professional, Home) 32- and 64 bit
- Windows EPOS SP2 32-bit

V4.0 Legacy Agent-only Operating Environments (no Packager)

- Windows Mobile 6 (Classic, Standard, Professional) (ARM-based, including StrongARM, XScale, TI OMAP)
- Windows Mobile 5 (ARM-based, including StrongARM, XScale)
- Windows Mobile 6.1 (ARM-based, including StrongARM, XScale)

Image Prepare System Operating Environments (OS Images, Boot Images)

- Windows Server 2003 R2 SP2 (Enterprise, Standard) 32- and 64-bit
- Windows Server 2003 SP2 (Enterprise, Standard, Web) 32- and 64-bit
- Windows XP Professional SP2 32- and 64-bit
- Windows XP Professional SP3 32-bit
- Windows Vista SP1 (Enterprise, Business, Ultimate) 32- and 64-bit
- Windows Vista SP2 (Enterprise, Business, Ultimate) 32- and 64-bit
- Windows Server 2008 SP2 (Enterprise Edition, Standard Edition) 32- and 64-bit

Linux Operating Environments

CA ITCM r12 SP1 supports the following Linux operating environments.

Note: You should be aware of the following exceptions:

- 64-bit support includes AMD64 and Intel EM64T chips, but not IA64 Itanium.
- ENC Gateway and Client are not supported on Linux.
- On Linux operating environments with the SELinux security system enabled, the CA ITCM software will be installed in the unconfined domain. This is not configurable at install time.

Web Console and Web Services Operating Environments

- Red Hat Enterprise Linux 5 Update 2 ("Regular", Advanced Platform) (32- and 64-bit)
- Red Hat Enterprise Linux 4 Update 7 (ES, AS) (32- and 64-bit)
- SuSE Linux Enterprise Server 10 SP2 (32- and 64-bit)
- SuSE Linux Enterprise Server 9 SP4 (32- and 64-bit)

Scalability Server Operating Environments

- Red Hat Enterprise Linux 5 Update 3 (Server) (32- and 64-bit)
- Red Hat Enterprise Linux 5 Update 2 ("Regular", Advanced Platform) (32- and 64-bit)
- Red Hat Enterprise Linux 4 Update 7 (ES, WS, AS) (32- and 64-bit)
- SuSE Linux Enterprise Server 10 SP2 (32- and 64-bit)
- SuSE Linux Enterprise Server 9 SP4 (32- and 64-bit)

Agent and Packager Operating Environments

- Red Hat Enterprise Linux 5 Update 3 (Server) (32- and 64-bit)
- Red Hat Enterprise Linux 5 Update 2 (32- and 64-bit)
- Red Hat Enterprise Linux 4 Update 7 (ES, WS, AS) (32- and 64-bit)
- SuSE Linux Enterprise Server 10 SP2 (32- and 64-bit)
- SuSE Linux Enterprise Server 9 SP4 (32- and 64-bit)
- SuSE Linux Professional 10.1 (32- and 64-bit)
- SuSE Linux Professional 10 (32- and 64-bit)
- SuSE Linux Professional 9.3 (32- and 64-bit)
- SuSE Linux Professional 9.2 (32- and 64-bit)
- SuSE Linux Professional 9.1 (32- and 64-bit)
- SuSE Linux Desktop 9 (32- and 64-bit)
- Open SUSE 11.0 (32- and 64-bit)
- Open SUSE 11.1 (32- and 64-bit)
- Oracle Enterprise Linux 5 Update 1 (32- and 64-bit)

Agent-only Operating Environment (no Packager)

- VMWare ESX 3.5

Note: VMWare ESX operating environment does not support the remote control agent.

UNIX and MAC OS X Operating Environments

CA ITCM r12 SP1 supports the following UNIX and Mac OS X operating environments.

Note: ENC Gateway and Client are not supported on UNIX and Mac OS X.

Oracle Management Database (MDB) Operating Environment

- Sun Solaris 10 for SPARC (64-bit)

Scalability Server Operating Environments (r11.2 only)

- SCO UnixWare 7.1.4 Maintenance Pack 3 (32-bit)
- SCO UnixWare 7.1.3 Maintenance Pack 5 (32-bit)

Agent and Packager Operating Environments

- IBM AIX 6.1 (64-bit)
- IBM AIX 5.3 (32- and 64-bit)
- IBM AIX 5.2 (32- and 64-bit)
- HP-UX 11.31 pa-risc (64-bit)
- HP-UX 11.31 ia64 (64-bit)

  Important! To use the HP-UX 11.31 operating environment, apply the following HP patch to the computer: PHSS_36520 (11.31 Aries Cumulative Patch). This patch may be superseded by another patch; therefore, check the HP maintenance fixes for the latest cumulative patch.

- HP-UX 11.23 pa-risc (64-bit)
- HP-UX 11.23 ia64 (64-bit)
- HP-UX 11.11 pa-risc (32- and 64-bit)

  Note: The CA Systems Performance LiteAgent is not installed on HP-UX 11.11 as this component is no longer supported on this platform.

  Important! HP-UX 11.23 and 11.1 operating environments do not support IPv6. Apply the PHSS_37516 patch (or any superseding HP patch), PHCO_35743 (or any superseding HP patch), PHSS_33945 (or any superseding HP patch), and any other critical patches as recommended by HP.

  Description of the above mentioned patches are available in HP's patch database, which is accessible from

  http://www13.itrc.hp.com

- Sun Solaris 10 for SPARC (64-bit)
- Sun Solaris 10 for x86 and x64
- Sun Solaris 9 for SPARC (32- and 64-bit)
- Sun Solaris 9 for x86
- Sun Solaris 8 for SPARC (32- and 64-bit)
- Sun Solaris 8 for x86

  Note: The SUNWzlib package is required for the Software Signature Scanner to work properly. Use the pkginfo SUNWzlib command to verify whether the package is installed.

- SCO UnixWare 7.1.4 Maintenance Pack 3 (32-bit)

  Note: Unicenter DSM r11.2 version is shipped for this operating environment

- SCO UnixWare 7.1.3 Maintenance Pack 5 (32-bit)

  Note: Unicenter DSM r11.2 version is shipped for this operating environment

- Apple Mac OS X 10.5 Update 2 to 6 (for PowerPC * and Intel)
- Apple Mac OS X 10.4 Update 11 (for PowerPC * and Intel)

* The remote control host is not supported on Power PC.

OS Installation Management Target Operating Environments

Target Operating Environments When Using the Original Setup Install Method

- **Windows Intel 32-bit**
  - Windows Server 2008 (Enterprise, Standard, Web) 32-bit and 64-bit
  - Windows Vista (Enterprise, Business, Ultimate)
  - Windows XP Professional
  - Windows Server 2003 R2
  - Windows Server 2003 (Enterprise, Standard, Web)
  - Windows 2000 (Server, Professional)
- **Windows Intel 64-bit (AMD64 architecture, not IA64)**
  - Windows Server 2008 x64
  - Windows Vista x64
  - Windows XP Professional x64
  - Windows Server 2003 R2 x64
  - Windows Server 2003 x64

- **Linux (i386, AMD64, EM64T)**
  - Red Hat Enterprise Linux Server 4 Update 4 to Update 7 (32-bit) (AS, WS, ES)
  - Red Hat Enterprise Linux Server 5 Update 0 to Update 2 (Server , Client Operating Environment) (32- and 64-bit)
  - SuSE Linux Enterprise Server 9 (32-bit)

    Note: When agent installation is required with such an OS installation, a legacy agent is needed. For example, DSM r11.2 SP4.
  - SuSE Linux Enterprise Server 10 SP2 (32-bit and 64-bit)

Target Operating Environments When Using Imaging Tools

Imaging Tool	Target Operating Environments
Symantec Norton Ghost	Windows 2000, Windows XP Professional, Windows Server 2003
Symantec Norton Ghost32	Windows 2000, Windows XP Professional, Windows Server 2003
Symantec Norton Ghost32	Windows XP Professional x64, Windows Server 2003 x64, Windows Server 2003 R2 x64
Microsoft ImageX	Windows 2000, Windows XP Professional, Windows Server 2003, Windows Server 2003 R2, Windows Server 2008, Windows Vista
Microsoft ImageX	Windows XP Professional x64, Windows Server 2003 x64, Windows Server 2003 R2 x64, Windows Vista x64, Windows Server 2008 x64

Proxy Agent Operating Environments

Asset Management and Software Delivery support the following proxy agent operating environments:

- Windows Mobile 6.0 (Classic, Standard, Professional) (ARM-based, including StrongARM, XScale, TI OMAP)
- Windows Mobile 5.0 (ARM-based, including StrongARM, XScale)

Supported Databases for the MDB

CA ITCM r12 SP1 supports the following databases for the Management Database (MDB):

- Microsoft SQL Server 2005 SP3
- Microsoft SQL Server 2005 SP2
- Microsoft SQL Server 2008 SP1 (Enterprise, Standard) 32- and 64-bit

  Note: Microsoft 32-bit SQL Server is not supported on x64 operating environments.
- Oracle 10g Release 2 SP4

  Note: You should be aware of the following Oracle installation considerations:

  - Oracle 10g Release 2 SP4 database is supported as an MDB for CA ITCM r12 SP1, but the Oracle database must be installed as a remote MDB on a dedicated Sun Solaris operating environment
  - On Solaris platforms, installing the MDB on Oracle requires Oracle 10g Release 2 SP4 with the latest Oracle patches p7008262_10204_Solaris-64, p5718815_10204_Solaris-64, and p7706710_10204_Solaris-64
  - Oracle 10g Release 2 SP4 must be applied on any Oracle client installations
  - CA ITCM supports only the EZCONNECT method of connection to the Oracle database. For more information on setting the connection method to EZCONNECT, see the Oracle documentation.

Supported Web Browsers and Web Servers

CA ITCM r12 SP1 supports the following web browsers to access the Web Console:

- Microsoft Internet Explorer (IE) Versions 6,7, and 8
- Firefox 2.0 and 3.0

The Web Console supports the following web server versions:

- Microsoft Internet Information Server (IIS) 6.0 and 7.0 on Windows
- Apache httpd Server 2.0 and 2.2 on Linux

Network Protocols

The following network protocols are supported:

- IPv4
- IPv6

Transport Protocols

The following transport protocols are supported:

- TCP
- UDP

Language Certification

An *internationalized* product is an English product that runs correctly on local language versions of the required operating environments, required third-party products, and supports local language data for input and output. Internationalized products also support the ability to specify local language conventions for date, time, currency, and number formats.

The English release of CA ITCM r12 SP1 is certified for the following operating environment language variants on Windows, Linux, and UNIX:

- English
- French
- German
- Italian
- Japanese
- Korean
- Portuguese (Brazil)
- Simplified Chinese
- Spanish
- Traditional Chinese

Supported Languages

This release of CA ITCM supports the following localized languages:

- English
- French
- German
- Japanese
- Italian - Agent components only
- Korean - Agent components only
- Portuguese (Brazil) - Agent components only
- Simplified Chinese - Agent components only
- Spanish - Agent components only

Hardware Specifications and Requirements

We recommend the following hardware specifications and requirements for CA ITCM r12 SP1.

Actual hardware requirement depends on the load placed on the computer, including factors such as data transferred, data collected, frequency, and number of operations.

Enterprise Manager Specifications

We recommend the following hardware prerequisites for a DSM enterprise manager:

Component	Speed/Size
DVD-ROM Drive	Any
CPU	1-2 CPUs, 2 GHz or better 2 CPUs mandatory, if the MDB is hosted on the same computer
Memory	2 GB minimum 4 GB RAM minimum, if the MDB is hosted on the same computer
Disk Space	30 GB minimum 100 GB minimum, if the MDB is hosted on the same computer

Component	Speed/Size
	The required disk space for the MDB must be available in the disk partition where the MDB is located. Allow additional space for the Software Package Library. The total space requirement depends on the number and size of packages to be stored.
NIC	100 Mbps or higher

Domain Manager Specifications

We recommend the following hardware prerequisites for a DSM domain manager:

Component	Speed/Size
DVD-ROM Drive	Any
CPU	1-2 CPUs, 2 GHz or better 2 CPUs mandatory, if the MDB is hosted on the same computer
Memory	2 GB minimum 4 GB RAM minimum, if the MDB is hosted on the same computer
Disk Space	30 GB minimum 100 GB minimum, if the MDB is hosted on the same computer The required disk space for the MDB must be available in the disk partition where the MDB is located. Allow additional space for the Software Package Library. The total space requirement depends on the number and size of packages to be stored
NIC	100 Mbps or higher

Scalability Server Specifications

We recommend the following hardware prerequisites for a DSM scalability server and apply to all supported Windows, RedHat, and SuSE operating environments:

Component	Speed/Size
CPU	1 x 2 GHz
Memory	2 GB minimum
Disk Space	30 GB
NIC	100 Mbps or higher

Agent Specifications

We recommend the following hardware prerequisites for a DSM agent and apply to all supported agent operating environments:

Component	Speed/Size
CPU	1 x 2 GHz
Memory	256 MB minimum
Disk Space	300 MB minimum
NIC	10 Mbps or higher

DSM Explorer Specifications

We recommend the following hardware prerequisites for the DSM Explorer and apply only to the supported Windows operating environments:

Component	Speed/Size
DVD-ROM Drive	Any
CPU	1 x 2 GHz
Memory	2 GB minimum
Disk Space	30 GB
NIC	100 Mbps or higher
Display Adapter	Minimum resolution of 1024x768

Specifications for an SQL Server MDB on Windows

We recommend the following hardware prerequisites for a Microsoft SQL Server management database (MDB) on Windows:

Component	Speed/Size
DVD-ROM Drive	Any
CPU	2 x 2 GHz or better
Memory	4 GB minimum
Disk Space	100 GB minimum
NIC	100 Mbps or higher

Specifications for an Oracle MDB on Sun Solaris

The following hardware prerequisites are minimum requirements when installing more than one instance of an Oracle MDB on a computer running Sun Solaris:

Component	Speed/Size
DVD-ROM Drive	Any
CPU	2 SPARC processors with 1.5 GHz or better
Memory	For each configured Oracle database instance, allow a minimum of 3.2GB (SGA: 2.7GB, PGA: 0.5GB) of main memory. We recommended this for an installation with up to 10,000 computer assets.
Disk Space	100 GB minimum
NIC	100 Mbps or higher

Chapter 2: CA ITCM Upgrade Considerations and Known Issues

This section contains the following topics:

General Considerations

CA ITCM r12 SP1 supports upgrades from the following products and versions:

- For manager components, the upgrade is supported from:
  - CA ITCM r12
  - Unicenter Desktop and Server Management (Unicenter DSM) r11.2 SP4
- For scalability server and agent components, the upgrade is supported from Unicenter DSM r11.2 and above.
- For computers running r11.1 agent, direct upgrade to CA ITCM r12 SP1 is supported from:
  - Unicenter DSM r11.1 - HP agent
  - Unicenter DSM r11.1 - Solaris agent
  - Unicenter DSM r11.1 - AIX agent
- For new CA ITCM components, the upgrade is supported from:
  - Unicenter Asset Intelligence r11.2 incremental patch 1
  - Unicenter Asset Intelligence r11.2 cumulative patch 1
  - CA Asset Intelligence r12
  - Unicenter Patch Management r11.2
  - CA Patch Manager r12
  - CA DMM r11.1
  - CA DMM r12
  - CA DMM r12.1

Web Console and Web Services

From this release, Web Console and Web Services support IIS 7.0. However, the default installation of IIS 7.0 does not install the components required to run Web Console and Web Services.

Install *Internet Server Application Program Interface* (ISAPI) Extensions and Filters before you install Web Console and Web Services.

Upgrade Process

This release of CA ITCM supports a strict top-down upgrade strategy. The order in which you perform the upgrade of components is important and should be performed as follows:

1. Phase 1: Upgrade the DSM enterprise manager
2. Phase 2: Upgrade the DSM domain manager
3. Phase 3: Upgrade the DSM scalability servers
4. Phase 4: Upgrade the DSM agents

After each upgrade phase the configuration is fully functional, that is, the upgraded components can communicate with components not yet upgraded.

Note: For more information about upgrading and the steps within the above phases, see the Upgrading Process section in the "Upgrading and Migration Considerations" chapter of the *r12 Implementation Guide*.

Upgrading from r12 with CCS Installed

If you are upgrading from CA ITCM r12 to r12 SP1 and you are using CCS, you will need to apply additional patches to CCS if you want to upgrade your database to Microsoft SQL Server 2008 or your operating system to Windows 2008. Please check the relevant knowledge document for details or contact CA Technical Support.

Upgrading in Oracle MDB Environments

Before upgrading from CA ITCM r12 to r12 SP1 in an Oracle MDB operating environment, you must ensure that the ORACLE_HOME variable is set in the environment of the root user. To set this variable, perform the following steps:

1. At the command prompt, enter the following command:

   export ORACLE_HOME=<*folder of your Oracle installation*>

   Example:

   export ORACLE_HOME=/oracle/product/10.2.0/Db_1

2. Run r12 SP1 setup and choose the upgrade option.

Chapter 3: Asset Management Changes and Enhancements

This section contains the following topics:

Changes and Enhancements

Asset management, as a part of this CA ITCM release, now supports the following:

- Non Resident Inventory (NRI) on Linux and UNIX operating environments (see page 31)
- Device Compliance Scanner (DCS) (see page 33)

The following sections describe the NRI and DCS installation and configuration instructions for this release.

NRI on Linux and UNIX Operating Environments

This release of CA ITCM supports NRI on Linux and UNIX operating environments in addition to the existing support for Windows operating environments.

The NRI solution provides a simple way to inventory a Windows, Linux, or UNIX computer without having to deploy the CA ITCM agent (DSM agent).

The NRI solution is based on existing CA ITCM inventory components. It provides the same robust discovery capability that the installed agent-based discovery does, but works on computers without any CA software installed prior to or after the inventory scan has been performed.

Launch NRI from Linux or UNIX Computer

You cannot launch NRI on Linux or UNIX from the NRI website. NRI on these operating environments is designed to run with minimum requirements. The distribution of the NRI agent and analysis of the collected result is done manually.

To launch NRI from a Linux or UNIX computer

1. From the command shell, go to:

   <dvd_root>/*ProductFiles_x86*/nriagent/nriagent.tar

   Note: The nriagent.tar file is located under the platform specific folder. You can also copy it to any shared location and launch the NRI.

2. Extract the file to any location using the command:

   ```
   tar –xf nriagent.tar
   ```

   The files are extracted to the folder *nriagent*.

3. To register a computer, run the script:

   ```
   ./cmnriagent –script register.ini
   ```

   An inventory file is created to register the computer.

4. NRI allows you to perform two types of inventory:

   - Basic hardware inventory and heuristic software scan
   - Full hardware inventory and software signature scan.

   To perform a basic hardware inventory and heuristic software scan, run the script:

   ```
   ./cmnriagent –script basic.ini
   ```

   To perform a full hardware inventory and software signature scan, run the script:

   ```
   ./cmnriagent –script adv.ini
   ```

   Note: To use additional inventory modules, create a customized .ini file and copy it to the nriagent folder. For more information see the *r12 Asset Management Administration Guide*.

   The inventory starts and an inventory report is created in the *nriagent* folder and is named after the generated host UUID on the computer, for example, 12FDBEBA-572D-4408-BFC8-E7922AD4A998.xiu.

5. Copy the inventory report to one of the AssetCollectorCollect folders belonging to a running Asset Collector.

   The Asset Collector detects the new inventory file and extracts the asset inventory information.

Note: For more information about Asset Collector, see the Asset Collector section in the "Customizing Asset Management" chapter in *r12 Asset Management Administration Guide*.

Introduction to Desktop Compliance Scanner

DCS performs an automated evaluation on the target computers based on checklists that the National Institute for Standards and Technology (NIST) has created using the Secure Content Automation Protocol (SCAP), and is included as a part this CA ITCM release.

The CA ITCM r12 SP1 installer includes all the FDCC checklists released by NIST at the time of this release. The scanner can also perform a compliance check on any other valid SCAP data stream. You can configure the scanner to perform a compliance check on additional or custom checklists.

DCS is fully compatible with the previous versions of FDCC checklists, and the checklists can be used to perform compliance checks.

Checklists Bundled with This Release

The following checklists are bundled with this release:

- Windows XP checklist
- Windows Vista checklist
- Windows XP Firewall checklist
- Windows Vista Firewall checklist
- IE7 checklist

For more information about these checklists, go to http://nvd.nist.gov/.

Note: If the checklists are valid SCAP data streams, the scanner can also process additional checklists.

How Checklists Are Distributed

When DCS scans an agent computer, it requires the checklists to be present on the agent computer. The following process explains how the checklists are distributed automatically to the agent computers and the actions to take for the automatic distribution of the checklists:

1. When DCS is installed on the domain manager, the installer copies the checklists to the *ITCM_installpath*\SCAP_Checklists directory on the domain manager.

   Note: If you have additional or custom checklists, manually copy them to the SCAP_Checklists directory.

2. The DSM engine runs the Default SCAP Checklist Processing Job to perform the following tasks:

   - Monitor the SCAP_Checklists directory in the domain manager for new or updated checklists
   - Package the new or updated checklists in compressed archive files, digitally sign them to prevent data tampering, and save them under the \Documents and Settings\All Users\Application Data\CA\scap_checklists directory.
   - Update the MDB with the list of the new and updated checklists

3. The DSM engines run the engine collect task to push the compressed archive files of the new or updated checklists to the scalability servers.

4. The agent runs the hardware inventory collect task that is configured to scan the checklists, pulls the compressed archive files of the new or updated checklists from the scalability server, and stores them on the agent computer.

5. The agent verifies the signature on the compressed archive files. If it is unable to verify the signature, a log entry is added to the TRC_AMAGENT*.log file.

   If the signature verification failed because of a change in the DSM basic host identity certificate, redistribute the checklist files.

Note: When new versions of checklists are available in the SCAP_Checklists folder, the domain manager distributes the checklists throughout the CA ITCM environment. However, only one version of a checklist will be distributed at any given time. For example, you cannot have versions 1.1.1.0 and 1.2.1.0 of the Windows XP checklist distributed by the automatic checklist distribution process.

Basic Host Identity Certificate for Signing the Compressed Checklists

The digital signature of the compressed checklist files is created using the DSM basic host identity certificate, also referred to as dsmcommon. The generated signature is sent with the compressed checklist file to the scalability server, from where the asset management agent retrieves the checklist files when running a DCS scan. The agent then verifies the signature on the compressed checklist files and proceeds with the scan only if the signature verification is successful.

Redistribute the Checklists When the Certificate Changes

If the basic host identity certificate changes after the checklist has been signed and distributed, the verification of the signature on the agent will fail and the configured DCS inventory module will not run. To resolve this problem, alter the version of the checklist so that it will be redistributed with a newly generated signature to the scalability server and the Asset Management agent computer.

To redistribute the checklists when the certificate changes

1. Open the *checklist*_xccdf.xml file on the domain manager and locate the <version> tag.
2. Change the version number to enable the redistribution of the checklist.

   Note: Specify an earlier version number as this reduces the chances of a version number conflict when a new checklist is released.
3. Save the XCCDF file.
4. Open the DSM Explorer and run the Default SCAP Checklist Processing Job so that the modified checklist is compressed and signed.

   The checklist is now ready for redistribution to the scalability server.

How DCS Works

DCS is implemented as an Asset Management inventory detection module. You can configure this inventory detection module as part of a hardware inventory collect task. The following process helps you understand how the scanner works and the actions to take for the working of the scanner:

1. During DCS installation on the domain manager, the installer creates inventory detection modules for each of the checklists. For additional or custom checklists, create new inventory detection module definition.
2. Configure one or more hardware inventory collect tasks to schedule the scan and collect the results from the FDCC inventory detection modules. You can create a new collect task or modify the existing one to schedule the scan.
3. When the collect task runs at the agent computer, the scanner starts the scan based on the checklists available on the agent computer. Each checklist has an SCAP data stream. An SCAP data stream consists of the following files:
   - An eXtensible Configuration Checklist Description Format (XCCDF) file that defines a set of rules
   - One or more Open Vulnerability and Assessment Language (OVAL) files that specify how to check for compliance, using the rules defined in the XCCDF file
   - (Optional) A Common Platform Enumeration (CPE) dictionary file that specifies how to check whether the target computer has the required operating environment or applications. For example, if the checklist is for Windows XP, the CPE dictionary file specifies how to check whether the target computer has Windows XP.
4. The scanner parses the rules in the XCCDF file and invokes an OVAL interpreter to evaluate the OVAL definitions referenced in the SCAP data stream.
5. The interpreter produces OVAL result files that contain the values for each OVAL definition.
6. The scanner then reads the result files and determines the outcome of compliance check for each rule in the checklist and produces the following files:
   - XCCDF compliant test result file in the XML format
   - Asset Management inventory file

   Note: All the result files are stored in a subdirectory under the asset management agent's working directory.
7. The information in the inventory file is stored in the management database (MDB), and the results of the scan are displayed in the DSM Explorer and Web Console. You can create queries and reports based on this inventory information just as you do with any other inventory data.

Collection of Result Files from the Agent Computer

The scanner stores the XCCDF and OVAL result files on the agent computer by default. You can configure the FDCC inventory detection modules to enable the collection of result files from the agent computer to the scalability server. When the engine runs the collect task next time, it collects the result files from the scalability server and stores them on the domain manager. Storing the result files on the domain manager helps you manage them centrally and retrieve the files quickly when required.

Note: The result files are signed with a digital signature to prevent data tampering between the agent and the manager. If the manager is unable to verify the signature, an event is raised and logged in the default event log.

Installation of DCS

The following sections describe the installation of DCS on the manager and agent computers.

Install DCS on a Manager

DCS, as a part of this CA ITCM release, is integrated into the CA ITCM r12 SP1 installer. When you install Asset Management on the manager, the DCS management capabilities are installed but not the DCS itself.

The option to install DCS is available during the custom installation of CA ITCM.

To install DCS on a manager

1. Start the CA ITCM setup from the installation media. Follow the installation wizard until you reach the Select Product Functionality page.
2. Select Asset Management, and click Next.

   The Select Installation Method page appears.
3. Select Custom Installation, and Click Next.

   The Select Features page appears.
4. Select Domain Manager, Device Compliance Scanner for Asset Management, and click Next.
5. Follow the instructions in the installation wizard and complete the installation.

   DCS is installed as a part of CA ITCM installation.

Install DCS on Agents

Depending on your deployment size, you can choose one of the following methods:

- Install DCS manually on each agent computer
- Create a deployment job that targets multiple agent computers
- Create a software delivery job that can be pushed to multiple agent computers

Install DCS on Agents Manually

To install DCS on a few agent computers, install DCS manually on each of them.

To install DCS on agent computers manually

1. Start the CA ITCM setup from the installation media. Follow the installation wizard until you reach the Select Product Functionality page.
2. Select Asset Management, and click Next.

   The Select Installation Method page appears.
3. Select Custom Installation, and Click Next.

   The Select Features page appears.
4. Select Agent, Device Compliance Scanner for Asset Management, and click Next.
5. Follow the instructions in the installation wizard and complete the installation.

   DCS is installed as a part of CA ITCM Asset Management Agent installation.

Install DCS Using Infrastructure Deployment Package

If your deployment size is large, you can install DCS using the DCS infrastructure deployment package. The package is added automatically to the deployment package library when you select DCS option during the domain manager installation. Deploying the DCS package is similar to deploying any other package. For more information about deploying packages, see the *DSM Explorer* online help.

Install DCS Using the Software Delivery Package

If you have installed software delivery and your deployment size is large, you can use the DCS package. The DCS package is registered automatically in the software delivery library during the domain manager installation. Deploying the DCS package is similar to deploying any other software delivery package. Before you begin the deployment, ensure that you have the software delivery agent installed on the target agent computers. For more information about deploying software delivery packages, see the *r12 Software Delivery Administration Guide*.

Upgrade DCS

The following upgrade scenarios are possible:

- You are upgrading from the r11.2 SP4 or r12 versions of CA ITCM with the NIST-SCAP patch installed.
- You are upgrading from the r11.2 SP4 or r12 versions of CA ITCM without the NIST-SCAP patch installed.

Upgrade with the NIST-SCAP patch installed

Start the CA ITCM r12 SP1 upgrade (see page 28), the installer detects the existing scanner, and automatically selects DCS for upgrade.

Upgrade without the NIST-SCAP patch installed

Complete CA ITCM upgrade and manually install DCS (see page 37).

Note: If you upgrade from CA ITCM r12 with the NIST-SCAP patch installed, the latest FDCC 1.2.1.0 inventory detection modules are not enabled automatically. To use the latest inventory detection modules, clear the existing SCAP detection modules which are a part of the inventory configuration and select the relevant FDCC 1.2.1.0 versions.

Repair DCS Installation

If you delete any of the installation files, you can repair the DCS installation.

To repair the DCS installation

1. Open a Command Prompt window and change the directory to <install-dir>:\Program Files\CA\SharedComponents\installer\bin
2. Run the following command:

   lsm -i CA DSM Agent AM Device Compliance Scanner plugin.Any.@pif

   A confirmation message appears, and the DCS installation repair is complete.

Disable the Scanner

You can disable the scanner module if you do not want to perform the FDCC compliance check on the agent computers.

Note: Perform these steps only if you have configured your collect tasks for the FDCC inventory modules.

To disable the scanner

1. In the DSM Explorer, navigate to Control Panel, Configuration, Collect Tasks, Hardware Inventory.

   The existing hardware inventory collect tasks appear.

2. Right-click the collect task that you want to modify to disable the FDCC inventory modules and select Properties.

   The Properties for Collect Task Name dialog appears.

3. Click the Detection Modules tab, clear the FDCC inventory detection modules check boxes, and click OK.

   The FDCC inventory scan is disabled.

Chapter 4: Configure the Scanner

The following sections describe the steps to configure the scanner for inventory.

This section contains the following topics:

Configure the Collection of Test Result Files

The XCCDF and OVAL test result files are stored in a subdirectory under the Asset Management agent's working directory. To collect these files after the scan and store them centrally in the domain manager, configure the DCS inventory detection modules to enable the automatic collection of the result files.

Note: Typically, the default inventory detection modules do not require further configuration, other than the configuration to collect test result files. To configure other parameters in the inventory detection module, see the description of each parameter in the Creating Inventory Detection Modules for Additional Checklists (see page 44) section.

To configure the collection of test result files

1. Navigate to Control Panel, Configuration, Inventory Detection Modules.

   The new DCS inventory detection modules appear with the other inventory detection modules.

2. Double-click the inventory detection module you want to configure.

   The Properties for *Module Name* dialog appears.

3. Click the Launch button on the Configuration tab.

   The SCAP Configuration dialog appears with the default configuration.

4. Select the following check boxes in the General tab:

   - Collect XCCDF Result File
   - Collect OVAL Result Files

   Note: The OVAL test result files can be huge in size. If you do not have specific reasons for storing them on the domain manager, you can collect only the XCCDF result files.

5. Click OK.

   When the collect task runs again, the engine collects the test result files and stores it on the domain manager.

   Note: The result files are signed with a digital signature to prevent data tampering between the agent and the manager. If the manager is unable to verify the signature, an event is raised and logged in the default event log.

6. (Optional) Execute the following command to store the result files in a non-default directory. By default, the result files are stored under the *ITCM_installpath*\SCAP_Result_Files directory in the domain manager:

   ccnfcmda -cmd SetParameterValue -ps itrm/am/scapft -pn resultfilelocation -v "*Directory_path*"

   Directory_path

   Specifies the path to the directory on the domain manager under which you want to store the result files.

   Note: The path must contain a trailing backslash, for example, c:\anotherDirectory\.

   For the change to take effect, use the "caf stop amSCAPPlugin" command to stop the plug-in amSCAPPlugin , and use the "caf start amSCAPPlugin" command to restart the plug-in.

   When the collect task runs again, the engine collects the test result files and stores them in the directory specified.

Configure Hardware Inventory Collect Tasks to Collect DCS Inventory

To schedule the FDCC checklist scan and collect the test results, configure a hardware inventory collect task.

Note: If you have multiple hardware inventory collect tasks, decide whether you want to schedule the checklist scan on all of them or only on a selected few. For example, if you have grouped all your Windows Vista computers and created a specific collect task for the group, you can configure the collect task for WinVista, VistaFirewall, and IE7 checklists. However, even if you configure the checklists on all computers, the scanner will scan only those computers that meet the OS requirement.

To configure the hardware inventory collect task

1. In the DSM Explorer, navigate to Control Panel, Configuration, Collect Tasks, Hardware Inventory.

   The existing hardware inventory collect tasks appear.

2. Right-click the collect task that you want to configure and select Properties.

   The Properties for *Collect Task Name* dialog appears.

3. Click the Detection Modules tab, select the DCS inventory detection modules, and click OK.

   The changes are saved. When the collect task runs next time, it will collect the scan results for the configured checklists.

Additional SCAP Data Streams

In addition to the checklists bundled with this patch, the scanner can scan any valid SCAP data stream. The additional SCAP data stream can be a new or an updated FDCC checklist, a custom checklist, or an SCAP data from any source.

How to Configure Additional SCAP Data Streams

CA ITCM r12 SP1 can distribute additional SCAP data streams to the target agent computer automatically. Configuring additional SCAP data streams for automatic distribution involves the following tasks:

1. Copying the SCAP Data stream to the domain manager (see page 44)
2. Creating Inventory Detection Modules for Additional Checklists (see page 44)
3. Configuring the Hardware Inventory Collect Task (see page 43)

Copy the SCAP Data Stream to the Domain Manager

The checklist files (SCAP data stream) that you want DCS to scan must be available in a specific directory in the domain manager. The DSM engine checks this directory for new or updated checklists when it runs the Default SCAP Checklist Processing Job.

Copy the SCAP data stream to the *ITCM_installpath*\SCAP_Checklists directory in the domain manager.

Note: You must place all the files belonging to an SCAP data stream or checklist in the directory under the SCAP_Checklists directory.

Create Inventory Detection Modules for Additional Checklists

For each additional checklist that you want the scanner to scan, create an inventory detection module. The scanner uses the configuration information provided in the inventory detection module to perform the compliance check for the given checklist.

To create inventory detection modules for additional checklists

1. In the DSM Explorer, navigate to Control Panel, Configuration, Collection Modules, Inventory Detection Modules.

   The existing detection modules appear in the right pane.

2. Right-click Inventory Detection Modules folder and click New from the Context menu.

   The Create New Inventory Module dialog appears.

3. In the General tab, specify the inventory module name. Specify a name that represents the checklist name.

   In the Configuration tab, click the ellipsis (…) against the Tool field and select gui_am_scapcfg.exe under the *ITCM_installpath*\bin directory.

4. Click Launch.

   The SCAP Configuration dialog appears.

   Note: You can either use the tool to configure the checklists or enter the parameters manually in the text field provided in the Configuration tab. For more information about the parameter names and their descriptions, see the appendix SCAP Configuration Parameters (see page 125).

5. Specify the following information in the General tab:

   Note: If you have exported an SCAP configuration earlier, you can import the configuration file to fill in the information in the respective fields.

   Data Stream Path

   Specifies the path to the SCAP data stream directory on the agent computer. This path must match the SCAP data stream directory on the domain manager. For example, for the IE7 checklist, specify FDCC-Major-Version-1.2.1.0\ie7. When the checklist is distributed to the agent computer, a similar directory structure is created under the *ITCM_installpath*\Agent\units\00000001\UAM\ SCAP_Content directory on the agent computer.

   XCCDF File Name

   Specifies the name of the XCCDF file in the SCAP data stream that determines the compliance benchmark.

   Note: This file must be present in the location specified in the Data Stream Path field.

   XCCDF Id

   Specifies the ID given against the Benchmark tag in the XCCDF file. For example, the benchmark ID for Windows XP checklist is FDCC-Windows-XP.

   CPE Dictionary File Name

   (Optional) Defines the name of the CPE dictionary file. If the SCAP data stream contains a dictionary file, specify the file name against this parameter; otherwise, you can omit this parameter.

   Note: The file must be present in the location given in Data Stream Path field.

   Inventory Node Name

   Defines the component name to use in the inventory file produced by the scanner. This value is used as the top-level group name in the inventory file and hence also appears as the inventory component name under the Inventory, SCAP category in the DSM Explorer.

   Collect XCCDF Result File

   Configures the collection of XCCDF result files for the checklist from the Asset Management agent's working directory to the domain manager.

   Collect OVAL Results Files

   Configures the collection of OVAL result files for the checklist from the Asset Management agent's working directory to the domain manager.

6. In the Advanced tab, specify the values for the following fields:

   XCCDF Profile

   Defines the title of the XCCDF profile to be applied for the compliance check. Selecting Default from the drop-down list lets the scanner use the first available profile in the XCCDF file. Selecting Other lets you specify the profile title in the text field. Selecting None applies no profile and uses all the settings in the XCCDF file.

   Output Path

   Defines the directory in which the OVAL and XCCDF result files are to be placed. You can either specify an absolute path or a path relative to the SCAP_Result_Files directory, which is under the Asset Management agent's working directory. If this field is empty, the files are stored under the default path, which is *agent working directory*\SCAP_Result_Files*Data Stream Path*.

   Note: The user account that runs the scan must have write access to the directory specified in this field.

   OVAL Interpreter Path

   Defines the directory on the agent computer that contains the Ovaldi interpreter. You can specify either an absolute path or a path relative to the bin directory of the agent installation. The OVAL interpreter shipped with this release of CA ITCM is installed under the *ITCM_installpath*\bin\ovaldi-CA directory. If your SCAP data stream requires an OVAL interpreter other than the one shipped with this release, ensure to distribute the OVAL interpreter to all the agent computers and specify the path in this field.

   Default: *ITCM_installpath*\ovaldi-CA

   Organization

   (Optional) Defines the name of the organization that you want the <*organization*> tag to contain in the XCCDF result file. Specify the organization name and click Add to List.

   Note: You can add any number organizations and move them in the order that you want. The values are hierarchical with the highest level appearing first.

7. In the Platforms tab, select Windows 32 bit, click Win32 generic, and then enter **amiscap.exe** in the text field next to the option button.

8. Click OK.

   The inventory detection module for the configured checklist is created and appears under the Inventory Detection Modules folder. Configure one or more hardware inventory collect tasks to include the new inventory detection modules.

Export the SCAP Configuration

You can export the configuration information from the SCAP Configuration dialog to a .CFG file. You can use this file to import the configuration information into the SCAP Configuration dialog when creating inventory detection modules for the custom or additional SCAP data streams.

To export the SCAP configuration

1. Double-click the DCS inventory detection module, the SCAP configuration of which you want to export.

   The Properties for Module Name dialog appears.

2. In the Configuration tab, ensure that it uses the gui_am_scapcfg.exe configuration tool.

3. Click Launch.

   The SCAP Configuration dialog appears with the existing configuration.

4. From the System Menu icon in the top-left corner of the dialog, select Export Configuration.

   The Save As dialog appears.

5. Specify the file name and click Save.

   The configuration is exported to a file in the location you specified.

Import an SCAP Configuration

When you are creating inventory detection modules, you can import information from an SCAP configuration file into the SCAP Configuration dialog. Importing the SCAP configuration fills in the configuration details in the respective fields in the SCAP Configuration dialog.

To import an SCAP Configuration

1. In the SCAP Configuration dialog of the new inventory module, select Import Configuration from the System Menu icon in the top-left corner of the dialog.

   The Select File to Import dialog appears.

2. Select a valid SCAP configuration file, and click Open.

   The configuration information is imported into the respective fields in the SCAP Configuration dialog.

   Following is the content of a sample SCAP Configuration file:

```
[SCAP]
SCAPPath=FDCC-Major-Version-1.2.1.0\ie7
XCCDFFile=fdcc-ie7-xccdf.xml
XCCDFID=fdcc-ie-7
CPEDictionary=fdcc-ie7-cpe-dictionary.xml
InvComponent=$SCAP$FDCC IE7
CollectXCCDFResultFile=false
CollectOVALResultFiles=false
OvaldiPath=ovaldi-ca
```

Chapter 5: Working with the Scanned Results

The following sections describe the reports generated by DCS and the instructions to view them.

This section contains the following topics:

Results Reported by the Scanner

After the compliance check, the scanner reports the following results for each rule in the XCCDF file:

Pass

Indicates that the computer has passed the compliance check for the selected rule.

Fail

Indicates that the computer has failed the compliance check for the selected rule.

Error

Indicates that there was an error while performing the compliance check for the selected rule.

Not Checked

Indicates that the rule does not contain a check defined, making it impossible for the scanner to perform a compliance check for it.

Unknown

Indicates that the characteristics being evaluated cannot be found or the characteristics can be found but collected object flag is "not collected".

Not Applicable

Indicates that the rule is not applicable to the operating environment installed on the agent computer.

View Scan Results

You can view the scan results to see if an agent computer passed or failed the compliance check. The results display against each rule in the XCCDF file. The DSM Explorer and the Web Console present the scan results in an easy-to-read format. You can also open the XCCDF and OVAL test result files to view the results of the scan.

To view the scan results from the result files

Navigate to the following directory to view the XCCDF and OVAL test result files:

- *agent working directory*\SCAP_Result_Files on the agent computer
- *ITCM_installpath*\SCAP_Result_Files on the domain manager if you have configured the collection of test result files

  Note: The paths mentioned above are the default locations of the test result files.

To view the scan results from the GUI

1. Navigate to Computers and Users, All Computers, Computer Name, Inventory, SCAP, Inventory Component Name.

   Note: Inventory Component Name is the value you specified for the Inventory Node Name field in the SCAP Configuration dialog when you created the inventory detection module.

   The inventory information collected is displayed under respective groups.

2. Expand each category to view more details of the scan.

   The inventory is displayed under the following categories:

   Detailed patch results

   Provides detailed information about each patch result. The details include the OVAL ID, result, and the CVE reference information such as CVE ID, CVE URL, and the NVD URL. You can right-click a URL and select Browse to go to the URL.

   General

   Provides information regarding the configuration used to perform the scan such as, the name of the XCCDF file against which the scanner performed the compliance check, the profile used, and so on. This category also provides details about the user account that performed the scan.

Patch results overview

Provides an overview of all the patch results in a single pane. You can sort or filter any column.

Rule Results

Lists all the results and the weight age against each rule in the XCCDF file. It also provides any reference information defined for each rule.

Rule Results Overview

Provides the results for all the rules in the checklist in a single pane. You can sort or filter any column.

Scores

Provides the scores based on the scoring models defined in the XCCDF file. For FDCC checklists, the scoring models are default and flat.

Set Values

Lists the values used during the scan for each of the variables defined in the XCCDF file.

Status

Provides information regarding the status of the scan. If the scan could not be completed, the status attribute indicates the reason for failure. The scanner cannot complete the scan if the benchmark does not apply to the operating environment on the agent computer or due to an error in the XCCDF file or one of the OVAL files. This category also provides details about the SCAP data stream used as an input, and the results generated as output files.

Summary

Provides a quick summary of the scan. This category indicates the number of rules the computer has passed or failed. It also displays the number of rules that resulted in error, not applicable, not checked, and so on.

Target

Displays the name of the target computer on which the compliance check was performed. This is typically the name of the agent computer.

Queries and Reports

You can create queries or reports based on the results produced by DCS, just as you do with any other inventory data. For more information on queries and reports, see the *DSM Explorer* online help and *DSM Reporter* online help.

Predefined Report Templates

The DSM Reporter provides the following CA ITCM r12 SP1 predefined report templates for DCS scan results:

SCAP Scan Summary

Reports the summary of the scan results for each computer in the domain manager.

Flat Score

Reports flat score results for each computer in the domain manager.

Rule Results Overview

Reports the scan results for all the rules in a checklist for a particular computer. This report invokes a runtime query that lets you filter the computers for which you want to view the rule results overview.

Patch Results Overview

Reports the scan result for all the patches in a checklist for a particular computer. This report invokes a runtime query that lets you filter the computers for which you want to view the patch results overview.

SCAP Input Files Information

Reports the details of the input files (SCAP data stream) used in a particular computer for DCS scan. This report invokes a runtime query that lets you filter the computers for which you want to view the input files information.

SCAP Output Files Information

Reports the details of the result files produced by DCS scan on a particular computer. This report invokes a runtime query that lets you filter the computers for which you want to view the output files information.

Troubleshooting the Errors Reported

Following are some of the ways to resolve the errors reported by the scan:

- In the DSM Explorer, navigate to *Computer Name,* Inventory, SCAP, *Checklist Name,* Status. The Status attribute in the right pane displays the reason why the scan resulted in an error. This attribute can reveal errors such as, benchmark not being applicable to the operating environment, errors in XCCDF file, or OVAL file.
- You can investigate the rule errors by examining the output from the OVAL interpreter, which contains the results of each OVAL definition used by the checklist. To investigate the rule errors, do one of the following:
  - View the *MachineName-fdcc-checklistname*-oval-ovaldi-stdout.txt file under the *agent working directory*\SCAP_Result_Files directory.
  - View the *MachineName-fdcc-checklistname*-oval-ovaldi-stdout.txt file under the *ITCM_installpath*\SCAP_Result_Files*checklistname**version_number* directory on the domain manager if you have configured the collection of OVAL test result files.
- You can set the trace level to detail using the following command and investigate the Asset Management log files for any errors generated by the scan:

  ```
  cftrace -c set -f UAM -l DETAIL
  ```

  Check the log files generated by the scanner for more details.

DCS Log Files

DCS logs are added to the following log files on the agent computer:

TRC_UAM_*.log

Contains the logs related to compression and decompression of the checklist files, creation and verification of the signatures for the checklist files, and the actual checklist processing.

TRC_AMAGENT*.log

Contains the logs related to compression and decompression of the checklist files, creation and verification of the signatures for the checklist files, and the actual checklist processing.

TRC_AMRAPI*.log

Contains the logs related to the transfer of checklist files and result files to and from the agent.

On the Manager, DCS scanner logs are added to the following file:

TRC_AMSCAP_FTPLUGIN*.log

Contains the logs related to the transfer of XCCDF result files, OVAL result files, and compressed checklist files to and from the DSM engine.

The log files are available under *ITCM_installpath*\logs directory. Apart from these logs, the scanner also saves the output of running the OVAL interpreter for each OVAL file in an *ovalfilename*-ovaldi-stdout.txt file under the checklist output directory on the agent computer.

Implementation of SCAP Standards

The following sections describe the implementation of SCAP standards.

SCAP

DCS is built around Security Content Automation Protocol (SCAP). SCAP is a suite of selected open standards that enumerate software flaws, security-related configuration issues, and product names; measure systems to determine the presence of vulnerabilities; and provide mechanisms to rank (score) the results of these measurements to evaluate the impact of the discovered security issues.

CA ITCM implements compliance checking of any SCAP 1.0 data stream written in the XML formats leveraged by the SCAP standard: XCCDF, CCE, CVE, CPE, CVSS, and OVAL. DCS is implemented as an asset management inventory module. DCS is distributed to all the agents, which then performs the compliance check at the scheduled time and produces the output files required by the specifications. It uses the XCCDF and OVAL assessment protocols to determine what items to check and how to check them. It also uses the CPE, CCE, CVSS, and CVE reference protocols to verify that all rules are accurately and appropriately reflected in the system. The scanner reports the results to the central management database for inspection, reporting, and querying. The result files are generated for each file in the input SCAP data stream and are stored on the agent computer and domain manager (if configured) for verification.

XCCDF

eXtensible Configuration Checklist Description Format (XCCDF) is a specification language for writing security checklists, benchmarks, and related kinds of documents. An XCCDF document represents a structured collection of security configuration rules for a set of target computers. The specification is designed to support information interchange, document generation, organizational and situational customization, automated compliance testing, and compliance scoring.

DCS reads the XCCDF file and scans the target computers based on the rules given in the XCCDF file and provide the results for each rule. The XCCDF output file is stored in the agent's working directory on each agent computer. The results for each rule and the final scores are displayed in the DSM Explorer under Inventory, SCAP, Checklist Inventory Component, Rule Results.

You can view the name and location of the XCCDF files and processed result files in the DSM Explorer under Inventory, SCAP, Checklist Inventory Component, Status group.

OVAL

Checklist rule definitions in XCCDF files typically use references to OVAL definitions in OVAL files to indicate how to check a target computer for compliance with the rule. Similarly, CPE Names listed in CPE dictionary also use references to OVAL definitions to specify how to check for the presence of the software indicated by the name. All the bundled DCS SCAP data streams contain at least one OVAL file for each of these purposes.

For each evaluated OVAL file, the OVAL interpreter produces an OVAL results file in the agent's working directory. You can view the name and location of all the OVAL files and processed result files in the DSM Explorer under Inventory, SCAP, Checklist Inventory Component, Status group.

CCE

Common Configuration Enumeration (CCE) provides unique identifiers to system configuration issues to facilitate fast and accurate correlation of configuration data across multiple information sources and tools. For example, CCE Identifiers can be used to associate checks in configuration assessment tools with statements in configuration best-practice documents.

In a SCAP data stream, references to CCE IDs may be present in either the XCCDF file or the OVAL files. In the XCCDF file, the CCE reference takes the form of <ident> tags listing CCE IDs associated with each rule in the list. If the

CCE IDs are present in the XCCDF file, DCS includes these references for each rule result. This information is available both in the produced XCCDF result file and the inventory data sent to the database. In the DSM Explorer, the CCE reference information is available under Inventory, SCAP, Checklist Name, Rule Results, Rule Name, Idents.

In OVAL files there can be CCE IDs associated with each OVAL definition. These are contained in <reference> tags. If such references are present they are included in the OVAL result files produced when processing the OVAL definitions.

All the packaged FDCC checklists packaged with this patch include CCE ID references both in the XCCDF files and the OVAL files. The name and location of the output files can be viewed from the DSM Explorer under the Inventory, SCAP, Checklist Inventory Component, Status group.

CPE

Common Platform Enumeration (CPE) is a structured naming scheme for information technology systems, platforms, and packages. Based upon the generic syntax for Uniform Resource Identifiers (URI), CPE includes a formal name format, a language for describing complex platforms, a method for checking names against a system, and a description format for binding text and tests to a name.

A SCAP data stream may optionally include a CPE dictionary, which maps CPE names to OVAL definitions that test for the presence of the OS or application identified by that CPE name. DCS uses this dictionary when the XCCDF file from the data stream contains <*platform*> tags, which indicate that the XCCDF file requires the presence of the specified CPE name. All the packaged FDCC checklists contain CPE dictionary files and their reference in the XCCDF files. The XCCDF results files contain the CPE names in the <*platform*> tags to indicate a successful platform test for the entire checklist. The name and location of the output files can be viewed from the DSM Explorer under the Inventory, SCAP, Checklist Inventory Component, Status group.

CVSS

CA ITCM r12 SP1 implements the Common Vulnerability Scoring System (CVSS) standard. CVSS provides an open framework for communicating the characteristics and impacts of IT vulnerabilities. Its quantitative model ensures repeatable accurate measurement while enabling users to see the underlying vulnerability characteristics that were used to generate the scores. Thus, CVSS is well suited as a standard measurement system for industries, organizations, and governments that need accurate and consistent vulnerability impact scores. Two common uses of CVSS are prioritization of vulnerability remediation activities and calculating the severity of vulnerabilities discovered on computers. The National Vulnerability Database (NVD) provides CVSS scores for almost all known vulnerabilities.

For every patch or vulnerability CVE ID references are provided in the DSM Explorer. The DSM Explorer provides detailed patch results that contain the CVE URL and the NVD URL. The user can use the URL to visit the NIST's web page for the corresponding CVE ID's entry in their National Vulnerability Database, where the CVSS score and further information about the vulnerability are found. The CVE reference details are available under the Inventory, SCAP, Checklist Inventory Component, Detailed patch results group.

CVE

Common Vulnerabilities and Exposures (CVE) is a list or dictionary that provides standard identifiers for publicly known information security vulnerabilities and software flaws. The compliance check results produced by CA ITCM r12 SP1 includes the relevant Common Vulnerabilities and Exposures (CVE) ID references in the output for every rule checked, provided such references are included in the checklist definition itself. The CVE information is stored in the patch result XML file generated by the scanner and is available in the agent's working directory.

In SCAP data streams, OVAL content meant for the detection of applications, patches, or vulnerabilities contains CVE ID references identifying the exact element in the CVE list. The FDCC checklists for Windows XP, Windows Vista, and IE7 contain separate OVAL files that include CVE IDs and are dedicated to this purpose.

When processing these SCAP data streams, the OVAL result files also include the CVE ID references for each OVAL definition. Additionally, the inventory data presented for the target computer in the DSM Explorer contain a Detailed patch results category where every OVAL definition meant for detecting patches or vulnerabilities has its own subgroup. This subgroup contains a CVE References table wherever the OVAL definition has such references defined in the SCAP data stream itself. Each CVE reference contains CVE URL and NVD URL. The DSM Explorer allows browsing directly to these URLs.

Chapter 6: CA Patch Manager Changes and Enhancements

This chapter describes the changes and enhancements in CA Patch Manager.

This section contains the following topics:

Changes and Enhancements

CA Patch Manager, as a part of this CA ITCM release, now supports the following:

- Installation in the following languages:
  - English
  - French
  - German
  - Japanese
- Oracle 10g Release 2 on Solaris, Solaris 10 (64-bit) operating environment for SPARC, and Microsoft SQL Server 2008 SP1 (Enterprise, Standard) 32- and 64-bit

  Note: The Oracle installation must be case insensitive. An install kit is provided to set up the Oracle MDB on Solaris which can be remotely accessed by CA Patch Manager.

  For a complete list of supported databases, see Supported Databases for the MDB (see page 20).
- Windows Server 2008 SP2 (Enterprise, Standard, Datacenter) 32- and 64-bit

  For a complete list of supported Microsoft Windows operating environment, see Microsoft Windows Operating Environments. (see page 13)
- Independent installation of CA Patch Manager on any computer that has the Web Console and Web Services installed

  Note: You can install CA Patch Manager on any computer which does not CA ITCM Manager installed. However, to enable CA Patch Manager download software patches, you must register CA Patch Manager with CA ITCM (see page 63).
- Installation of CA Patch Manager on computers running Microsoft Cluster

CA Patch Manager, from this release, lets you:

- Edit a roll-up patch (see page 61)
- Uninstall a patch (see page 62), which is outside the patch policy

CA Patch Manager, in this release, does not support the following:

- CleverPath Reporter to generate reports

  Note: Use the DSM Reporter for generating reports.
- UltraSPARC 32-bit and Solaris x86
- Installation on a Solaris or Oracle cluster

The following sections describe the procedures associated with the above changes, including CA Patch Manager installation and upgrade instructions for this release.

Edit Roll-up Patch

Roll-up patch contains the patches released by Microsoft per their "Patch Tuesday" policy that includes only the security patches. The CA Patch Manager content team takes these patches and rolls them into a single patch bundle.

If one of the patches in the roll-up patch results in failure of an application on a computer in your test environment, you can edit the roll-up patch and exclude the patch.

Note: You can only edit full roll-up patches, which are in either Testing or Approved state.

To edit a roll-up patch

1. Click Start, Programs, CA, CA Patch Manager, Launch CA Patch Manager.

   The CA Patch Manager login window appears.

2. Log in as CA Patch Manager administrator, and select the Patches tab.

   The Patches page appears.

3. Select Saved Filter from the Filter By drop-down list, and select either the All Patches – Testing filter or All Patches – Approved option.

   The list of patches appears.

4. Select the patch you want to edit, and click Edit.

   The Custom Roll-up Page appears.

5. Enter any name in the Enter Unique Name Field, select the patch files to be included, and click Next.

   The Summary Roll-up Page appears.

6. Review your selection, and click Finish.

   A copy of the roll-up patch is created and made available for testing under Patch Pending Testing portlet on the Dashboard page.

Uninstall a Patch

CA Patch Manager allows you to uninstall a patch that is outside your patch policy. This option is limited to individual patches that are either in Approved or Testing state, were deployed using the DSM manager, and have an uninstall patch associated with it.

Note: You cannot uninstall roll-up patches because not all patches in the roll-up patch have an uninstall script.

To uninstall a patch

1. Click Start, Programs, CA, CA Patch Manager, Launch CA Patch Manager.

   The CA Patch Manager login window appears.

2. Log in as CA Patch Manager administrator, and select the Patches tab.

   The Patches page appears.

3. Select Saved Filter from the Filter By drop-down list, and select either the All Patches – Testing filter or All Patches – Approved option.

   The list of patches appears.

4. Select the patch you want to uninstall.

   The Patch Details page appears listing all details of the patch.

5. Click Uninstall Patch under Advanced Options in the left pane.

   The Select Targets page appears listing the available target computers and computer groups.

6. Select the targets for deployment, click the arrow to add the target to Selected Targets list box, and click Next.

   The Schedule Deployment page appears.

7. Specify whether you want to deploy the patch immediately or at a later date and time, and click Next.

   The Deployment Options page appears with the default deployment options.

8. (Optional) Select the Override default DSM deployment parameters with these settings check box and change the Execution, Reboot, and Job Timeout parameters, and click Next.

Note: You can click the Load CAPM Defaults button to revert to the default deployment settings.

The Confirm Deployment page appears.

9. Review the collected information and click Finish to approve the deployment.

   When the deployment is approved, the patch is deployed at the scheduled time.

Register CA Patch Manager with CA ITCM

CA Patch Manager can be installed independently on any computer that has the Web Console and Web Services installed. CA ITCM is no longer an installation prerequisite.

However, to enable CA Patch Manager to download software patches, you must register CA Patch Manager with CA ITCM by executing *util.bat* on the computer that has CA ITCM.

To Register CA Patch Manager with CA ITCM

1. Open a Command Prompt window and change directory to <install-dir>\Program Files\CA\SC\CIC\bin
2. Run the following command:

   ```
   util.bat -r UPM 682DCD15-5C94-4321-842D-E3944D3CA000 PMUPM-00000-00000-00001 upmuser_group
   ```

   CA Patch Manager registers with CA ITCM.

Installation and Upgrade

The following sections describe the installation of CA Patch Manager as a stand-alone and on a cluster.

Install CA Patch Manager as a Stand-alone

CA Patch Manager provides a web-based wizard-driven user interface to simplify the patch management process. You can use CA Patch Manager for package creation, patch testing, enterprise deployment, and patch level assurance.

Note: Installation of CA Patch Manager requires a reboot of the computer. Close any open applications before you begin the installation.

To install CA Patch Manager as a stand-alone installation

1. Insert the CA Patch Manager installation media into your drive.

   The Choose Setup Language option appears.

   Note: If the wizard does not appear, run Setup.exe from the root directory on the installation media.

2. Select the desired language, and click OK.

   The Welcome page appears.

3. Click Next on the Welcome page and accept the terms of the Licensing Agreement.

   The Configure Node page appears.

4. Click Next.

   The Select Features page appears.

5. Select the features you want to install, and click Next.

   The UPMAdmin and UPMUser Passwords page appears.

6. Enter the password for the UPMAdmin, UPMUser accounts, and click Next.

   The MDB Database Configuration page appears.

7. Select Database Server Type as Microsoft SQL Server or Oracle, complete all required information, and click Next.

   The CA ITCM Webservice Configuration page appears.

8. Enter the user ID and password to connect to CA ITCM Web Services. This is the administrator ID used to install CA ITCM. Click Next.

   The Install Location page appears with the default installation folder.

   Note: The CA ITCM Server Name field, by default, has the local computer name. If you are installing CA Patch Manager on a computer that does not have CA ITCM, change CA ITCM Server Name to the name of the computer on which you have installed CA ITCM Manager.

9. (Optional) select a different installation folder. Click Next.

   The Start Copying Files page appears listing the selected options and configurations as a summary.

10. Click Next to start installation of the selected components.

    The selected components are installed and you are prompted to reboot the machine.

11. Click Reboot.

    The computer restarts and the installation is complete.

Note: If you are installing CA Patch Manager on a computer that does not have CA ITCM Manager installed, you must register CA Patch Manager with CA ITCM (see page 63) to enable CA Patch Manager download software patches.

More information:

Upgrade Procedure and Considerations (see page 67)

Install CA Patch Manager on a Cluster

CA Patch Manager has no functionality in place to detect system failures and to automatically switch from the active to the passive node in a system failure.

CA Patch Manager can be installed in two modes: either as an Active Patch Manager or as a Passive Patch Manager. The terms "Active" and "Passive" refer to whether the CA Patch Manager is active or passive; they do not refer to the cluster node (which may itself be active or passive).

When installing CA Patch Manager on a cluster, one instance of the CA Patch Manager is installed as the Active Patch Manager and each of the other instances are installed as a Passive Patch Manager.

Note: Installation of CA Patch Manager requires a reboot of the computer. Close any open applications before you begin the installation.

To install CA Patch Manager on a cluster

1. Insert the CA Patch Manager installation media into your drive.

   The Choose Setup Language option appears.

   Note: If the wizard does not appear, run Setup.exe from the root directory on the installation media.

2. Select the desired language, and click OK.

   The Welcome page appears.

3. Click Next on the Welcome page and accept the terms of the Licensing Agreement.

   The Configure Node page appears.

4. Select Enable Recovery Support, select the Node Configuration as Active or Passive, and provide a path to install the configuration data. Click Next.

   The Select Features page appears.

5. Select the features you want to install, and click Next.

   The UPMAdmin and UPMUser Passwords page appears.

6. Enter the password for the UPMAdmin and UPMUser accounts, and click Next.

   The MDB Database Configuration page appears.

7. Select Database Server Type as Microsoft SQL Server, complete all required information, and click Next.

   The CA ITCM Webservice Configuration page appears.

   Note: CA Patch Manager does not support installation on an Oracle cluster.

8. Enter the userID and password to connect to CA ITCM Web Services. This is the administrator ID used to install CA ITCM. Click Next.

   The Install Location page appears with the default installation folder.

9. (Optional) select a different installation folder, and click Next.

   The Start Copying Files page appears listing the selected options and configurations as a summary.

10. Click Next to start installation of the selected components.

    The selected components are installed and you are prompted to reboot the machine.

11. Click Reboot.

    The computer restarts and the installation is complete.

More information:

Install CA Patch Manager as a Stand-alone (see page 64)

Upgrade Procedure and Considerations

You may upgrade CA Patch Manager from r11.2 or r12 to r12 SP1.

Note: Upgrading from versions prior to CA Patch Manager 11.2 is not supported.

Upgrade CA Patch Manager Using a Local MDB

If you have earlier versions of CA ITCM and CA Patch Manager running on the same computer as your SQL Server MDB, you need to perform the following steps on CA ITCM before you can upgrade CA Patch Manager.

To upgrade CA Patch Manager on a local MDB

1. Upgrade to CA ITCM r12 SP1.
2. From the DSM Explorer:
   a. Navigate to *Domain Manager*, Control Panel, Engines, All Engines, SystemEngine.
   b. From the Tasks section, select Link Existing Task.

      The Select Engine Tasks window appears.
   c. Select Default Software Contents Download Job and click OK.

      The job is now linked to the CA ITCM system engine.

      Note: CA ITCM r12 SP1 is compatible only with CA Patch Manager r12 SP1. When you upgrade to CA ITCM r12 SP1, you must also upgrade r11.2 or r12 version of CA Patch Manager to CA Patch Manager r12 SP1.
3. Run the CA Patch Manager r12 SP1 installer on the computer. The installer detects the earlier version of CA Patch Manager and offers to upgrade it for you.
4. Follow the installation wizard to perform the upgrade.

   Note: We recommend a reboot of the computer after the upgrade.

Upgrade CA Patch Manager Using a Remote MDB

If you have earlier versions of CA ITCM and CA Patch Manager using a Microsoft SQL Server MDB that resides on a remote computer, you need to perform the following steps on CA ITCM before you can upgrade CA Patch Manager.

To upgrade CA Patch Manager on a remote MDB

1. Upgrade the remote Microsoft SQL Server MDB using the CA ITCM r12 SP1 installation procedure for a remote MDB.
2. On the local computer upgrade to CA ITCM r12 SP1.
3. From the DSM Explorer:
   a. Navigate to *Domain Manager*, Control Panel, Engines, All Engines, SystemEngine
   b. From the Tasks section, select Link Existing Task.

      The Select Engine Tasks window appears.
   c. Select Default Software Contents Download Job and click OK.

      The job is now linked to the CA ITCM system engine.

      Note: CA ITCM r12 SP1 is compatible only with CA Patch Manager r12 SP1. When you upgrade to CA ITCM r12 SP1, you must also upgrade r11.2 or r12 version of CA Patch Manager to CA Patch Manager r12 SP1.
4. Run the CA Patch Manager r12 SP1 installer on the computer. The installer detects the earlier version of CA Patch Manager and offers to upgrade it for you.
5. Follow the installation wizard to perform the upgrade.

   Note: We recommend a reboot of the computer after the upgrade.

Chapter 7: CA Asset Intelligence Changes and Enhancements

This chapter describes the changes, enhancements, and improvements that have been made to CA Asset Intelligence.

This section contains the following topics:

Changes and Enhancements

CA Asset Intelligence, as a part of this CA ITCM release, now supports the following:

- Installation in the following languages:
  - English
  - French
  - German
  - Japanese
- Oracle 10g Release 2 on Solaris, Solaris 10 (64-bit) operating environment for SPARC, and Microsoft SQL Server 2008 SP1 (Enterprise, Standard) 32- and 64-bit. An install kit is provided to set up the Oracle MDB on Solaris which can be remotely accessed by CA Asset Intelligence.

  Note: We recommend the Oracle installation to be case insensitive for CA Asset Intelligence.

  For a complete list of supported databases, see Supported Databases for the MDB (see page 20).
- Windows Server 2008 SP2 (Enterprise, Standard, Datacenter) 32- and 64-bit

  For a complete list of supported Microsoft Windows operating environment, see Microsoft Windows Operating Environments. (see page 13)
- Installation of CA Asset Intelligence on computers running Microsoft Cluster
- Installation of CA Asset Intelligence from a shared location without mapping a network drive

CA Asset Intelligence, in this release, does not require you to install:

- CA Asset Intelligence schema

  Note: CA Asset Intelligence schema is now merged into the schema of CA ITCM r12 SP1.
- SQL and Oracle JDBC drivers

  Note: These drivers are automatically installed as a part of the installation.

CA Asset Intelligence, in this release, does not support the following:

- UltraSPARC 32-bit and Solaris x86
- Installation on a Solaris or Oracle cluster
- Ingres database

The following sections describe the procedures associated with the above changes, including CA Asset Intelligence installation and upgrade instructions for this release.

Installation and Upgrade

The following sections describe the installation of CA Asset Intelligence as a stand-alone and on a cluster.

General Considerations

The following are the general considerations for CA Asset Intelligence:

- If you have installed CA Asset Intelligence on a Microsoft SQL Server MDB and you want to extract Oracle data sources, ensure that xblkld4.dll is present on the computer running CA Asset Intelligence in the path <install-dir>:\Program Files\Common Files\System\Ole DB.

  The xblkld4.dll is used to extract the data from Oracle data source to CA Asset Intelligence. If the DLL is not present, run Microsoft SQLXML 4.0 SP1. You can download Microsoft SQLXML 4.0 SP1 from the download center in http://www.microsoft.com

- Add the following JAR files in the Classpath:
  - <install-dir>:\oracle\product\10.2.0\client_1\jlib\orai18n.jar
  - <install-dir>:\oracle\product\10.2.0\client_1\lib\xmlparserv2.jar
  - <install-dir>:\oracle\product\10.2.0\client_1\lib\xsu12.jar
  - <install-dir>:\oracle\product\10.2.0\client_1\lib\xml.jar
  - <install-dir>:\oracle\product\10.2.0\client_1\lib\xmlmesg.jar
  - <install-dir>:\oracle\product\10.2.0\client_1\lib\oraclexsql.jar
  - <install-dir>:\oracle\product\10.2.0\client_1\jdbc\lib\nls_charset12.jar
  - <install-dir>:\oracle\product\10.2.0\client_1\RDBMS\jlib\xdb.jar

  Note: The JAR files must be added in the Classpath when CA Asset Intelligence is installed on an Oracle MDB and you are extracting data from an Oracle or SQL data source.

- If you have installed CA Asset Intelligence on an Oracle MDB, install Windows Oracle client with Administration Option, and apply Service Pack 4 to the Oracle 10g client installation.

- Only one CA Service Desk Manager and one CA Asset Portfolio Management data source are supported on CA Asset Intelligence at a time.

If you are installing CA Asset Intelligence on Windows Server 2008, ensure that the following are available before installation:

- Add the roles Web Server (IIS) and Application Server from the Server Manager with the following:
  - For the Web Server role, install the features CGI and IIS 6.0 Management Compatibility in addition to the default features
  - For the Application Server role, install the feature Web Server (IIS) Support in addition to the default features
- PHP with CGI or FastCGI

  Note: For more information about PHP with CGI, see the PHP requirements in the "Installing CA Asset Intelligence" chapter of the *r12 CA Asset Intelligence Product Guide.*
- PHP is configured to work with IIS 7.0
  - **Note:** For more information about configuring PHP with IIS 7.0, see http://www.iis.net

CA Asset Intelligence Stand-alone Installation

CA Asset Intelligence provides an interface that is designed for time-challenged management. It gives you access to the information you require to manage your IT assets and services in a proactive and decisive manner.

To install CA Asset Intelligence as a stand-alone installation

1. Insert the CA Asset Intelligence installation media into your drive.

   The Choose Setup Language option appears.

   Note: If the wizard does not appear, run Setup.exe from the root directory on the installation media or from the shared location to which you have copied the contents of the installation media.
2. Select the desired language.

   The Welcome page appears.
3. Select Install CA Asset Intelligence, enter the Customer Information, and accept the terms of the Licensing Agreement on the subsequent installation pages.

   The Configure Node page appears.
4. Click Next.

   The Choose Destination page appears.
5. Select the default or enter the destination folder path, and click Next.

   The Choose Virtual Directory Path page appears.

6. Select the default or enter the virtual directory path, and click Next.

   The Asset Intelligence Web Server Users page appears.

7. Enter the domain name, user name, and click Next.

   The Choose Database Management System page appears.

8. Select the database management system as Microsoft SQL Server or Oracle, and click Next.

   The CA Asset Intelligence Database Credentials page appears.

9. Enter the database details, click Test Login to verify the database access, and click Next.

   The CA Asset Intelligence MDB User and Password page appears.

   Note: The installation does not progress until the Test Login to verify the database access to the local or remote database is successful. The aiowner and aiuser are automatically created as users within the selected MDB if they do not already exist.

10. Enter the aiowner and aiuser passwords in the subsequent installer pages, and click Next.

    The CA Asset Intelligence MDB Installation Confirmation page appears.

    Note: If the aiowner and aiuser already exist in the MDB, the existing passwords of aiowner and aiuser are reset with the new passwords.

11. Select No if this is a first time CA Asset Intelligence installation on the MDB. Otherwise, select Yes and click Next.

    The Asset Intelligence Installation Checklist dialog appears.

12. Review the settings and click Next to start installation.

    The Setup Status dialog appears showing the status of the installation.

13. Click Finish.

    The CA Asset Intelligence installation is complete.

Installation of CA Asset Intelligence on a Cluster

CA Asset Intelligence has no functionality in place to detect system failures and to automatically switch from the active to the passive node in a system failure.

CA Asset Intelligence can be installed either as Active CA Asset Intelligence installation or Passive CA Asset Intelligence installation. The terms Active and Passive refer to whether the CA Asset Intelligence is active or passive; they do not refer to the cluster node (which may itself be active or passive).

To install CA Asset Intelligence on a cluster

1. Insert the CA Asset Intelligence installation media into your drive.

   The Choose Setup Language option appears.

   Note: If the wizard does not appear, run Setup.exe from the root directory on the installation media or from the shared location to which you have copied the contents of the installation media.

2. Select the desired language.

   The Welcome page appears.

3. Select Install CA Asset Intelligence, enter the Customer Information, and accept the terms of the Licensing Agreement on the subsequent installation pages.

   The Configure Node page appears.

4. Select Enable Recovery Support, select the Node Configuration as Active or Passive, and provide a path to install the configuration data. Click Next.

   The Choose Destination page appears.

5. Select the default or enter the destination folder path, and click Next.

   The Choose Virtual Directory Path page appears.

6. Select the default or enter the virtual directory path, and click Next.

   The Asset Intelligence Web Server Users page appears.

7. Enter the domain name, user name, and click Next.

   The Choose Database Management System page appears.

8. The database management system is selected as Microsoft SQL Server by default. Click Next.

   The CA Asset Intelligence Database Credentials page appears.

   Note: The option to select Oracle as the database in disabled as CA Asset Intelligence does not support installation on an Oracle cluster.

9. Enter the database details, click Test Login to verify the database access, and click Next.

   The CA Asset Intelligence MDB User and Password page appears.

   Note: The installation does not progress until the Test Login to verify the database access to the local or remote database is successful. The aiowner and aiuser are automatically created as users within the selected MDB if they do not already exist.

10. Enter the aiowner and aiuser passwords in the subsequent installer pages and click Next.

    The CA Asset Intelligence MDB Installation Confirmation page appears.

    Note: If the aiowner and aiuser already exist in the MDB, the existing passwords of aiowner and aiuser are reset with the new passwords.

11. Select Yes if this is a first time CA Asset Intelligence installation on the MDB. Otherwise, select No and click Next.

    The Asset Intelligence Installation Checklist dialog appears.

12. Review the settings and click Next to start installation.

    The Setup Status dialog appears showing the status of the installation.

13. Click Finish.

14. The CA Asset Intelligence installation is complete.

CA Service Desk Manager Data Extraction

Please select the CA Service Desk Manager r11, r12 data source type option from the Database Settings page of the AI Admin console for data extraction from CA Service Desk Manager r11 and r12 releases. See Define a Data Source (see page 77) for more information.

CA Asset Intelligence Upgrade Procedure and Considerations

You may upgrade CA Asset Intelligence from r11.2 or r12 to r12 SP1.

Note: Upgrading from versions prior to CA Asset Intelligence 11.2 is not supported.

Upgrade CA Asset Intelligence Using a Local or Remote Microsoft SQL Server MDB

For earlier versions of CA ITCM and CA Asset Intelligence using a Microsoft SQL Server MDB that resides on a local or remote computer, you must upgrade CA ITCM to r12 SP1 before you upgrade CA Asset Intelligence to r12 SP1.

Note: The upgrade process overwrites the user customized settings. You can preserve settings and customizations (see page 80) of the previous version and use it in CA Asset Intelligence r12 SP1.

To upgrade CA Asset Intelligence on a local or remote Microsoft SQL Server MDB:

1. Upgrade to CA ITCM r12 SP1.

   Note: For a remote Microsoft SQL Server MDB, use the CA ITCM r12 SP1 installation procedure for a remote MDB.

2. Run the CA Asset Intelligence r12 SP1 installer on the computer. The installer detects the earlier version of CA Asset Intelligence and offers to upgrade it for you.

3. Follow the installation wizard to perform the upgrade.

Note: You cannot change the database from Microsoft SQL Server to Oracle during the upgrade process. You can only add Oracle data sources after upgrade using the mdbadmin credentials.

Oracle as a database is available only in case of a new installation of CA Asset Intelligence r12 SP1. To set Oracle as your database, uninstall the previous version of CA Asset Intelligence and install CA Asset Intelligence r12 SP1.

Define a Data Source

You can define a data source to extract CA product data from a database on Oracle or Microsoft SQL Server.

To define a data source

1. Click the Database Settings link.

   The Database Settings page appears.

2. Enter the details in the Add Data Source field to define a data source, the Add Data Sources portlet must be completed and saved for each desired data source.

   The following fields must be completed to define a data source:

   Type

   Indicates the CA product data that is to be extracted and the release level. Valid options are as follows:

   - Asset Management 4.0
   - Asset Management r11
   - CA Asset Portfolio Management r11
   - CA Service Desk Manager r11, r12
   - CA ITCM r12
   - Unicenter Asset Maintenance System r11

   Select Asset Management r11 if you are extracting data for CA IT Client Manager r11.

   Database Engine

   Indicates whether the underlying database for that data source is Microsoft SQL Server or Oracle.

   Note: Oracle is available only when the above selected Type is supported on Oracle. Microsoft SQL Server will be the only selectable Database Engine type if either CA Asset Portfolio Management r11 or Unicenter Asset Maintenance System r11 is selected from the data source Type drop-down list. The Port control will change to 1433 if these are selected.

   Server Name

   Identifies the server on which the data source is located.

   Port

   Identifies the port number of the JDBC server. For SQL the default is 1433 and for Oracle the default is 1521, however, this value can be edited if required.

Username and Password

Identifies the user ID and password that will be used to access the database tables on the data source. This user ID must have read access to those tables.

Note: If the underlying database is Oracle, you need to provide the mdbadmin credentials. Also, for Asset Management r11, CA ITCMr12, and CA ITCM r12 SP1, you need to add "AIADMIN" role to mdbadmin before running the extraction.

SID

Identifies the SID that hosts the data source on the Oracle database.

Note: This option is available only when the Oracle database engine is selected.

If any of the following types are selected and the corresponding application exists on the specified server, the Application URL displays the website address that is used to access the application:

- Asset Management 4.0
- Asset Management r11
- CA Asset Portfolio Management r11
- Unicenter Service Desk r11
- Unicenter Asset Maintenance System r11

This URL can be changed to another valid address if desired. The URL is used in the Public User Interface when displaying detailed report lists. This feature allows the user to launch into the source application to see more detail about the selected service activity or asset. The user, however, must still have the appropriate access credentials for the source application.

3. Click Connect.

   The databases that exist on the selected server appear in the Database Name drop-down combo box for selection.

4. Select the desired database, and click Save.

   When you click Save, the data source is created and appears in the Active Data Sources portlet. Data sources in this list use the following naming convention:

   ServerName::Database name/port number

The portlet contains the following columns:

Data Source

ServerName::Database name/port number.

Type

Displays the data source release level.

Enabled

Indicates whether the database is enabled (green) or disabled (blue). You can also click the icon in the column to change the current selection from enabled to disabled and back again.

Delete

Permanently deletes the data source in the current row from the list of active data sources.

Status

Indicates whether the server is currently running (green) or not (red).

Edit

Edits the data source in the current row.

Preserve Settings and Customizations While Migrating to r12 SP1

The upgrade process of CA Asset Intelligence r12 SP1 overwrites the customized user settings of the previous version.

However, you can preserve settings and customizations of a previous version of CA Asset Intelligence and reuse it in CA Asset Intelligence r12 SP1.

To preserve configuration settings when you migrate to CA Asset Intelligence r12 SP1

1. Save the configuration files listed in the table below before you upgrade or uninstall the previous version of CA Asset Intelligence. Save the files in a directory outside CA product directories, for example, %TEMP% directory.
2. Upgrade to CA Asset Intelligence r12 SP1 and replace the saved files in the appropriate locations.
3. Recreate data sources that were created in the previous versions of CA Asset Intelligence and Unicenter Service Intelligence in CA Asset Intelligence r12 SP1.
4. Run dbextract after migration and data source creation.
5. Modify "ExtractSchedule" parameter and all other parameters in the uai.dat file.

   Note: This file is not migrated during migration.
6. Regenerate aibValSet.php using CA Asset Intelligence r12 SP1

The following table represents the customization files you must save before uninstalling the previous version:

No.	Setting to Preserve	Save from Directory	File(s)	Comment
1	LDAP import configuration	\admin\xxx\cache\	aig_ldap.dat	
2	Customized Global Views	\admin\xxx\GlobalView\	All .dat files (*.DAT)	Copy only .dat files in this directory, not in default subdirectories within.
3	Links in L1 Views (Customized Global Views)	\public\xxx\linklist\	All files	
4	Charts in L1 Views (Customized Global Views)	\public\xxx\charts\	All files	
5	Saved Reports	\public\xxx\views\	All files	

No.	Setting to Preserve	Save from Directory	File(s)	Comment
6	User-defined Hardware and Software Categories	\public\common\inc\	aic_dataArray.inc, aic_hwcat.inc, aic_QueryArray.inc	
7	Roles and Additional (Customized) Roles	\public\common\role\YYYYY\	All role.inc files from the directory of each role (YYYY) in the system	Save the role.inc files of each default role and additional roles (created using process outlined in TechDoc TEC390743). Follow the process outlined in TechDoc TEC390743 to add each of the additional or customized roles back into the system, after CA Asset Intelligence r12 SP1 is installed.
8	History	\admin\XXX\cache\ \PHP\sessiondata\ %UAI_ENGINE_HOME%\log\	All log files	This is optional. The log files are for informational purposes only.
9	Organization Browser	\public\common\inc\	aiOrgMenuTree.inc	The organization browser does not work if this file is missing. This file is regenerated each time an LDAP Collect is successfully completed. However, it is useful to save this file in case regeneration is a formidable task due to incomplete or multiple LDAP repositories.

No.	Setting to Preserve	Save from Directory	File(s)	Comment
10	Asset Management Hardware and Software Data Collection Information	%UAI_ENGINE_HOME%\config	ai_attribute_sets.xml ai_software_filters.xml	These files specify which CA Asset Intelligence hardware and software attributes to be collected, and where to find the data within CA Asset Intelligence. **Note:** These files have been updated in CA Asset Intelligence r12 SP1 and must not be overwritten by the saved files from the previous installation. Any client-specific customization to the files in the previous version must be applied to the new (r12 SP1) files using the saved XML files as a template.

In the virtual directories listed in the table above:

- xxx denotes the three-letter code for the language being used (for example, 'enu' corresponds to English).
- YYYY denotes one of the default roles (admin, auth, public, or restricted) or an additional or customized role created by following the procedure outlined in TechDoc TEC390743.

Note: The directories listed in the Save from Directory column in the table are available relative to this default location. If the installation path was modified during the installation of the previous version of CA Asset Intelligence, you must navigate to the corresponding directory structure.

The new CA Asset Intelligence r12 SP1 directory structure to use when copying saved files from a previous version of CA Asset Intelligence is:

- install_dir\webroot\asset\public\...
- install_dir\webroot\asset\admin\...

Note: If the default directory for CA Asset Intelligence r12 SP1 has been changed during the install, the "webroot" folder above will be removed from the installed path.

The default location of %UAI_ENGINE_HOME% for CA Asset Intelligence r12 SP1 is C:\Program Files\CA\Asset Intelligence\bin

\PHP\sessiondata\ is specific to where PHP has been installed.

Chapter 8: Known Issues

This chapter describes known issues, workarounds, and solutions for this release of CA ITCM.

This section contains the following topics:

Considerations That Apply to All Components

This section describes known issues, workarounds, and solutions that apply to all or most of the components of CA ITCM.

Problem with DOS Boot Images on Certain Hardware

Symptom:

When I perform an OS installation with a DOS-based boot image and an appropriate OS image, the installation stops during the DOS phase, and the partitioning tool "cafdisk" fails with the error messages:

- Cannot read block
- Cannot write block

Solution:

Cannot read block or cannot write block messages appear when the BIOS functions used by cafdisk to access the hard disk (INT13) fail to read or write sectors. This problem is observed on a Dell PowerEdge 1950 III (BIOS version 2.6.1) with PERC 6/i RAID controller (BIOS version NT13-2).

To fix the problem, update the firmware (BIOS) of the target computer.

If the problem persists, use WinPE-based Boot Images.

Note: There is currently no solution if this problem occurs during the installation of Linux.

Login Field Missing while Accessing WAC

Symptom:

When I access the Web Access Console (WAC), I do not see the login fields.

Solution:

The login fields do not appear if the web browser is unable to identify WAC as an intranet application.

Add http://<hostname>/wac in the trusted sites list, and access WAC.

CA APM and CA ITCM Integration Error

If you install CA ITCM on a computer which has an existing installation of CA APM, login to WAC fails with the message "Warning: Unable to connect to Web Service (CMM000066)".

For a successful CA ITCM and CA APM integration, after the CA ITCM installation, edit the Path environment variable and make the variable *<install-dir>:\Program Files\CA\DSM\bin* as the first entry in the list.

CA APM and CA ITCM Integration Using Older CORA Version

If you install CA APM on a computer which has an existing CA ITCM installation, the latest version of CORA is not used.

To use the latest version of CORA, edit the Path environment variable and make the variable *<install-dir>:\Program Files\CA\SC\CORA* as the first entry in the list.

Software Content Download Engine Task Fails

The software content download engine task by default is configured to run once a day between 00:00 hours and 06:00 hours. The time is sufficient to download new software signatures published by CA.

If you configure the software content download engine task to run "all the time," the resources on the servers hosting the software content may become overloaded or believe that there is a denial of service attack. In such cases, the servers reject those incoming connections to do load balancing and the software download engine task fails.

CCS Components Help Does Not Work on Windows Vista and Windows Server 2008

Starting with the release of Windows Vista and Windows Server 2008, Microsoft has decided to no longer include WinHlp32.exe as a component of the Windows operating system.

The CCS components help system uses the WinHelp system. To view help, you can download and install WinHelp32.exe from Microsoft. For more information, see the Microsoft knowledge base article 917607.

CCS Installation Fails on a Localized Microsoft SQL Server 2008 Instance

If you set up an instance on the Microsoft SQL Server 2008 with non US-ASCII characters, the CCS installation fails.

For a successful installation of CA ITCM, ensure that the Microsoft SQL Server instance does not contain any non US-ASCII characters.

CCS Installation on Windows Server 2008

Symptom:

I am installing CCS on Windows Server 2008. During the installation, I see the following message:

"The setup for component Distributed Intelligence Architecture has failed.

Cause: Unable to start DIA Knowledge Base Service. DIA Knowledge Base service setup failed."

Solution:

Click OK to complete the installation.

After the installation completes, the DIA Knowledge Base Service will be in a Started state and there is no functional impact.

CCS Installation Fails in Pure IPv6 Network

CCS installation fails in a pure IPv6 network when the domain manager on Windows Server 2003 is configured with a remote Microsoft SQL 2008 MDB. It is advised that you configure a dual stack routing in the IPv6 network to work around this issue.

Maximum Open Cursors Exceeded

You can a encounter maximum open cursors exceeded error when multiple transactions take place on an Oracle instance.

Increase the maximum open cursors limit in the Oracle client configuration parameters for uninterrupted data extraction.

cfSysTray Does Not Appear Immediately After CA ITCM Installation on Open SUSE 11

The CA ITCM notification icon, cfSysTray, does not appear immediately after CA ITCM installation on Open SUSE versions 11 and 11.1.

If you want the cfSysTray to appear immediately after CA ITCM installation, restart the window manager (log out and log in).

System Status Shows DSM Service as Failed in CA Patch Manager after Failover

Symptom:

My computer crashed and I manually switched the CA Patch Manager passive node to active. When I logged into the CA Patch Manager console, I noticed that the System Status showed the status of DSM Service resource as failed. What should I do?

Solution:

To change the status of the DSM Service, do the following:

1. Click Start, Programs, CA Patch Manager, Launch CA Patch Manager.

   The CA Patch Manager login window appears.

2. Log in as CA Patch Manager administrator, and select the Administrator tab.

   The Administrator page appears.

3. Navigate to Configuration, System Settings, DSM.

   The DSM Connection page appears.

4. Change the Web Service URL field to the show the active node and click Save.

   The DSM Connection settings are saved and DSM Service status changes.

DCS Installation Summary Shows "no Install return code available"

Symptom:

I installed DCS using the installation media. In the installation summary I see the following:

CA DSM Device Compliance Scanner

-no Install return code available

Solution:

no Install return code does not mean that the DCS installation has failed.

This behavior is noticed when you install or upgrade DCS using the installation media.

Note: The "no Install return code" message appears in English even if you install DCS in other supported languages.

Platform Shows Windows Vista Instead of Windows Server 2008

If Windows Server 2008 has JRE 1.5.0_11 installed, it has been found that the name of the operating system is reported as Windows Vista and not Windows Server 2008.

Due to this behaviour, the About page of CA Patch Manager on Windows Server 2008 displays the Platform Name as Windows Vista instead of Windows Server 2008.

Browser Warning on NRI Website

When you collect inventory using the NRI website on Windows Server 2008, you may receive a browser message "Program needs your permission to continue”.

Click Continue to collect the inventory.

CA Asset Intelligence Database Connectivity May Fail

After CA Asset Intelligence installation, you may encounter the following database-related issues:

- The Administrative Console shows the Status as "r12 Database Connectivity: Failed"
- In the Administrative Console, Database Settings page, under Add Data Sources, the Database Engine field does not list the options to select Microsoft SQL Server, Oracle, or both
- The Public User Interface, Level 2 view displays an error "Directory open failed for webroot"

To fix the preceding issues, restart the IIS server.

CA Asset Intelligence 500.19-Internal Server Error

Symptom:

When I launch the CA Asset Intelligence Administrative Console or Public User Interface, I get 500.19-Internal Server error. What should I do?

Solution:

If you get 500.19-Internal Server error when you launch the CA Asset Intelligence Administrative Console or Public User Interface, manually add IIS_IUSERS to the Webroot folder wth read permissions.For more information, see the Microsoft knowledge base article 942055.

CA Asset Intelligence on Windows Server 2008 with IIS 7.0

Symptom:

I have installed CA Asset Intelligence on Windows Server 2008 which has IIS 7.0 configured with FastCGI. The installation is successful, but when I try to access the links on the CA Asset Intelligence user interface, I receive an HTTP 500 error.

Solution:

You may get an HTTP 500 error if IIS 7.0 is configured with FastCGI and if FastCGI logging is enabled.

Open the php.ini file and change the *fastcgi.logging* configuration setting to zero. For more information about the configuration settings, see http://www.iis.net.

Port 7163 Not Used by CA ITCM

On Windows operating environments, CA ITCM utilizes a new common CA port multiplexer that listens on TCP/IP port 7163 along with existing CAM TCP port 4105 and CA ITCM TCP port 4728.

However, CA ITCM does not use the port 7163 although other CA products may use this port.

If you have only CA ITCM installed on the computer, you need not configure the firewall for the port 7163 and you can safely ignore the port.

IPv6 and NWLink IPX/SPX Protocol

If you install IPv6 along with NWLink IPX/SPX protocol, and if you do not have any active IPX hosts and naming services on the local network, the name resolution will be delayed.

To avoid the delay in name resolution, disable or remove the IPX protocol.

Network Installation of MSI Package Fails

Symptom:

When I perform a network installation of an MSI package on Windows Server 2008, the installation fails with an error "1619: This installation package could not be opened". How do I fix this problem?

Solution:

The network installation of an MSI package fails with the error code "1619: This installation package could not be opened" when both the scalability server and the agent are installed on Windows Server 2008, Windows Vista SP2, or Windows 7 operating environments.

To perform a successful network installation of an MSI package, disable SMB2.0 and restart the scalability server.

To disable SMB2.0 on the scalability server, do the following:

1. Open Registry Editor and navigate to HKLM,System, CurrentControlSet, Services, LanmanServer, Parameters.
2. Create a DWORD Value and name it smb2
3. To disable SMB2.0,set the value of smb2 to 0.

   Note: To enable SMB2.0, set the value to 1.
4. Restart the scalability server

   SMB2.0 is disabled on the scalability server.

Libxcb Message When Installing on OpenSUSE

When you install CA ITCM on openSUSE, a libxcb warning message stating that a connection is unlocked without first being locked can appear.

The warning does not have any impact on the CA ITCM installation. You can safely ignore the warning.

Installation on OpenSUSE using Java GUI

If you install CA ITCM using the Java GUI on Japanese or Korean openSUSE operating environments, the installation wizard displays junk characters.

Use the VT100-style (character-based) user interface to install CA ITCM.

Installation May Fail on Windows Systems with an Unpatched Version of Windows Installer V4.5

With the exception of Microsoft SQL Server 2008, Windows Installer v 3.0 is installed by default on Windows systems and is also the version available from Windows Update. In the case of Microsoft SQL Server 2008, Windows Installer V 4.5 is a prerequisite and is therefore installed automatically on the system. Note, however, that a CA ITCM installation may fail with error 1603 if you have Windows Installer V 4.5 installed and you have not installed Microsoft hotfix KB958655.

To check which version of Windows Installer you have, enter "msiexec /help" at the command prompt.

Microsoft hotfix KB958655 can be downloaded from the following location: http://support.microsoft.com/kb/958655

Some Help Buttons May Display the ? Symbol

System-generated dialogs, such as the various Properties windows and messages, may display the ? symbol in localized versions of CA ITCM rather than localized text.

Using Software Delivery to Uninstall Windows Agent DSM Packages

DSM packages can be split into two classes: base packages and custom packages. Custom packages "contain" base packages and base packages are the "atoms." Base packages are registered when installed or discovered and are listed as "installed software." When a custom package is delivered and installed using Software Delivery, an installation record is created for the custom package. However, this custom package installation record is not created for a manual installation or installation using infrastructure deployment.

When using Software Delivery to uninstall DSM packages, only the base packages should be uninstalled. The order in which the base packages should be uninstalled is important. First, uninstall the agent language packages, then the DCS add-on, then Asset Management and/or Remote Control. Obviously, the software delivery agent needs to be uninstalled last. One way of implementing this would be to create an software delivery uninstall job container with a job for each stage. When the base packages have been uninstalled, the installation records for the custom packages should be removed using DSM Explorer.

Note that plug-ins like Secure Socket Adapter and DMPrimer are not removed. To remove these plug-ins, uninstall any remaining CA ITCM components on the target computer manually using Add/Remove programs. See the *r12 Implementation Guide* for more information.

Problem with Repair Mode

If the CA ITCM agent installation on Linux or UNIX is corrupted, you can use the installer's repair mode to repair the installation. However, the repair mode can fix only simple breakages. If the installation is severely corrupted, uninstall the corrupt installation and reinstall CA ITCM again.

Repair a Corrupted CA ITCM Manager Installation

CA ITCM supports only simple repairs. If you attempt to repair a corrupted CA ITCM manager installation, the repair fails.

Use your backup to restore CA ITCM and fix the breakages. For more information about backup and restore procedure of CA ITCM, see http://ca.com/support.

Junk Characters in Japanese CA Workflow for CA ITCM Command Prompt Window

In a Japanese CA Workflow for CA ITCM installation, when you launch the CA Workflow for CA ITCM, the Command Prompt window that comes up has junk characters in the status message.

You can ignore the junk characters as they do not affect the working of the product.

English Chart Titles in Japanese Version of CA Asset Intelligence

Currently, chart titles are displayed in English in the Japanese version of the CA Asset Intelligence public user interface.

English Chart Titles in French Version of CA Asset Intelligence

Currently, some chart titles, for example, "Desktop" and "Server," are displayed in English in the French version of the CA Asset Intelligence public user interface.

Content Download After Installing CA ITCM r12 SP1 on Top of CA SWCM r12

If you are installing CA ITCM r12 SP1 after installing CA Software Compliance Manager (CA SWCM) r12 on the same machine, perform the following procedure to ensure that the content download is successful.

1. Disable the CA Content Import Client service running on the CA Software Compliance Manager application server.
2. On the DSM domain manager at the command prompt, go to the Program Files\CA\SC\CIC\bin folder and run the following two commands:

   Util.bat -R appname id licensekey role

   util -L mdbhostname SQLAdminAccount SQLAdminAccountPassword

   Example:

   util.bat -R DSM B1B13849-08D1-4DA6-91EA-2D278E5F00CC PMDSM-00000-00000-00001 ca_itrm_group
3. Create a folder named "baseline" under \Program Files\CA\SC\CIC and copy the baseline files from the ITCM_Install_Media\WindowsProductFiles_x86\CIC\baseline To C:\Program Files\CA\SC\CIC\baseline folder.
4. Apply testfix T5KW086, available from the Technical Support website.

Core Files Are Generated

Occasionally, during upgrades or reinstallation of CA ITCM product files on HPUX platforms, core files are generated of DSM product binaries. This core file generation has no functional impact and the core files can be removed.

Considerations for Asset Management

NRI Agent Inventory Overwrites the AM Agent Inventory

The NRI agent collects a full inventory and not a delta inventory. If you run the NRI agent inventory using a privileged user account, the NRI agent inventory deletes and replaces the existing AM agent inventory.

Software Usage Agent on Windows Server 2008 Itanium (IA64)

The Software Usage agent on Windows Server 2008 Itanium (IA64) supports usage monitoring only for 32-bit applications. Monitoring the usage of 64-bit applications is not supported.

User Defined Software Signature on Linux and UNIX Operating Environments

When you create a new release of a software product with Linux or UNIX as the operating system, the following characters must be preceded by a backslash (\ ) in the OS version field of the Advanced tab:

- *
- +
- ?

The following example shows the OS Version in a software definition:

#1 SMP 2008-12-04 18:10:04 \+0100

Considerations for Windows Server 2008 Core Operating Environments

This section describes known issues, workarounds, and solutions that apply to Windows Server 2008 server core operating environments.

Dependency on Graphical User Interface (GUI)

Windows Server 2008 server core provides limited GUI functionality. Due to the dependency on the GUI, the following CA ITCM agent options are not supported:

- Remote Control chat
- Remote Control viewer
- Software catalog
- Systray

Dependency on IE

Windows Server 2008 server core does not support HTML-based installers due to the dependency on IE.

To install the CA ITCM agents, do *one* of the following:

- From the installation media, go to WindowsProductFiles directory and run setup.exe.
- From the DSM Explorer, use DMDeploy to deploy the agent plugins.

Uninstall the Agents

Windows Server 2008 server core does not provide support for Add or Remove Programs. To uninstall the agents, run msiexec from the command line.

For more information about using msiexec, see the Installation Tool msiexec section in the "Installation of CA ITCM" chapter of the *r12 Implementation Guide*.

Options Not Supported

Windows Server 2008 server core does not support the following:

- Online help for agents.
- "Force user to log off before job executes" mode of operation for the Logon Shield
- The Logoff option of the Procedure options "Boot Level before execution" and "Boot Level after execution"

Known Issues from CA ITCM r12

The Known Issues of CA ITCM r12 which have not been fixed in this release are as follows:

- ENC Gateway server and uninstalling the IPv4 stack
- Secure socket adaptor upgrades
- Extra CCS dialogs appear after installer summary
- CCS functionality not available from DSM Explorer's menu
- Uninstallation of Unicenter NSM removes CCS
- Micro-CCS calendars do not work on 64-bit Windows platforms
- Installing or uninstalling other CA products causes CA ITCM to fail with ETPKI errors
- CA Service Desk r12 and CA ITCM integration error
- CAM communication to IPv4 addresses ending in 0 or 255 in Class B networks fails
- Web Console may stop responding when using IE6 on certain Windows platforms
- Unable to access Web Console in a Linux environment that has IPv4 loop back disabled
- Integrating CA ITCM with Unicenter APM r11.3.4 or earlier

- Viewing the asset management inventory data from CA Service Desk web client
- Installing Unicenter NSM r11.2 over the CA ITCM r12 Installation
- Unable to deploy over IPv6
- Content import client does not support IPv6 communication to the content server
- Uninstalling content import client manually after uninstalling CA ITCM
- Infrastructure deployment to Mac OS X using SSH fails with a timeout Error
- Infrastructure deployment to Mac OS X fails with an Incompatible Package error
- Cannot upgrade an agent and simultaneously change the scalability server to which it registers
- Generic error using sd_sscmd libraryaccess command
- Jobs do not run as per calendar settings
- Text truncation while selecting Advance Search option in Web Console
- Unable to view the discovered or owned inventory in Web Console
- OS name displays as unknown in infrastructure deployment
- MIF file format
- Software usage problem when connectivity to scalability server temporarily breaks
- Continuous discovery is not supported on Oracle MDB
- Asset converter and Microsoft SMS server on the same computer
- Additional inventory items not shown in CA ITCM r11.2 C3 DSM Explorer interface
- Context sensitive help does not work for error message AMM001200
- Instant diagnostics feature fails to report the correct status for agents running on Windows 2003 and XP in Pure IPv6 and dual-stack environments
- Hardware inventory reported for VMWare ESX
- Configuration Policy: Run the AM Agent in USD hint mode
- Online software usage is not supported on UNIX/Linux
- Limited basic inventory reported for Solaris 10 Zones
- Performance inventory is not reported for Mac OS X platforms
- Running software delivery job check on terminal or citrix client
- SXP packages converted to MSI fail to install on Windows 2008

Note: For more information about the CA ITCM r12 Known Issues, see the *r12 readme* which is a part of the CA ITCM r12 SP1 documentation set.

Secure Socket Adaptor Upgrades

Note: The following entry supersedes the corresponding entry in the CA IT Client Manager r12 Readme.

CA ITCM r12 includes the Secure Socket Adaptor (SSA) that helps with providing port multiplexing and ENC services. If a previous version of SSA (also known as Dylan) is installed on a 64-bit version of Windows, the SSA upgrade procedure will fail if Dylan is installed in "\program files" rather than "\program files(x86)". When this happens, port multiplexing, ENC, and networking do not function correctly because two versions of SSA are present.

This may manifest itself in the following ways:

- Inventory cannot be collected because the agent cannot connect to the scalability server.
- Remote control cannot listen for connections.
- ENC does not connect through firewalls.
- Software delivery jobs may fail with DTS errors or may be in waiting state continuously.

This has been seen when upgrading a machine that has an old version of CCS (r11.1) or some other CA products that use old versions of SSA.

To check if this is the case, look at the file "\program files\ca\sharedcomponents\csam\sockadapter\version.txt". If the file exists and contains the string "1.5.3", then Dylan is installed. In this case, it must be manually uninstalled before CA ITCM is upgraded using the following procedure:

- Check if other products are registered with SSA using the following command:

  ```
  dsadependencyinstall -l
  ```

  If the command lists any products, then execute the following command:

  ```
  dsadependencyinstall -d "<name>"
  ```

  The variable <name> is a product listed by the first step.

- Uninstall Dylan using the "Add/Remove programs" control panel applet or execute the following command:

  ```
  \Program Files\CA\SharedComponents\Csam\SockAdapter\_uninst\uninstaller.exe
  ```

If an upgrade of CA ITCM has already been performed but SSA has not upgraded, then uninstall Dylan as explained above and install the up-to-date version of SSA by running the following file from the installation DVD:

WindowsProductFiles_x86\SSA\CASockAdapterSetupWin32NoEtpki.msi

Configure SSA by executing the following commands in a command line window:

```
encutilcmd updateconfig
caf stop
caf start
```

Documentation Changes

This section describes the documentation changes that need to be incorporated for this release of CA ITCM.

Implementation Guide: Uninstallation of CA ITCM--Product Codes of CA ITCM

Replace the product codes of Asset Management Agent, Scalability Server, and DMPrimer with the following:

Asset Management Agent (ENU and multi-language):

{624FA386-3A39-4EBF-9CB9-C2B484D78B29}

Scalability Server:

{9654079C-BA1E-4628-8403-C7272FF1BD3E}

DMPrimer:

{A312C331-2E7A-42E1-9F31-902920C402EE}

Implementation Guide: Dependencies to Other Products on Windows Section

In the *r12 Implementation Guide*, Chapter 2, dependencies to other products on Windows section states iGateway as an installation prerequisite.

iGateway is no longer a prerequisite to install CA ITCM.

Implementation Guide: Engine Concept--Support of CA Products Section

In the *r12 Implementation Guide*, Chapter 1, Engine Concept, Support of CA Products section, add the following bullet points under SQL Bridge:

- CA Service Desk Manager r12.1 for Windows with Microsoft SQL Server MDB 1.5
- Unicenter Asset Portfolio Management r11.3.4 Cumulative #3 RO08547 with Microsoft SQL Server MDB 1.0.4

Implementation Guide: Engine Concept--Supported Database Scenarios Section

In the *r12 Implementation Guide*, Chapter 1, Engine Concept, Supported Database scenarios section, add the following bullet points:

The SQL Bridge and Oracle Bridge synchronization features support the following database scenarios:

- The SQL Bridge supports Microsoft SQL Server 2008 on Windows as the source MDB
- The Oracle Bridge supports Microsoft SQL Server 2008 on Windows as the source MDB

Implementation Guide: Installation of SQL Bridge Section

In the *r12 Implementation Guide*, Chapter 4, Installation of SQL Bridge, Upgrade the Target Side with Microsoft SQL Server MDB 1.0.4 section, the first step should be replaced with the following text:

1. Run the "Install MDB" setup from the Unicenter DSM r11.2 SP4 installation DVD.

   This procedure will apply MDB patches not yet available on the target MDB and create the ca_itrm database user.

Implementation Guide: Infrastructure Deployment--Deployment Triggered by Continuous Discovery Section

The following Note must be added to the discovery process:

Note: For the Continuous Discovery feature, configure Microsoft SQL Server with the default port 1433 on the domain manager.

Asset Management Administration Guide: Asset Collector Section

Remove the following text in its entirety from the Asset Collector, Restrictions and Limitations section of the "Customizing Asset Management" chapter:

Supported RDMS

MS SQL is supported in this version.

No restrictions with 64bit platforms.

Web Services Reference Guide: Enumerations Section

Add the following numbered items to the list under the computerClassID subsection:

252: 'SuSE Linux Professional 9.1'

138: 'Windows 2003 Standard'

139: 'Windows Small Business Server 2003'

140: 'Windows Enterprise Server 2003 64-bit'

141: 'Windows Enterprise Server 2003 Itanium 64-bit'

290: 'HPUX 10.00'

291: 'HPUX 10.10'

292: 'HPUX 10.20'

293: 'HPUX 10.30'

297: 'Windows Vista'

298: 'Windows Vista Business'

299: 'Windows Vista Enterprise'

300: 'Windows Vista Home Premium'

301: 'Windows Vista Home Basic'

302: 'Windows Vista Ultimate'

303: 'Windows Vista Business 64-bit'

304: 'Windows Vista Enterprise 64-bit'

305: 'Windows Vista Home Premium 64-bit'

306: 'Windows Vista Home Basic 64-bit'

307: 'Windows Vista Ultimate 64-bit'

308: 'Windows Mobile'

309: 'Windows Mobile 5.0'

5137: 'Windows Mobile 6.0'

5029: 'Mac 10.x or later'

5082: 'SuSE Linux Ent Server 10'

5083: 'SuSE Linux Ent Server 10.1'

5084: 'SuSE Linux Ent Desktop 10'

5085: 'SuSE Linux Ent Desktop 10.1'

5088: 'Windows Server 2003 Standard 64-bit'

5089: 'Windows Server 2003 Datacenter 64-bit'

5090: 'Unixware 7.1.3'

5091: 'Mac 10.5'

5092: 'RHEL Server 5'

5093: 'RHEL Desktop 5'

5094: 'RHEL Advanced Platform 5'

5116: 'RHEL Server 5.1'

5117 'RHEL Desktop 5.1'

5118: 'RHEL Advanced Platform 5.1'

```
5095:  'Solaris Domain Partition'
5096:          'Sun Servers'
5097:  'Sun Fire E25K'
5098:          'Sun Fire E20K'
5099:          'Sun Fire 15K'
5100:          'Sun Fire 12K'
5101:  'Sun Enterprise 10000'
5102:          'Sun Enterprise 6500'
5103:  'Sun Enterprise 5500'
5104:  'Sun Enterprise 4500'
5105:  'Sun Enterprise 3500'
5106:  'Windows Embedded for POS'
5107:  'Windows Embedded for Point Of Service Version 1'
5108:  'Windows Embedded'
5109:  'Windows Embedded'
5110:  'Windows Embedded for Point Of Service 1.0'
5111:  'HPUX 11.11'
5112:  'HPUX 11.31'
5114:  'ROOT RTOS'
5115:  'SUN RTOS '
5119:  'Windows Server 2008'
5120:  'Windows Server 2008 Standard Edition'
5121:  'Windows Server 2008 Standard Edition 64-bit'
5122:  'Windows Server 2008 Enterprise Edition'
5123:  'Windows Server 2008 Enterprise Edition 64-bit'
5124:  'Windows Server 2008 Datacenter Edition'
5125:  'Windows Server 2008 Datacenter Edition 64-bit'
5126:  'Windows Web Server 2008'
```

5127: 'Windows Web Server 2008 64-bit'

5128: 'Windows Storage Server 2008'

5129: 'Windows Storage Server 2008 64-bit'

5130: 'Windows Small Business Server 2008'

5131: 'Windows Essential Business Server 2008'

5132: 'Windows Server 2008 IA-64 Edition'

5133: 'Windows Server 2008 IA-64 or later'

5134: 'Windows Server 2008 or later'

5135: 'Windows Server 2008 Editions (32bit)'

5136: 'Windows Server 2008 (64-bit)'

5143: 'RIM OS'

5144: 'Virtualization Hypervisor'

5145: 'Microsoft Hyper-V'

5148: 'Windows Server 2008 Hyper-V'

5146: 'VMware ESX'

5149: 'VMware ESX 3.5'

5147: 'VMware ESXi'

5150: 'VMware ESXi 3.5'

5153: 'Virtual Host Machine'

5154: 'HP Chassis'

5155: 'IBM Server'

5188: 'Windows Server 2008 R2'

5189: 'Windows Server 2008 R2 Datacenter 64-bit'

5190: 'Windows Server 2008 R2 Enterprise 64-bit'

5191: 'Windows Server 2008 R2 IA-64 Edition'

5192: 'Windows Server 2008 R2 Standard 64-bit'

5195: 'Windows Server 2008 R2 Server Core Standard 64-bit'

5198: 'Windows Server 2008 R2 Server Core Enterprise 64-bit'

5201: 'Windows Server 2008 R2 Server Core Datacenter 64-bit

5202: 'Windows Web Server 2008 R2 64-bit'

5206: 'Windows Web Server 2008 R2 Server Core 64-bit'

5212: 'Windows Server 2008 R2 or later'

5213: 'Windows Server 2008 R2 Server Core Installation'

5210: 'Windows Server 2008 Server Core Installation,

5211: 'Windows Server 2008 (64-bit) Server Core Edition,

5193: 'Windows Server 2008 Server Core Standard Edition'

5194: 'Windows Server 2008 Server Core Standard 64-bit'

5196: 'Windows Server 2008 Server Core Enterprise Edition'

5197: 'Windows Server 2008 Server Core Enterprise 64-bit'

5199: 'Windows Server 2008 Server Core Datacenter Edition'

5200: 'Windows Server 2008 Server Core Datacenter 64-bit'

5203: 'Windows Web Server 2008 Server Core Edition'

5204: 'Windows Web Server 2008 Server Core 64-bit'

5156: 'Windows 7'

5157: 'Windows 7 Enterprise'

5158: 'Windows 7 Enterprise 64-bit'

5159: 'Windows 7 Home Premium'

5160: 'Windows 7 Home Premium 64-bit'

5161: 'Windows 7 Professional'

5162: 'Windows 7 Professional 64-bit Edition'

5163: 'Windows 7 Starter'

5164: 'Windows 7 Home Basic'

5165: 'Windows 7 Home Basic 64-bit'

5166: 'Windows 7 Ultimate'

5167: 'Windows 7 Ultimate 64-bit'

5214: 'Windows Vista or later'

5215: 'Windows 7 or later'

5217: 'Windows Vista (64-bit) or later'

5218: 'Windows 7 (64-bit) or later'

5216: 'Windows 7 Editions'

5219: 'Windows 7 (64-bit)'

5168: 'Macintosh 10.6'

5220: 'Open SUSE'

5221: 'Open SUSE 11.0'

5222: 'Open SUSE 11.1'

Web Services Reference Guide: Enumerations Section

Add the following enumerations to the Enumerations section:

LinkedObjectTypeRequired

CONSTRAINT_NONE

No related objects to unit group are listed

CONSTRAINT_ALL

All related objects to unit group are listed

PackageExportType

SOFTWAREPACKAGE

Exports as a software package

LIBRARYIMAGE

Exports as a library image

Web Services Reference Guide: Sequences Section

Add the following items that is missing from the list under the computerClassID subsection:

252: 'SuSE Linux Professional 9.1'

138: 'Windows 2003 Standard'

139: 'Windows Small Business Server 2003'

140: 'Windows Enterprise Server 2003 64-bit'

141: 'Windows Enterprise Server 2003 Itanium 64-bit'

290: 'HPUX 10.00'

291: 'HPUX 10.10'

292: 'HPUX 10.20'

293: 'HPUX 10.30'

297: 'Windows Vista'

298: 'Windows Vista Business'

299: 'Windows Vista Enterprise'

300: 'Windows Vista Home Premium'

301: 'Windows Vista Home Basic'

302: 'Windows Vista Ultimate'

303: 'Windows Vista Business 64-bit'

304: 'Windows Vista Enterprise 64-bit'

305: 'Windows Vista Home Premium 64-bit'

306: 'Windows Vista Home Basic 64-bit'

307: 'Windows Vista Ultimate 64-bit'

308: 'Windows Mobile'

309: 'Windows Mobile 5.0'

5137: 'Windows Mobile 6.0'

5029: 'Mac 10.x or later'

5082: 'SuSE Linux Ent Server 10'

5083: 'SuSE Linux Ent Server 10.1'

5084: 'SuSE Linux Ent Desktop 10'

5085: 'SuSE Linux Ent Desktop 10.1'

5088: 'Windows Server 2003 Standard 64-bit'

5089: 'Windows Server 2003 Datacenter 64-bit'

5090: 'Unixware 7.1.3'

5091: 'Mac 10.5'

5092: 'RHEL Server 5'

5093: 'RHEL Desktop 5'

5094: 'RHEL Advanced Platform 5'

5116: 'RHEL Server 5.1'

5117 'RHEL Desktop 5.1'

5118: 'RHEL Advanced Platform 5.1'

5095: 'Solaris Domain Partition'
5096: 'Sun Servers'
5097: 'Sun Fire E25K'
5098: 'Sun Fire E20K'
5099: 'Sun Fire 15K'
5100: 'Sun Fire 12K'
5101: 'Sun Enterprise 10000'
5102: 'Sun Enterprise 6500'
5103: 'Sun Enterprise 5500'
5104: 'Sun Enterprise 4500'
5105: 'Sun Enterprise 3500'
5106: 'Windows Embedded for POS'
5107: 'Windows Embedded for Point Of Service Version 1'
5108: 'Windows Embedded'
5109: 'Windows Embedded'
5110: 'Windows Embedded for Point Of Service 1.0'
5111: 'HPUX 11.11'
5112: 'HPUX 11.31'
5114: 'ROOT RTOS'
5115: 'SUN RTOS '
5119: 'Windows Server 2008'
5120: 'Windows Server 2008 Standard Edition'
5121: 'Windows Server 2008 Standard Edition 64-bit'
5122: 'Windows Server 2008 Enterprise Edition'
5123: 'Windows Server 2008 Enterprise Edition 64-bit'
5124: 'Windows Server 2008 Datacenter Edition'
5125: 'Windows Server 2008 Datacenter Edition 64-bit'
5126: 'Windows Web Server 2008'

5127: 'Windows Web Server 2008 64-bit'

5128: 'Windows Storage Server 2008'

5129: 'Windows Storage Server 2008 64-bit'

5130: 'Windows Small Business Server 2008'

5131: 'Windows Essential Business Server 2008'

5132: 'Windows Server 2008 IA-64 Edition'

5133: 'Windows Server 2008 IA-64 or later'

5134: 'Windows Server 2008 or later'

5135: 'Windows Server 2008 Editions (32bit)'

5136: 'Windows Server 2008 (64-bit)'

5143: 'RIM OS'

5144: 'Virtualization Hypervisor'

5145: 'Microsoft Hyper-V'

5148: 'Windows Server 2008 Hyper-V'

5146: 'VMware ESX'

5149: 'VMware ESX 3.5'

5147: 'VMware ESXi'

5150: 'VMware ESXi 3.5'

5153: 'Virtual Host Machine'

5154: 'HP Chassis'

5155: 'IBM Server'

5188: 'Windows Server 2008 R2'

5189: 'Windows Server 2008 R2 Datacenter 64-bit'

5190: 'Windows Server 2008 R2 Enterprise 64-bit'

5191: 'Windows Server 2008 R2 IA-64 Edition'

5192: 'Windows Server 2008 R2 Standard 64-bit'

5195: 'Windows Server 2008 R2 Server Core Standard 64-bit'

5198: 'Windows Server 2008 R2 Server Core Enterprise 64-bit'

5201: 'Windows Server 2008 R2 Server Core Datacenter 64-bit

5202: 'Windows Web Server 2008 R2 64-bit'

5206: 'Windows Web Server 2008 R2 Server Core 64-bit'

5212: 'Windows Server 2008 R2 or later'

5213: 'Windows Server 2008 R2 Server Core Installation'

5210: 'Windows Server 2008 Server Core Installation,

5211: 'Windows Server 2008 (64-bit) Server Core Edition,

5193: 'Windows Server 2008 Server Core Standard Edition'

5194: 'Windows Server 2008 Server Core Standard 64-bit'

5196: 'Windows Server 2008 Server Core Enterprise Edition'

5197: 'Windows Server 2008 Server Core Enterprise 64-bit'

5199: 'Windows Server 2008 Server Core Datacenter Edition'

5200: 'Windows Server 2008 Server Core Datacenter 64-bit'

5203: 'Windows Web Server 2008 Server Core Edition'

5204: 'Windows Web Server 2008 Server Core 64-bit'

5156: 'Windows 7'

5157: 'Windows 7 Enterprise'

5158: 'Windows 7 Enterprise 64-bit'

5159: 'Windows 7 Home Premium'

5160: 'Windows 7 Home Premium 64-bit'

5161: 'Windows 7 Professional'

5162: 'Windows 7 Professional 64-bit Edition'

5163: 'Windows 7 Starter'

5164: 'Windows 7 Home Basic'

5165: 'Windows 7 Home Basic 64-bit'

5166: 'Windows 7 Ultimate'

5167: 'Windows 7 Ultimate 64-bit'

5214: 'Windows Vista or later'

5215: 'Windows 7 or later'

5217: 'Windows Vista (64-bit) or later'

5218: 'Windows 7 (64-bit) or later'

5216: 'Windows 7 Editions'

5219: 'Windows 7 (64-bit)'

5168: 'Macintosh 10.6'

5220: 'Open SUSE'

5221: 'Open SUSE 11.0'

5222: 'Open SUSE 11.1'

Web Services Reference Guide: Sequences Section

Add the following to the Sequences section:

ExportSoftwarePkgProperties

xsd:string targetPath

Specifies the target directory path where the software package is exported. The path can be a local or a network path.

xsd:boolean targetOnServer

To export the software package to the manager, set the field to 1.

To export the software package to the computer which has WebServices installed, set the field to 0.

PackageExportType exportAs

Specifies if the software package is exported as a Software Package or a Library Image.

Web Services Reference Guide: Array of Elements Section

Add the following introductory sentence to the UnitPropertyFilter subsection:

This sequence of elements specifies a search filter when searching for or listing units.

Web Services Reference Guide: Methods--Software--Software Packages Section

Add the following software packages methods:

ExportSoftwarePackage

The ExportSoftwarePackage exports the software package to a location on a local computer or a network path.

Input

xsd:string sessionId (m)

The session identifier.

xsd:string softwarePackageId (m)

The UUID of the software package to be exported.

dsm:ExportSoftwarePkgProperties softwareProperties (m)

This parameter specifies which software package properties are required to export.

Output

None

Remarks

None

ExportSoftwarePackageByName

The ExportSoftwarePackageByName exports the software package identified by name and version to a location on a local computer or a network path.

Input

xsd:string sessionId (m)

The session identifier.

xsd:string softwarePkgName (m)

The name of the software package to be exported.

xsd:string softwarePkgVersion (m)

The version of the software package to be exported.

dsm:ExportSoftwarePkgProperties softwareProperties (m)

This parameter specifies which software package properties are required to export.

Output

None

Remarks

None

Web Services Reference Guide: Methods--Units and Groups--Unit Groups Section

Add the following unit group methods:

DeleteUnitGroups2

Input

xsd:string sessionId (m)

Specifies the session Id obtained from the login to the web service.

dsm:ArrayOfstring unitGroupIds

An array of UUIDs that identify the groups to delete.

xsd:boolean forceDelete

Deletes all the unit groups. If set to true, the relationship with the unit groups is ignored.

If the value is set to false, the API returns the objects that are related to the unit groups and deletes the groups that are not related to any objects.

dsm:LinkedObjectTypeRequired objectType

Specifies the object type. If forceDelete is set to true, set the ObjectType as CONSTRAINT_NONE. Else, set it to CONSTRAINT_ALL.

Output

None

DeleteUnitGroupsByName2

Input

xsd:string sessionId (m)

Specifies the session Id obtained from the login to the web service.

dsm: ArrayOfstring unitGroupNames

An array of names that identify the groups to delete.

xsd:boolean forceDelete

Deletes all the unit groups. If set to true, the relationship with the unit groups is ignored.

If the value is set to false, the API returns the objects that are related to the unit groups and deletes the groups that are related to any objects.

dsm:LinkedObjectTypeRequired objectType

Specifies the object type. If forceDelete is set to true, set the ObjectType as CONSTRAINT_NONE. Else, set it to CONSTRAINT_ALL.

Output

None

CADSMCMD Reference Guide: compgroup--Computer Group Management Section

Add the following under the General Group Management:

deletewithwarn – Delete a computer group with warning

This action allows you to delete computer groups with warnings for any sealed software policies or catalog groups linked to it.

This action has the following format:

```
compgroup action=deletewithwarn name=group_name
```

name

Specifies the name of a computer group to be deleted.

Example:

To delete the group qg with warning, enter the following command:

```
cadsmcmd compgroup action=deletewithwarn name= qg
```

Note: If the computer group is deleted at the enterprise manager, the dependency check is done only at the enterprise manager and not on the domain manager where the group is replicated. The replication silently unlinks any software catalog group, disables any software policy, and unlinks the group before deleting the replicated group.

CADSMCMD Reference Guide: swlibrary--Software Library Commands Section

Replace the example for the swlibrary.assignGroupToTarget command under the General Software Group Management subsection with the following example, because three separate lines of code are inadvertently "hidden," that is, the lines are too minuscule in size to be read.

This will generate the subsequent jobs with the listed attributes:

```
test_001 2.1: install_min
task=install
after=exacttime
promptUser
Parameters="-x -y -z"
preaction=log0ff
```

```
postaction=reboot
test_022 1.0/00:inst_002
task=install
after=exacttime
promptUser
allowCancel
Parameters="-xon xf -rs"
test_022 1.0/00:configure_022
task=configure
after=exacttime
preaction=logoff
promptUser
allowCancel
Repeat
noCalendar
Parameters="-xon xf -rs"
test_022 1.0/00:activate_022
task=activate
after=exacttime
preaction=logoff
promptUser
allowCancel
Repeat
noCalendar
Parameters="-xon xf -rs"
test_010 1.0:inst_010
task=install
after=exacttime
promptUser
allowCancel
Parameters="-xon xf -rs"
test_001 1.0/00:configure_001
task=configure
after=exacttime
promptUser
Parameters="-init"
preaction=reboot
```

It will test_001 of version 2.1 in swg_1 as well as activate_022 of test_022 and version 1.1/00 in pg_11 will be ignored.

Remote Control Viewer Help: Viewer Pane Section

The following procedure is inadvertently missing from the Local Address Book subsection of the online help:

Create a Local Address Book

Use this procedure to create a local address book. You can create multiple local address books.

To create a local address book

1. Right-click the Local Address Book node and click New, Address Book.

   Alternatively, select New Address Book from the Tasks portlet of the Local Address Book pane.

   The New Address Book dialog appears.

2. Enter the name of the address book.
3. Optionally, enter a description.

   Note: Address books can have duplicate descriptions.

4. Click OK.

   The new address book appears in the DSM Remote Control tree and in the Local Address Book pane.

DSM Explorer Help: Engines Folder Section

Please remove the last bulleted item, Migration Tasks, from the Engine Tasks help topic.

CMG000052 Common GUI Message Must be Added to DSM Messages Help

Warning! You are about to delete some objects that have relationships to other objects. Deleting these objects will break the listed relationships.

Reason:

You are trying to delete some objects that have relationships to other objects, for example, an asset group might be linked to a catalog group or to a software policy. Deleting such an asset group will break the relationship. It will require additional actions to set them up again, for example, you can re-link an affected catalog group by dragging and dropping another asset group to it. Similarly, you can re-link the affected policy by dragging and dropping it to another asset group.

Action:

Click Yes to continue the deletion or No to cancel it. Click Copy to copy the list of related objects to the clip board for further use to repair the broken relationships.

Fixes

This section describes the fixes of this release of CA ITCM.

Warning to Relink Catalog Groups

If you try to delete a computer group which is linked to a catalog group or a sealed software policy, a message now appears to warn you that you are about to delete some objects that have dependencies. Deleting these objects will break relationships and will require additional actions to set them up again.

Note: If the computer group is deleted at the enterprise manager, the dependency check is done only at the enterprise manager and not on the domain manager where the group is replicated. The replication silently unlinks any software catalog group, disables any software policy, and unlinks the group before deleting the replicated group.

comConf action=setParm Can Be Used to Modify Encrypted Parameters

The CADSMCMD command "comConf action=setParm" can now be used to modify configuration parameters of type "encrypted," for example, passwords.

View the Discovered or Owned Inventory in Web Console

In a deployment scenario where the Oracle domain manager MDB is running on a non-default port, you can now access the discovered or owned inventory from the Web Console on the domain or enterprise manager.

Appendix A: Inventory File Properties

DCS creates an inventory file for each inventory detection module that you configured in the collect task that is linked to the agent computer. The inventory file is available in the agent's working directory. It contains one component (top-level group), the name of which is taken from the inventory detection module configuration.

The following sections describe the tables, groups, and the attributes in the inventory file.

This section contains the following topics:

Status (Group)

The Status group contains the following information about the overall status of the compliance check:

Attribute	Type	Description
Check completed	boolean	Specifies if the check completed is successful or not
Status	string	Specifies the reasons if the check is not completed

Status/Input Files (Table)

The Status/Input Files table contains the following information about the SCAP data stream files that are processed:

Attribute	Type	Description
Name	string	Specifies the file name of the input SCAP data stream
Type	string	Specifies if the input file is an XCCDF or OVAL file
Location	string	Specifies the location of the input file
Timestamp	string	Specifies the date and time when the input file was created
Size	int64	Specifies the size of the input file in bytes

Status/Output Files (Table)

The Status/Output Files contains the following information about the output files that the scanner produces:

Note: This table does not include the inventory file.

Attribute	Type	Description
Name	string	Specifies the output file name
Type	string	Specifies if the output file is an XCCDF or OVAL file
Location	string	Specifies the location of the output file
Timestamp	string	Specifies the date and time when the output file was created
Size	int64	Specifies the size of the output file in bytes

General (Group)

The General group contains the following information about the benchmark and the test:

Attribute	Type	Description
ID	string	Specifies a unique ID for the test result reported in a particular inventory file
Profile	string	Optional. Specifies the ID of the profile applied during the benchmark application
Start time	string	Specifies the time when the benchmark application or compliance check started
End time	string	Specifies when the check ended. Both start and end times are given as strings in the format used for XCCDF files
Benchmark Ref	int64	Specifies a reference (filename or link) to the used XCCDF file
Title	string	Optional
Remark	string	Optional
Organization	string	Optional. Specifies the organization that is responsible for the results
Organization_2, Organization_3...	string	Optional. Specifies additional organizations. If the additional organizations are hierarchical then they must appear in high-to-low order

General/Identity (Optional Group)

The General/Identity optional group contains the following information about the user account used for the test:

Attribute	Type	Description
Name	string	Specifies the name of the identity (user account) of the benchmark
Privileged	bool	Specifies if the identity was privileged (administrator)
Authenticated	bool	Specifies if the identity was authenticated

Target (Group)

The Target group contains the following information about the target computer where scanner performed the benchmark test:

Attribute	Type	Description
Name	string	Specifies the name of the target computer on which the benchmark test was applied
Address	string	Optional. Specifies the network address of the target computer
Address 2, 3,...	string	Optional. Specifies additional network addresses

Target/Facts (Optional Table)

The Target/Facts optional table contains the following information about the target computer:

Attribute	Type	Description
Name	string	Specifies the name of the fact (a URL)
Type	string	Specifies the "number", "string" or "boolean"
Value	string	Specifies the value

Set Values (Table)

The Set Values table contains the following information about the values used for the value objects during the test:

Attribute	Type	Description
ID	string	Specifies the ID of the used value
Value	string	Specifies the used value

Rule Results/<rule id> (Group)

The Rule Results/*rule id* group contains the following information about the groups created for each rule that is selected during the test:

Attribute	Type	Description
Idref	string	Specifies the name of the fact (a URL)
Role	string	
Time	string	Specifies the time when the result was generated
Severity	string	
Version	string	
Weight	double	Specifies the weight of the result in the weighted scoring models
Result	string	Specifies the result such as, "pass", "fail", "error", "unknown", "notchecked" or "notapplicable"

Rule Results/<rule id>/Idents (Optional Table)

The Rule Results/*rule id*/Idents optional table contains a table of globally meaningful identifiers for the rule such as CCE IDs with the following information:

Attribute	Type	Description
System	string	Specifies a URL identifying the naming system
Name	string	Specifies the name of the identifier in the naming system

Scores (Table)

The Scores table contains the following information about the test scores according to the models specified in the benchmark:

Attribute	Type	Description
Model	string	Specifies the URL of the scoring model
Score	double	Specifies the achieved score
Maximum	double	Specifies the possible maximum score

Appendix B: SCAP Configuration Parameters

This section describes the SCAP configuration parameters that you need to specify while configuring an FDCC inventory detection module. You can either use the SCAP Configuration dialog or specify the following parameters in the text field provided on the Configuration tab of the Create New Inventory Module dialog:

SCAPPath

Specifies the path to the SCAP data stream directory on the agent computer. This path must match the SCAP data stream directory on the domain manager. For example, for the IE7 checklist, specify FDCC-Major-Version-1.2.1.0\ie7. When the checklist is distributed to the agent computer, a similar directory structure is created under the *ITCM_installpath*\Agent\units\00000001\UAM\ SCAP_Content directory on the agent computer.

XCCDFFile

Specifies the name of the XCCDF file in the SCAP data stream that determines the compliance benchmark.

Note: This file must be present in the location specified in the SCAPPath parameter.

XCCDFID

Specifies the ID given against the Benchmark tag in the XCCDF file. For example, the benchmark ID for Windows XP checklist is FDCC-Windows-XP.

CPEDictionary

(Optional) Defines the name of the CPE dictionary file. If the SCAP data stream contains a dictionary file, specify the file name against this parameter; otherwise, you can omit this parameter.

Note: This file must be present in the location specified in the SCAPPath parameter.

InvComponent

Defines the component name to use in the inventory file produced by the scanner. This value is used as the top-level group name in the inventory file and hence also appears as the inventory component name under the Inventory, SCAP category in the DSM Explorer.

CollectXCCDFResultFile

Configures the collection of XCCDF result files for the checklist from the Asset Management agent's working directory to the domain manager.

Default: false

CollectOVALResultFiles

Configures the collection of OVAL result files for the checklist from the Asset Management agent's working directory to the domain manager.

Default: false

XCCDFProfile

Specifies the title of the XCCDF profile to be applied for the compliance check. Leaving the value of this parameter empty applies no profile, and thus uses all the settings inthe XCCDF file.

OutputPath

Defines the directory in which the OVAL and XCCDF result files are to be placed. You can either specify an absolute path or a path relative to the SCAP_Result_Files directory, which is under the Asset Management agent's working directory. If this field is empty, the files are stored under the default path, which is *agent working directory*\SCAP_Result_Files\Data Stream Path.

Note: The user account that runs the scan must have write access to the directory specified in this field.

OvaldiPath

Defines the directory on the agent computer that contains the Ovaldi interpreter. You can specify either an absolute path or a path relative to the bin directory of the agent installation. The OVAL interpreter shipped with this release of CA ITCM is installed under the *ITCM_installpath*\bin\ovaldi-CA directory. If your SCAP data stream requires an OVAL interpreter other than the one shipped with this release, ensure to distribute the OVAL interpreter to all the agent computers and specify the path in this field.

Default: *ITCM_installpath*\ovaldi-CA

Organization

(Optional) Defines the name of the organization that you want the <*organization*> tag to contain in the XCCDF result file. Specify the organization name and click Add to List.

Note: You can add any number organizations and move them in the order that you want. The values are hierarchical with the highest level appearing first.

Appendix C: Third-Party Acknowledgments

This appendix provides software license agreements for components of third-party software used with DCS.

The OVALDI Software License, Version 5.5.4

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of The MITRE Corporation nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE,EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Glossary

Common Configuration Enumeration (CCE)

Common Configuration Enumeration (CCE) is one of the SCAP standards. It contains Standard identifiers and dictionary for system configuration issues related to security. A rule definition in an SCAP data stream can contain references to one or more CCE identifiers, indicating that the rule is a representation of a specific CCE configuration guidance statement or configuration control. For more information, go to http://cce.mitre.org/.

Common Platform Enumeration (CPE)

Common Platform Enumeration (CPE) is one of the SCAP standards. It contains standard identifiers and dictionary for platform or product naming. For example, some elements in XCCDF files can be restricted to only apply to certain platforms and this is done using CPE identifiers. For more information, go to http://cpe.mitre.org/.

Common Vulnerabilities and Exposures (CVE)

Common Vulnerabilities and Exposures (CVE) is a dictionary of common names (that is, CVE Identifiers) for publicly known information security vulnerabilities. These identifiers make it easier to share data across separate network security databases and tools. CVE is one of the components used in SCAP. See http://cve.mitre.org/ for details.

Common Vulnerability Scoring System (CVSS)

Common Vulnerability Scoring System (CVSS) is one of the SCAP standards. It contains standards for conveying and scoring the impact of vulnerabilities. For more information, go to http://www.first.org/cvss/index.html.

eXtensible Configuration Checklist Description Format (XCCDF)

eXtensible Configuration Checklist Description Format (XCCDF) is a specification language for writing security checklists, benchmarks, and related kinds of documents. An XCCDF document represents a structured collection of security configuration rules for some set of target computers. The specification is designed to support information interchange, document generation, organizational and situational tailoring, automated compliance testing, and compliance scoring. For more information, go to http://nvd.nist.gov/xccdf.cfm.

MITRE

The *MITRE Corporation* is a not-for-profit organization chartered to work in the public interest. MITRE offers the interpreters, source code, schemas, and data files at no cost so that individuals and organizations can build and expand upon them. Ovaldi is one such interpreter that is freely available.

National Institute of Standards and Technology (NIST)

National Institute of Standards and Technology (NIST) is a non-regulatory federal agency within the U.S. Department of Commerce. NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life. The United States (U.S.) National Vulnerability Database (NVD), operated by the NIST, provides a repository and data feeds of content that utilize the SCAP standards. It is also the repository for certain official SCAP standards data. Thus, NIST defines open standards within the SCAP context and defines the mappings between the SCAP enumeration standards.

Open Vulnerability and Assessment Language (OVAL)

Open Vulnerability and Assessment Language (OVAL) is one of the SCAP standards. It contains standard XML for testing procedures for security related software flaws, configuration issues, and patches as well as for reporting the results of the tests. All the rule checks in the checklists take the form of references to OVAL definitions contained in OVAL files from the SCAP data stream. For more information, go to http://oval.mitre.org/.

Ovaldi

Ovaldi is an OVAL Interpreter developed by the MITRE Corporation. It is a freely available reference implementation created to show how information can be collected from a computer for testing to evaluate and carry out the OVAL definitions for that platform, and to report the results of the tests. The interpreter demonstrates the usability of OVAL Definitions and ensures correct syntax and adherence to the OVAL Schemas.

SCAP data stream

SCAP data stream consists of security checklist data represented in automated XML formats, vulnerability and product name related enumerations, and mappings between the enumerations. An SCAP data stream consists of the XML following files:

- An XCCDF file
- One or more OVAL files
- (Optional) A CPE dictionary file

Security Content Automation Protocol (SCAP)

The *Security Content Automation Protocol (SCAP)*, pronounced "S Cap", is a method for using the standards such as XCCDF, CCE, CVE, CVSS, CPE, and OVAL to enable automated vulnerability management, measurement, and policy compliance evaluation (e.g., FISMA compliance). More specifically, SCAP is a suite of selected open standards that enumerate software flaws, security related configuration issues, and product names; measure systems to determine the presence of vulnerabilities; and provide mechanisms to rank (score) the results of these measurements in order to evaluate the impact of the discovered security issues. SCAP defines how these standards are combined. The National Vulnerability Database provides a repository and data feeds of content that use the SCAP standards. For more information, go to http://nvd.nist.gov/.

XCCDF profile

An *XCCDF profile* is a policy that is applied to the target computer or compared to the configuration of the target computer. The XCCDF file for each SCAP data stream defines the list of profiles supported. The XCCDF file must have at least one XCCDF profile, which specifies the rules to be used for checking a particular type of system. You can create separate XCCDF profiles for each applicable operational environment in which a system may be deployed.

Index

I

L

M

N

O

P

Q

R

S

T

U

V

W