CA IT Client Manager

Software Delivery Administration Guide

12.8

CA Technologies Product References

This documentation set references to the following CA products:

- CA Advantage® Data Transport® (CA Data Transport)
- CA Asset Intelligence
- CA Asset Portfolio Management (CA APM)
- CA Common Services™
- CA Desktop Migration Manager (CA DMM)
- CA Embedded Entitlements Manager (CA EEM)
- CA Network and Systems Management (CA NSM)
- CA Patch Manager
- CA Process Automation
- CA Business Intelligence
- CA Service Desk Manager
- CA WorldView™
- CleverPath™ Reporter

Contact CA Technologies

Contact CA Support

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

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

Providing Feedback About Product Documentation

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

To provide feedback about CA Technologies product documentation, complete our short customer survey which is available on the CA Support website at http://ca.com/docs.

Contents

Chapter 5: Using Software Delivery 35

Chapter 1: Introduction

The software delivery (SD) component within CA ITCM accelerates and automates the deployment of software and other digital content to resources across the extended enterprise. The SD component comprises flexible tools to build, distribute, install, and manage software packages and operating systems on target computers from anywhere to anywhere.

The software delivery functions enable the management of software on all computers belonging to interconnected or autonomous networks, and let you attain full control over the operation and performance of software installed on the computers connected to your network. The SD management capabilities allow installation, configuration, verification, and removal of software throughout your business environment in a controlled and standardized way, providing a broad platform and protocol coverage for software administration throughout the enterprise.

Using SD functions and tools, you can be sure that software is installed correctly and on time, ensuring that your distributed computing services are dependable and provide a better service to your users.

This guide describes the software delivery concepts and procedures that let you administer the controlled distribution and management of software at your site. Although this guide specifically addresses the concerns of the system administrator, it benefits anyone who wants to understand how SD functionality solves the problem of managing the distribution and installation of software packages across a system of networked computers.

This section contains the following topics:

Software Delivery as Part of CA ITCM

The software delivery functionality shares core pieces of the CA ITCM infrastructure, for example, database, communications, process control, and event management. This concept provides numerous benefits including simplified administration, unmatched capability, improved performance across all functionality areas, and consistent data and terminology.

Use of Data Transport Service Functionality

Data Transport Service (DTS) controls the flow of data transfers in the software delivery environment. DTS supports point-to-point and point-to-many data transfers including Broadcast, Multicast, and Fanout (which results in a single read with multiple sends and multiple writes). You can also optimize network performance by throttling parcel sends and restricting parcel size.

Through the integration of Data Transport Service with the software delivery functionality, you can halt, resume, and terminate data transfers from the software delivery dialogs. For more information see "Integration with Data Transport Service" (see page 171).

Chapter 2: Software Delivery Functions

The software delivery (SD) functionality within CA ITCM comprises flexible services to configure the different components in your network. Before you configure your software distribution environment, you need to understand the roles that the SD functions play.

This section contains the following topics:

Selecting Software Delivery Components

The software delivery functions you select and how you structure them, depends on how your organization is configured and how you want to control the distribution of software across that organization.

The minimal required implementation includes a standalone domain manager and agents. Additional scalability servers can be deployed, if management of remote networks is required or greater deployment concurrency is needed. Additional domain managers can be used, if even greater scalability or domain autonomy is required. If more than one domain manager is used, an enterprise manager can be deployed to allow for centralized management of the entire software delivery network.

Software Package Library

The Software Package Library is the location where all software is registered and stored. Software that is not registered cannot be managed.

Software Package Libraries can reside on enterprise managers, domain managers, and scalability servers. The Software Package Library stores all programs to be distributed to target computers regardless of the program's intended operating system, provided the manager can read the program's installation media.

For example, to register a Linux program on a manager on Windows, you must load the Linux program onto a media the computer hosting the manager on Windows can read.

Domain Manager

The domain manager is the only mandatory management tier. It supports management of individual agents and scalability servers and groups of those. The domain manager is responsible for the following tasks:

- Maintain configuration information of the CA ITCM domain
- Configure the security for administrators who can connect to the domain manager and the extent of permissions they have on each object class
- Trigger the engine to collect data stored in the scalability server
- Evaluate and build job containers and send them to scalability servers
- Receive job container results from the scalability servers and agents
- Evaluate dynamic computer groups
- Evaluate software policies
- Evaluate and build operating system deployments
- Replicate objects between itself and its enterprise manager

The operating system environments currently supported by the domain manager are listed in the *Certification Matrix* available at CA Support.

Enterprise Manager

The enterprise manager is an optional management tier that allows for central management of multiple domain managers and groups of agents and scalability servers. The enterprise manager is responsible for the following tasks:

- Provide visibility and control of the entire enterprise, where multiple CA ITCM domains have been implemented
- Maintain configuration information of the enterprise
- Configure the security for administrators who can connect to the enterprise manager and the extent of permissions they have on each object class
- Communicate with a domain manager to push jobs and collect results of those jobs

The operating system environments currently supported by the enterprise manager are listed in the *Certification Matrix* available at CA Support.

Scalability Server

A scalability server is an optional management-free tier that is used when handling large numbers of agents, usually on remote networks separated by a WAN. It can be seen as a fan out mechanism to optimize network utilization.

A software delivery scalability server has a Software Package Library (called staging library) where software packages can be permanently stored to avoid sending a package over the network every time it is required by the agent. Instead of all the individually managed end systems (agents) communicating directly with a single manager, the load can be shared across multiple scalability servers.

Scalability servers use a file store database as a local repository to store the information required to service the agents. In a minimal scalability server installation, the file database consists of a dictionary of registered agents and the basic inventory reported by these.

A scalability server includes the Boot Server, which is needed for operating system deployment.

Note: With virtual applications, the scalability server also functions as the streaming server for virtual application packages that are streamed to target computers running the Windows operating system. See Registering Virtual Applications (see page 49) and Delivering Virtual Applications (see page 105) for more information.

The operating system environments currently supported by the scalability server are listed in the *Certification Matrix* available at CA Support.

Software Delivery Agent

The software delivery (SD) agent is mandatory on a target computer, if that computer should be managed by software delivery functions. The SD agent provides software installation services and basic hardware inventory. The Windows agent also supports user profile management.

The SD agent supports the following:

- Agents for Linux and UNIX
- Docked device proxy agents
- PC agents

SD agents can be deployed by using the deployment mechanisms provided by CA ITCM, by using the CA ITCM installation DVD, or previous versions of the software delivery component (migration).

The operating system environments currently supported by the SD agent are listed in the *Certification Matrix* available at CA Support.

The software delivery component supports Windows Vista and above as an agent operating system environment. Due to restrictions in Windows Vista in context of running user interfaces from within a Windows service, the SD agent has been redesigned. The SD agent is able to detect, if it runs on a Windows Vista or Microsoft Server 2008 operating environment and act appropriately. In a non-Windows Vista operating environment, the SD agent runs as in previous releases.

Software Delivery Agent Bridge

The Software Delivery Agent Bridge (SD Agent Bridge) provides backwards compatibility for extended and legacy Unicenter Software Delivery (SD) agents and includes a common legacy server component and its process components and specific software delivery components

The SD Agent Bridge support for extended and legacy Unicenter SD agents is fully integrated with the scalability server. It is configurable by policy, and starts and stops as a software delivery scalability server thread.

For detailed information, in particular installation and configuration considerations, see Use of SD Agent Bridge (see page 133),

Docking Devices

The term "docking device" in the software delivery (SD) context is a computer type used to describe a mobile device that is connected to the SD infrastructure through a "desktop companion". The docking device represents the mobile device, although its address is that of its desktop companion.

The mobile device is connected to the desktop companion in some way (for example, through an attachment to the serial port.) The desktop companion is equipped with an SD agent.

Job Check is initiated on the desktop companion when the device is connected to the SD agent. This makes the mobile device (represented by a docking device icon), a member of the All Computers and Users group on the domain manager to which the SD agent is connected.

Any software that is going to be installed on a docking device must first be registered in the Software Package Library. This software is typically third-party software.

Jobs that are targeted for the mobile device are executed as long as the device is connected to its SD agent. If the device is moved to another location, from where it is connected to a SD agent computer that belongs to the same domain manager as the previous SD agent, then any pending jobs are executed at that connection time, provided the user is also configured at this other desktop computer.

The proxy agent platforms currently supported are listed in the *Certification Matrix* available at CA Support.

For a description on how to enable a docking device on Windows, see the section *How to Enable a Docking Device on Windows* in the *Installation of CA ITCM, Implementation Guide*.

Catalog

The Catalog is an optional user interface for placing software requests with the domain manager. With the Catalog, users can install software deemed optional by the administrator on their own systems using the software delivery network and its configuration.

Logon Shield for Windows Operating Environments

The Logon Shield ensures that the system can perform installations or updates of applications, without being disturbed by users logging on during the installation or update process. In other words, the Logon Shield, when activated, prevents users from logging on to a Windows operating system. The Logon Shield feature is available for all Windows NT operating environments and Windows Vista.

As Microsoft has changed the underlying technology for the Windows Vista operating system, the Logon shield feature has been aligned to meet the Windows Vista requirements. In pre-Windows Vista environments the logon shield works based on Microsoft's Graphical Identification and Authentication (GINA) concept, whereas in Windows Vista operating environments it works on the concept of credential provider filtering. On the target systems, the user interface of the logon shield differs slightly in Windows Vista and non-Windows Vista operating environments.

The Logon Shield can be enabled and configured using the Logon Shield configuration view on the DSM Explorer (see page 32). The Logon Shield can also be enabled implicitly when setting up a software distribution job (see page 34).

Note: When the Logon Shield is activated for the first time on pre-Windows Vista systems, a system reboot is initiated before executing the first job that uses Logon Shield protection.

Software Management Packager

The Software Management Packager (Packager) lets you package software and data into products, using a CA Technologies-specific packaging format, to make them available for installation on target computers.

The Packager is available for Windows, Linux, and UNIX operating environments.

The current operating system environment types and versions supported by the Packager are listed in the Certification Matrix available at CA Support.

Packager for Windows

The Packager for Windows resides on a separate dedicated Packaging Computer. Only the operating system and the Packager must be installed on the Packaging Computer. The Packaging Computer can run a Windows NT Technology or Windows Vista operating system.

During the packaging process, the product to be packaged is installed on the individual operating system of this Packaging Computer. You can specify product files, installation parameters, and other necessary changes. The Packager records this and all other information required for a successful later installation of the software package and generates an installable software image.

The installable product (image) is packaged in the SXP packaging format.

Important! The software image can be installed only on target computers that run the same operating system type as the Packaging Computer during the packaging process.

Packager for Linux and UNIX

The Packager for Linux and UNIX software does not require a separate computer for packaging, it can be run on any Linux or UNIX computer.

During the packaging process the product to be packaged, including all files and parameters, is defined in a prototype file. This can be done using the Packager GUI or through the command line. The installable product (image) is built from this prototype file.

The packaging format of the product is called PIF (product interchange format).

Desktop Management Script Generator and Editor

The Desktop Management Script Generator is a tool that lets you record configuration changes for an installed product, for example, registry modifications. The Script Generator takes a snapshot of the computer and builds an image and installation script. This script can then be registered in the Software Package Library and installed on target computers that have the script interpreter installed. The Desktop Management Script Generator is not suitable for complex product installations.

You can use the Desktop Management Script Editor to write, syntax-check, debug, and run scripts.

Chapter 3: Implementation

For a more complete understanding of the software delivery functionality and components, this chapter presents an implementation model and a scenario for managing the installation and removal of software.

This section contains the following topics:

Configuring the Manager Hierarchy

If you need centralized management and the number of managed systems does not exceed the recommended limits, as determined by the size of a domain manager, a single domain is recommended.

If you need centralized management and the number of managed systems exceeds the recommended limits, as determined by the size of a domain manager, an enterprise with multiple domains is recommended.

There may be other reasons for choosing an enterprise approach, even if a single domain is suitable for managing all managed systems. There may be requirements for administrators of individual sites to have full control over the managed systems within that site. In this case, a domain per site may be suitable. However, a degree of local autonomy may also be achieved using the security mechanisms in CA ITCM to split ownership of agents and other objects in the management database of a domain manager between multiple administrators.

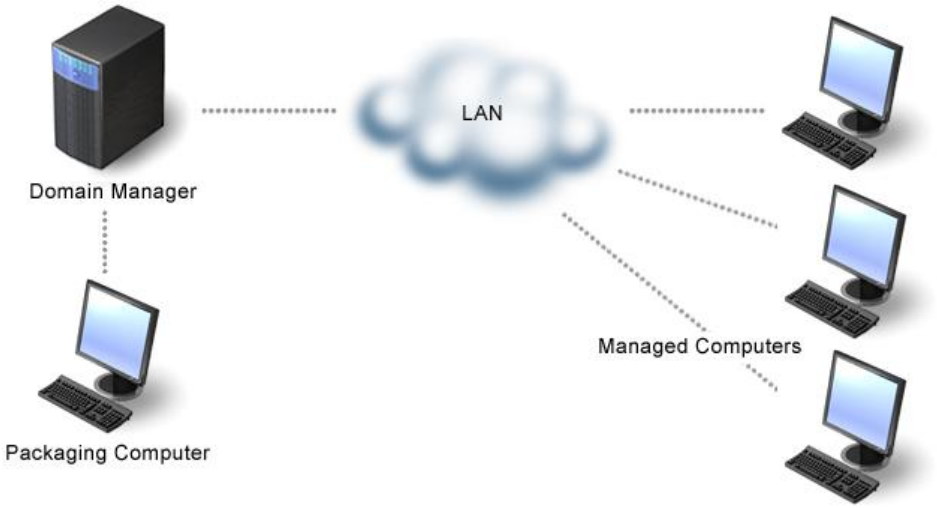
In most scenarios, it is useful to install the enterprise manager when multiple domains are being used. Enterprise reporting is one benefit. Even if management of agents is performed strictly by the domain administrators, it may be valuable to produce enterprise-wide reporting on all agents and software in the enterprise. An additional advantage of the enterprise is the integration between CA ITCM and other CA Technologies software, such as CA Service Desk Manager and Unicenter Asset Portfolio Management. Many companies prefer to have a centralized help desk or procurement function even though administration of managed systems is distributed between site administrators using multiple domains. In such scenarios, we recommend that you use an enterprise solution to achieve maximal benefit from the inter-product integration. Note that if a single domain is deemed sufficient, inter-product integration is also available at domain level.

The following configuration options are available when designing your distribution structure:

- A domain manager with a local administrator
- An enterprise manager with local administrators
- An enterprise manager without local administrators

Domain Implementation

In a domain implementation, the domain manager controls the distribution of software to one or more agents. The domain manager and the computers networked to that manager comprise a domain. Typically, in a domain implementation, agents are based at the same site and connected to the manager over a local area network (LAN), as shown in the following illustration:



When the domain manager functions without an enterprise manager, it is referred to as an autonomous (stand-alone) domain manager.

Advantages of an Autonomous Domain Manager

Using an autonomous domain manager works well when all managed computers are connected to the same logical network and the total number of participating computers is within the limit permitted, as determined by the size of the manager. In such a situation, this setup avoids unnecessary infrastructure and hardware, while preserving the benefits of manageability and uniformity offered by the software delivery functionality.

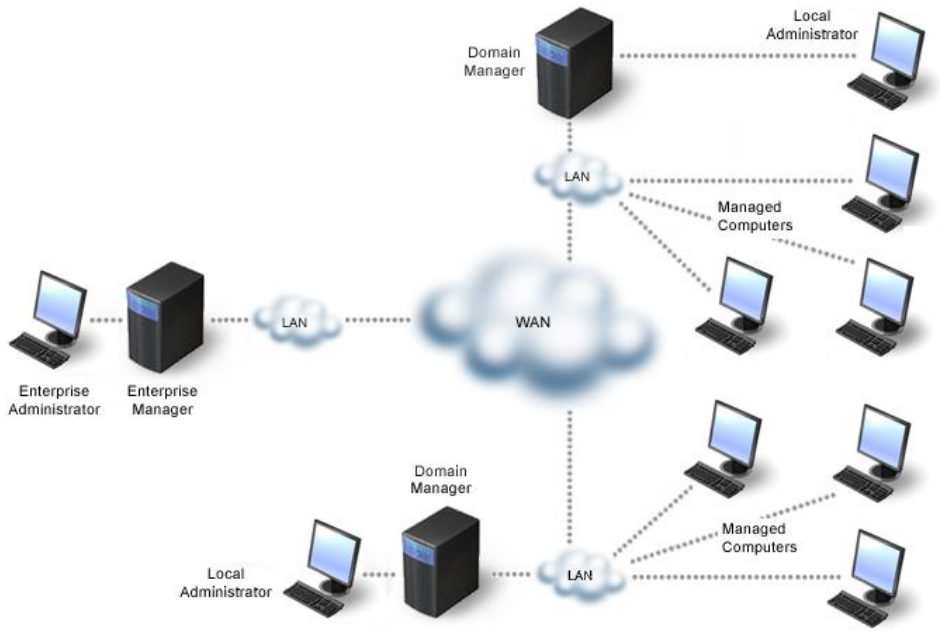
Disadvantages of an Autonomous Domain Manager

If your organization has more than one domain, using an autonomous domain structure at each site bypasses the centralized control offered by having an enterprise manager connected to several domains. Domain managers cannot use software delivery functionality to distribute software to each other.

Enterprise with Local Administrators Implementation

This system configuration consists of an enterprise manager and several domain managers (domains), where each domain manager can be administered by its own local administrator.

The following illustration shows a sample scenario of an enterprise implementation with local administrators:



In this implementation scenario the enterprise manager attached to several domain managers provides centralized control over a large system of multiple LANs connected by a WAN.

The enterprise administrator distributes software to the domain managers, and each local administrator installs and maintains these items on the computers in their domain. This way, local administrators provide an additional level of software installation and maintenance control over individual domains.

Advantages of an enterprise with local administrators

This system configuration has a centralized control, yet also allows domain managers to customize the distribution process to individual computers and thus operate independently of the enterprise manager.

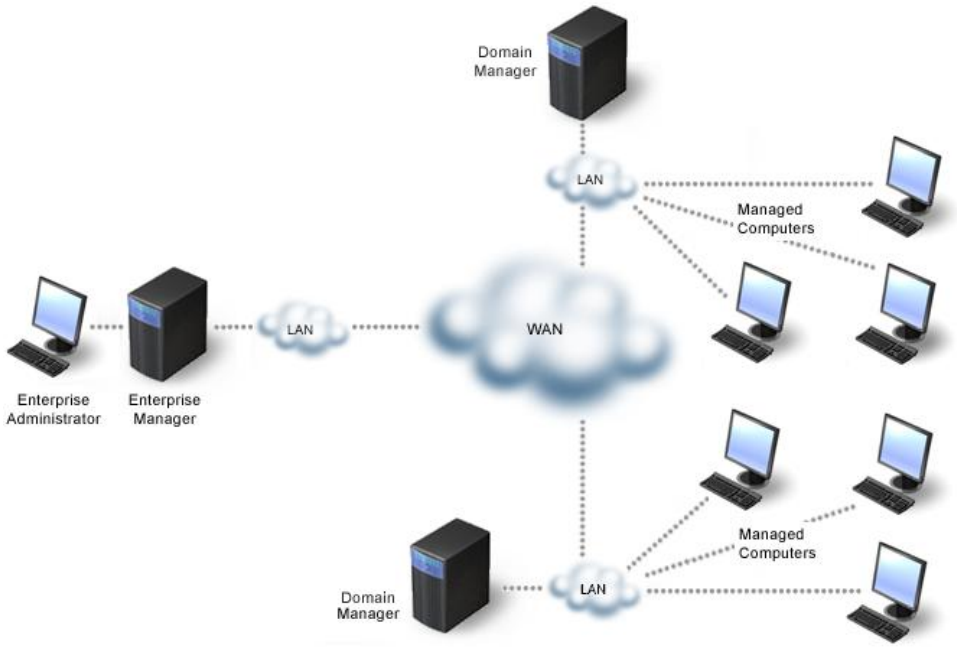
Disadvantages of an enterprise with local administrators

As the local administrator can distribute software without intervention by the enterprise administrator, this structure decreases centralized control. The enterprise administrator does, however, retain all monitoring capability and can send orders to remove unauthorized software.

Enterprise without Local Administrators Implementation

This system configuration consists of an enterprise manager and several domain managers (domains), where the domain managers are administered solely by the enterprise administrator from the enterprise manager.

The following illustration shows a sample scenario of an enterprise implementation without local administrators:



In this implementation scenario the enterprise manager attached to several domain managers provides centralized control over a large system of multiple LANs connected by a WAN.

The enterprise administrator distributes software to the domain managers, manages the software in the domain libraries, and is able to install and maintain software on the target computers. This way, the implementation of an enterprise manager with several domains and no local administrators provides completely centralized control over the software installed on computers at the domains.

Advantages of an enterprise without local administrators

This system configuration provides for centralized control over all domain managers and target computers from a single location and eliminates the need for intervention by local administrators at each domain manager.

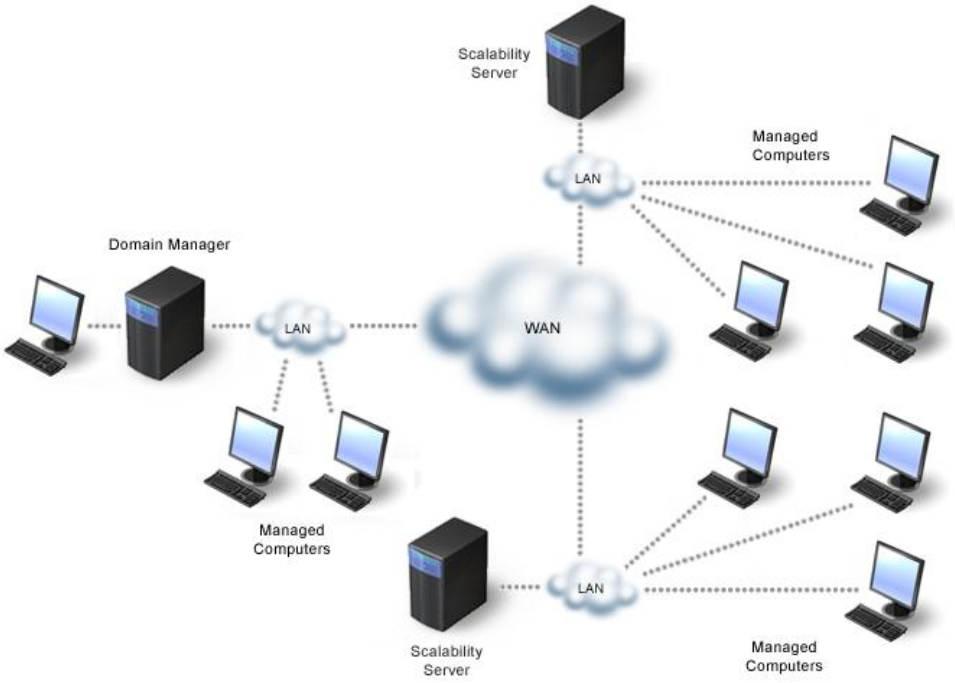
Disadvantages of an enterprise without local administrators

This system configuration makes no provision for customization and variation at the domain managers.

Use of Scalability Servers

Scalability servers improve scalability and performance. The domain manager is bundled with a scalability server; additional scalability servers are optional.

The following illustration shows a typical scenario for using scalability servers in a network:



To avoid unnecessary network traffic over the WAN, scalability servers are deployed to each remote location or site in the network. By also using the software libraries of the scalability servers for permanent storage of software packages, only control data needs to be transferred across the WAN. The initial deployment of the software packages to the remote libraries can be done over the WAN, but local registration is also supported if the WAN links are very slow.

Geographical dispersion is one of the main reasons for using scalability servers, but other factors should be considered when planning the software delivery network, including the delivery window and library access methods:

- **Delivery window:**

  The delivery window is defined by the maximum accepted time to deliver and execute a particular software package to all managed systems. The delivery window is defined by the software delivery user and not by CA Technologies.

- **Library access methods:**

  Consider which library access method is to be used by the agents. Different access methods expose the scalability server and network to different loads. The scalability server can be configured by how many concurrent software jobs are allowed.

Software Delivery Enhancements for Interactive Software Deployment on Windows Vista or Later

When you deploy a software package to a Windows agent, the installation program starts in the SYSTEM context.

In Windows versions before Vista, all of the services ran in Session 0 and applications started in the SYSTEM context. This posed a security risk. In Windows Vista and later versions, the operating system isolates services in Session 0 and runs applications in other user sessions. Services are protected from attacks that originate in the application code. Windows Vista and later adds an Interactive Services Detection service, that detects, if running, whether any application must show a user interface, then displays the Interactive Service Detection dialog to switch to Session 0 and continue. For more information about the Interactive Services Detection service, see the Microsoft documentation.

In Windows Vista and later, the Interactive Services Detection design change created an issue for interactive software installations that require user input.

If the software being deployed has the following characteristics, the installation remains in Session 0 awaiting user input:

- The software is interactive
- The software is not session-aware
- The Interactive Service Detection service is turned-off

As no input UI is displayed, the Software Delivery job times-out.

The Software Delivery agent has supported this scenario since CA ITCM r12 SP1 by turning on the Interactive Services Detection service, allowing user input, then turning off the service before exiting.

To ensure the ability to install interactive software even if the software is not session-aware and to completely remove the dependency on the Interactive Services Detection service, CA ITCM now provides an option to specify that a software package being registered or deployed is interactive and requires user interaction on the agent computer.

To use this functionality, the administrator selects the Enable user interaction (Win LH Only) option in the procedure options when registering a software package or in the job settings when deploying a package. The agent starts the software installer in user sessions that are currently logged in and active, and also starts in the SYSTEM context.

Note: This feature helps you to install interactive applications, however, compromises the isolation feature that Microsoft provides to increase security. Use this feature carefully.

For software packages that were sealed before DM upgrade, an available option lets you enable user interaction (even in sealed state) as long as you do not select the Prevent user from being logged on while the job executes option.

If no users are logged in, the SD Agent waits for a user to login, then runs the job.

This feature uses the following configuration parameters in specific situations related to Logon Shield and restart/logoff. These parameters reside under DSM > Software Delivery > Agent:

Interactive Jobs: Launch in user session on Longhorn OS family

Specifies the session in which the job runs on agents that run Windows Vista and later versions.

Values:

- **TRUE:** Based on the Enable user interaction (WinLH only) job property, the job runs in the logged-on user session. This parameter is only applicable for jobs deployed to machine agents. This parameter has no effect on jobs deployed to user profiles and for non-interactive jobs.
- **FALSE:** The job runs in session 0.

Default: TRUE

Limits:

- This parameter only applies to jobs that are deployed to machine agents.
- This parameter has no effect on non-interactive jobs or jobs that are deployed to user profiles.

Interactive Jobs: Ignore Logon Shield mode in case of conflict on Longhorn OS Family

Specifies the SD Agent behavior when the Logon Shield status is *Wait until user logs off before job executes* or *Force user to log off before job executes* and *Enable user interaction (WinLH only)* job property is TRUE.

Values:

- **TRUE:** The job property suppresses the Logon Shield behavior.
- **FALSE:** A conflict is detected and jobs will fail with an appropriate error message.

Default: FALSE

Interactive jobs: Postpone remaining jobs in no linkage container on Longhorn OS family

Specifies the following actions:

Values:

- **TRUE:** Postpone all jobs after the first job with the option Enable user interaction (WinLH only) set.

- **FALSE:** Postpone the interactive jobs in the container and run all non-interactive jobs.

Default: TRUE

Limits: This parameter applies when there are no users logged on to the computer and *Interactive Jobs: Run in user session on Longhorn OS family* is TRUE.

Chapter 4: Configuring Software Delivery

You can configure the software delivery functionality after installation.

Generally, components like managers, scalability servers, and agents are managed by configuration policies. A configuration policy is a set of parameters that govern how a particular component behaves.

This section contains the following topics:

Software Delivery Policy Group

The software delivery policy group lets you view or edit the existing policy properties for software delivery management.

The software delivery policy group contains the following folders:

- Agent
- File compression
- File transfer
- Manager
- Scalability server
- Shared
- Software management

Modifying Configuration Policies

Configuration policies can be viewed and modified from the DSM Explorer using the Control Panel, Configuration, Configuration Policy, Default Computer Policy, DSM node.

To change a configuration policy setting, double-click the specific policy. The Setting Properties dialog appears and lets you modify the configuration policy.

For detailed information on how to configure or modify software delivery configuration policies, see the Configuration Policy section in the *DSM Explorer Help*.

Software Job Configuration

In the Control Panel, the Configuration folder contains the subfolder Software Job Management where you can configure the Job Cleanup, Job Handling, and Reinstall After Crash (RAC) tasks.

If you right-click a target computer or a group, you can select and configure further job properties like job execution calendar, download method, and RAC policy. You can specify configuration settings by selecting Properties from the context menu.

Scalability Server Configuration

A scalability server consists of a number of system processes that run in the background. A scalability server can be started and stopped by the administrator, and its configuration can be changed.

You configure the scalability server using the configuration feature from the manager's DSM Explorer or through the Application Framework (CAF) command line, for example:
`cserver config -h new_manager`

Note: If CA Common Services (CCS) is installed, moving the domain manager of a scalability server will also reconfigure CCS to point to the new manager computer. To ensure that CCS values are not changed when re-registering the server, use the cserver command with the "-i" option instead of "-h".

Logon Shield Configuration

The Logon Shield configuration is controlled by the common configuration component. A customized user interface, called the Logon Shield configuration view, lets you set and modify the data in a configuration policy.

When starting the Logon Shield configuration view from the DSM Explorer, the Logon Shield configuration dialog is displayed.

You can select the mode of operation for the Logon Shield, which determines the log on conditions under which Software Delivery jobs (SD jobs) are executed and the installation status of the Logon Shield.

The modes of operation for the Logon Shield include:

Logon Shield not installed

Indicates, that in a Windows Vista operating environment, the Logon Shield credential provider and filter COM modules are unregistered. In a non-Windows Vista environment, the sxpgina.dll is uninstalled.

No restriction on job execution

Determines that the Logon Shield is not activated when an SD job executes.

Force user to log off before job executes

Determines that the user is forced to log off when an SD job is waiting to be executed. The Logon Shield is activated during job execution.

Apply job-defined condition

Determines that the option "Prevent user from being logged on when job executes", which has been selected by the administrator during set-up of the SD job, is applied. When the Apply job-defined condition mode of operation is selected, the user is forced to log off when the job is waiting to be executed and the Logon Shield is activated during job execution.

Wait until user logs off before job executes

Determines that the user is not asked to log off when an SD job is pending. However, the job is executed only after the user has logged off. The Logon Shield is active during job execution.

Wait until user logs on before job executes

Specifies that pending SD jobs are executed only when a user is logged on.

To avoid a permanent blocking of a system in case of malfunction, you can specify a period of time after which the system will be unblocked. The maximum blocking time defines the maximum time, in minutes, for which logon will be prevented. This parameter has already been remotely managed in previous releases.

In Windows Vista and newer operating environments, we strongly recommend that you run the Logon Shield with specific Windows security options. The Logon Shield applies the Windows security options every time it is activated, provided Apply Windows security options is set to Enabled in the Logon Shield configuration dialog. The Apply Windows security options feature of the Logon Shield does not apply to pre-Windows Vista operating environments.

To select the specific Windows security options click the Settings button on the Logon Shield configuration dialog. The Windows security options dialog opens where you can enable (or disable) the following Windows policies:

Disable Ctrl+Alt+Del

This Windows policy determines whether pressing Ctrl+Alt+Del is required before a user can log on. If this policy is disabled, any user must press Ctrl+Alt+Del before logging on to Windows.

We strongly recommend to disable this policy when using the Logon Shield.

Shutdown without log on

This Windows policy determines whether a computer can be shut down without having to log on to Windows. If this policy is disabled, any user must log on to Windows before shutting down the computer.

We strongly recommend to disable this policy when using the Logon Shield.

Enabling the Logon Shield Implicitly

Apart from enabling and configuring the Logon Shield explicitly using the Logon Shield configuration view on the DSM Explorer, the Logon Shield can be enabled implicitly when setting up a software distribution job. Select the *Prevent user from being logged-on while job executes (WinNT only)* option on the Procedure Options tab of the Setup jobs dialog.

Important! Enabling the Logon Shield implicitly works only as long as the Logon Shield's mode of operation has the value Apply job-defined condition or the Mode of operation parameter is locally managed. Note that the Mode of operation parameter is locally managed per default.

Chapter 5: Using Software Delivery

This chapter describes the software delivery functionality in detail and how to make the best use of it.

This section contains the following topics:

Computers and User Profiles

Computers and user profiles have DSM agents installed on them, and these agents are connected to the domain manager over a network. A user profile is an instance of a local account or domain account on a specific computer.

Defining Computers

A computer on which the software delivery (SD) agent is installed, is automatically registered to the domain manager and is included in the list of computers on the DSM Explorer. Use the Deploy Agent function of CA ITCM to automatically push out the agent to computers in the network.

You can define computers manually, which means that new computers can be registered and assigned software beforehand. When the SD agent is installed on the computer, it can immediately receive software, which minimizes the startup time for new computers. When you define a computer manually, you provide general information (such as host name, network address, operating system, scalability server name) about the new computer using the New Computer preregistration Wizard. You can also define a job calendar to determine the days, dates, and times when jobs can be executed on that computer (Computer Properties).

Defining User Profiles

User profiles are login accounts on computers running a Windows operating environment. They are identified as the name of the machine plus the user account name. User profiles can be targets for software package deployments and allow installing software for a particular user rather than all users, which is the case when delivering to a computer.

User profiles are defined when a computer registers with the domain manager. Registration is not enabled by default. To do so, create a configuration policy with the DSM/Agent/common agent/software delivery/Supported unit types parameter set to Computer+User Profile.

Static and Dynamic Computer Groups

Static and dynamic groups are collections of assets. Static groups are created manually, whilst dynamic groups are updated from the results of queries. All these asset groups are shared between all products in CA ITCM.

Defining Computer Groups

Individual computers can be made part of a computer group to allow for easier distribution of software packages to a number of computers. These groups can be assigned based on criteria such as similar attributes, uses, or domains.

Computer groups are typically defined at the enterprise manager, if the enterprise tier is used, and then replicated to the domain manager. Groups may of course also be defined at domains.

You can create a new computer group using the New Group dialog. The options available on the New Group dialog specify if the group is query enabled, that is, a dynamic group.

Dynamic Computer Groups

To define a dynamic group you can use a predefined query or create a new one. The software delivery functions make use of queries for computers and user profiles.

For details of how to use the query designer, see the software delivery online help.

Linking, Unlinking, and Moving Computers and Computer Groups

Computers and computer groups can be linked to another static computer group. You can use drag-and-drop or copy-and-paste features to link a computer from a defined static computer group to another static computer group.

You cannot insert a copied computer into a computer group at a level at which it is already a member, but you can insert the copied computer at another level in a nested computer group.

You can use the Remove from Group process to break a previously established link. If, for example, you remove a computer from a static computer group, then the selected computer disappears from the computer group.

Removing from group is not the same as deleting. When you delete a computer from a computer group, then the selected computer is permanently removed from the CA ITCM database, not only from the group.

Computers and computer groups can also be moved to other computer groups. When you move a computer or computer group to another group, it becomes a member of that group, and ceases to be a member of the previous group. System folders cannot be manipulated; for example, you cannot move a computer from the All Computers folder.

Queries

Software delivery uses the common query feature of CA ITCM for querying the database and for defining the procedure prerequisites. You can define these queries using the Query Designer dialog. For more information on general query design, see the Asset Management Administration Guide.

In some cases, software delivery uses the queries created in Unicenter Software Delivery 4.0 and in other cases, it creates queries that follow the Unicenter Software Delivery 4.0 query format. These queries differ from the queries created by the CA ITCM Query Designer. For more information on Unicenter Software Delivery 4.0 queries, see the Appendix Importing Unicenter Software Delivery 4.0 Query Strings (see page 199).

Using the Software Package Library

Before a software program (software package) can be distributed using software delivery (SD) functions, it needs to be defined to the Software Package Library on the enterprise or domain manager through the registration process.

During the registration process, information about the software item, such as its name, version, source, and installation procedures are defined to the database.

In this section, you will read how to

- Prepare programs for registration in the Software Package Library
- Register software programs
- Register virtual application packages
- Define startup procedures and customized scripts, known as item procedures, to install, activate, configure and remove a program
- Add new item procedures to a program that is already registered in the Software Package Library
- Use automatic registration to register SD packages in additional SD networks
- Create software groups to bundle individual software products
- Create catalog groups to make software available to a particular group of users through the Software Catalog

Registration Process Overview

The registration process identifies and stores a program as an item in a domain or enterprise manager library. Library items can be initially registered in one of these libraries before distribution to target computers. The following graphic depicts the registration of an item in a local library.

The procedure for registering a program is the same for enterprise and domain managers but you must keep the following in mind:

- Software that is registered *only in a domain manager's library* cannot be distributed to other domain manager's libraries or to the enterprise manager.
- Software that is registered *only in the enterprise manager's library* cannot be installed on a domain until the item is delivered to the domain manager using a distribution container.
- Depending on the type of item you are defining, the registration process can take several progressive steps.
  - Identify the program (name, version, vendor, comments).
  - Identify the source and copy the item into the Software Package Library.
  - Identify the item procedures used to install or maintain the program.
  - Save the registration, that is, seal the software item.
- After a program has been registered, it is ready for distribution.

Types of Packages for Registration

The software packages that you can register in the Software Package Library include the following types:

- Software packages that are provided with CA ITCM
- Virtual application packages created from Microsoft App-V or VMware ThinApp virtual application images
- Software Management products in the standard packaging formats PKG and RPM (Red Hat Package Manager), as well as in the CA Technologies-specific packaging formats, SXP (for Windows) and PIF (for Linux and UNIX), that are created using CA Technologies's Software Management Packagers
- MSI packages that are generated in the Microsoft Installer packaging format (refer to Registering MSI Packages in the Software Package Library (see page 61))
- Windows CE and Palm packages for Windows CE and Palm devices. (refer to Registering Windows CE and Palm Packages in the Software Package Library (see page 66)).

Example for a Registration

Suppose you have received the following new software products:

- MemoPlus, a Windows NT Technology-based word processing package to be used by members of the administrative support staff to construct memos, letters, and so on
- MasterCalc, a Linux-based accounting program that is targeted for the accounting group at the JUPITER domain

Before you can distribute these programs to the domains and departments, you need to register them and their associated installation procedures in the enterprise manager's Software Package Library (or the domain manager's library, if you are not using an enterprise manager).

Because the files for MasterCalc reside on a tape device, the necessary files must first be extracted and converted to an installable format, such as a hard disk directory, without using software delivery functionality. You must then create the necessary item procedure files and register the program into the Software Package Library from the directory. The item procedures are registered as embedded, added, or external item procedures.

Notes on Registering Software Packages

The following list provides relevant notes concerning the registration of software packages:

- Before registering a software package in the Software Package Library, you need to know the following:

  Source

  Storage medium where the package is located, such as CD/DVD, disk, or directory.

  Name and Version

  Package name such as MemoPlus 3.0

  Item Procedures

  Procedures (executables, batch files, command files, or scripts) that are used to install, configure, activate, or remove the program. Each of these must be registered as an item procedure.

- When you register a software package as a new version, you can use the Send delta distribution function, from an enterprise manager down to domain managers. The Send delta distribution function effects that not the complete package is sent to a domain manager that already has the previous version of the package registered. This function is useful, for example, when the software package is exported from the packaging environment and imported into the production environment.
- To register packages to the Software Package Library the user account must have write access to the domain's library path (..\SD\ASM\LIBRARY).
- When storing software packages in the Software Package Library, CA ITCM uses path names that contain a UUID (40 characters), instead of an Object ID (12 characters) as used in pre-r11 releases. The implication of this is that the registration of a pre-r11 package, where the path name length in the Software Package Library was near the maximum, imposed by the operating system, may fail.

Note on Registration Information

The registration information, reginfo, for a software item registered in a Software Package Library is never changed. However, observe the following.

If you change any of the information listed following, after registering a software package at the enterprise manager, the modified information will be distributed, along with the original reginfo, when you distribute the software package for registration at domain managers:

- Comment for the software item
- Comment for a procedure in the software item

- Default selected procedure for jobs (checkbox setting)
- Catalog enabled (checkbox setting)
- Exclude from Reinstall After Crash (RAC) (checkbox setting)

Making changes to the listed information on the enterprise manager, and distributing the software package in this state, may result in software packages on the domain manager, that differ from the original distribution of the software package.

Copy Registered Items for Automatic Registration

Once an item has been registered in the Software Package Library, both the item and the registration information can be copied for automatic registration in another library. This can be useful, if you have multiple managers or if you have software delivery functionality installed at different sites that are not networked.

Preparing Programs for Registration

Before you register a software product in the Software Package Library, review the procedures supplied with the product. The following sections describe further considerations.

Identify a Program and its Source

To begin the program registration process, the software program first needs to be identified. Once identified, the next step is to copy it into the enterprise or domain manager's Software Package Library. To do this, you need to define its source (either disks, directories, or CD-ROM).

Because installation files are only copied to, and not actually installed in the Software Package Library, you can register any Windows, Linux, WinCE, or Palm software program on any manager, regardless of its operating system. The only restriction is that the program's media be readable by the manager.

Locate Source Files

The files are supplied from the Software Package Library (see page 14) and not from the product media (for example, DVD or CD-ROM). You may need to change the source file location maintained in the current installation procedure so that it points to a library subdirectory. For more information, see Library Tree Structure (see page 44).

Other Procedures

In addition to installations, you can write procedures to activate, uninstall, or configure a product installation. You can add entirely new, fully customized, installation procedures.

If an installation fails, you can also recover the failed installation at the target computers.

Customize Existing Procedures

Other than any required modifications, you can optionally customize installation files to produce automated and semi-automated installations.

Perform Windows Installer Tasks

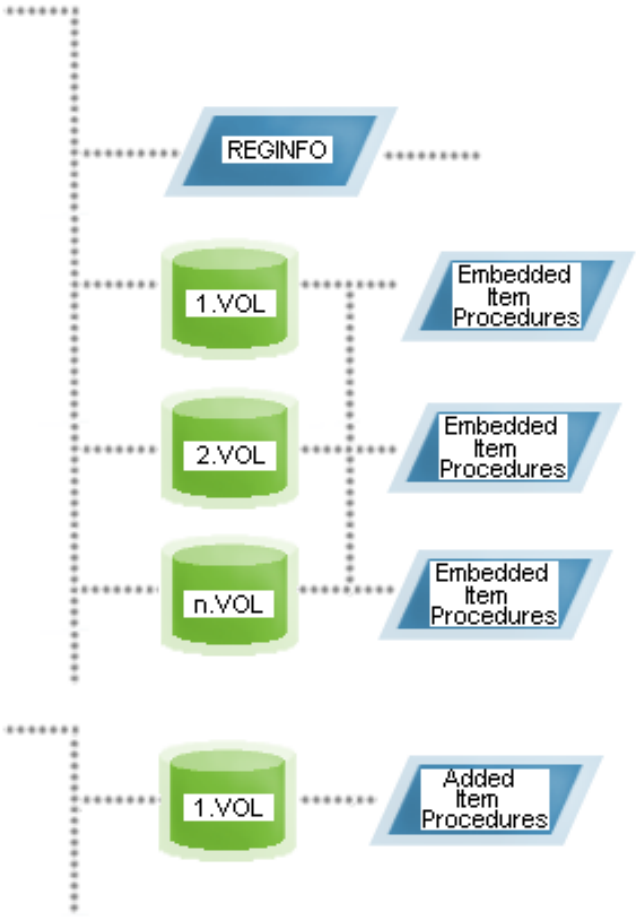
The software delivery functionality includes a tool, called sd_msiexe.exe, that you can use to perform Windows Installer tasks. It is similar to the Microsoft Windows Installer tool msiexec.exe, in that the Windows Installer uses a command line tool. The command line tool sd_msiexe.exe uses the same command line options as msiexec.exe and has been optimized for software delivery purposes.

Note: If you intend to make minor modifications to existing procedures or create new procedures, make sure that you are familiar with the directory tree structure used by the software delivery functionality.

Note: For a description of the command line options of the Microsoft Windows Installer tool, msiexec.exe, see the appropriate Microsoft Help and Support web page.

Library Tree Structure

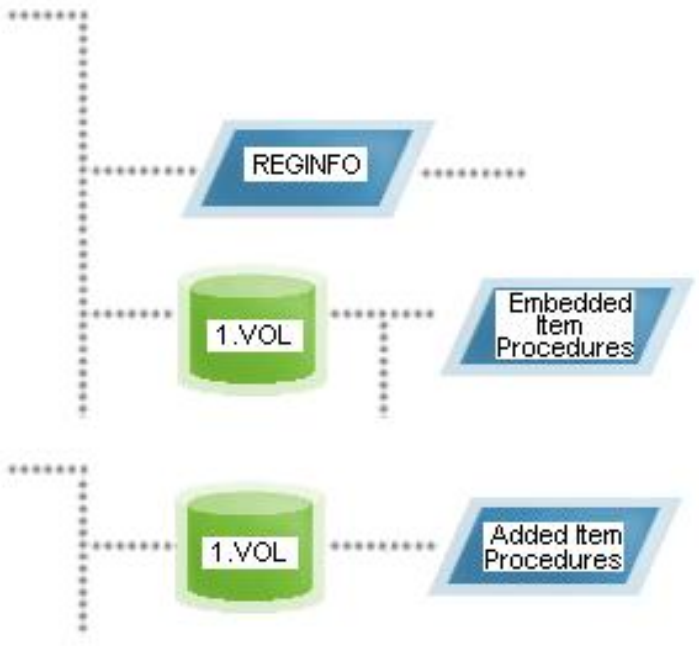
When an item is added to the Software Package Library, its files are stored in a directory structure based on the type of media from which it was copied. If the program is copied from multiple data carriers (for example, CD-ROMs), a typical directory structure would be as shown in the following illustration:



Each data carrier is stored as a volume under the program directory. The first volume is called 1.VOL, the second 2.VOL, and so on.

Note: The importance of volumes has decreased over the years as most packages nowadays fit onto a single installation medium.

If the program is copied from a single data carrier or directory, it is considered a single volume source and is distributed as shown in the following illustration:



In both single or multiple data carrier scenarios, item procedures that are identified at the time the product is originally registered (also known as embedded item procedures) typically appear in subdirectories under the main volumes, unless the procedure is included in the root directory of the original install data carrier or directory.

Note: Different media types cannot be combined into the same source.

Required Installation File Modifications

When installing from diskettes or CD-ROMs, the installation programs sometimes fetch data from information files located on the first installation diskette. This file contains the media's identification information. During the installation process, these programs normally check the current directory for all necessary install files. If the program consists of two or more diskettes or CD-ROMs, which you have copied into a single directory prior to registration, you do not need to make any modifications. If there are multiple media and you have registered each media individually, you need to modify the volume labels of the install information file (*.INS or *.INF) to point to the files in the Software Package Library structure. For example, if the volume labels are given in numerical order ("VOL_LABL1", "VOL_LABL2", and so on.), they should be changed to \1.VOL "VOL_LABL1", \2.VOL "VOL_LABL2", and so on. The modified *.INS or *.INF file should then be registered along with the installation program as an added item procedure after the initial library item is registered. For more information on registering added item procedures, see Defining Added Item Procedures (see page 74).

Linux and UNIX Installation Modifications

Modifications made to Linux or UNIX programs depend on which Linux or UNIX environment and release level you are using. In general, you should:

1. Decide which installation program you are going to use to install the product. This determines which command is used to perform the installation.

   Note: Remember that the files to be installed are found in the temporary directory structure described previously and not on the installation media. You must create an installation script that issues this command.

2. Verify that the installation process does not require user input at the target computer. If so, your installation script needs to contain answers to those questions. The manner in which you provide these answers depends on the system in use.

3. Register the script as an item procedure for the program.

Optional Customization Tools

Customized procedures consist of additional site-written files that

- Modify the Linux or UNIX installation script using the appropriate installation program
- Include replies to some or all installation questions to produce an automated or semi-automated installation procedure
- Initiate a remote activation of the product
- Alter the target computer's configuration files
- Uninstall the product at a later date

Important! Test each procedure before registration and distribution.

Modify Existing Procedures

You can

- Modify the Linux/UNIX installation script as described under the topic "Required Installation File Modifications"
- Modify the Installer response file
- Modify the response file for IBM CID-enabled products

Create New Procedures

Use the script language to

- Create a script file with the .dms extension using a text editor (for details of the script language, see the CA ITCM Script Editor online help).
- Create own executables (using, for example, C/C++)
- Copy any other installation program or script

Library Items

The Software Package Library contains different types of software items, as listed following:

Open

A software item is open while being registered and until the registration process is terminated by sealing the software item.

Closed/Sealed

A software item is closed when having been sealed. When a software item is registered as a software delivery package, it is automatically sealed.

Programs

Programs can be registered with item procedures used to install, activate, configure, or remove the application. Item procedures can be registered along with the program or subsequent to registration.

Detected

Detected software is already installed on a computer but not registered in the enterprise manager's or domain manager's library. These items are actually placeholders in the Software Package Library and do not contain any actual programs.

Program Registration on Scalability Servers

Scalability servers contain a permanent Software Package Library (called Staging Library). To add library items from a domain manager to a downstream scalability server, you can select a library item or software group, and copy and paste or drag and drop it onto the scalability server. If you are connected to an enterprise manager, you can schedule a distribution that delivers library items to the library of a scalability server that is downstream of the domain manager to which the distribution is sent. Again, copy-and-paste or drag-and-drop can be used.

The Staging Wizard is an enhanced easy-to-use method of delivering software to scalability servers; for example, it enables you to select software from more than one software group. The wizard can be launched in context of library items, scalability servers and software jobs; for example, right-click a scalability server and select Software Job, Stage Software Packages to launch the wizard. On the enterprise manager you can also select domains to where the library items are first distributed before they are relayed to the selected scalability server groups.

Programs can also be registered and unregistered in the Staging Library from the command line. Using the command sd_sscmd aregsw, you can add software to a Staging Library that is not included in the domain manager's Software Package Library folder. This software will not become visible in the Staging Library of the domain manager's DSM Explorer even if the procedure Synchronize Software Staging Library is started.

Before using the permanent Staging Libraries, you must do the following:

- Store all products from the domain manager's Software Package Library into the Staging Library.
- Assign products and target computers using the Install function.

To track the contents of the Staging Library, there is a file, library.dct, in the LIBRARY folder, in which each registered item is entered.

Registering Virtual Applications

You can import virtual applications into the Software Package Library and register them at the enterprise or domain management tier. The following sections provide an overview of application virtualization and supply details on the overall packaging process and procedures:

- Application Virtualization
- Virtual Application Image Content and Format
- How Virtual Application Packaging Works
- Virtual Application Packages
- Create a Virtual Application Software Package
- Create a Virtual Application Software Package Update
- Virtual Application Infrastructure Package Templates
- Create Infrastructure Software Packages for Microsoft App-V
- Create Infrastructure Software Packages for VMware ThinApp

Application Virtualization

Application virtualization is a software technology that facilitates the deployment and management of applications by separating them from the underlying operating system on which they would normally run. You do not install a virtual application in the traditional manner, although you execute it as if you did. At runtime, the application acts as if it is directly interfacing with the original operating system and all the resources managed by the operating system. In reality, the application is running in an environment ("bubble") that is isolated from the operating system.

Virtual applications can run directly from a local hard drive on a target computer, or they can be streamed from a remote server. With streaming, the virtual application is stored on the server. A “sandbox” is created on the server or the target computer for each user of a streamed virtual application. The sandbox contains all sub-folders, configuration files, and application-specific registry entries that are needed to run the application. After the user closes the virtual application, the application is removed from the computer’s memory. Only small configuration files and a link to start the application remain. However, the sandbox containing all user-specific settings is still available on the server or the target computer for the next time that the user wants to run the application.

Virtual applications are regular applications captured into a virtual application image. This image contains all files and configuration data necessary to run an application, as well as all installation information that would normally be used during application installation. The creation of a virtual application image is done by means of tools that the vendor of the virtualization technology supplies. These vendor tools can generate a virtual application image from a regular application.

CA ITCM manages the virtual application life cycle after the virtual application image has been created with one of the vendor tools. The image can be imported into the Software Delivery Library as a standard software package and deployed to target computers through the standard CA ITCM deployment methods. The package can also be updated, upgraded, and retired through the standard CA ITCM methods.

Virtual Application Image Content and Format

You create a virtual application image from a regular application by using the tools provided by your application virtualization vendor. CA ITCM supports Microsoft Application Virtualization (Microsoft App-V) and VMware ThinApp. You need to create the virtual application images with one of these tools before you can use CA ITCM to package, deploy, and manage virtual applications.

Note: For information about creating virtual application images, see the vendor documentation for your application virtualization product.

Microsoft App-V

Virtual application image preparation (sequencing) results in a number of files, including the following files:

- XML-based Open Software Description files (.osd)
- Icon files (.ico)
- A file that stores the complete application code of the virtualized application (.sft)
- An XML-based manifest file (.xml)
- A project file (.sprj)

Note: The end user on the target computer should not start the virtual application by double-clicking on the .osd file. If the user does so, the communications with the streaming server may not function properly. The user should start the application by using the desktop shortcut or the Start menu.

VMware ThinApp

Virtual application image preparation (capturing) results in a number of files and folders, including the following files and folders:

- A bin folder that contains a single executable file. For program suites, several executable files are required for the user interface. In this case, the bin folder contains a .dat file holding the entire virtual package and small executable files that provide access to the virtual package.
- A configuration file (.ini)

How Virtual Application Packaging Works

You can create a standard software delivery package from a virtual application image by using the Virtual Application Package Registration Wizard. The virtual application image must already be available before you use the Wizard to create the software delivery package. The image must be accessible from the computer where CA ITCM is running. This Wizard also allows you to create update packages for virtual applications that were previously converted to software delivery packages.

The process to create and import virtual application packages uses the following general steps:

1. The administrator opens the Virtual Application Package Registration Wizard and locates a virtual application image. Images must be available on or accessible to the computer running CA ITCM.
2. The administrator browses the virtual application image. This step allows the administrator to verify that the selected image is a valid virtual application image. The Wizard analyzes the virtual image and extracts the information needed to create the Software Delivery packages.

   Note: The package name is based on the virtual application name and is limited to 20 characters (for example, *my_productname_is_20*-TA-SG). If there is a duplicate product name, the administrator must modify the current package name to create the package.
3. (Optional) If the virtual application image represents an update to a virtual application, the administrator identifies the Staging package that was originally created for the virtual application.
4. The administrator reviews the summary of the virtual application package just created and finishes the Wizard.

5. The Virtual Application Package Registration Wizard creates three software packages for each virtual application image:

   Standalone

   This package is used to install and execute the virtual application locally on the target computer.

   Streaming

   This package is used to downstream the virtual application from a streaming server and execute it on the local computer.

   Staging

   This package provides access to the virtual application for both standalone and streaming modes of package delivery. This package contains the virtual application image.

   Note: For more information on the types of virtual application packages, see the description in the Virtual Application Packages (see page 53) section.

6. The Wizard begins the process of importing the virtual application packages into the Software Delivery Library by determining if the package names are already listed in the Library.

   a. If the package names are already in the Library, an error message appears stating that the package names are not unique. The packages are not imported.

   b. If the package names are not already in the Library, the Wizard imports the three packages: Staging, Standalone, and Streaming.

   c. If the packages are update packages, they are imported and registered with higher version numbers. Two packages only are created for updates: Staging and Standalone.

7. The administrator creates the definitions for the new virtual application packages. The descriptions of Virtual Application Discovery and Inventory provide more information about creating definitions for virtual application packages.

After a virtual application package is included in the Software Delivery Library, the administrator can then deploy it and manage it using standard Software Delivery methods.

Virtual Application Packages

The software delivery software packaging process for virtual applications (through the Virtual Application Package Registration Wizard) creates three software packages for the first packaging of a virtual application:

Standalone

This package installs and executes the virtual application locally on the target computer. The Standalone package contains procedures and, for Microsoft App-V, configuration files. It also contains a dependency to the Staging package, which holds the virtual application image. Therefore, the Staging package is installed on the target computer before the Standalone package is installed.

This package creates all shortcuts and file associations (as created by the original installation). The Standalone package does not contain the application bulk data. The bulk data is stored in the Staging package and installed on the target computer as a dependency to the Standalone package.

This package is named using the following format:

application name–vendor tool abbreviation–SA

Example: DeveloperStudio–AV–SA (Microsoft App-V) or DeveloperStudio–TA–SA (VMware ThinApp)

Streaming

This package consists of procedures, tools, and configuration files. It creates shortcuts and file associations on the target computer. The shortcuts on the target computer allow the launch of the application from the scalability server, which acts as the streaming server. The virtual application image is not part of the Streaming package, which implies that the application image is not staged on the target computer. Instead, the application image needs to be staged on the scalability server. The administrator must verify that the Staging package is installed on the scalability server first in order for the Streaming package to work.

Note: The Streaming package is not created when a virtual application is imported as an update to an existing virtual application package. The Streaming package does not need to be updated because the included shortcuts are already pointing to the Staging package (which is updated).

This package is named using the following format:

application name–vendor tool abbreviation–SM

Example: DeveloperStudio–AV–SM (Microsoft App-V) or DeveloperStudio–TA–SM (VMware ThinApp)

Staging

This package provides access to the virtual application for both standalone and streaming modes of package delivery. The Staging package contains the bulk data, that is, the virtual application image. For standalone delivery, the image is staged locally on the target computer. For streaming delivery, contents from the image are streamed to the target computer. As specific parts of the application are requested by the user, those parts are streamed to the target computer from the scalability server (which acts as the streaming server).

Note: The Staging package is installed automatically (as a dependent package) when you install a Standalone package on a target computer. However, if you uninstall a Standalone package, the corresponding Staging package is not uninstalled automatically. You need to schedule an uninstall job to remove the Staging package.

This package is named using the following format:

application name–vendor tool abbreviation–SG

Example: DeveloperStudio–AV–SG (Microsoft App-V) or DeveloperStudio–TA–SG (VMware ThinApp)

Updates to Virtual Applications

When packaging virtual application updates, the software delivery packaging process creates two software packages only: Standalone and Staging. The Streaming package is not created, since this package includes just the client links to the Staging package and the virtual application. These links are not affected by application updates. The Standalone and Staging packages for updates are registered with a version number that is higher than the original packages.

Update packages have the same name that was used for the former packages, with a higher version number. While the version number is not part of the package name (it is stored internally), it is displayed as a suffix to the package name when shown in the DSM Explorer, Software Delivery Library.

Downgrades to Virtual Applications

You can also downgrade a virtual application package. A downgrade is similar to an update. You need to create the virtual application image (which includes the application) with the target version for the downgrade. The packaging of a downgrade is similar to the packaging of an update. The Standalone and Staging packages only are created. The downgraded packages have the same name that was used for the former packages, with a *higher* version number (similar to update packages).

Create a Virtual Application Software Package

The Virtual Application Package Registration Wizard lets you create a virtual application package and import it into the Software Package Library.

To create a virtual application software package

1. Verify that a virtual application image has been created for the application you want to package. The image should be located on or accessible from the same computer where CA ITCM is running.
2. Navigate to the Software Package Library folder in DSM Explorer where you want to create the package.
3. Right-click the folder and select Import, Virtual Application Package.

   The Virtual Application Package Registration Wizard opens.
4. Proceed through the Wizard pages selecting the virtual application image.

   The Wizard creates three virtual application packages: Standalone, Streaming, and Staging. The packages are placed under the Software Package Library folder where you launched the Wizard.

Create a Virtual Application Software Package Update

The Virtual Application Package Registration Wizard lets you create a virtual application package update and import it into the Software Package Library.

To create a virtual application software package update

1. Verify that an updated virtual application image has been created for the update application you want to package. The image should be located on or accessible from the same computer where CA ITCM is running.

   Note: For Microsoft App-V, you must create the updated virtual application image using the Active Upgrade method of the App-V sequencer. For more information about the Active Upgrade method, see the Microsoft App-V product documentation. You can also access the Microsoft web site (http://www.microsoft.com) and search the Microsoft TechNet information for the "Methods for Upgrading or Updating Virtualized Applications" article.
2. Navigate to the Software Package Library folder in DSM Explorer where you want to create the package update.
3. Right-click the folder and select Import, Virtual Application Package.

   The Virtual Application Package Registration Wizard opens.
4. Proceed through the Wizard pages and select the updated virtual application.

   The Wizard asks you to select the Staging package for your updated virtual application.

5. Select the former Staging package (latest version) that was created for the original virtual application.

   The Wizard creates two virtual application packages: Standalone and Staging. The packages are placed under the Software Package Library folder where you launched the Wizard.

Note: You can also downgrade a virtual application package. A downgrade is similar to an update. You need to create the virtual application image (which includes the application) with the target version for the downgrade. The packaging of a downgrade is similar to the packaging of an update. The Standalone and Staging packages only are created. The downgraded packages have the same name that was used for the former packages, with a *higher* version number (similar to update packages).

Virtual Application Infrastructure Package Templates

CA ITCM lets you create virtual application software packages from Microsoft Application Virtualization (Microsoft App-V) images or VMware ThinApp images. However, before you can deploy and run these virtual application packages, you must install specific vendor infrastructure software on the servers and target computers where you want to deploy the virtual applications. The infrastructure software contains vendor tools and modules that allow the virtual application to be installed and run.

Note: For more information on vendor infrastructure software requirements, see the descriptions of Preparing a Target Computer for Deployment of a Microsoft App-V Virtual Application (see page 106) and Preparing a Target Computer for Deployment of a VMware ThinApp Virtual Application (see page 108).

You can use CA-provided templates to create vendor infrastructure software packages. The following templates are available for your use:

- Microsoft App-V Virtualization Desktop Client (App-V Client for standard desktops)
- Microsoft App-V Virtual Client for Remote Desktop Services (App-V Client for Terminal Servers)
- Microsoft App-V Server
- VMware ThinApp

You need to insert the appropriate vendor software modules into these templates. The packages you create with the templates are standard software delivery software packages. You can register the infrastructure software packages in the Software Package Library.

The file structure in the infrastructure package template is the same as the structure found in a standard Software Delivery software package – a root folder, the “reginfo” folder, and additional folders and/or files.

reginfo subfolder

The templates contain all information needed to register the package in the Software Package Library and link it to other dependent infrastructure packages.

Additional folders and files

The templates include installation modules for the software packages. For infrastructure packages, you must copy these modules from the vendor’s installation media.

The template assists you with identifying the installation modules that you need to copy into its subfolders. In each template, there is an image file that lists the vendor files that are required. For example, the template for Microsoft App-V Desktop Client includes a “client_files.JPG” file. This file indicates that three files are needed:

- AppVirtReadme.htm
- Setup.exe
- Setup.msi

Note: The infrastructure package templates are provided for your convenience. However, you may choose to install the vendor infrastructure software on your own. If you do so, ensure that the software is installed on all servers and target computers where you want to deploy virtual applications and that required permission keys are set in the registry.

In addition to the infrastructure package templates, the CA ITCM DVD kit includes the following package: Microsoft Application Error Reporting 11.0.6558.0. You can deploy this error reporting package with the client and server packages. For more information about this package, see the Microsoft product documentation.

Create Infrastructure Software Packages for Microsoft App-V

You can create Microsoft App-V infrastructure software packages using CA-provided templates. The packages you create with the templates are standard software delivery packages.

Note: This procedure assumes that you have the following products available: Microsoft System Center Application Virtualization Streaming Server, Microsoft Application Virtualization Desktop Client, and Microsoft Application Virtualization Client for Remote Desktop Services. The following procedure describes how to create packages for the server and both types of clients.

To create infrastructure software packages for Microsoft App-V

1. Access the following folder on the CA ITCM installation media:

   `examples\AV_Templates\Microsoft AppV packages`

2. Copy the Microsoft AppV packages folder (and the entire tree structure below it) to your local machine (for example, to D:\AppV-Packages).

3. Open the image file “server_files.JPG” in the 1.vol subfolder and view the Microsoft product files that are required:

   `Microsoft AppV packages\Infrastructure Package for AppV Server\1.vol`

4. Copy the required files (as shown in “server_files.JPG”) from the Microsoft System Center Application Virtualization Streaming Server installation media to the following subfolder:

   `Microsoft AppV packages\Infrastructure Package for AppV Server\1.vol`

5. Remove the file “server_files.JPG” from the following subfolder:

   `Microsoft AppV packages\Infrastructure Package for AppV Server\1.vol`

6. Open the image file “client_files.JPG” in the Desktop Client template and view the Microsoft product files that are required:

   `Microsoft AppV packages\Microsoft Application Virtualization Desktop Client`

7. Copy the required files (as shown in “client_files.JPG”) from the Microsoft Application Virtualization Desktop Client installation media to the template:

   `Microsoft AppV packages\Microsoft Application Virtualization Desktop Client`

8. Remove the file “client_files.JPG” from the Desktop Client template:

   `Microsoft AppV packages\Microsoft Application Virtualization Desktop Client`

9. Open the image file “client_files.JPG” in the Desktop Client for Remote Desktop Services template and view the Microsoft product files that are required:

   `Microsoft AppV packages\Microsoft Application Virtualization Desktop Client for Remote Desktop Services`

10. Copy the required files (as shown in “client_files.JPG”) from the Microsoft Application Virtualization Desktop Client for Remote Desktop Services installation media to the template:

    `Microsoft AppV packages\Microsoft Application Virtualization Desktop Client for Remote Desktop Services`

11. Remove the file “client_files.JPG” from the Desktop Client for Remote Desktop Services template:

    `Microsoft AppV packages\Microsoft Application Virtualization Desktop Client for Remote Desktop Services`

12. Copy the required files (as shown in “files.JPG”) from the Microsoft Application Error Reporting installation media to the template:

    `Microsoft AppV packages\Microsoft Application Error Reporting`

13. Remove the file “files.JPG” from the Application Error Reporting template:

    `Microsoft AppV packages\Microsoft Application Error Reporting\1.vol`

14. Open the image file “files.JPG” in the Application Error Reporting template and view the Microsoft product files that are required:

    `Microsoft AppV packages\Microsoft Application Error Reporting\1.vol`

15. Select all folders under the AppV packages folder (for example, D:\AppV-Packages) in Windows Explorer and drag and drop them into the Software Package Library in the EGC GUI.

    Microsoft App-V infrastructure software packages are created and registered in the Software Package Library. You need to deploy the following packages on target computers.

    - The infrastructure package for the server is named using the following format:

      `Infrastructure Package for AppV Server`

    - The infrastructure package for the standard desktop computer is named using the following format:

      `Infrastructure Package for AppV Client`

    - The infrastructure package for the terminal server is named using the following format:

      `Infrastructure Package for AppV Client for Remote Desktop Services`

Create Infrastructure Software Packages for VMware ThinApp

You can create VMware ThinApp infrastructure software packages using CA-provided templates. The packages you create with the templates are standard software delivery software packages.

Note: This procedure assumes that you have already installed the following product: VMware ThinApp.

To create infrastructure software packages for VMware ThinApp

1. Access the following folder on the CA ITCM installation media:

   `examples\AV_Templates\VMWare ThinApp packages\Infrastructure Package for ThinApp Client`

2. Copy the Infrastructure Package for ThinApp Client folder to your local machine.

   Note: The location on your local machine must be accessible to the Virtual Application Package Registration Wizard.

3. Open the image file “vmware_file.JPG” from the following subfolder and view the VMware product file that is required:

   `Infrastructure Package for ThinApp Client\1.vol`

4. Copy the Thinreg.exe executable file from the VMware ThinApp installation media to the following subfolder:

   `Infrastructure Package for ThinApp Client\1.vol`

5. Remove the file “vmware_file.JPG” from the following subfolder:

   `Infrastructure Package for ThinApp Client\1.vol`

6. Select the Infrastructure Package for ThinApp Client folder in Windows Explorer and drag and drop it into the Software Package Library in the EGC GUI.

7. The infrastructure packages are named using the following format:

   `Infrastructure Package for ThinApp Client`

   The VMware ThinApp infrastructure software package is now registered as a standard software delivery package in the Software Package Library.

Registering MSI Packages in the Software Package Library

The Microsoft Windows Installer (MSI) is an installer service, on the agent side, that manages the installation of applications on Windows platforms. These applications must be encapsulated in a package, called MSI package. The MSI package consists of an MSI file (*.msi) and any external source files that are pointed to by this file. The package contains all of the information needed by the Microsoft Windows Installer to run the user interface and to install or uninstall the application.

The MSI file (*.msi) contains an installation database, a summary information stream, and data streams for various parts of the installation. The logic and data necessary for an installation are maintained in a relational database, also in the MSI file. In addition, the MSI file can also contain one or more transforms, internal source files, and external source files or cabinet files required by the installation.

A transform is a collection of changes applied to an installation. The Installer can add or replace data in the installation database by applying a transform to a base installation package. For instance, a transform can change the text in an application interface from one language to another. Transforms are specified by one or more transform files (.mst). The Installer can only apply transforms during an installation.

A cabinet file is a single file, usually with a .cab extension, that stores compressed files in a file library.

The Microsoft Windows Installer organizes installations based on the concept of components and features. Components are pieces of the application or product that is to be installed. These are usually hidden from the user. Features are presented to the users, and are typically determined by the application's functionality from the user's perspective.

MSI packages can be registered in the Software Package Library using the Register MSI Package wizard. Using this wizard, you can choose to register the MSI package, use an administrative installation, or perform and use an administrative installation. The wizard guides you through the registration process, where you can, for example, add procedures, and properties. You can also specify separate paths for the MSI package and the MSI file.

You may later receive an MSI patch package from one of your software vendors. For information on how to add these patch packages to administrative or local installations, see Registering and Installing a MSI Patch Package (see page 63).

You can distribute registered MSI packages offline to target computers, using a data carrier like CD. The combined use of a registered procedure and a data carrier can be of value, if you want to create an administrative installation not only on the domain manager but also on its downstream scalability servers to reduce bandwidth requirements. For instructions on how to create an offline administrative install procedure for use with a CD, see Using an Offline Administrative Install Procedure with a CD (see page 65).

Note: Because some products may update system files or make changes to the Windows registry, an installation may fail when an installation job is sent to a User Profile that has inadequate access rights.

Using Windows Installer with Elevated Privileges

For the Windows Installer to run with elevated privileges, use the System Policy Editor (poledit.exe for Windows NT) or the Group Policy Editor (gpedit.msc and the Active Directory for Windows 2000/2003/XP) to enable 'Always install with elevated privileges for the Windows Installer'. Both the Computer and User configurations must be changed.

If you enable 'Always install with elevated privileges for the Windows Installer' in this way, it overrides any CA ITCM settings, as CA ITCM never lowers Windows Installer privileges. It only raises them.

If you do not want to enable 'Always install with elevated privileges for the Windows Installer', you still have the option of working with two other CA ITCM tools:

- If you do not check the box 'Do not install with elevated privileges', the property 'sdprop_installelevated' is set for all install, uninstall, and configure procedures that are registered for the current software item. In other words, the property is set for all procedures registered with the item except for Administrative install, Remove admin install, Detect, and Verify.
- If you check the box 'Do not install with elevated privileges', you still have the option of installing with elevated privileges by setting the property 'sdprop_installelevated' for the appropriate install, uninstall, and configure procedures that are registered for the current software item. You can do this by not sealing the item and using Properties for the procedures in which you are interested after registration. Select the Embedded File tab first and then select the MSI Properties tab, on which you can add or remove MSI properties.

Unattended Distribution of Microsoft Windows Installer

The Microsoft Windows Installer (MSI) engine is a part of Windows operating environments. Crucial for the installations to run is that the Windows Installer is present on the target computer. Computers running Windows operating systems need to get the Windows Installer service installed.

Registering and Installing a MSI Patch Package

The Microsoft Windows Installer uses a patch package, which has a .msp file extension, to patch administrative installations or local installations.

Patching Administrative Installations

If you have used the Register MSI Package method, when you registered the software that you now want to patch, proceed in the following way to patch an administrative installation using Network install procedures.

1. Select the MSI item to be patched in the Software Package Library.
2. Right-click the Procedures folder and select New, Added procedure with new files in the context menu.
3. On the General tab, provide a name for the procedure. The task should be Configure, the OS should be Windows 32-bit.
4. On the Added Files tab, browse to the .msp file. The type should be set to MSI file.
5. On the bottom three tabs that open for MSI files, you should select MSI method to be Patch Administrative Installation on the General tab.

   The package field states $msi\... $msi expands to the path of the directory, into which an Administrative Installation of the current item once was made.
6. Provide the name of the MSI file, which was used when originally registering the package.
7. Click OK to finish registering the patch procedure.

Note: If you selected Use an administrative installation or Perform and use an administrative installation when registering the MSI package to be patched, you should use the browse button to the right of the Package field to point to the actual MSI file of the administrative installation.

Finally, execute the new configure procedure on the software delivery manager to apply the patch to the administrative installation

Patching Actual Installations

Since a patch now has been applied to the administrative installation for your MSI package, all new installation orders sent to targets using any of the Network Install procedures (which always use an administrative installation) uses the updated install package.

For existing installations, you need to run an Apply patch procedure to install the latest files from the patch. To run the patch, follow these steps:

1. Select the MSI item for which the procedure is to be created in the Software Package Library (the MSI file, which was used when originally registering the package).
2. Right-click the Procedures folder and select New, Added procedure with new files in the context menu.
3. On the General tab, provide a name for the procedure. The task should be Configure, the OS should be Windows 32-bit. On the Added Files tab, browse to the .msp file. The type should be set to MSI file. On the General tab for MSI files, select MSI method to be Patch Installation.

   There is no package field this time.
4. Click OK to finish registering the patch procedure.

You can now use this procedure to update the targets with the old MSI package installed.

Patching Local Installations

If you selected the Register MSI Package method at the registration of the MSI package that is to be patched, and intend to use the local install procedures that are registered in this case, you should proceed in the following way to create the patch procedure.

Note: In this case, there is no way to patch the product in the Software Package Library. Packages using local install procedures need to get a patch applied afterwards to be updated to the latest version.

1. Select the MSI item for which the procedure is to be created, in the Software Package Library.
2. Right-click the Procedures folder and select New, Added procedure with new files in the context menu.
3. On the General tab, provide a name for the procedure. The task should be Configure, the OS should be Windows 32-bit.

4. On the Added Files tab, browse to the .msp file. The type should be set to MSI file.
5. On the bottom three tabs that open for MSI files, you should select MSI method to be Patch Installation, on the General tab.

   There is no package field this time.
6. Click OK to finish registering the patch procedure.

You can now use this procedure to update the targets. For targets with the old MSI packages installed, it is enough to execute the new configure procedure. For new installations, both the local install procedure and the new configure procedure must be executed.

Use of an Existing Administrative Installation as Source for a Software Item

During registration of an MSI package you can optionally select either Use an administrative installation, or Perform and use an administrative installation.

This is useful, for example, if you already have a number of existing administrative installations in your environment and want to manage those using software delivery functionality without having to reinstall them or even register their source into the software library. However, you will not be able to distribute the files associated with these items to downstream domain managers or scalability servers as the source is defined as external. All procedures will refer to the original location of the administrative installation. Not even by choosing the MSI library as location for the external administrative installation, will you be able to distribute the files associated with the item to downstream scalability servers. The only supported way of distributing source as part of the item to downstream servers is if it is truly registered or embedded into the Software Package Library.

Use of an Offline Administrative Install Procedure with a CD

To create an offline distribution administrative install procedure for a registered MSI package

1. Locate the MSI item in the Software Package Library
2. Find the registered package procedure CD install
3. Right-click the procedure and select New based on
4. Select Administrative Install as MSI method in the External file / General tab
5. Save the procedure

You can now drag and drop the created procedure on the targets. The target computers prompt for the CD and perform the administrative installation.

The combined use of a registered procedure and a CD can be of value if you need to create an administrative installation on the domain manager and on its downstream scalability servers as it can reduce bandwidth requirements.

Note: To create the administrative installations on the scalability servers, use the first method offered by the MSI package registration wizard, Register MSI package to the Software Package Library, when registering the MSI item in the Software Package Library. Check the box Enable installation from CD-ROM, on the CD options dialog.

When the item has been registered in the Software Package Library, select the Administrative Install procedure and use drag-and-drop to the scalability servers.

Registering Windows CE and Palm Packages in the Software Library

Windows CE and Palm packages can be registered in the Software Package Library using individual dialogs, the Register WinCE Package dialog and the Register Palm Package dialog. Using these dialogs, you can register and file new software items, when the registration information is on the source medium.

The instructions and data that are required to install a Windows CE application are contained in either a Windows CE cabinet (.cab) or Windows CE Application Manager (.ini) file.

The instructions and data that are required to install a Palm package are contained in a .prc file.

Package Consistency Check

Package consistency checking provides protection of packages against becoming corrupted. In effect, this means that if files are added, removed, or replaced with files of a different size in a package, and consistency checking is enabled on the package, then the software delivery functions refuse to distribute it and an error message is returned.

You can enable or disable package consistency check through the DSM Explorer, opening the Properties page of the software package in question. By default, the package consistency check feature is enabled when importing and creating new packages.

A checksum refers to the number of files, their names and size, but it does not involve the actual contents of the files.

The checksum is updated, when the following applies:

- An update is made to the package (like adding files)
- Registering new software packages
- Restoring software packages
- Auto-registering software
- Sealing a software package

The checksum is verified against the previously calculated checksum in the following cases:

- When enabling consistency checking
- When setting up new delivery environments
- Prior to execution of a nonexternal procedure on the agent

Notes on Checksum Calculation:

- Checksum control is also enabled by default when registering products through the command line.
- If a job has been set up for many targets, and a checksum error is detected during job distribution, all jobs that are not yet successfully completed will end with error. For example, the job for the first target computer executes OK, but when the job is to be delivered to the next computer, the software delivery manager detects a checksum error. Then the jobs for the next, and all subsequent target computers, will fail unless the checksum error is corrected.
- No checksum calculation is made on an software delivery agent unless it executes a job.

Defining Catalog Groups

Catalog groups assemble software items to make them available to particular groups of users through the Catalog user interface. You can create catalog groups in the Catalog folder, which is a predefined directory in the Software Package Library, by copying or dragging and dropping a computer group or user group on the Catalog node. After software has been moved or linked into a catalog group, an association is set up between a specific computer group and the catalog group. The catalog group is automatically created with the same name as the computer group.

The Publish in Catalog wizard is an enhanced easy-to-use method to publish software to users; for example, it enables you to select software from more than one software group. The wizard can be launched in context of library items and computer groups. For example, right-click a Computer Group and select Software Job, Publish software in Catalog… to launch the wizard. When a user, who belongs to one or more computer groups, and therefore to one or more catalog groups, logs on, a software delivery function determines what software is available for those catalog groups. This software is then displayed through the Catalog interface.

For example, if user 1 belongs to catalog group A, then user 1 sees all software available for catalog group A, as well as the software that has been linked into the Catalog folder. If user 2 belongs to catalog groups A and B, then user 2 sees all software available for catalog groups A and B, as well as the software that has been linked into the Catalog folder. If user 3 does not belong to any catalog group, then user 3 sees only the software that has been linked into the Catalog folder, if any has been linked.

If you drag and drop, or copy and link software into the Catalog folder, this software is available to all Catalog users. Users can also see the software installed on their computers.

Note: Only software packages with at least one catalog-enabled procedure are visible through the Catalog GUI.

Linking Catalog-Enabled Procedures

You can specify that auto-registered software containing Catalog-enabled procedures be linked into the Catalog folder while being registered in the Software Package Library by setting the Software Library: Automatically add Software Packages to Catalog folder policy to True (Configuration Policy, Default Computer Policy, DSM, software delivery, Manager policy group).

This will apply in the following cases:

- The software is distributed from the enterprise manager to a domain manager.
- The software is registered from the DSM Explorer, using either of the following methods:

  Register SD Package, Paste Folders to register SD Packages, Register SD Package as new version, and Converting detected software to registered.
- The software is registered using the command line.

Viewing Library Item Data

You can view additional information on programs that have already been registered in the Enterprise or Domain Libraries. The information displayed is that, which was provided when the program was originally registered. This includes the name and version of the program, and optionally, who filed it, when it was registered, who the vendor is, and any comments the administrator may have added during registration.

Unseal Software Item

The normal state of a software item (program) in the Software Package Library is sealed, also referred to as closed. In the sealed state a program can be distributed, installed, and exported.

Under certain circumstances, you can unseal a sealed software item for editing. Unsealing a software item is not possible when the program is installed, delivered, or distributed. For more information, see the DSM Explorer online help.

To unseal the software item right-click the item in the Software Package Library and select Unseal from the context menu.

Note: Displaying software items is controlled by the security component of CA ITCM, You must have the following access rights to view or work with software items:

- View permission to see a software item in the library
- Read permission to select a software item
- Write permission to seal or unseal a software item

Archiving and Restoring a Software Item

You can archive software items by using the software delivery archive option. Using this option, you can archive a closed software item from the Software Package Library. When an item is archived, its icon changes to indicate that it has been archived. Each archived item has the same structure as on the source media (for example, DVD). When a software item is archived, its Source directory is removed, because all files previously residing there are moved to the specified archive location.

After a software item has been archived, it can later be restored using the software delivery restore function. If the software item is still in the same location in which it was archived, then the restore process starts immediately. If it is not, you receive an error message indicating that there is no registration information (reginfo) found at the original archive location.

Note: If the files have been moved, for example, to a tape, you must first retrieve the files and then put them back to a known location before executing the Restore operation.

After a software item has been restored, its icon returns to what it was originally, before the item was archived. The software item's Source directory is also restored.

Notes on Virus Checking

An administrator running the DSM Explorer on a Windows NT Technology system - either installed locally with the manager or stand alone on a remote computer - can use eTrust Antivirus, if it has been installed on the manager.

All library items, a single library item, a library item volume, a library item volume file, or a fetched item file can be scanned.

An administrator running the DSM Explorer on Windows NT Technology with eTrust Antivirus installed, can do the same scanning on the Windows NT Technology enterprise and domain manager.

Note: The remote DSM Explorer cannot use a NOS-less connection to the manager; the library has to be shared on the network.

The manager checks if eTrust Antivirus, InocuLAN, or cavscan is present. If one of them is found, it is used. If none is found, a search is made for inocmd32, which is then used, if found. The integration with inocmd32 enables automatic virus scan when jobs are created.

A manual virus check of software delivery library packages and fetched item files can be performed from the DSM Explorer by right-clicking a folder or object and selecting Scan Viruses on the context menu. If InocuLAN or eTrust Antivirus is used, you may need to check the Include Subdirectory check box in the InocuLAN or eTrust Antivirus Shell Scanner dialog before starting the scan.

If inocmd32 is used, the scan starts and opens a DOS box, which is initially empty. When the scan has executed, the result is presented in that DOS box. Close the box after reading the result.

Software and Procedures

This section describes how you define item procedures and introduces software and procedure groups:

- Defining Embedded Item Procedures (see page 71)
- Defining Added Item Procedures (see page 74)
- Software and Procedure Groups (see page 78)

Defining Embedded Item Procedures

Item procedures are the means by which a program is installed, activated, configured, and uninstalled. There can be embedded item procedures or added item procedures. Embedded item procedures are registered automatically at the same time as the program. Added item procedures are registered separately, after the item is registered. For more information on added item procedures, see Defining Added Item Procedures (see page 74).

Embedded item procedures are marked Original Delivery in the Created column of the Procedures detail display.

Item procedures identify the following:

- Operating system under which the item procedure executes
- Procedure type, such as command file, executable file, SWD file, MSI file, SXP file, PKG file, PIF file, RPM file, IPS file, Palm file, or WinCE file
- Startup procedure name, such as SETUP.EXE
- If the procedure is an external procedure (in other words, it already exists on a target computer, or somewhere accessible from the target computer), external procedures provides the means to refer to programs not registered to the Software Package Library, that is, present in an absolute path on each agent but still manage their execution using the product.
- Type of task being performed by the procedure, such as INSTALL, ACTIVATE, UNINSTALL, or CONFIGURE
- Parameters to be used when starting the procedure
- Additional files needed for the procedure to perform
- Whether the item is to be enabled for the Software Catalog

You can use the item procedures that are delivered with the program (such as SETUP.EXE), or you can create your own customized procedures using batch or command files. For example, you may want to create a customized install for all Windows computers that have disabled mouse devices.

Exclude Item Procedures from Reinstall After Crash

If you do not want an item procedure to execute as part of the Reinstall After Crash (RAC) process, you can select the Exclude from RAC option in the Properties dialog of the actual procedure. This option can be changed, even for sealed software items, and so enables the administrator to exclude obsolete packages from RAC. For more information see RAC Configuration (see page 126).

The following item procedures have the Exclude from RAC option set:

- All activate procedures on the software delivery agent:
  The three scan procedures (Scan MSI, Scan SWD, and Scan SM Installer installations) and the SM Installer activate procedures.
- The following configure procedure on the software delivery agent:
  Network Repair
- The following activate procedures on the scalability server:
  - Synchronize Software Staging Library
  - Synchronize Software Job Records
  - Synchronize CCS Calendar
  - Enable SDLIB share
  - Disable SDLIB share
  - Enable MSILIB share
  - Disable MSILIB share
  - Enable Boot Server share
  - Disable Boot Server share
- All reinstall procedures for all packaging formats.

Item Procedures in Batch Programs

You can ensure that the job for which the procedure is to be used, does not end with OK status, if the batch script has failed by performing conditional processing in batch programs.

In Windows NT Technology, you can use the built-in IF with ERRORLEVEL, EXIST, or string comparison, followed by a specified command to make your batch script end with an error code and exit, making the software delivery functions aware of the error.

For example, the following item procedure command file copies the file, myfile.txt, to the root of the hard disk, if the file exists in the source directory. If it does not, the procedure file ends with an error code.

```
@echo off
copy myfile.txt C:\*.*
IF ERRORLEVEL 1 EXIT
```

If the file, myfile.txt, is not found, the job ends with error code SDM228001.

For information about performing conditional processing in batch programs, see the platform-specific documentation. In Windows NT Technology, you can open a command prompt, type help if, or help exit to find more information.

Item Procedure Task Types

The tasks performed by an item procedure fall into one of four categories of which Install is the most common.

The other tasks are Activate, Configure, and Uninstall, which are also called noninstall tasks.

ACTIVATE

Triggers the product to run. For example, an ACTIVATE task can be used to remotely trigger the start of a backup or archive program. You should identify an item procedure as an ACTIVATE task if it does not fall under any of the other three categories or if it performs a combination of any or all of the other three tasks.

CONFIGURE

Reconfigures an existing installation.

INSTALL

Installs the product.

UNINSTALL

Removes the installation.

Note: ACTIVATE, CONFIGURE, and UNINSTALL procedures can be performed only on computers on which the item has already been installed, that is, installed using any of the procedures of type INSTALL. Most packages contain only an INSTALL and an UNINSTALL procedure. CONFIGURE, and customized INSTALL and ACTIVATE tasks can be created by registering site-written scripts, command, or batch files. For more information on customized item procedures, see Optional Customization Tools (see page 46).

Unlike other software delivery agents, NOS-less agents do not have access to the manager's local library. Therefore, the software delivery component cannot determine which item procedures are necessary for noninstall task types, and the whole library item is transmitted to the agent. In the case of a large library item, this process may be time and resource consuming. Use external procedures to avoid delivering the package.

Defining Added Item Procedures

If you have written an item procedure before registering a program, you can include it during the registration as an embedded item procedure; however, most customized procedures are defined as added item procedures.

Added item procedures are created and registered in the Software Package Library after registration of the program they concern. They can be created from scratch or they can be copied from existing item procedures.

Added item procedures are not automatically delivered from the enterprise manager to the domain managers along with the software product. However, when you are adding a registration order for a software item containing added item procedures to a distribution container, you can use software delivery functionality to try to automatically add registration orders for associated item procedures to the distribution container. You can also determine that registration orders are created only for selected procedures. If a failure occurs during automatic generation of a registration order for one of the added item procedures, you can decide to continue with automatic generation of registration orders for the remaining procedures.

Added procedures can only be registered to the enterprise and domain manager libraries. They cannot be registered to scalability server libraries. This is important as when added procedures with new files are scheduled to be installed on agents connecting through remote scalability servers the entire original software item and the added files will be delivered from the domain manager's library rather than reusing any files registered to the scalability server. Take this into account before deciding on using added procedures.

The alternative to added procedures is creation of new independent software items that can be stored in the scalability server libraries.

Copying Existing Item Procedures

You can copy existing item procedures to create a new item procedure, if the new item procedure is the same type (such as CMD or EXE files) as an existing item procedure. In this case, the existing item procedure is used as a model, and you can change everything except the type of procedure and the program.

Linking, Unlinking, and Adding New Item Procedures

Item procedures can be linked or unlinked, and new procedures added, into Procedure Groups. When a procedure is dragged to a procedure group, the resulting shortcut menu lets you link the procedure to the targeted procedure group.

Procedures can also be unlinked from the procedure group of which they are a part. When a procedure is unlinked from a procedure group, it disappears from that group.

The order in the procedure group is of importance (see the order number column in the GUI) and can be changed afterwards, using a context menu.

Defining Procedure Dependencies

Procedure dependencies allow for prerequisite procedures to be defined for library items. This can be useful when a procedure requires one or more other procedures to have already been successfully executed before the current procedure can be executed.

If you select a procedure with dependencies from the Software Package Library, the dependencies are listed in the Procedure Dependencies folder in the right pane. Only installation procedures can be dependent procedures. When a job is to be executed using the parent procedure in the folder, a software delivery function checks whether the dependent prerequisite procedures have been executed. If they have not, then those procedures are executed first, in the order they are listed in the Procedure Dependencies folder.

Note: Uninstallation of dependent prerequisite procedures does not automatically cause the uninstallation of the depending procedures.

Procedures can have more than one level of dependency. For instance, a procedure in the Procedure Dependencies folder can also have a procedure dependency. When the job container is evaluated, all of these dependencies are addressed. Jobs are then generated, which can in turn generate other jobs.

Special Agent Procedures

In addition to the installation procedures used to install various types of software, the software delivery agents also contain a number of specialized procedures. These include:

- Microsoft Installer (MSI) related procedure (see page 75)
- Software detection (SWD) related procedure (see page 76)
- Software Management Installer options (see page 76)

Microsoft Installer Related Procedure

For Windows NT Technology agents, the Microsoft Installer (MSI)-related procedure, Scan MSI, scans the software installed by the Microsoft Installer.

Software Detection (SWD) Related Procedure

The Scan SWD procedure scans for software using software detection scripts for software delivery agents on Windows NT Technology, Linux, and UNIX.

Software Management Installer Options

The following Software Management-related procedures are available for Windows and Linux/UNIX agents, unless otherwise noted.

SM Installer: Enable Trace

Enables the Software Management Installer's trace facility.

SM Installer: Disable Trace

Disables the Software Management Installer's trace facility.

SM Installer: Get all traces

Gets all the Software Management Installer traces.

SM Installer: Get latest trace

Gets the latest Software Management Installer trace.

SM Installer: Get history

(Not available for Linux and UNIX agents)

Gets Software Management Installer's history of install and uninstall operations.

SM Installer: Get user trace

Gets the latest Software Management Installer user trace.

SM Installer: Get user history

Gets Software Management Installer's history of user-specific install and uninstall operations.

Scan SM Installer installations

Scans for software installed by the Software Management agent installer and reports back to the domain manager.

Software Catalog Procedures

The Software Catalog is available through the CA DSM Agent + Software Delivery Plugin installation package.

The installation package contains the following installation procedures:

Catalog: Add

Installs the catalog to an agent system.

Catalog: Remove

Removes the catalog installation from an agent system.

Scalability Server Procedures

The scalability server procedures include configure and activate procedures.

The following are scalability server configure procedures:

Disable Boot Server share

Disables the Boot Server share access.

Disable MSILIB share

Prevents the MSI library from being accessed by agents.

Disable SDLIB share

Prevents the software staging library from being directly accessed by MS NOS agents.

Enable Boot Server share

Enables the Boot Server share access.

Enable MSILIB share

Enables the MSI library to be accessed by agents.

Enable SDLIB share

Enables the software staging library to be directly accessed by MS NOS agents.

The following are scalability server activate procedures:

Synchronize CCS Calendar

Synchronizes the CCS calendars on the scalability server and the manager after updating the calendar on the manager.

Synchronize Software Job Records

Run only after a catastrophic manager failure to restore any lost job results and synchronize the contents of delivered items with the software staging library.

Synchronize Software Staging Library

Synchronizes the contents of delivered items with the software staging library.

Software and Procedure Groups

Software groups are used to bundle software packages in the Software Package Library. Each software group can contain individual software packages, install procedure groups, or other software groups, each of which can be a part of one or more software groups. For instance, a software package called Word Processing can be part of the “Office Software” software group and part of the “Popular Software” software group also.

The Software Package Library initially contains three predefined software groups, including All Software, DSM Software Packages, and Catalog. The All Software group contains all registered software packages. The DSM Software Packages group contains all auto-registered DSM packages. The Catalog folder is initially empty. However, catalog groups can later be added. For more information on catalog groups, see Defining Catalog Groups (see page 67).

Using a software group provides a quick and easy means of installing a number of individual software packages. For instance, the Office Software group may contain a word processing package, a drawing package, and a spreadsheet package. These packages can be installed together as part of the Office Software installation.

Procedure groups contain links to individual software packages and are used when defining installation jobs.

The procedure group contains the procedures used for installation of the software packages. The procedures in a procedure group can be ordered.

Renewing and Recovering Failed Installations

If an installation order has failed for one or more target computers, you can clean up the failed job using an uninstall procedure registered for that library item.

You can renew a failed installation rather than recover it if:

- Job execution has failed for one or more target computers, and
- No other computers are waiting to be activated.

Note: When renewing a job container the property "Ignore cascading install of dependent packages" is automatically checked and disabled for edit. The reason for this is to make sure the renewed job container includes the exact same jobs as the failed job container. If the original job container failed because of a missing procedure dependency, the renewal of that job container will ignore the procedure dependency and attempt to install the depending software package. This will only happen if the procedure is physically missing. If the cascaded procedure exists and simply fails to install, a renewal will include it.

Delivery and Staging of Software

After a software package has been registered in the library on the enterprise or domain manager, you can distribute it to other networked computers by creating and sending an order. Orders sent from the enterprise are bundled into *containers*, which may or may not contain other orders. Orders originating from a domain manager are sent in *job containers* to the targeted computer or computer groups.

Note: If CA Technologies's virus scan software is installed on the enterprise or domain manager, CA ITCM automatically scans the contents of a distribution container on an enterprise manager when a distribution is sent. It also automatically scans the contents of a job container on a domain manager when a distribution is received. When a job container is set up, the contents of the job container are automatically scanned.

Orders

There are several different types of orders for software delivery purposes, including:

Library Item Registration orders

Distribute registered items and item procedures from the Software Package Library on the enterprise manager to the domain manager libraries. The item registration orders include the library item and its registration information files.

To be distributed from a domain manager, software programs must be registered in the Software Package Library on the domain manager. You can also create new versions of software packages and make use of the delta delivery mechanism; that is, only distribute the files that are different from the previously distributed version.

Installation and Removal orders

Install or uninstall a program on a computer or computer group.

Fetch Item orders

Retrieve a specific file or files from the domain managers to a designated place on the enterprise manager.

Library Item Deregistration orders

Deregister and delete items from a domain manager's Software Package Library or computer groups. When a program is deregistered and deleted, all associated item procedures (both embedded and added) are deregistered as well.
Items from the Software Package Library on a domain manager can only be deregistered and deleted, if they were initially distributed from the enterprise manager, and have not been installed on a computer at the domain.

Activation orders

Initiate the program itself. For example, an activation order can be used to trigger the start of an archive program on a remote computer.

Configuration orders

Initiate changes in the configuration files on a remote computer. Configuration type tasks are defined as item procedures.

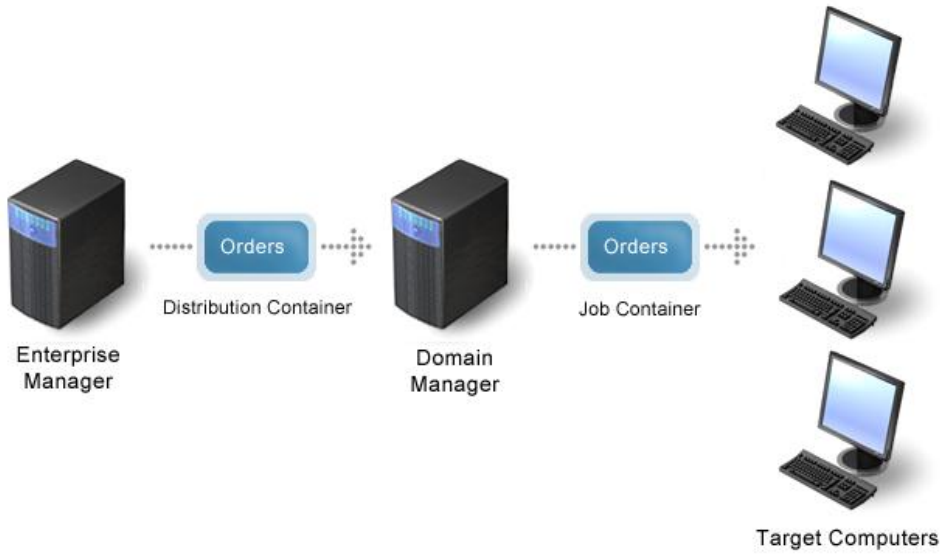
Software Policy orders

Register and deregister software policies on domain managers.

Library maintenance orders

Purge software and set as archived on the domain managers' libraries; for example, software not frequently used. This is useful to preserve disk space. The software can be restored on demand.

The following illustration shows the flow of orders from the enterprise manager to the domain manager (using distribution containers) and from the domain manager to the target computers (using job containers).



Once jobs are delivered to the target computer, the software delivery (SD) manager or the SD agent can initiate job execution on the target computer.

Orders can include a trigger so that the SD manager initiates job execution. In the absence of a trigger, the agent uses Job Check to contact the manager and initiate job execution. Orders are queued until Job Check checks for held orders. The frequency, with which that check occurs depends on the Job Check options available to the operating system under which the targeted computer is running.

Item procedures carry orders to install, uninstall, activate, and configure items on target computers. When an order is received and activated, it proceeds as if the item procedure was initiated directly on that computer.

Orders Sent from the Domain Manager

Orders are sent from the domain manager to the target computers using a job container. The domain managers can target both individual computers and computer groups.

All orders sent from a domain manager can be distributed using either of two methods:

- A simplified method that uses default settings
- A customized method from which you can define job options and flags

Reinstall procedures are useful when managing software. For more information, see Reinstallation Procedures (see page 86).

You can attach a job execution calendar to a specific computer or computer group, or to the All Computers / All User Profiles groups. The calendar is attached by right-clicking the computer or group icon, and selecting Software Jobs, Job execution calendar, Attach. It can later be detached in a similar manner. The calendar definitions of the days, dates, and times when processes can be performed are then used to control the execution of software jobs.

You can also use a job delivery calendar. On the Job Options tab you can specify for each job whether you want to use a job delivery calendar. This calendar serves to control deliveries using Data Transport Service.

Configuration orders are similar to activation orders; both require that the associated library item already be installed. This is also a prerequisite for uninstall orders.

Setting Up Job Containers on the Domain Manager

Jobs can be added to a job container to allow for a number of jobs to be grouped together. Job containers are implicitly created when setting up jobs for computers or computer groups. There are several ways to create a job container:

- Drag and drop library items (software, software group, procedure or procedure group) on a computer or computer group.

  By using the left mouse button during the drag operation, the job is set up immediately using default settings. By using the right mouse button, a small popup menu is displayed on drop, allowing you to use customized options.
- Copy library items to the clipboard and use the paste operation on the computer or computer group.
- Use the Deploy Software wizard.

  The wizard can be launched in context of a library item, computer, or computer group, and from the software jobs folder.
- Clone the installations on a target computer by selecting Software Jobs, New, Software Deployment job based on Targets Installation.
- Create a new job container, using an existing job container or software policy as template, by right clicking and selecting New, Software Deployment Job based on.

By using the customized method, you can assign a name to the job container, and establish job linkage options for the container. With the job linkage options, you can specify if jobs in the container are run independently of one another (no linkage), or if upon failure of one job, the remaining jobs for that target are aborted (batch).

Note: The batch behavior can be customized using the 'Enable Transaction' property of the job container. If this property is checked, all jobs in the job container, regardless of software procedure type, for a target which has at least one failed job will be set to error during evaluation at the domain manager. If the 'Enable Transaction' property is not checked, all jobs *after* the failed job will set to error during evaluation at the domain manager, but any successfully set up jobs *before* the failed job will be allowed to run.

Regardless of a job container linkage, procedures of type SXP, PKG, PIF, RPM, or MSI are, if possible, rolled back on execution failure. If the job container linkage is batch and the 'Enable Transaction' property of the job container is set, then entire chains of consecutive jobs of procedures of types SXP, PKG, and RPM will be treated as a single atomic operation by the agent. On failure, the entire chain will automatically get rolled back, if possible. Note that if the job container only contains procedures of types SXP, PKG, PIF, and RPM, the entire container forms one single chain. However, it is possible to mix SXP, PKG, PIF, and RPM procedures with other procedure types, like MSI or generic. In this case, multiple chains may be formed within a single job container, but only the active chain will be considered for complete rollback on failure. In addition, the execution order set by the manager for jobs within the job container may not be honored by the agent for procedures of types SXP, PKG, PIF, and RPM. The Software Management component of the software delivery (SD) agent sorts the jobs in an order suiting it best. This means, if the job order on the SD manager is A, B, C for three jobs, it may very well be executed in the order B, C, A on the SD agent. Furthermore, if the 'Enable Transaction' property of the job container is not set and, for example, job B fails, Software Management does not stop, but tries to execute jobs C and A, too.

Job execution can also be synchronized, meaning that a job is only activated when the previously contained job has completed successfully, that is, all target computers have executed the job successfully.

For job containers with batch or synchronized job linkage, the automatic cascade of dependent packages can be disabled. For job containers with no linkage, the automatic cascade of dependent packages is always disabled.

If you click Set as default, you can save the settings in the Registry of the computer you are currently using. If there is more than one person connecting to the same SD manager, and each is using Set as Default, then each user has unique settings in a personal user registry.

Specifying Job Options

The Jobs tab on the Setup jobs dialogs lets you specify options for the individual jobs. The options can be applied to one or more of the jobs (operates on the jobs selected in the list). You can also manipulate the order in which the jobs execute and remove undesired jobs, using the buttons on the right hand side of the job list.

Job Execution Permission

The job execution permission feature allows administrators to enable or disable the execution of any software delivery or asset management jobs on a target computer. The job execution permission feature can be activated or deactivated either on the target computer or remotely from the DSM Explorer.

Job execution permission on a target computer is controlled through the Restrict job execution configuration policy, which indicates whether a software or asset job is disabled on the target computer.

If the management policy allows (that is, if the Restrict job execution configuration policy is locally managed on the target computer), an administrator on a target computer may locally enable or disable asset jobs and software jobs from running on the target computer. This can be set using the "Restrict Agent Jobs" check box on the General tab of the DSM Properties, Common Agent dialog of the system tray.

As an alternative to this method the following command can be used from the command line:

```
caf restrictjobs [1 | 0]
```

Specifying 1 in the caf restrictjobs command disables jobs from executing on the target computer, specifying 0 enables job execution. Specifying neither 1 nor 0 displays the current setting.

Prioritization of Software Jobs

The software delivery functionality allows the user to prioritize software jobs to achieve a dynamic and quicker deployment of software packages, for example, patches, to end systems.

With this job prioritization feature, software packages are processed by their current priority rather than pushing them to systems in the order they were scheduled. The priority basically controls in which order jobs are built and executed; the higher the priority the more urgent the delivery.

The priority does not guarantee execution order. Even though jobs with higher priority are handled more often the original activation time is honored and a job of lower priority may be executed before jobs of higher priority, if the delivery process for the lower priority jobs has completed before the high priority job.

Priorities are set when setting up software policies or job containers (on the domain or enterprise manager) or distribution containers (on the enterprise manager). Priority 1 is the highest, 5 is the default, and 10 is the lowest priority.

Job Execution on System Shutdown

When updating, for example, kernel drivers on a Linux scalability server, a reboot is required. Since these types of managers are rebooted only occasionally, you need to schedule jobs for execution, while the computer is going to shutdown.

By checking the *Run at shutdown (UNIX only)* box in the Job Properties, Procedure Options tab, a type of job is created that is postponed on the target computer until the system is shut down.

If the box is checked, the Jobs will be triggered by Scalability Server box is automatically dimmed and not selectable, since these two options are mutually exclusive.

The box is set by default, if the *Run at shutdown (UNIX only)* box is checked on the Options tab of the procedure used for the job.

Note: Do not check the for the jobs targeted at non-UNIX computers. In such a case, the job never runs but times out.

Jobs for execution on shutdown must not be combined with standard jobs in the same container, since this postpones all jobs of the container.

Enabling Checking of Software Based Policies

The configuration policy, DSM/software delivery/ Manager/Check template policies, enables checks of software policies when evaluating a job container.

For example, a software policy has a job assigned that ensures that the Software Catalog is not installed for the members of the group associated with the software policy. Then, a job that installs the Software Catalog will fail in the evaluation step for all targets that also belong to the given software policy.

If the Check template policies parameter is set to True, every job being set up fails in the evaluation step of the job container, if the target is also a member of a template group that has been assigned contradicting jobs.

For example, software policy X has a job assigned that uninstalls an application. If a job is being set up to install the same application, it fails for all computers that are members of the group associated with software policy X.

This task can be controlled from the DSM Explorer through Tasks, Policy, Job Policy.

Disabling Implicit Deliveries to Scalability Servers

Jobs through scalability servers will implicitly deliver software from the domain manager if not present in the scalability server's library. To maintain a better control of the deliveries in the network, you can turn off implicit deliveries. If turned off, jobs will fail if the required software is not present in the scalability server's library.

This task can be controlled in the tree view by navigating to Control Panel, Configuration, Software Job Management, or Job Handling.

Using Scalability Server Libraries for Deliveries to Agents

Data Transport Service transfers are initiated by the Data Transport Service agent on the scalability server. The software is extracted from the scalability server library. If the job uses an added procedure with new files (since a scalability server library does not maintain such added procedures) or the software package is not registered with the scalability server library, the domain manager library remains as the source for the transfers.

A transfer that fails causes all agents in the job depending on that transfer to fail. If the transfer completes with errors, or the job is deleted, Data Transport Service cleans up all staging areas.

This function only covers Data Transport Service deliveries to agents only. Any other download method, like internal NOS or NOS-less, is not covered by this function.

Reinstallation Procedures

Reinstalling SXP software on a target computer was a rather inconvenient procedure in the past, since you had first to uninstall the software before installing it again. In addition, there always was a period of time when the software was not available on the target computer. The reason was that it was not possible to have an uninstallation job and an installation job in the same job container.

Software Management packages registered with the sd_registerproduct command are provided with an additional reinstall configuration procedure, which is able to repair an existing product installation.

For Palm and Windows CE packages registered in the Software Package Library using individual Register commands from the DSM Explorer, a reinstall procedure is always created together with an install procedure.

You can easily select a reinstallation procedure from the DSM Explorer.

Empty Jobs and Job Containers

There are a number of situations that a job is set up but there are no target computers to receive that job. Or, a job was set up for a group that has no Execute permissions. This resulted, in the first case, in an empty job which was marked OK, or, in the second case, in a job container with no jobs.

The software delivery system behavior is as follows:

- If it can be determined when the job is set up that there are no target computers, an error is returned immediately.
- If no jobs could be set up, the job container is deleted.
- If the background evaluation of a job container results in no targets for the job, the job is marked by a warning symbol. This can happen under the following circumstances:
  - A job container with ACTIVATE, CONFIGURE, or UNINSTALL procedures has been set up with target computer groups or computers as targets. When the container is evaluated, it is found that none of the target computers has an installation of the item to which the item procedure belongs.
  - A job container has been set up using any procedure, with target computer groups as targets. When the container is evaluated, it is found out that the software delivery agent is not installed at all on the machine (for example, the asset management agent only has been installed on the target computers.)

In these cases, a new job message states why no targets were found, for example, "No target computers found in evaluation step" or "No target installations found in evaluation step".

Synchronize Software Job Records Procedure

The scalability server job procedure "Synchronize Software Job Records" is available for both Windows and Linux operating environments. The procedure is of type activate.

Run this procedure only after a catastrophic manager failure to restore any lost job results and synchronize the contents of delivered items with the staging library.

The procedure should only be run on all downstream scalability servers and on the domain manager machine itself, after a domain manager machine has been restored after a crash. The procedure ensures that possible lost job results are restored to the manager and that the staging library content is synchronized for the scalability servers.

Optimization of SXP Software Package Procedure Prerequisite Evaluation

This performance improvement concerns the evaluation of procedure prerequisites in SXP software packages as of Unicenter Desktop and Server Management (Unicenter DSM) r11.2.

Only SXP packages that are created using the Software Management Packager for Windows, or using the CLI, or are migrated from a pre-r11 manager, that is, Unicenter Software Delivery 4.0 SP1, are capable of delivering the optimization.

The improved procedure prerequisite evaluation is not backwards compatible with earlier versions of Unicenter DSM r11. Therefore, it is switched off by default and must be enabled before any SXP packages containing procedure prerequisites are registered in the Software Package Library.

Enabling the improved evaluation mechanism works only if all CA ITCM managers in the enterprise are at the minimum release r11.2. Enabling the mechanism on a manager of an earlier Unicenter DSM r11 release has no effect.

Exporting SXP packages that contain procedure prerequisites from an r11.2 manager with the improved evaluation mechanism enabled to an r11.2 manager with this mechanism disabled works and delivers the optimization. Exporting into the other direction works but does not deliver the optimization.

Exporting packages that contain procedure prerequisites from an r11.2 manager with the improved evaluation mechanism enabled to a pre-r11.2 manager will produce internal process errors in CA ITCM. This includes the scenario where the enterprise manager is at release r11.2 but some or all linked domain managers are still at a pre-r11.2 release.

Exporting packages that contain procedure prerequisites from a pre-r11.2 manager (that is, at Unicenter DSM releases r11.0 or r11.1) and importing into r11.2 works but does not deliver the optimization.

Migrating or importing SXP packages that contain procedure prerequisites from a pre-r11 manager (that is, Unicenter Software Delivery 4.0 SP1) into r11.2 works but delivers the optimization only if the mechanism is enabled before the migration is started.

Registered packages containing nonoptimized procedure prerequisites can only get optimized by deleting them from the Software Package Library and recreating or remigrating them after the improved evaluation mechanism has been enabled.

To enable the improved procedure prerequisite evaluation use the following command:

```
ccnfcmda -cmd SetParameterValue -psitrm/usd/shared
        -pnBuildQuerySQLWithParameters -v1
```

To disable the improved procedure prerequisite evaluation use the following command:

```
ccnfcmda -cmd SetParameterValue -psitrm/usd/shared
        -pnBuildQuerySQLWithParameters -v0
```

Wake-on-LAN Control when Initiated by Job Check

Currently, any software delivery (SD) job sends Wake-on-LAN packets to wake up the target computer.

The SD scalability server configuration parameter 'Jobcheck: Disable Wake-on-LAN' controls the behavior of Wake-on-LAN when initiated by SD job check. If.this configuration parameter is set to True, no Wake-on-LAN signature is set in the job check trigger message.

The default value of this configuration parameter is False.

Note on Sending a Job to a Computer Running Apple Mac OS X

If a software delivery (SD) job is sent to a sleeping computer running Apple Mac OS X, the computer first gets woken up, but the SD job itself is not started. This is because the computer running Mac OS X is still waking up when it receives the trigger to perform the SD job.

However, the SD scalability server or manager will trigger the computer running Mac OS X again after 10 minutes because the SD job is still active.

Activating the Item Procedure

After an order has been detected, the program identified by the item procedure is initiated. A Job Check dialog appears for Windows target computers if the administrator selected the Prompt user option on the installation order. If the user clicks Run, the installation begins immediately. If the user clicks Postpone, he can specify how much to postpone the execution. If the user clicks Abort, the order is canceled and no further prompts are issued.

Agent Users

Additionally, if the administrator checks Boot before, as well as Prompt user, when defining a job order for a Windows target computer, a Reboot dialog prompts the Agent user.

The Agent user must indicate, before the job executes, if the reboot should be done now or postponed.

If the administrator checks Boot after (as well as Prompt user) when defining a job order for a Windows target computer, the previous dialog prompts the Agent user after the job has been executed.

Administrators

For a job order with the Boot option that is to be executed on the domain manager, the Administrator is first warned that other jobs may fail.

If the warning is ignored and the administrator clicks Yes, the previous Job Check prompt appears asking when the reboot is to be performed.

After the order has been received and accepted, the degree of user interaction required is determined by the item procedure. If the item procedure prompts for target directories, those prompts are conveyed to the user.

Note: The domain manager is not allowed to be targeted with a combination of the 'Reboot' and 'Job will be Triggered by Server' options, as booting the scalability server at the specified job start time can lead to unexpected results.

Triggering an Immediate Check for Queued Jobs

The Start Job Check link in the System Tray triggers an immediate check for queued software delivery (SD) jobs. On Windows a Job Check dialog appears.

If the SD agent detects a queued job, installation is initiated.

Note: The job option, "Jobs will be triggered by scalability server," is enabled for SD jobs by default. That means that the scalability server activates the job at the scheduled time. If that option is disabled, the user on the target computer is supposed to run the Job Check manually.

Pre- and Post-Job Check Processing

The pre- and post-Job Check processing features make it possible to run external executables before or after a software delivery (SD) job. You can specify an executable that should run before the actual SD job is processed and an executable that should run after the SD job, or the last SD job in a job chain, has run.

These executables are specified through the agent policies 'Jobcheck: Pre-command' and 'Jobcheck: Post-command", as follows:

Jobcheck: Pre-command

Specifies an executable that runs before an SD job or before the first SD job in a batch is processed. An example is switching off an antivirus realtime monitor for the duration of a job container.

Default: empty

Jobcheck: Post-command

Specifies an executable that runs after an SD job or after the last SD job in a batch is processed.

Default: empty

The Post-command is only run, if a Pre-command is also specified!

Pre- and post-Job Check processing takes place regardless of the job linkage setting (batch job, synchronized, or no linkage) for a Job container tab.

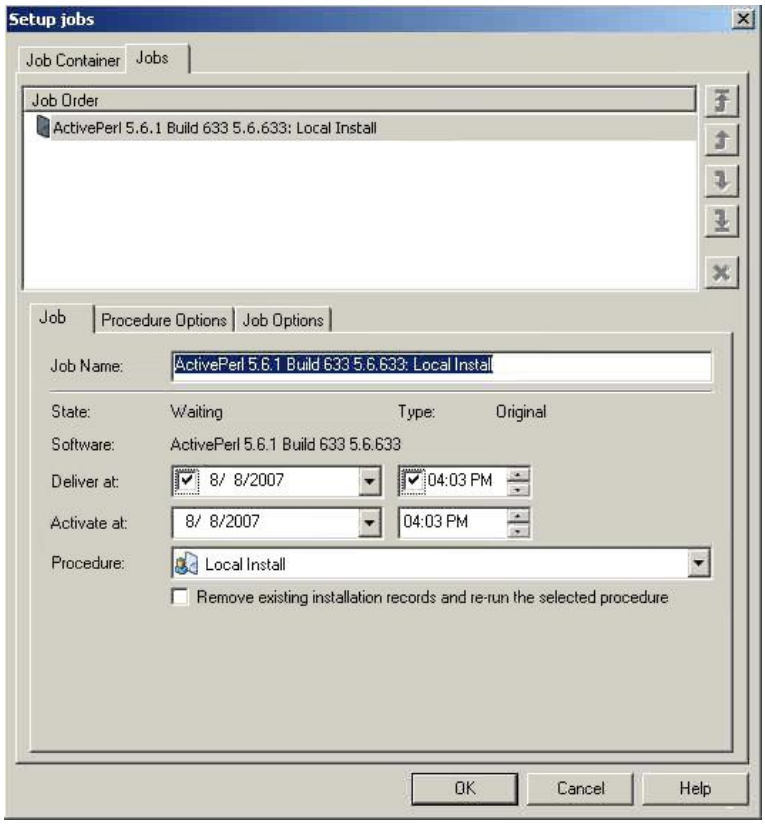
Notes:

- If more than one job is run for a specific computer or user target, first the pre-Job Check executable is run, then all jobs, and finally the post-Job Check executable. If an intervening reboot or logoff takes place during job execution, the SD agent will run the post-Job Check executable, execute the reboot or logoff, then run the pre-Job Check executable, and continue with job execution.
- If Restart machine or Logoff user is specified as an SD procedure option to take place before job execution, no pre- or post-Job Check processing is done, until the first job in the job chain is to start executing.

  If Restart machine or Logoff user is specified as an SD procedure option to take place after execution of a job or after the last job in a chain, this does not cause any pre- or post-Job Check executables to run.
- Pre- and post-Job Check processing only takes place, if Job Check detects a waiting SD job. Job Check does not automatically start pre- and post-Job Check processing.

Separated Delivery or Staging and Job Activation

If you create a job container when setting up jobs, a different dialog is displayed. For example, if you drag and drop a job onto a computer or computer group and select Schedule jobs, a dialog similar to the following is displayed:



It is possible to define separate delivery and activation times, which allows you to separate the delivery of software and the staging of jobs to the staging area on the scalability server or the target computers (if DTS NOS-less computers) from the actual activation time of the job.

The activation time reflects the earliest possible activation time. If the delivery or staging exceeds the activation time, the activation is postponed accordingly for the affected target computers.

The delivery time is set on each job. By default, the delivery time is set to the activation time for all jobs.

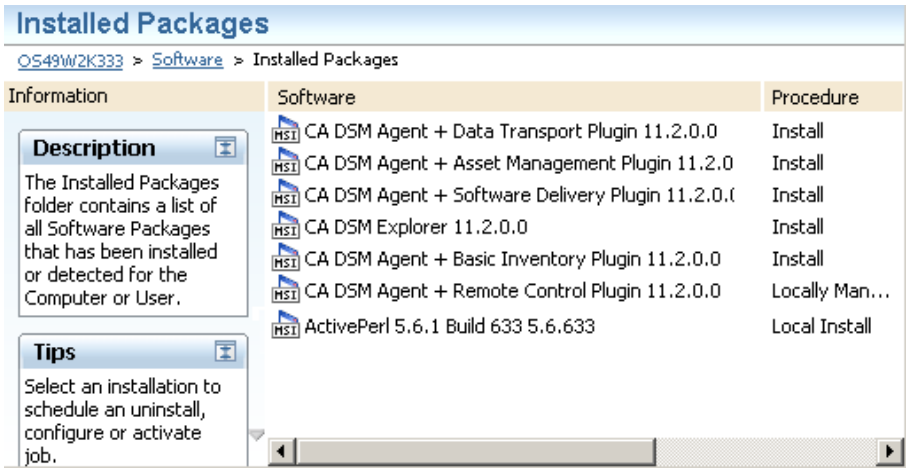
Synchronized job containers perform delivery and activation for each job processed, that is, the delivery of a job does not start before the previous job has successfully completed.

Note: From a domain manager you can also choose the Schedule delivery to a Staging Library option when you drag and drop a job onto a scalability server or scalability server group. This option displays another dialog that lets you add items to the library of a downstream scalability server.

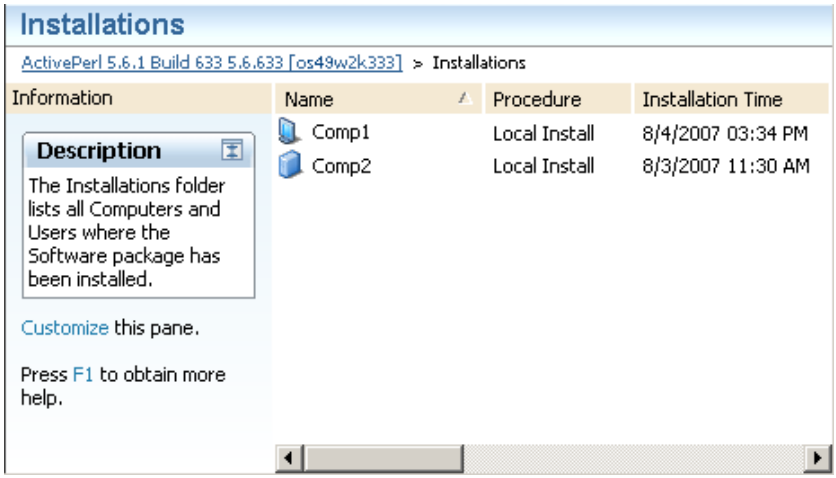
Viewing Current Installations

CA ITCM maintains a record of all current product installations. This record can be viewed from the perspective of the number of products installed on a particular computer or from the perspective of the number of computers on which a particular program has been installed. Examples of each view follow.

The following illustration shows installed packages on a designated computer:



The following illustration shows installations of a designated item:



Download Options

The download options apply to all agent operating environments currently supported by CA ITCM, unless otherwise noted.

The current agent operating system versions are listed in in the Certification Matrix available at CA Support.

DTS - NOS-less

This download method, which does not apply to Windows CE agents, makes use of Data Transport Service for downloading to NOS-less agents from their associated domain manager.

On Windows, the CA DSM Agent + Data Transport Plugin needs to be installed on the target before you can use this download method.

On Linux and UNIX, the CA DSM Agent + Data Transport Plugin is installed together with the CA DSM Agent + Software Delivery Plugin.

If you no longer need the DTS - NOS-less configuration, you can remove the DTS agent plug-in from the target using an uninstall job, unless you need the DTS agent plugin.

Internal - NOS-less

This procedure makes use of software delivery-internal protocols for downloading to NOS-less agents from their associated domain manager or scalability server.

Internal - NOS

This procedure makes use of the Microsoft Network or NFS for agent access to files on the domain manager or scalability server, that is, network shares.

Configuration of Download Method

The default download method for a computer is defined in the MDB on the manager. The computer properties dialog can be used to set the download method for individual computers. In addition, the in-context pop-up menu for computers and computer groups allow for setting the download method for multiple computers in one go.

The download method stored in the MDB is used during software deployment. Each software job will honor the download method the target computer is configured to use at the time the job container is sealed and evaluated. Changing the download method of a computer after a job container has been sealed and evaluated will not be honored by the software jobs. Obviously, consecutive job containers will honor the new download method.

The default download method for a computer can also be configured from the agent. The agent command line interface (sd_acmd SetDownloadMethod) provides the means to set the download method in the MDB. After a successful job check and scalability server/domain manager information exchange the new value will appear in the MDB.

Note: The manager will only allow the download method to be set to DTS, if both the Software Delivery and Data Transport Service agent components are registered for that agent in the MDB.

In addition to the command line method, the advanced tab in the DSM software delivery properties dialog of the CAF system tray provides a graphical way of modifying the default download method for a computer. By modifying the row named “Software Delivery: Request a specific Network Operating System”, the default download method MDB update sequence is triggered.

Do not confuse the row named “Software Delivery: Request a specific Network Operating System” with the row “Software Delivery: Network Operating System”. The latter modifies only the local configuration store of the agent with the purpose of forcing the agent to use NOS-less download methods, even if the scalability server provides network shares. Setting it to, for example, MS, does not guarantee the use of shares and it may get overridden by the default download method or the scalability servers capabilities and configuration. The default download method of DTS cannot be overridden by the agent.

Optimizing the Creation of Compressed Job Files

The following configuration policy parameters control the creation of compressed files:

- DSM/software delivery/shared/NOS-less attached
- DSM/software delivery/shared/NOS-less on the fly

NOS-less attached

The 'NOS-less attached' parameter is used by domain manager and scalability server and defines support for NOS-less agents connected to the scalability server or manager.

If set to Yes (which is the default), it forces the creation of a compressed package needed by NOS-less targets.

If set to No, the scalability server or manager attempts to determine the need of this file (used in conjunction with the 'NOS-less on the fly' parameter).

NOS-less on the fly

The 'NOS-less on the fly' parameter defines support for NOS-less agents connected to the manager.

If set to False, no compressed files will be created, if the above 'NOS-less attached' parameter is set to No.

If set to True, and the 'NOS-less attached' parameter is set to No at the same time, you can optimize CPU and disk usage as in this case the compressed file is created only if needed.

Use of Symbolic Links

The software delivery (SD) functionality provides an option to use symbolic links (also known as junction points in Windows NT Technology) on domain managers or scalability servers running Windows NT Technology or Linux. The SD system checks by itself, if it is possible to use symbolic links.

The advantage with using symbolic links is that they are very fast. The SD manager does not have to perform any unnecessary copying of data which consumes both I/O bandwidth and CPU time, and disk space is not wasted.

The restrictions for the use of symbolic links are the following:

- The use of symbolic links only works in versions of Linux that support this feature.
- On Windows NT Technology, the use of symbolic links only works with the file system type NTFS5. No versions of FAT support this option.
- The packages are not allowed to write into the ACTIVATE area folders. Doing so would affect the original source of the packages. If *any* package writes into the ACTIVATE area, this feature has to be disabled by setting the DSM/software delivery/shared/Use symbolic links configuration policy to False.

Note: You must have sufficient authority (user rights) on the computer when trying to use symbolic links, for example, Administrator or Backup Operator.

Exporting a Library Image

You can use the Export Library Image function to export software packages for so-called offline software delivery, using the agent's command line (sd_acmd) to execute container order files (COF). Multiple files can be exported simultaneously by selecting them in the right pane of the DSM Explorer.

If multiple files are selected, the structure at the target directory is as follows:

```
Item 1
:
Item n
library.dct
```

The library.dct file contains the information about the names, versions, and types of the items.

Each exported software item has the same structure as in the Software Package Library.

Note: An installation source associated with external procedures is not exported into the location specified. Only an embedded source will be exported. During execution of external procedures, the absolute paths defined in these procedures will be used by the software delivery agent.

Offline Agent Operation

The software delivery (SD) functionality comprises offline distribution possibilities for Windows and Linux agents that let you install and uninstall software packages for target computers that are offline of the domain manager or scalability server and update the software inventory the next time the target computer comes online.

The offline distribution features can be particularly useful in case of communication breakdown (that is, no connection between agents and the manager) or for Laptops that seldom dock.

Software packages exported from the Software Package Library can be installed and uninstalled using the "Agent Administrative Commands" interface, sd_acmd, which is part of the Windows and Linux agents. A Job Container Order file (COF), containing paths to packages to install or uninstall, is given to the command line interface.

The SD agent service executes the Job Container, and manages necessary log offs and reboots. The execution is either of the type no linkage or in batch form with an option to rollback SXP, PIF, and PKG packages in case of failure.

The job linkage option synchronized is not supported in this context.

You can use a batch file (.bat) to set up execution of more than one COF, with multiple calls to sd_acmd ExecuteContainer. The container files should be executed in the same order as specified in the batch file.

Optionally, you can use sd_acmd WaitContainers after sd_acmd ExecuteContainer calls (in batch files) to wait for all pending or running jobs to finish.

During execution, feedback is given through an output result file and optionally through message dialogs. Information about jobs executed by sd_acmd is stored in a local log file on the target computer for tracking purposes.

The offline software inventory for the SD agent is updated and next time the agent contacts the scalability server the inventory is uploaded.

A template file, template.cof, is present in the CONF directory.

Note: There is a special offline feature where you can place an offline container named Runonce.cof in the %sdroot%\ASM\CONF directory and have it run once before the agent connects to the scalability server.

For details on the three sd_acmd commands that are used in handling COF files, ExecuteContainer, SecureContainer, and WaitContainers, see the *References* guide, which is part of the CA ITCM online documentation set.

Note: You cannot execute unsecured Job Container Order Files. Use the sd_acmd command SecureContainer to secure the COF. If the container is secured with the optional p (password) parameter, the same password must be supplied on the command line when executing the container.

You cannot execute a modified secured job container order file. To resecure a COF, set the entry secured=1 to secured=0, and reenter user account (Library section) and passwords (Library and Container sections) in the COF.

In a Windows NT Technology environment, everyone can secure containers. To be able to successfully execute an SD offline job using sd_acmd ExecuteContainer, sufficient security privileges are needed. By default, only users assigned local or global administrative rights are privileged to run the SD offline jobs.

Optionally, users who are members of the Windows NT Technology local group SDOFFLIN, or global domain group SDOFFLIN, are privileged to run SD offline jobs.

The local group SDOFFLIN is created on all Windows NT Technology computers when installing SD functionality.
Administrators can create the global domain group SDOFFLIN, and add users to these groups, to enable the users to run SD offline jobs.

UNIX has NIS, which acts similarly to domain user validation in Windows NT Technology. The NIS user group for offline jobs is also called SDOFFLIN.

Restrictions

There is no support for $msi macro expansion. Hence, you cannot use job container order files to create MSI administrative installations or network installations based on administrative installations (using the $msi macro). There is no support for added procedures. Only procedures created before the software package was sealed are possible to execute with job container order files.

There is no support for scheduling of containers or for renewing them. Only one Job Container Order File (COF) can be executed at any given time. If an order is placed during the execution of another order, a queuing of the second sd_acmd takes place.

The sd_acmd execution fails with an exit code indicating the error, if Job Check is currently running. On the other hand, Job Check cannot be run while sd_acmd is executing. The software delivery (SD) functionality handles this synchronization lockout internally.

There is no support for Prompt user functionality or for expanding $cl macros to scalability server time; these macros expand to local agent time. There is no support for NOS-less configuration or for NFS protocol connection to the SD manager.

In a Windows NT Technology environment, the COF Executor only supports execution in the System context. This implies the need to provide a user account and password when accessing a network share, which is not a NULL-session share (the account should be one with the necessary access rights to the share).

Specific UNIX Restrictions

LogonShield and reboot logoff are not supported in UNIX environments.

Distributing Orders from the Enterprise Manager

Orders are distributed from the enterprise manager to the domains using a distribution *container*, which is basically a to-do list sent from the enterprise to the domains. A distribution container includes one or more orders. There is no limit to the number of orders that can be included in a single container. Distribution containers can include orders to perform any of the following actions:

- Register an item or item procedure in a domain Software Package Library
- Install or uninstall a program
- Activate or cancel an activation order
- Deregister and remove programs
- Fetch items (files) from the domain
- Register or deregister a software policy on the domain
- Archive (purge) and restore library items

These actions occur in the order in which they are listed in the distribution container. When orders are sent from the enterprise to a domain manager, they are processed automatically at the domain, without intervention by the local administrator, if one exists.

Prerequisite to Setup a Distribution Order

As soon as a domain is linked to an enterprise manager, all its computers and scalability servers are replicated to the enterprise manager.

Before you can distribute a delivery or staging order to a domain manager you will need to create a static or dynamic computer group or a scalability server group, which is automatically replicated to the domains.

Individual computers and computer groups cannot be targeted from the enterprise manager. All targeting must be performed using Computer and User Groups.

Defining Delivery Distribution Orders

To define delivery distribution orders open the Deploy Software Package wizard by right-clicking either the computer group or a software package and follow the steps in the wizard.

Defining Deployment Distribution Orders

Open the Deploy Software Package wizard by right-clicking either the computer group or a software package and follow the steps in the wizard.

It is also possible to drag and drop (and copy/paste) library items onto computer groups. The advantage of using the wizard is that it allows you to specify which domains to distribute the container to and to automatically include registration orders of the software. The drag-and-drop approach only creates a distribution container which has to be sent to the domains in an additional step.

Defining Staging Distribution Orders

Open the Stage Software Package Wizard by right-clicking either the Scalability Server group or a software package and follow the steps in the wizard.

It is also possible to drag and drop (and copy/paste) library items onto scalability server groups. The advantage of using the wizard is that it allows you to specify which domains to distribute the container to and to automatically include registration orders of the software.

Defining Software Policy on Enterprise

When you run the Create Software Policy Wizard on the enterprise manager you can specify domains to where the policy should be distributed. You also have the option to include registration orders of the software packages referred.

Software policies that are created on the enterprise manager and then distributed to the domain can be linked with locally created and managed domain asset groups.

Monitoring Distribution Status

After an installation order has been distributed, you can monitor its progress by checking either status:

- **Job status**—if the order was delivered from a domain manager
- **Distribution status**—if the order was distributed from the enterprise manager

On the enterprise manager, you can find information about a distribution in the DSM Explorer from the Jobs/Software Distributions folder. This folder displays the current status and distribution time of all distributed containers. The distribution status for a particular library item can be viewed in the Software Package Library branch of the DSM Explorer.

Software Policies Settings

Using the Create Software Policy wizard you can define which Software should be installed automatically on members of a computer group.

In the advanced software policy settings dialog you can establish whether the group is to be enabled for automatic evaluation of group conformance. This lets you determine how jobs are executed on those computers that do not fulfill all the conditions of group membership. Jobs can be automatically set up or set up and activated for members that do not conform.

You can set job linkage options to specify if jobs are run independently, or if on failure of one job, the remaining jobs for that target are aborted. Job execution can also be synchronized, meaning that a job is only activated when the previously contained job has completed.

For an alternative template group evaluation mechanism, see Ad Hoc Evaluation (see page 102).

The Evaluation tab on the New Software Policy dialog covers both scheduled and ad hoc evaluation settings.

Scheduled Evaluation

Using the options on the Evaluation tab of the New Software Policy dialog, evaluation schedules can be established. Computer group membership can be evaluated on a specified schedule, or dynamically, meaning that the group is evaluated every time it is used.

You can also use a CA Common Services (CCS) calendar to determine the days, dates, and times during which group membership evaluation is allowed.

For details of an alternative template group evaluation mechanism, see Ad Hoc Evaluation (see page 102).

Ad Hoc Evaluation

When new computers are introduced or existing computers are reimaged, it is important to get them as quickly as possible into the desired state, that jobs are set up for those target computers according to their software policy.

The evaluation mechanism runs not only on a scheduled basis but also at target registration time (called "ad hoc"). Newly registered targets are evaluated when they get registered, without having to consider all other registered targets in the database. Using this approach, the scheduled evaluation frequency can be reduced to avoid the heavy evaluation operations during business hours.

Two general mechanisms exist for introducing new managed computers into CA ITCM: preregistration and regular registration.

Preregistration

Preregistration is performed using any of the CA ITCM user interfaces, for example, the DSM Explorer. Preregistration is also performed by Operating System Installation Management (OSIM) as part of computer reimaging.

Regular registration

Regular registration is performed by the engine during collection from the scalability servers.

The main difference between the two mechanisms is in the collected inventory, or the lack of it in the case of preregistration. This fact has an impact on the results of query evaluation and effectively on computer membership of dynamic computer groups. Software policies are associated with computer groups and may as part of evaluation trigger the evaluation of the associated computer group. The lack of collected inventory for preregistered computers may have an impact on their membership in dynamic groups, and the evaluation of software policies may therefore not target the preregistered computers. To address this, the configuration policy DSM/software delivery/Manager/Delay agent preregistration actions can be used to postpone the evaluation of software policies for preregistered computers until the first regular registration is performed by the engine.

Configuration Aspects

- A configuration policy parameter, DSM/software delivery/Manager/Computer evaluation policy, controls whether the entire ad hoc functionality should be switched on or off for all groups, thus overriding the individual group configurations. By default, the entire ad hoc functionality is switched on.
- When agents are locked by either moving, roaming, or reinstall after crash operations and are scheduled for ad hoc evaluation, the evaluation attempt will be aborted and a new attempt made later. You can control the delay time using the configuration parameter ‘Software policy evaluation: Ad-Hoc task evaluation delay time locked targets’ with a default delay time of 30 minutes for the next evaluation attempt. This parameter lets you better control the evaluation behavior than through the configuration parameter ‘Software policy evaluation: Ad-Hoc task evaluation delay time’, which has a default delay time of 10 minutes.

Target Evaluation

During registration, targets are marked to be scheduled for evaluation. The configuration policy, DSM/software delivery/Manager/Computer evaluation task computer count limit, controls how many targets can be evaluated in one go.

For software policy evaluations observe the following:

- Activation and configuration type jobs may be assigned to rerun every time the scheduled evaluation is performed. This is not enforced during ad hoc evaluation.
- If the check box “Do not regenerate jobs for the members that have earlier failed for this policy” is checked, new job containers for exception members are not set up, if a failed job container exists from a previous activation ordered by the evaluation. If the previous job container has been deleted manually, reevaluation of the template will set up jobs as appropriate.

Relation to Moving Targets and Reinstall After Crash (RAC)

Targets involved in ongoing move or RAC operations are excluded from the ad hoc (and scheduled or unscheduled) evaluation, until the other operations have completed. The reason is, that any moved or RAC records may satisfy the conditions made by the Software Policy.

If some targets are not evaluated due to ongoing move or RAC operations, the evaluation task remains, until the other operations have completed and the targets have been evaluated.

Rerunning Installation Procedures Using Software Policies

Through job templates defined in software policies, you can specify "Remove existing installation records and rerun the selected procedure" that, on Policy evaluation removes existing installation records and reruns the installation procedure regardless of whether the software is already recorded as being installed.

For example, if software has been uninstalled manually without using the software catalog, this change is not reflected in the Software Delivery job history in the MDB. With this feature you can rerun the installation procedure even if the Software Delivery job history indicates that the software is already installed.

Important! Use this feature with great care. If set up wrongly, jobs may be scheduled to run each time the software policy is evaluated, potentially causing an undesired load on the infrastructure! Also, the software policy reruns the specified procedure not taking into account whether that procedure is suitable for rerunning or not. The decision if the use of the rerun feature with any particular installation procedure is appropriate is left to the user!

Delivering Virtual Applications

After a virtual application software package has been registered in the Software Package Library on the enterprise or domain manager, you can distribute it to other networked computers using the standard software delivery methods. However, there are some requirements and processes that are unique to virtual application package delivery. The following sections provide details about these requirements and processes:

- How Virtual Application Deployment Works
- Preparing a Target Computer for Deployment of a Microsoft App-V Virtual Application Package
- Preparing a Target Computer for Deployment of a VMware ThinApp Virtual Application Package
- Deploy a Virtual Application Software Package
- Deploy a Virtual Application Software Package Update
- Roaming and Virtual Application Deployment
- How Roaming Works with Virtual Applications

How Virtual Application Deployment Works

After the virtual application package that you created with the Virtual Application Package Registration Wizard is included in the Software Package Library, you can then deploy it and manage it using standard software delivery methods. You can deploy virtual applications to systems (or groups of systems), make the applications available in the Software Delivery Catalog, include them in policies, and perform other standard software delivery activities.

Virtual application packages can be registered on the enterprise (EP) management tier or the domain management tier. A virtual application package should not be registered on both the EP and domain management tiers. If you register a virtual application package on the EP management tier, it can then be distributed to the domain management tiers and lower levels. From the domain manager, the packages can be distributed to agents and scalability servers. With virtual applications that are streamed, the scalability servers also function as streaming servers.

Virtual application package deployment goes through the following general stages:

1. The administrator verifies that the vendor infrastructure software for the virtual applications is installed on the target computers.

   Note: You may need to reboot the target server after installing the Microsoft System Center Application Virtualization Streaming Server. The Streaming Server set-up process initiates this reboot.

2. The administrator creates software jobs to deploy the virtual application packages to target computers (after virtual application packaging and registering have been completed). The administrator can create software jobs for virtual application packages using the same methods used to create software jobs for regular application packages.

3. The administrator deploys the virtual application Staging package to the scalability server. The scalability server also functions as the streaming server. Therefore, Staging packages are deployed to the scalability server for streaming of the virtual application to the target computers.

   Note: If the target computer roams to a new scalability server, the new server must have the Staging package installed as well. For more information on roaming, see the description of Roaming and Virtual Application Deployment (see page 111).

4. The administrator deploys the Standalone and Streaming packages from the domain manager to the target computers. The administrator can also stage packages on the scalability server before deployment to target computers. The administrator can use standard software delivery deployment methods to deploy virtual application packages to target computers.

Preparing a Target Computer for Deployment of a Microsoft App-V Virtual Application

Before you can deploy a Microsoft App-V virtual application package to a target computer, you need to verify that the target computer is ready for the virtual application. The following description explains the preparation of the target computers.

Dependencies—For virtual application packages created from a Microsoft App-V image, certain dependencies are required. The following table identifies these dependencies based on the type of virtual application package you want to deploy.

Package Type	Dependencies
Server Staging	Microsoft System Center Application Virtualization Streaming Server
Client Standalone or Streaming	Microsoft Application Virtualization Desktop Client Microsoft SML Parser 6.0 Microsoft Visual C++ 2005 SP1

Package Type	Dependencies
Client Standalone or Streaming for Remote Desktop Services	Microsoft Application Virtualization Desktop Client Microsoft SML Parser 6.0 Microsoft Visual C++ 2005 SP1

The infrastructure components must be available on the target servers and clients in order for the virtual application to work. You can use your own local procedures to make these components available on the target computers, or you can use CA ITCM to create software delivery packages for the infrastructure components of Microsoft App-V. (Microsoft provides these components as MSI-based installation images.) These infrastructure packages can then be imported into the Software Package Library using existing software delivery methods.

Note: You can create the infrastructure packages on your own, or you can use the software delivery infrastructure package templates (included on your DVD kit). For more information on the infrastructure package templates, see the description in Virtual Application Infrastructure Package Templates (see page 56).

Server configuration for streaming communications—For virtual applications that are streamed to target computers, the target computer must recognize the name of the streaming server. The DSM scalability server acts as the App-V streaming server. Therefore, the App-V streaming server must be installed on the DSM scalability server.

The Microsoft App-V streaming server uses two protocols for streaming communications: RTSP (not secured) and RTSPS (secured). The default protocol and port for the Microsoft App-V streaming server are RTSP and port 554. If you want to use the secured RTSPS protocol with port 322, you must configure the streaming server. If you are using the CA-provided infrastructure package templates, you must configure the streaming server before including it in the template. For information about configuring the Microsoft App-V streaming server, see the Microsoft product documentation.

Client configuration for streaming communications—The default protocol and port for the Microsoft App-V client are RTSP (not secured) and port 554. If you want to use the secured RTSPS protocol with port 322 (for example, to match the streaming server configuration), you can set the Deploy Virtual Applications Policy Group accordingly and apply it to the agents. (See the DSM Explorer online help for more information on the Deploy Virtual Applications Policy Group.) Then, if a new Microsoft App-V virtual application package is registered and deployed with the default protocol and port, the agent replaces the default settings with the protocol and port specified in the policy. For an existing application installation on the target computer, you must deploy the Streaming package again using the procedure "reinstall", which is part of the Streaming package. This procedure uses the new protocol and port when the user launches the application. Also, the shortcuts on the target computer are updated the next time the user logs onto the computer.

Notes:

You can deploy virtual application packages on target scalability servers and target computers running the Windows operating system, but not UNIX or Linux operating systems.

The Microsoft App-V sequencer does not support Windows 2000. Thus, Windows 2000 cannot be supported as a client for running App-V virtual applications.

Microsoft Application Virtualization Desktop Client Version 4.51 does not support 64-bit Windows operating systems. Thus, computers with 64-bit Windows cannot be supported for running App-V virtual applications (Standalone and Streaming packages).

Authorization—The end user on the target computer needs authorization to access a virtual application, which is located on a network drive on the scalability server. Authorization can be achieved by a trusted connection between the target computer and the server. If a trusted connection does not exist, the end user will be prompted for a user name and password.

Preparing a Target Computer for Deployment of a VMware ThinApp Virtual Application

Before you can deploy a VMware ThinApp virtual application package to a target computer, you need to verify that the target computer is ready for the virtual application. The following sections explain the preparation of the target computers.

Dependencies—For virtual application packages created from a VMware ThinApp image, certain dependencies are required. The following table identifies these dependencies based on the type of virtual application package you want to deploy.

Package Type	Dependencies
Server Staging	No dependencies
Client Standalone or Client Streaming	ThinReg.exe utility

ThinApp virtual application Staging packages for the server do not need any prerequisites. However, the Standalone and Streaming packages that deploy ThinApp packages to target computers call the ThinReg.exe utility. This program provides the end user with easy access to the virtual application.

Important! The ThinReg.exe utility must be found in the PATH environment on the target computer. If it is not, the deployment of the virtual application package on the target computer will fail.

You can use your own local procedures to make the ThinReg.exe utility available on the target computers, or you can use CA ITCM to create a software delivery package for the ThinReg.exe utility. This infrastructure package can then be imported into the Software Package Library using existing methods for importing packages. For more information on creating infrastructure packages, see the description in Virtual Application Infrastructure Package Templates (see page 56).

Note: You can deploy virtual application packages on target scalability servers and target computers running the Windows operating system, but not UNIX or Linux operating systems.

Authorization—The end user on the target computer needs authorization to access a virtual application, which is located on a network drive on the scalability server. Authorization can be achieved by a trusted connection between the target computer and the server. If a trusted connection does not exist, the end user will be prompted for a user name and password.

Detection of ThinApp Packages in Non-Domain Environments

The detection of streaming ThinApp packages is intermittent in a non-domain environment. Unless the per-user scan is run at a time that a user is authenticated with the server share, the scan cannot detect the contents of the share.

Typically, the scan runs immediately after logon (in which case it is quite likely the user has not been authenticated with the scalability server yet), and also whenever the full signature scan is run, which may occur only infrequently and may not occur when the user is logged on.

Therefore, CA strongly recommends using Domain/Active Directory environments for streaming ThinApp applications and deploying ThinApp virtual application packages.

Deploy a Virtual Application Software Package

You can use the following overall procedure, along with the standard software delivery deployment methods, to deploy a virtual application package.

To deploy a virtual application software package

1. Verify that the target servers and clients are ready for deployment of virtual applications.

   Notes:

   Vendor infrastructure software must be installed on the target servers and clients. You can complete this step using your own local procedures or you can use the infrastructure package templates provided with CA ITCM. See the following descriptions for more information: Preparing a Target Computer for Deployment of a Microsoft App-V Virtual Application and Preparing a Target Computer for Deployment of a VMware ThinApp Virtual Application.

   You may need to reboot the target server after installing the Microsoft System Center Application Virtualization Streaming Server. The Streaming Server set-up process initiates this reboot.

2. Verify that there are three software packages – Staging (SG), Standalone (SA), and Streaming (SM) – in the Software Package Library for the virtual application that you want to deploy.

3. Deploy the Staging package to all required scalability servers (servers connected to target computers where a streamed virtual application is deployed).

   You should deploy any infrastructure packages first.

   Note: After you install a Microsoft App-V Staging package on a scalability server, there may be a delay (possibly up to 30 minutes) before the package becomes available for use. If the end user launches an App-V Streaming virtual application before the Staging package is available, an error message appears.

4. Deploy a Standalone or a Streaming package to each target computer.

   You should deploy any infrastructure packages first.

   The virtual application software packages are installed.

Notes:

When you uninstall a Standalone virtual application, uninstall the SA package first from the target computer and then uninstall the SG package. For a Streaming virtual application, uninstall the SM package on the client first and then uninstall the SG package on the server.

The end user on the target computer should not start a Microsoft App-V virtual application by double-clicking on the .osd file. If the user does so, the communications with the streaming server may not function properly. The user should start the application by using the desktop shortcut or the Start menu.

Deploy a Virtual Application Software Package Update

You can use the following overall procedure, along with the standard software delivery deployment methods, to deploy a virtual application package update.

To deploy a virtual application software package update

1. Verify that the target servers and clients are ready for deployment of virtual applications.

   Notes:

   Vendor infrastructure software must be installed on the target servers and clients. You can complete this step using your own local procedures or you can use the infrastructure package templates provided with CA ITCM. See the following descriptions for more information: Preparing a Target Computer for Deployment of a Microsoft App-V Virtual Application and Preparing a Target Computer for Deployment of a VMware ThinApp Virtual Application.

   You may need to reboot the target server after installing the Microsoft System Center Application Virtualization Streaming Server. The Streaming Server set-up process initiates this reboot.

2. Verify that there are two software packages – Staging (SG) and Standalone (SA) – in the Software Package Library for the virtual application update that you want to deploy.

   Note: Staging and Standalone packages only are needed for virtual application updates. The Streaming package contains only links to the Staging package and the virtual application. These links do not need to be updated.

3. Deploy the Staging package to all required scalability servers (servers connected to target computers where a streamed virtual application is deployed).

4. Deploy the Standalone package to each target computer where it is required.

   The virtual application software package updates are installed.

Roaming and Virtual Application Deployment

A target computer is said to be roaming when it moves from one location to another within the enterprise network. As a result of the move, the target computer may need to connect to a new scalability server. This move may happen because the user is working in a new office, and the user's computer needs to connect to the local scalability server instead of the original scalability server. Also, if there are organizational changes in the enterprise that affect the structure of the network, some target computers may be assigned to different scalability servers.

For target computers that run virtual applications in streaming mode, the scalability server also functions as the streaming server. With streamed virtual applications, the applications must be staged on the scalability server connected to the target computer in order for the applications to run on the target computer. Thus, if a target computer moves to a new location and a new scalability server, the new scalability server may also become the new streaming server. The Staging packages for all virtual applications that are streamed to the target computer must be installed on the new scalability server before the new server can function as a streaming server. See the description of Virtual Application Packages (see page 53) for more information on the types of virtual application packages.

To avoid problems with running streamed virtual applications on a roaming target computer, the CA ITCM agent on the target computer performs some checks before changing the computer's streaming server. These checks do not affect the switch to the new scalability server. The target computer does roam to the new scalability server. The checks determine whether the new scalability server also functions as the streaming server. If the result of the checks is successful, the streaming server is changed to the new scalability server. If the result of the checks is not successful, the original scalability server continues to function as the streaming server. See the description of How Roaming Works with Virtual Applications for more information.

Notes:

- Roaming does not affect the deployment of Standalone virtual application packages or the preparation of scalability servers for streaming mode operation.
- You can turn roaming off by setting common configuration policy parameters. If you do so, the original scalability server is always kept as the streaming server. See the *DSM Explorer Help* for more information about configuration policies and the Deploy Virtual Applications policy group in particular.

How Roaming Works with Virtual Applications

Virtual applications that are streamed to a target computer need to have their corresponding Staging packages installed on the scalability (streaming) server connected to the target computer. If a target computer roams (moves) to a new location and a new scalability server, the Staging packages for all streamed virtual applications must be installed on the new scalability server before the applications can run on the target computer.

To avoid problems with running streamed virtual applications on roaming computers, the CA ITCM agent on the target computer performs some checks before changing the computer's streaming server. These checks do not affect the switch to the new scalability server. The target computer does roam to the new scalability server. The checks determine whether the new scalability server also functions as the streaming server. If the result of the checks is successful, the streaming server is changed to the new scalability server. If the result of the checks is not successful, the original scalability server continues to function as the streaming server.

Different checks and procedures are performed depending on the technology that was used to create the virtual applications. In the case of VMware ThinApp, for example, the check for roaming is carried out with the user login. These checks are run each time the user logs into the target computer.

Note: For Microsoft App-V virtual applications streamed to roaming computers, the switch to the new streaming server needs to be performed by reinstalling the streamed virtual application packages on the target computer.

The following sections describe the process of checking a new scalability server for VMware ThinApp and Microsoft App-V virtual applications.

VMware ThinApp

1. CA ITCM checks if the scalability server has changed when the user logs into the target computer.
2. CA ITCM connects to the new scalability server if it has changed.
3. CA ITCM searches the new scalability server for the Staging package that corresponds to each virtual application that is deployed on the target computer.
    a. CA ITCM uses the new scalability server as a streaming server for all applications that have corresponding Staging packages on the new server.
    b. CA ITCM uses the original scalability server as a streaming server for all applications that do not have corresponding Staging packages on the new server.

Microsoft App-V

In the case of roaming, the switch to the new streaming server needs to be performed by reinstalling the streamed virtual application packages on the target computer.

No further checks are performed for Microsoft App-V, since the technology does not currently permit them.

Note: As a best practice, deploy the Staging package for each virtual application on all scalability servers (running the Windows operating system) in your network.

1. CA ITCM allows adoption to a new scalability server in case it has changed.
2. CA ITCM connects to the new scalability server if it has changed.
3. CA ITCM uses the new scalability server as a streaming server for all virtual applications that are deployed on the target computer.

Software Catalog

The Software Catalog is an easy-to-use software delivery tool that lets you manage software on your computer from a library provided by the administrator.

The administrator creates packages of software products that are licensed within the company and places them in the Software Catalog library. You can place an order for this package using the Software Catalog. The software is delivered to your computer, installed, and made ready to use with little or no additional input.

The Software Catalog lets you perform the following tasks:

- Add software
- Customize software
- Remove software
- Check the status of the software order

Important! The Software Catalog is available only for Windows operating environments and requires the software delivery agent plug-in.

Accessing and Viewing the Software Catalog

The administrator can fill the catalog folder in the Software Package Library with registered software from the other folders. Normally this software is for the use of all desktop users.

The administrator can restrict software to special computers or users by using the context menu option Software Jobs, Publish software in Catalog for computer or user groups and select dedicated software in the wizard dialog.

The administrator can also copy and paste Computer, User or Software Groups to the Catalog folder and configure them or register software directly into it.

Note: Software is only visible in the Software Catalog at client side, if it contains at least one Catalog-enabled installation procedure.

Configuring the Software Catalog for the Desktop User

The administrator is responsible for distributing the Software Catalog to a number of agents and needs to set up a library of software and make it available in the Software Catalog.

If the agent is configured to register User Profiles, the Software Catalog offers the user to install software for their own personal usage. A typical scenario for this feature is when a computer is shared among several users.

Disable Job Check

The Job Check icon in the Software Order Status screen enables the desktop user to initiate a software delivery process, if the software package has been staged and is ready to be delivered. This always happens automatically, but not necessarily immediately.

The administrator can disable the Job Check icon by setting the DSM/software delivery/Agent/HideJobCheckIcons parameter in the configuration store (comstore). If this paremeter is set, the Job Check icon does not appear in the Software Order Status screen. For the change to take effect, you must restart the Software Catalog.

Specify the Type of Installation

Most software packages can typically be installed in only one way; however, depending on the company, the administrator may decide to package the same software program in a number of different ways. For example, the marketing department wants a word processor with a lot of extra clipart and fonts, whereas the accounting department only wants the bare bones installation. These types of installations are left at the discretion of the administrator.

The administrator may have a default type of installation, and this can be specified when registering the software package using software delivery functions. If there is a default type, the user can choose the default type of installation in the Select Type of Installation step or must explicitly select another type of installation.

User Parameters and the Software Catalog

You cannot enable procedures that use the $up macro for use from the Software Catalog. This is because the Software Catalog dialogs provide no means for the desktop user to enter a user parameter.

Installation of the Software Catalog

Currently, there is one kind of installation, the default installation. If you perform the express agent installation, the Catalog is selected by default.

Performing a custom installation and selecting Software Delivery as functionality and Agent as feature, you can use the Software Delivery button in the Configure Agent screen. The default selection is Install Software Catalog.

The Software Catalog can be installed additionally to a software delivery agent through the Software Package Library. In the DSM Explorer, open the package CA DSM Agent + Software Delivery Plug-in in the Software Package Library and drag and drop the procedure 'Catalog: Add' onto the target computer.

Note: To use the Software Catalog, Microsoft Internet Explorer 6.0 or newer is required.

Adding Software from the Software Catalog

Using the Add Software wizard you can order software to be delivered to your computer or, if the User Agent is enabled on your computer, personal account (user profile).

The Add Software task consists of the following steps:

- **Choose Software to Order**

  Select one software package to install on your computer or account. Only software is listed that you are allowed to install from the Catalog library.

- **Select Type of Installation**

  Most software packages can typically be installed in only one way; however, the administrator may have decided to provide different ways to install the software package you are ordering.

- **Confirm Order**

  The software package and installation type you selected are listed and you can confirm the order with Order Now. Optionally, you can specify to be notified before the delivery starts.

  Note: If you choose a software package that has already been installed on the local computer using the chosen installation type (item procedure), you will be notified. If you proceed with the order, the software will be reinstalled as opposed to installed, which is useful if your computer has been reinstalled with a fresh copy of the operating system, but the software delivery function still has its old installation records.

Finally, an acknowledgement dialog confirms that your order is in progress and lets you select to monitor the order status.

For detailed information on each of the steps, see the Software Catalog online help.

Maintaining Computers

This section provides information about:

- Moving computers between domain managers in different domains or in the same domain (roaming) (see page 117)
- Reinstall After Crash (RAC) (see page 125)

Moving Computers

CA ITCM supports movement of agents or the targets of an agent, such as user profiles, user accounts, and docking devices, and their job history between domain managers. This functionality has become crucial with increasingly mobile environments. Computers are relocated between offices that belong to different domains and are managed by different domain managers. Often the computers are not reinstalled between the moves, and the history (for example, the records of the installation, activation and configuration jobs) of the computer residing on the previous domain manager is still valid.

The move function primarily focuses on permanent moves between domain managers rather than frequent roams of mobile workers, when they stay with the management by the same domain manager.

Moving Computers Between Domains

This section provides information about the following features for moving computers between domains:

- Permanent Move and Prerequisites
- Scope of the Move Operation
- Permanent Move Operation
- Role of the Scalability Servers
- Connecting for the Move and Moving Target Records
- Moving Scalability Server Records
- Moving and Reinstalling After Crash
- Status of Move Operation in DSM Explorer Interface
- Canceling a Move Operation
- Restrictions of Move Functionality
- MSI Support for Moving or Roaming Targets

Permanent Move and Prerequisites

A permanent move means that:

- The new domain manager manages the agent and all targets (that is, user profiles and user accounts) handled by the agent.
- Any successful job records for installed software stored on the previous domain manager are imported to the new domain manager.
- The agent and its targets are deleted from the previous domain manager, as they no longer are managed by it.

Prerequisites for a successful move operation are:

- All domain managers between which moves are to be supported must have a communications link between them, because communication failures will cause the registration of new agents to report a previous domain manager to fail (these agents will stay locked by the move operation until they become obsolete).
- All managers' UTC times (Coordinated Universal Time) should be synchronized in order for the record age comparison to work as designed. Different time zones have been considered. If the manager UTC times are not synchronized, the age of the records cannot be correctly determined. This will lead to unexpected moves.
- All software delivery components should have the same version. Contact CA Technologies Technical Support for technical assistance and instructions for older software delivery agent versions.

Scope of the Move Operation

A move operation includes the movement of all (successful) installation records and corresponding successful activation and configuration records. The installation history of successfully uninstalled software is not moved, and failed activation or configuration records are not moved, because they are not relevant to describe the current status of an agent. The move operation moves only the currently logged in user profile. This ensures that inactive users are not stored in the MDB forever. If the computer has multiple user profiles, you can move the required profiles by logging into each user account that you want to move.

Note: A move can be seen as a rather resource consuming operation, including connecting to the previous domain manager, enumerating all job records, and updating the job history for the target. In the case of a massive move operation covering at least many hundreds of computers, we recommend that multiple targets be moved from the same previous domain manager at the same time, because one connection can be shared for all the moves.

When the agent is reconfigured, it is imperative that the installation records for the agent are moved from the previous to the new domain manager for continued successful management of that particular agent.

A scalability server is not directly involved in permanent moves between domain managers. However, the moving agent can connect to the domain manager through a scalability server, and the scalability server itself can move to a new domain manager.

If a scalability server is moved, every delivery record is also moved. Even though the scalability server objects themselves are moved with their corresponding installation, activation, configuration, and delivery records, the targets connecting through that scalability server are moved on the next successful connection. This means that there can be a considerable time delay between the move of the scalability server and the targets connecting through that scalability server.

A move operation is a transaction. This means, that any failures during a move, like software exceptions or communication errors, will rollback the move operation. A new attempt will be made the next time the computer move operation is run.

For More information about agents and scalability servers move operations, refer to ITCM Implementation Guide.

Permanent Move Operation

It is important that the UTC times of all managers and scalability servers, which are involved in a move operation, are synchronized in order for record age comparison to work. Consideration has been taken to different time zones.

It is assumed that software on the computer being moved is left intact during the move. If any software is manually removed or added during the move, it is imperative that any changes are also recorded at the new domain manager, which now manages the computer, for example, by manually deleting install records for software, which was manually removed.

Every time an software delivery (SD) agent connects to a manager or scalability server, a message is passed to the agent. The message contains information about the address of the domain manager managing the agent and the current scalability server's UTC time. The agent stores the domain manager address locally. When the agent detects a change in the domain manager address between two consecutive connections, the previous domain manager address is remembered for each of the targets handled by the SD agent (for example the user profiles)

The previous domain manager address is passed up the SD infrastructure to the new domain manager, which attempts to perform the move operation.

This activity is repeated for each of the targets handled by the agent and every time the agent moves to a new domain manager.

The agent is using the passed scalability server UTC time in calculating its reference counter, which is a sort of timestamp of every connection. The reference counter is passed up the infrastructure to the domain manager. It is used to determine which of two compared target records are more recent during a move operation.

Since the SD manager time cannot always be trusted, the SD agent performs a sanity check by comparing it with its previous reference counter. If the current scalability server UTC time indicates that the previous reference counter should be increased, the UTC time is used to calculate the new reference counter.

However, if the current manager UTC time indicates that the reference counter should be decreased, the SD agent discards this UTC time, and just increments the previous reference counter to ensure that a greater value is used for each connection to the scalability server.

For newly installed SD agents, the reference counter is always initialized using the current scalability server UTC time.

Role of the Scalability Servers

A scalability server is responsible for passing the previous domain manager address on behalf of the target to the domain manager. If a target is removed from the domain manager due to a move or remove operation, it will be removed from the scalability server as well.

If a scalability server is moved from one domain manager to another domain manager, make sure that the agents of this scalability server register with the new manager before moving one of the agents; otherwise, the move of the agent will fail. You can register the agents manually using the command, caf register, or wait until the agents automatically register with the new domain manager according to the schedule.

Connecting for the Move and Moving Target Records

On a successful connection between the two domain managers, the previous domain manager is queried for the existence of a record of the currently processed target (for example, the user account and user profile), as follows:

- If the previous domain manager does not hold a record for the target, the move is ignored.
- If the previous domain manager holds a record for the target, a comparison of the reference counters of the two target records is performed. If the previous domain manager stores a newer reference counter, the move is aborted. Otherwise, the move operation continues.
- The attributes of the target on the previous domain manager are not moved, since the ones that were currently reported are assumed to be more up to date.
- If the target record on the previous domain manager is locked by a move operation, a check is made to find out if the two domain managers are waiting to move records between each other. If this is the case, the target with the highest (that is, latest) reference counter is assumed to be valid and the move operation continues, if the current domain manager holds the record. If the move operation on the previous domain manager is waiting to move records from a third domain manager, the move operation is postponed until the other move is completed.

Next, the previous domain manager is inquired for its current time. The returned time is compared with the time of the current domain manager, and the time deviation (time zone) is determined. For every installation record associated with the target on the previous domain manager, a new record is created on the current domain manager, maintaining its completion date and time by applying the calculated time deviation. Any successful activation and configuration records associated with a moved installation record are also moved. Software items not registered in the current domain manager's Software Package Library are marked as detected. The output file is not moved due to performance reasons.

After a successful move of all the records, the target record on the previous domain manager is deleted together with all associated installation, activation, configuration, and un-installation records.

After a move has been successfully performed and completed, the target is unlocked.

Note: The move operation is a transaction. If an error occurs during the move, the whole operation is rolled back to be reattempted the next time the computer move operation is run.

Moving Scalability Server Records

If the target being moved is a scalability server, it will follow the same logic as for regular targets, with one addition: any successful scalability server delivery records are moved as well.

If the delivery records are associated with software not registered in the new domain manager's Software Package Library, they will be ignored. However, registering the software in the new domain manager's Software Package Library and then running the scalability server synchronization procedure can recreate them.

Moving targets connecting through a moved scalability server is not part of the scalability server move operation. All targets connecting through the moved scalability server will eventually register to the new domain manager through the scalability server, and move from the previous domain manager using the conventional auto registration and move mechanisms.

Scalability Server and Agent Move Operation

If a scalability server is moved from one domain manager to another domain manager, make sure that the agents of this scalability server register with the new manager before moving one of the agents; otherwise, the move of the agent will fail.

Also, if you move a scalability server from one domain manager to another domain manager, make sure that the agents of this scalability server register with the new manager before using of the Software Catalog on individual agents connected to that scalability server; otherwise, using the catalog will fail.

You can register the agents manually using the "caf register" command or wait until the agents automatically register with the new domain manager according to the schedule.

Moving and Reinstalling After Crash

If a target is moving and the new domain manager detects the occurrence of a reinstall after crash (RAC), the move operation will take precedence over the reinstall functionality. After a successful move, the RAC operation is invoked to reinstall all moved job records.

Reinstall after crash is initiated if the UUID (Universal Unique Identifier) changes after the target has registered to the new domain manager, but before the move operation is completed.

Note: If the target is reinstalled during the physical move (that is, before the move operation has been initiated), no move of job records will occur, because the software delivery (SD) agent holds the previous domain manager address, and this information is lost after a reinstall of the agent or operating system.

If a target has moved to a new domain manager, and RAC is detected for the target on the previous domain manager, the move operation will be postponed until the remote RAC has completed.

For example, the SD agent was connected to a scalability server downstream of the previous domain manager before it moved to the current domain manager. The target has executed all RAC jobs, but the scalability server has still not reported the RAC results to its domain manager. When the scalability server has reported the RAC results to its domain manager, the move of records between the two domain managers takes place.

Status of Move Operation in DSM Explorer Interface

The DSM Explorer GUI shows the progress of the move operations. The Status column shows the status of the Move operation, for example, choose All Computers and have a look at the right-hand pane.

Canceling a Move Operation

A move may be impossible, for example, if the previous domain manager has been lost because of a hardware crash. After the software delivery agents have been reconfigured to connect to a new domain manager, the name of the previous domain manager is still reported to the new one, and a move is scheduled. To handle these scenarios, you can select one or more targets, right-click, and select Abort move operation, which leads to loss of the job history for the affected targets.

Restrictions of Move Functionality

Moves between different versions of domain managers may be not supported, if great changes in the API protocol have been incorporated between two versions of the software delivery functionality. Also, moves from legacy Unicenter Software Delivery 4.0 Local Servers are not supported.

No job output files are moved due to performance considerations.

The move of computers is supported for automatically registering target computers.

Target computers registered manually, using the DSM Explorer, do not support a move from a previous domain manager at registration time with the current domain manager

The move operation handles upgrades, but if the agent system is reimaged between the moves, no automatic move operation can be performed, since all information about the previous domain manager is lost with the new operating system image. The same applies, if the agent is uninstalled and later reinstalled.

The move functionality is not intended for frequently roaming agents, but rather solves the problem of infrequent permanent moves of agents between different domain managers. Therefore, it will not scale in a scenario of hundreds or thousands of roaming agents every day.

The move functionality does not include automatic move of target computers between Boot Servers.

MSI Support for Moving or Roaming Targets

When a computer roams or moves, MSI-based applications may lose the network install image location. Access to this install image is crucial for “advertised” products and products using "self healing" and "install on demand."

An MSI based product contains a SOURCELIST in the Registry where multiple source paths may be specified. This source list is updated whenever a roam or move is detected, and an installed product is found in MSILIB on the new scalability server. The update is controlled by the software delivery agent policy "MSI source update".

Moving Computers in the Same Domain (Roaming)

CA ITCM supports the movement of software delivery agents between scalability servers connecting to the same domain manager.

All records of the software delivery agent are destroyed on the previous scalability server after any outstanding job results have been collected. Jobs that are active during the roam will be allowed to continue their execution through the new scalability server.

Since the targets do not change the domain manager in these scenarios, there is no need for movement of job history.

Roaming Jobs

A job is considered roaming as soon as the job has been ordered to scalability server A, and the software delivery (SD) agent registers through scalability server B.

The SD agent roams from scalability server A to scalability server B. The SD agent is automatically registered with scalability server A. A number of jobs have been set up to the agent and are staged in the file database on scalability server A. Then the agent is registered through scalability server B.

When scalability server B reports its new agent to its domain manager, the domain manager triggers the scalability server A. Scalability server A reports the job results for the agent, and the domain manager realizes that this agent has roamed to scalability server B. All jobs that have not yet executed are reset and scalability server B is triggered. Scalability server B picks up the reset jobs.

Additionally, to guarantee that a batch is not broken, the name of the manager that received the jobs, is internally handled by software delivery functions. In the previously shown scenario, the new SD manager will not pick up any job, unless the results have been reported from the old manager, or the jobs have been removed by the administrator, or timed out. During this time new jobs will not be allowed to be setup to the roaming agent.

Reinstall After Crash

The software delivery (SD) functionality can restore the state of computers by automatically invoking the reinstall after crash (RAC) feature. This happens when the SD agent reports a new operating system installation. All software that was present earlier will be reinstalled and configured according to the computer's job history stored in the database. During RAC the computer is locked and no other jobs can be initiated.

Generic RAC is accomplished by creating a job container based on the current job history for a target computer. In its nature, it is very similar to creating a job container from a template.

Generic RAC is a function that can be used for all package types (for example, SD, SXP, and MSI items), and is available for operating environments that support the UUID mechanism, that is, all Linux/UNIX and all Windows 32-bit and 64-bit operating environments. Generic RAC can be used to configure and activate procedures.

Note: Software versions that are no longer used but still registered can be excluded from RAC by checking the Exclude from RAC option on the installation procedure.

RAC Configuration

How the domain manager handles RAC depends on the value of the RAC Policy and RAC Automation parameters in the configuration store (comstore).

You can set the RAC Automation parameter through the Control Panel in the DSM Explorer, by invoking the Reinstall After Crash dialog in the Configuration\Software Job Management subfolder.

If the RAC Policy is selected, when a new operating system has been installed, the software delivery (SD) agent notifies the domain manager. The domain manager sets the state of the computer to Reinstall After Crash and locks the computer. All installation records in the Jobs folder for the SD agent are marked as uninstalled.

The domain manager does one of the following:

- Takes no further action, except unlocking the computer again (disabled RAC automation).
- Creates an RAC job container for the SD agent, fills the container with orders to execute all previously successfully executed jobs and leaves the container unsealed (deferred RAC automation). The container can be reviewed and modified, since it has to be activated manually.
- Creates an RAC job container for the SD agent, fills it with orders to execute all jobs that were previously successfully executed, seals and activates the job container (automatic RAC automation).

If a Windows 2000, Windows XP, or Windows 2003 computer has user profile agents, the computer profile and each user profile agent will be handled separately. Each SD agent will have its installation records deleted separately and get its own job container, if any are to be generated.

Procedure Option Exclude From RAC

If you do not want an item procedure to execute as part of the Reinstall After Crash (RAC) process, you can set the Exclude from RAC option for that procedure. The purpose of this option is to automatically exclude certain procedures from a RAC container. You find more information on the Exclude from RAC option in the section "Exclude Item Procedures from Reinstall After Crash (RAC)" (see page 72).

Configure Individual RAC Policies for Computers

You can define an individual Reinstall After Crash (RAC) setting for a computer. This individual setting overrides the RAC policy that is defined on the domain manager the computer connects to.

To define an individual RAC setting for a computer

1. Right-click the computer in the tree view of the DSM Explorer on the manager.

   The context menu appears.

2. Select Properties in the context menu.

   The Properties dialog appears.

3. Select the Software Delivery tab, and change the value in the RAC Policy entry field.

   The default value is Common, which means that the common policy for the domain manager is used.

Note: If the Common RAC Policy is set to Disabled, individual RAC settings for computers have no effect.

RAC Job Container

When a target computer reports that it has had a new operating system (OS) installation (visible by a change in the HostUUID), all old successful installation and delivery records will be marked with "*Removed by RAC" in the job history of the target computer.

Note: If the configuration policy "DSM/software delivery/Manager/RAC" is set to False, existing records remain untouched and no RAC job container is created.

Then, depending on the current RAC policy configuration setting, a job container will automatically be created or not by a domain manager. All old successful jobs associated with the installation and delivery records previously mentioned are included in the container that will appear in the list of job containers, with its name prefixed by RAC. The name of the job container follows the scheme:

RAC: *computer_name* [*current_date current_time*]

All RAC containers are tagged with the UUID of the actual computer at the time it got the new OS installation. This ensures that only RAC containers with an up-to-date UUID will be performed. Jobs in an RAC container with an old UUID will fail and set in error state: RAC container obsolete. This situation may occur if the software delivery agent is reinstalled with a new operating system, before a previously generated RAC container has finished executing.

New installations and jobs, generated off-line and reported along with the new OS installation (that is, using the new UUID), are not included in the RAC container. Old and new installations for targets are separated, by recording the UUID for each job. All job records generated off-line are tagged with the UUID.

The restriction in previous software delivery versions to prohibit execution of activate and configure procedures, unless bound to an existing installation for the current target, has been weakened to let an RAC container carry out all jobs, based on the job history of the job target, in one attempt.

To regenerate as much as possible of the target, the default values used for an RAC job container are:

- Batch linkage
- Enable transaction is not set
- Ignore cascading install of dependent packages is not set

Note: Batch linkage can be changed to synchronized for an unsealed job container.

When creating the RAC container, the completion time of the computer jobs (job history) is used to establish the initial order of the jobs. Deliveries are always placed first. As long as the job container is unsealed, jobs can be deleted or repositioned. More jobs can also be added to the container.

If a job cannot be set up, since the software to use is archived, the job is set in warning state and the job container is left unsealed.

Jobs that had not finished executing before RAC was initiated are set in error state. They are not included in the RAC container and cannot be renewed, since they are tagged with the old UUID. After the RAC process has finished, check whether they should be set up again.

When a RAC job container has been created for a target, the target is locked until the container has completed successfully, or has been deleted. While the target is locked, the computer name is displayed in red text in the DSM Explorer tree.

During this time, it is not possible to deliver, execute, or delete any other jobs to the target computer. Any jobs that are set up will fail with the error status: Job is not allowed. Target is locked for RAC.

During the time the target computer is locked, template jobs for the actual target are set up and added to the Exceptions folder. However, when activated they will fail if the lock still remains. Jobs requested from the enterprise manager are set to error, if activated when the target computer is locked. Installation and job records cannot be deleted during the time the target computer is locked.

In situations where an RAC container fails, the standard renew function is accessible. If a job fails because it cannot execute on the new OS installation, that job can be deleted from the RAC container, before it is renewed.

If a complete renew with a new operating system is required, the RAC container should be deleted and a new OS installation be initiated.

If the selected RAC policy states that no RAC automation shall take place or if no jobs were set up, the target computer is unlocked as soon as its installation register has been cleaned up.

Job History with Retained Job Order Data

The job order option, User parameters, is retained in computer jobs. For other options, the default values are used.

Procedure options are inherited from the procedure used. Job options are as configured by the administrator. The following Job option values are the default:

- Triggered by Server=Yes
- Use delivery calendar=No

There are two parameters, JobTimeout, and StoreInSSLibrary, in the RAC section of the configuration store that can also be used to control job timeout and whether packages should be stored in the library.

Included or Omitted Jobs in a RAC Job Container

Jobs are always included in a RAC job container, if they involve the following:

- Detected software, if the software has been converted to a real software item (registered), and has a default install procedure.
- Delivery records for a scalability server.

The following jobs are omitted from a RAC job container:

- Jobs referring to uninstalled software and procedures marked with Exclude from RAC.
- Jobs set up by an activation or configuration procedure, if their associated installation procedure is marked with Exclude from RAC.

Relation to Move Operation

Information about the relation between RAC and move operations can be found under "Moving and Reinstalling After Crash" (see page 86).

RAC Restrictions

Only target computers with the UUID mechanism are subject for reinstall after crash (RAC), that is, all 32-bit and 64-bit Windows operating environments and all Linux/UNIX platforms are covered. However, docking devices are excluded from RAC, since they report the UUID of the hosting computer.

RAC on target computers configured using DTS download will fall back to internal NOS-less download. One reason is that packages sent out are staged on the target computer, the disk of which will be overwritten when the operating system is reinstalled. Another reason is that DTS is not bundled with the software delivery agent but sent out as a job.

RAC on a scalability server (including its library) is only possible, if the scalability server is installed from the very beginning. That is, it is not possible to restore the scalability server from an agent installation, since then any delivery records will be marked as removed. Only the part of the library known by the domain manager is restored.

No synchronization is available between RAC for computer and user profile targets. For example, if a user profile job is depending on a computer job, there is no mechanism except using procedure prerequisites.

The job history order will be retained with one exception. For scalability servers, delivery jobs are set up first, then all other jobs. However, the order between deliveries, as well as between the other type of jobs, will be kept.

Custom Administrator Message

You can use software delivery to create, define, and associate a text message to a job container, individual jobs (activities within a job container), or both at the time of creating a job container. You can also add the text message for a procedure of a software package. The message is displayed to the end users during the execution of the associated job container and its jobs. You can use these messages to convey appropriate information to the end users, for example, you can provide the following information in the message:

- Inform end users about the purpose of the task that is being performed on the target computers.
- Inform end users about any specific actions that you (as an administrator) want to perform on the target computers before or after the task.
- Inform end users about any specific actions that they (end users) must perform before or after the task.
- Include hyperlinks in the messages to direct end users to the appropriate resources for more information.

Note: For more information on how to define and associate a custom administrator message, see the Software Delivery section of the *DSM Explorer Help*.

Moving the OSIM Job Information

The software delivery functionality lets you transfer the OSIM job information while moving a target computer from one domain manager to another. All the information about completed, planned, and activated OSIM jobs is preserved and moved as part of any standard SD computer move operation. You do not need to perform any manual steps to export or import the information across different domain managers. You can automatically transfer the complete OSIM job information along with the SD installation records while performing any normal computer move operation.

Note: For more information on how to move the OSIM job information during an SD computer move operation, see the Software Delivery section of the *DSM Explorer Help*.

Optimization of Manager Concurrency

Software delivery optimizes the process of handling multiple tasks by improving the Task Manager and the Installation Manager concurrency. Software delivery provides configuration policies that let the Task Manager and the Installation Manager run in the concurrent mode to handle multiple tasks at the same. This multiprocessing approach that the concurrent mode provides helps you optimize manager concurrency, and consequently performance of the software delivery engine.

Note: For more information on how to optimize manager concurrency, see the Software Delivery section of the *DSM Explorer Help*.

Encryption and Throttling for NOS-less Software Package Transfers

Software delivery lets you configure encryption and throttling for NOS-less software package transfers. Appropriate configuration and application of the encryption and throttling parameters help ensure optimal utilization of the network resources. Using these configurations, you can control the transfer of NOS-less software packages from a scalability server to a software delivery agent for executing software jobs.

Note: For more information on how to configure encryption and throttling for NOS-less software package transfers, see the Software Delivery section of the *DSM Explorer Help*.

Optimization of Database Updates

Software delivery lets you configure the scalability server and the Installation Manager to achieve better performance with respect to database updates. By configuring the scalability server and the Installation Manager appropriately, you can collect, transfer, and commit multiple individual messages in bulk in one single database transaction. This ability to perform one large transaction, in place of several individual transactions one by one, helps optimize the database updates.

The messages that are considered for optimization are the job status messages and the software records. The job status messages include the job in-progress messages and the job completion messages. The software records include the software detection records and the software job records.

Note: For more information on how to optimize database updates, see the Software Delivery section of the *DSM Explorer Help*.

Shut Down a Computer after Last SD Job

Software delivery lets you shut down a target computer after completion of the last software delivery job. SD provides the shutdown-related job and calendar options. A combination of these job and calendar options controls the shutdown behavior of the target computer. You can use these options to decide when to shut down a computer, whether to shut it down or not, or how to define non-conflicting time ranges within which it is appropriate to shut down. This ability to shut down a computer after completion of the last SD job helps ensure that the target computers use power in an optimal manner and support the defined Green IT policies of the organization.

Note: For more information on how to shut down a computer after completion of the last SD job, see the Software Delivery section of the *DSM Explorer Help*.

Use of SD Agent Bridge

The SD Agent Bridge feature provides backwards compatibility for extended and legacy SD agents based on Unicenter DSM r11.2 C1. You can gather information obtained from mobile agents and then distribute jobs, modules, templates, and configurations to those agents.

The SD Agent Bridge is fully integrated in CA ITCM since r11.2 C3.

Note: The Agent Bridge is supported on Microsoft Windows only.

Note: The agent platforms supported by the Agent Bridge in this release are Windows Mobile 6.1 (ARM-based, including StrongARM, XScale), Windows Mobile 6 (Classic, Standard, Professional) (ARM-based, including StrongARM, XScale, TI OMAP), and Windows Mobile 5 (ARM-based, including StrongARM, XScale).

Major Components

The SD Agent Bridge consists of the following components:

- Common legacy server component and its process components

  Handles communication for the Agent Bridge, configuration, and agent registration.

- Software delivery components

  Provide server support for extended and legacy software delivery agents.

UUID Generator for Agent Bridge

A UUID generator allows Agent Bridge to generate an agent UUID for a legacy agent if one has not been reported. Additionally, a new configuration policy has been added to control the UUID generation behavior.

Note: You should always use the latest agents possible for your operating environment. To check the certification status of a legacy agent, see the appropriate Compatibility Matrix available on the CA Support Online web site, http://support.ca.com.

SD Agent Bridge Limitations

As CA ITCM is a new generation of asset management, software delivery, and remote control functionality, there are certain new features and functions that were not in the previous versions of these components and, therefore, will not work with legacy agents. SD Agent Bridge support does *not* include the following CA ITCM features:

- Performance module extraction
- Configuration policies

  Note: The Configuration Policy tree node is suppressed for legacy agents, and the Activate Job Check option is likewise disabled for legacy agents.
- Instant diagnostics
- DMDeploy functionality

Due to the changes in technology in CA ITCM, there are also some existing Unicenter Software Delivery 4.0 features that are *not* supported on legacy agents in CA ITCM using Agent Bridge. These unsupported features are as follows:

- Docking devices based on Unicenter Software Delivery 4.0 legacy agents
- Software Catalog for software delivery legacy agents
- Auto-installations of software delivery legacy agents

Known Issues with SD Agent Bridge

Currently, the following issues have been identified for SD Agent Bridge.

Active Job Check

The Active Job Check on the Unicenter Software Delivery legacy agent might fail in the following situation:

1. During package deployment the option, Jobs will be triggered by scalability server, is not selected.
2. And once the job container is created and is in the Active state, you select either the Active Job Check option from the DSM Explorer or run sdacmd jobcheck on the agent machine.

The result is that the status of the job remains in the Active state.

The workaround for this problem is to run sdjexec.exe on a Unicenter Software Delivery 4.0 agent machine, or asminst on a Unicenter Software Delivery 3.*x* or 2.0 agent machine. The status of the job will then be displayed as successful in the DSM Explorer.

Windows Mobile 5.0 Devices

When a Unicenter Asset Management 4.0 SP1 C2 agent is installed first, followed by a Unicenter Software Delivery 4.0 SP1 C3 agent, on a Windows Mobile 5.0 device pointing to Agent Bridge, the version number of the Unicenter Asset Management agent shown in the DSM Explorer might be incorrect.

Also, when a Unicenter Software Delivery 4.0 SP1 C3 agent is installed first, followed by a Unicenter Asset Management 4.0 SP1 C2 agent, on a Windows Mobile 5.0 device pointing to Agent Bridge, the Unicenter Asset Management 4.0 SP1 C2 agent might not get reported.

Agent Registration

The CA ITCM agent registers with the MDB by providing the following information:

- Host name
- Host Universal Unique Identifier (UUID)
- Operating system class ID
- IP address
- MAC address

With Agent Bridge, the host UUID is provided by the legacy agent, and the legacy agent is registered to the CA ITCM system using the Agent Bridge. The agent registration method used by CA ITCM and Agent Bridge maps the legacy information to that in CA ITCM. For example, a Unicenter Software Delivery 8-byte file ID is mapped to a CA ITCM formatted, 32-byte alphanumeric host UUID. The host UUID that is generated for a legacy agent is stored in the common usage file.

If a legacy agent does not provide a unique host UUID and the UUID generator is not enabled, it is not registered by the Agent Bridge, and the agent is treated as an invalid agent.

If the UUID generator is enabled, the correct procedures for registering Unicenter Software Delivery and Unicenter Asset Management legacy agents are as follows:

To register legacy agents, some of which may not report their own UUIDs

- If both the Unicenter Asset Management and Unicenter Software Delivery agents do not report host UUIDs, then you can register the Unicenter Asset Management and Unicenter Software Delivery agents in any order. However, you need to give time between the registrations of the two agents, typically, at least five (5) minutes apart.
- If the Unicenter Asset Management agent does not report a host UUID but the Unicenter Software Delivery agent does, then you should always register the Unicenter Software Delivery agent first. Then after five (5) minutes register the Unicenter Asset Management agent.
- If the Unicenter Software Delivery agent does not report a host UUID but the Unicenter Asset Management agent does, then you should always register the Unicenter Asset Management agent first. Then after five (5) minutes register the Unicenter Software Delivery agent.

In general, the majority of Unicenter Asset Management 4.0 agents and Unicenter Software Delivery 4.0 agents report host UUIDs when registering with the server.

The registration of all legacy Unicenter Software Delivery 2.0, 3.*x*, and 4.0 agents is supported by the agent registration method used by CA ITCM and Agent Bridge.

Agent Migration Considerations

When migrating legacy agents to CA ITCM using Agent Bridge, keep in mind the following limitations:

- After a migrated agent has performed a "reinstall after crash" (RAC), a new migration for the same agent creates a new unit rather than updating the existing agent.
- If you already have a migrated Unicenter Software Delivery (SD) legacy agent in your CA ITCM environment, then installing a Unicenter Asset Management 4.0 legacy agent or CA ITCM asset management agent afterwards results in the status of the migrated legacy SD agent being overwritten. The SD status will be changed from "Locked by Migration" to "Not Installed." Therefore, do not use this method to migrate and register legacy agent data. Instead, use the DSM migration tool.

SD Agent Bridge Prerequisites

The SD Agent Bridge does not necessarily have to be installed on the same computer as the domain manager. However, it must be installed on the same computer as the software delivery scalability server, and this is handled automatically by the installation procedure.

Unicenter Software Delivery 4.0 SP1 agents may need to have one of the following test or cumulative fixes applied, depending on the operating environment and language:

- **English (ENU)**

QO77129	Windows NT - USD 4.0 SP1C3 CD1
T18C930	4.0 SP1 Fix for Novell Netware (NW)
QO77130	Windows NT-4.0 SP1 C3 FIX FOR NT & NW
QO77876	4.0 SP1 C3 FIX FOR LINUX
QO77874	4.0 SP1 C3 FIX FOR HP-UX
QO77877	4.0 SP1 C3 FIX FOR SOLARIS
QO77869	4.0 SP1 C3 FIX FOR AIX
QO77878	4.0 SP1 C3 FIX FOR SOLARIS Intel

- **German (DEU)**

QO81439	T1B1339	Windows CD1
QO81451	T1B1359	Windows CD2
QO81456	T1B1340	AIX
QO81457	T1B1341	HP-UX
QO81458	T1B1342	Sun Solaris

- **French (FRA)**

  T1B1344 Windows CD1

  T1B1360 Windows CD2

  T1B1345 AIX

  T1B1346 HP-UX

  T1B1347 Sun Solaris

- **Japanese (JPN)**

  QO83580 T1B1373

These fixes can be obtained from Technical Support at http://ca.com/support.

Supported Operating Environments and SD Agents

The CA ITCM media includes an agent for Windows Mobile 5.0, 6.0, and 6.1. This agent requires the use of the legacy Agent Bridge. No other agents are supported with the legacy Agent Bridge.

Note: You should always use the latest software delivery agent possible for your operating environment. To check for the latest version, see the software delivery Certification Matrix available on the CA Support Online web site, http://support.ca.com.

SD Agent Bridge Configuration

Like all other CA ITCM plug-ins, the SD Agent Bridge is configurable.

Therefore, use the policy group folders under the Control Panel, Configuration, Configuration Policy, Default Computer Policy, DSM, software delivery, Scalability Server subnode in the DSM Explorer tree to configure SD Agent Bridge.

Backwards Compatibility Support Policy Group

The Backwards Compatibility Support policy group lets you view or edit Agent Bridge support policies for Unicenter Software Delivery legacy and extended agents. You can modify policy parameter values by double-clicking a policy to display the Setting Properties dialog.

This policy group contains the following policy group folder:

Communication

The Backwards Compatibility Support policy group also contains the following policies:

Backwards compatibility support: Enable

Enables Agent Bridge scalability server support for Unicenter Software Delivery legacy agents and Windows CE agents, if set to True. If False, this policy disables server support for Unicenter Software Delivery legacy and extended agents.

Note: Enabling SD Agent Bridge support does not mean that the AM Agent Bridge support is automatically enabled. For more information, see the Enable Agent Bridge configuration policy in Asset Management Policy Group.

Default: False

Backwards compatibility support: Use the SDOUTPUT share

Enables support for a new writable share, SDOUTPUT, under SDLIBRARY$ on the server, if set to True. If False, this policy disables support for the new writable share, SDOUTPUT. This server policy should be set to True if legacy agents prior to Unicenter Software Delivery 4.0 are connected to the server and using the NOS connection method for software delivery library access. This policy allows job output files to be written directly to the SDOUTPUT library share.

Default: False

Communication Policy Group

The Communication policy group governs CA-SD communication protocols for Unicenter Software Delivery extended and legacy agents.

The Communication policy group contains the following policies:

Backwards compatibility support: Agent connect port

Specifies the port for the server to listen for legacy Unicenter Software Delivery agent connection requests.

Default: 4721

Backwards compatibility support: FileTransferBlockSize

Specifies the size of file transfer blocks in kilobytes (KB). If you are running on fast networks, increasing the size generally improves performance.

Limits: 4–32

Default: 4

Backwards compatibility support: Max Connections

Indicates the maximum number of network connections allowed to and from this computer.

Default: 550

Backwards compatibility support: Max Peers

Indicates the maximum number of allowed network application peers for this computer.

Default: 200

Backwards compatibility support: SysRcvTimeout

Specifies the common system receive timeout interval in seconds.

Note: If -1 is specified, the timeout is indefinite.

Default: -1

Backwards compatibility support: Trigger port

Specifies the port number of the trigger process (TRIGGER).

Default: 4725

Backwards compatibility support: WaitCCTimeout

Specifies the wait timeout interval in seconds for connection confirmations.

Note: If -1 is specified, the timeout is indefinite.

Limits: 1–1000

Default: 120

Backwards compatibility support: WaitCRTimeout

Specifies the wait timeout interval in seconds for connection requests.

Note: If -1 is specified, the timeout is indefinite.

Limits: 1–1000

Default: 120

Wake-on-LAN Server Configuration

You can set up advanced Wake-on-LAN server configuration for the legacy agents. These configuration policies are locally managed and need to be set on the servers by modifying comstore locally.

Example: Specifying Remote Subnet Masks and Sending Wake-on-LAN Broadcasts

```
[itrm/usd/SUBNETMASKS]
;   This section is related to the following one.

[itrm/usd/CUSTOMBROADCAST]
;   This section defines the TCP/IP subnet masks to use when sending
;   out the Wake-on-LAN broadcasts. By default, broadcasts are sent
;   on the network on which a machine resides. For the local network, the subnet
;   is automatically retrieved from the machine's configuration.
;   However, if a remote network is using subnets, you will need to specify
;   its subnet mask here.
;
;   Example:
;   100.0.0.0   = 255.255.255.0
```

This is done, for example, by running the following command on the server:

```
ccnfcmda -cmd SetParameterValue -ps itrm/usd/SUBNETMASKS -pn 100.0.0.0 -v
255.255.255.0
```

To remove this setting, run:

```
ccnfcmda -cmd DeleteParameter -ps itrm/usd/SUBNETMASKS -pn 100.0.0.0
```

```
[itrm/usd/CUSTOMBROADCAST]
;   This section is related to the one above, [itrm/usd/SUBNETMASKS], and
;   contains three parameters, DisableBroadcast, NoBroadcast, and
;   CustomBroadcast.

DisableBroadcast=
;   If DisableBroadcast=1, Wake-on-LAN broadcasts are disabled.
;   If DisableBroadcast=0, Wake-on-LAN broadcasts are enabled.
```

For example:

```
ccnfcmda -cmd SetParameterValue -ps itrm/usd/CUSTOMBROADCAST  -pn DisableBroadcast
-v 1
```

```
NoBroadcast=
;   If NoBroadcast=1, a direct broadcast will be sent to a specific IP-address
;   (preceding the Trigger message). Then broadcast is not allowed.
;   If NoBroadcast=0, a direct Wake-on-LAN broadcast to a specific
;   IP-address is disabled.

CustomBroadcast=
;   If CustomBroadcast =0, Wake-on-LAN broadcasts to non-standard
;   subnets is disabled. Then standard broadcast using the
;   [SUBNETMASKS] entry is made.
;   If CustomBroadcast =1, a Wake-on-LAN broadcast will be sent to
;   non-standard (custom) subnets.
;   Example:
;   If you have a subnet with subnet mask 255.255.255.224 (32 addresses
;   on this subnet), then 31,63,95... are values corresponding to broadcast
;   addresses xxx.xxx.xxx.31, xxx.xxx.xxx.63, xxx.xxx.xxx.95, ...
;   Append this list at the end.
;

“ccnfcmda -cmd SetParameterValue -ps itrm/usd/CUSTOMBROADCAST  -pn  NoBroadcast –v
0”
“ccnfcmda -cmd SetParameterValue -ps itrm/usd/CUSTOMBROADCAST  -pn  CustomBroadcast
–v 1”

“ccnfcmda -cmd SetParameterValue -ps itrm/usd/CUSTOMBROADCAST  -pn  xxx.xxx.xxx.0 –v
31,63,95,127,159,191,223,255”
;
;   When Software Delivery sends a job to the IP address xxx.xxx.xxx.69, a
;   Wake-on-LAN broadcast xxx.xxx.xxx.95 should be sent.
```

How to Add Legacy Software to the Software Package Library

The following ways are available to add legacy Unicenter Software Delivery software to the Software Package Library:

- Exporting from a legacy Local Server
- Importing from the original legacy CD ROM

The following scenarios demonstrate how to add legacy Unicenter Software Delivery software to the Software Package Library.

Scenario 1—Exporting legacy agent software from a Unicenter Software Delivery 4.0 Local Server:

1. From a Unicenter Software Delivery 4.0 Local Server, navigate to the Software Delivery, software library node, and locate the legacy agent software you want to add.
2. Right-click the software package and then click Export, Software package.

   The Export Software Package dialog appears.
3. Enter the directory path and name where you want to store the software package.

   Enter the path where to copy the software package or click Browse to browse through the Explorer.
4. Click OK.
5. From the DSM Explorer, right-click the DSM Software Packages node and then click Import, Software package.

   The Import Software Package dialog appears.
6. Select the legacy agent software package from the directory specified in Step 3, and click OK.

   The legacy agent software is added to the Software Package Library.

Scenario 2—Importing legacy software from an original Unicenter Software Delivery CD ROM:

1. Insert the Unicenter Software Delivery CD.
2. From the DSM Explorer, right-click the DSM Software Packages node and then click Import, Software package.

   The Import Software Packages dialog appears.

3. Select the legacy agent software package.
4. Click OK.

   The legacy agent software is added to the Software Package Library.

   Note: When importing the software, you may get a message like, “The software you are registering exists as a detected package. Do you want to replace it with the real one?” Click Yes. (This is the case when an agent using this agent software already has connected and has been registered to the DSM system.)

Download Method Error Messages in Context of SD Agent Bridge

In context of the SD Agent Bridge feature, the following error messages may occur with the software delivery download method:

- **SDM001043**

  Download method can not be set on a computer with a legacy agent.

- **SDM001044**

  One or more computers with legacy agents was found. Download method could not be set for these computers.

Installing Wrapper Packages from External Repositories

This chapter describes the installation of wrapper packages from external repositories using software delivery functionality in detail.

Sample DSM Architecture with External Debian Repositories

Forward Inc is a mid-sized banking organization that deployed CA ITCM to manage its physical and virtual infrastructure. Forward Inc is headquartered in New York and has branch offices in US and India. Each country has a data center and has several branch offices.

The current CA ITCM implementation looks like the following:

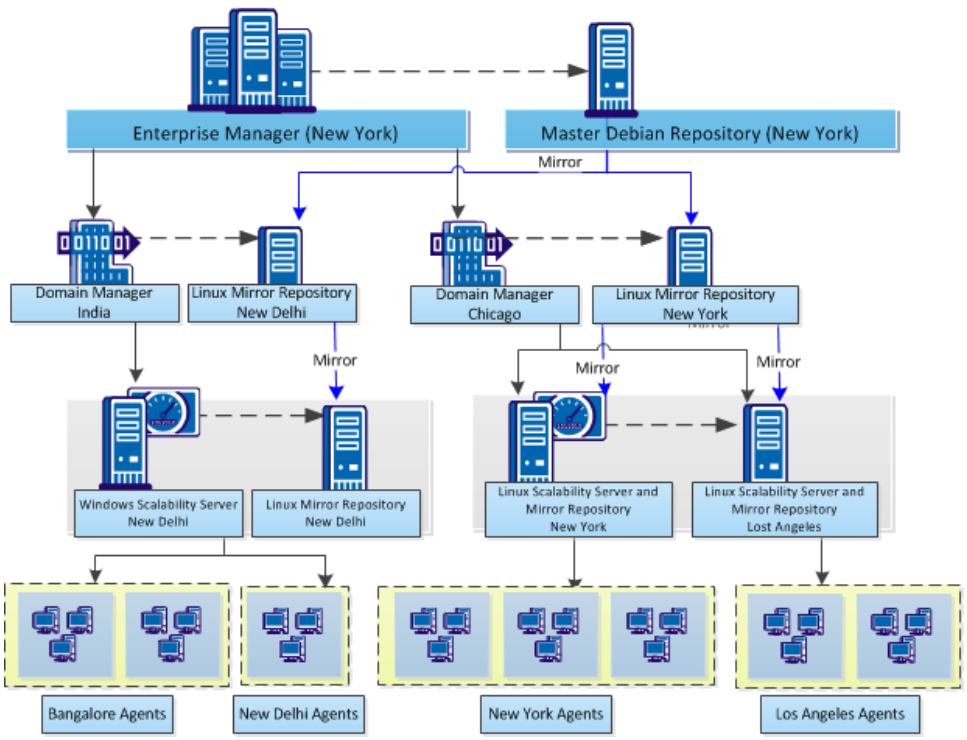
- The DSM enterprise manager is located in the headquarters.
- A DSM domain manager is located in the data center of each country.
- A scalability server is located in major cities serving various neighboring branches.

Forward Inc has a few thousand computers that are on Debian OS and requires the ability to deploy Debian software packages from CA ITCM. The master Debian repository is located in the headquarters. The company wants to create and deploy wrapper packages on each domain manager so that deployment is faster. Here is how they do it:

- Added the external Debian repository as the master repository to the enterprise manager
- Created a mirror of the master Debian repository in each data center
- Associated the mirrors in each data center as the master repository to the respective domain managers so that wrapper packages can be created from the mirror on the data center. Wrapper packages that are applicable to the entire organization is created at the enterprise manager and distributed to the domain managers.
- Created mirrors on the scalability servers from the mirror on the data center, by configuring the respective domain managers

The following architecture diagram illustrates the DSM Architecture with the Debian repositories and mirrors:

DSM Architecture with External Debian Repositories at Forward Inc.



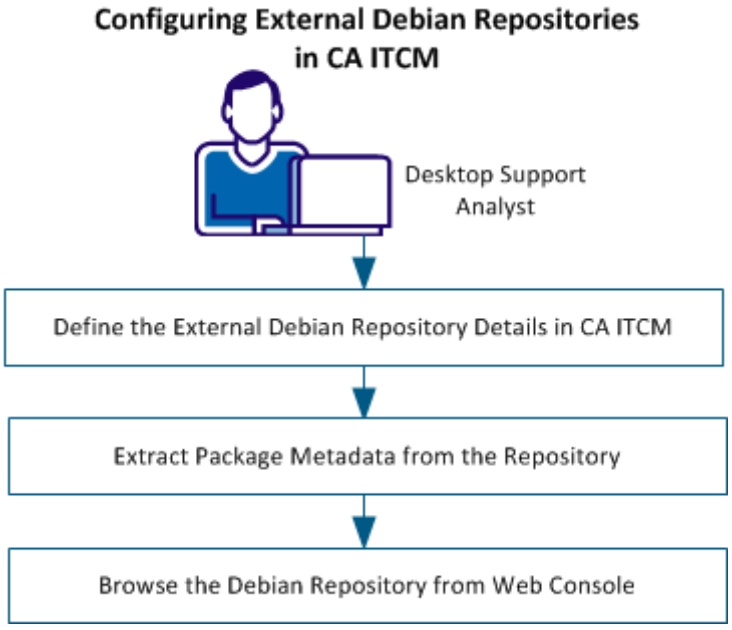
How to Deploy Packages from Debian Repositories

The following process describes how you configure CA ITCM to deploy packages from Debian repositories:

1. Add the external Debian repository details in CA ITCM (see page 147)
2. Set up mirror repositories (see page 158)
3. Set up HTTP and FTP shares on repository servers
4. Deploy Debian packages using software delivery (see page 152)

Configuring External Debian Repositories in CA ITCM

As a desktop support analyst, you configure the external Debian repository details in CA ITCM. This configuration lets you browse the repository from CA ITCM, create mirrors of the repository, and deploy Debian packages using software delivery. The following diagram illustrates the steps that you perform to configure external Debian repositories details in CA ITCM:



Perform the following tasks to configure external Debian repositories in CA ITCM:

1. Define the External Debian Repository Details in CA ITCM (see page 148)
2. Extract Package Metadata from the Repository (see page 150)
3. Browse the Debian Repository from Web Console (see page 151)

Define the External Debian Repository Details in CA ITCM

Define the details of the external Debian repository that CA ITCM must connect to. CA ITCM uses this information to browse the repository, create mirrors, and deploy software packages.

Follow these steps:

1. Navigate to Control Panel, Configuration, Configuration Policy.
2. Right-click Default Configuration Policy and select Unseal.

   Note: The changed configuration policy must be applied to all the target computers. Hence, select the Default Configuration Policy.

   The policy becomes editable.
3. Navigate to DSM, Software Delivery, Shared, External Repository, Debian and select Repositories on the right pane.
4. Provide the following details for each repository that you want CA ITCM to connect to, in the Repositories table:

   Repository Name

   Specifies a unique repository name. You can specify any name but verify that the name is unique across the Repositories table.

   Repository Relation

   Specifies whether the repository is a master, mirror, or mirror template.

   Master

   Specifies that the repository is a master. A master repository is used while creating wrapper packages. CA ITCM cannot deploy native Debian packages directly. Create wrapper packages that include references to the native Debian packages and then deploy the wrapper packages.

   Following guidelines apply for master repositories:

   - Add at least one master repository to create and deploy Debian wrapper packages.
   - You can add multiple master repositories; however, you can create wrapper packages only from the first (alphabetically) available master.
   - You can configure different master repositories at the enterprise manager and domain manager level. A master repository can be an external Debian repository or another mirror repository that acts as a master for creating wrapper packages. For example, you have an external Debian repository co-located with the enterprise manager. You created mirrors of this repository on a Linux computer that is co-located with each of your domain managers. You can configure these mirrors as the master for the respective domain managers so that you can create wrapper packages from the mirrors co-located with your domain managers.

Mirror

Specifies that the repository is a mirror that is created from a master or another mirror.

Mirror-Template

Specifies that the mirror is only a template and not a physical repository. The mirror template is only a placeholder for multiple mirror repositories that have the same configuration. When you have numerous mirrors, you can create one mirror template per parent instead of creating a row each for all the mirrors. Mirror templates are used for software deployment and repository extraction but not for mirror synchronization. The host name of the computers hosting the mirrors is dynamically replaced at run time.

Repository Type

Specifies the repository type.

Repository Method

Specifies the transfer protocol that is used for transferring the packages from the repository to the target computers. Select HTTP, FTP depending on what you have configured. For more information about this configuration, see Setting Up FTP and HTTP Share for Software Packages and OS Images.

Note: If the repository is a master and you want to browse the repository and create wrapper packages from it, configure the repository as an FTP share.

Hostname

Specifies the host name of the computer that hosts the repository. For mirror template repositories, do not specify the host name because the host name is dynamically provided at run time. Even if you specify, the host name is ignored for mirror templates.

Root

Specifies the root node of the repository.

5. Repeat step 4 to add more repositories.
6. Save and seal the policy. Verify that the policy is applied on all the target computers.

   The repositories information is updated on all target computers.

Extract Package Metadata from the Repository

Extracting package metadata from the repository lets you view the Debian package details on DSM Web Console.

Note: The following steps apply for extracting the package metadata from both master and mirror repositories.

Follow these steps:

1. Navigate to Control Panel, Engines, All Engines, SystemEngine from DSM Explorer.

   The engine log is displayed.

2. Right-click the SystemEngine and select Add New Task.

   The New Task Wizard opens.

3. Follow the instructions and perform the following steps in the wizard:

   a. Select the task type as CA Repository Extraction, and enter a task name and description. Click Next.

      Note: Ensure that you disable the system firewall to execute the task successfully.

   b. Provide the following details:

      Note: As the repository server is on Linux, values provided in the following Distribution and Components Name fields must be case-sensitive; they must match the case in the repository server. For example, if the repository server location for ftp://172.16.0.12/ubuntu/dists/lucid/main/binary-i386/, the distribution name must be specified as lucid and not as Lucid or LUCID.

      Repository Name

      Specifies the repository name from which you want to extract the package metadata. The list displays the repositories you had defined in the Repositories configuration table.

      Note: You cannot create two engine tasks with the same repository and distribution combination.

      Host Name

      Specifies the host name of the repository. This field is enabled only for repositories of type Mirror-Template. For the master and mirror repositories, the host name is automatically taken from the Repositories configuration table.

Distribution

Specifies the distribution from which you want to extract the package details.

Note: An engine task can extract data only from a single distribution. If you want to extract data from multiple distributions, create additional engine tasks.

Components Name

Specifies the components that you want to extract. Click Add to add more components.

c. Specify scheduling options.

4. Click Finish on the last page.

The System Engine creates the task and executes it at the schedule time. You can monitor the task by clicking the SystemEngine and review the status in the Task List section on the right pane.

Note: You can also browse the repository from Web Console while the engine task is still in progress. The Web Console displays the distributions and packages as and when they are extracted from the repository.

Browse the Debian Repository from Web Console

You can browse the contents of a Debian repository in Web Console to know what packages are present in the repository.

Follow these steps:

1. Log in to DSM Web Console.
2. Navigate to Console, Software, External Repositories, *repository*.

A list of distributions in the selected repository is displayed. The Synchronization Status column shows the status of the repository extraction task. You can also click View under the Synchronization Log column to view the progress of metadata extraction and errors that are encountered, if any.

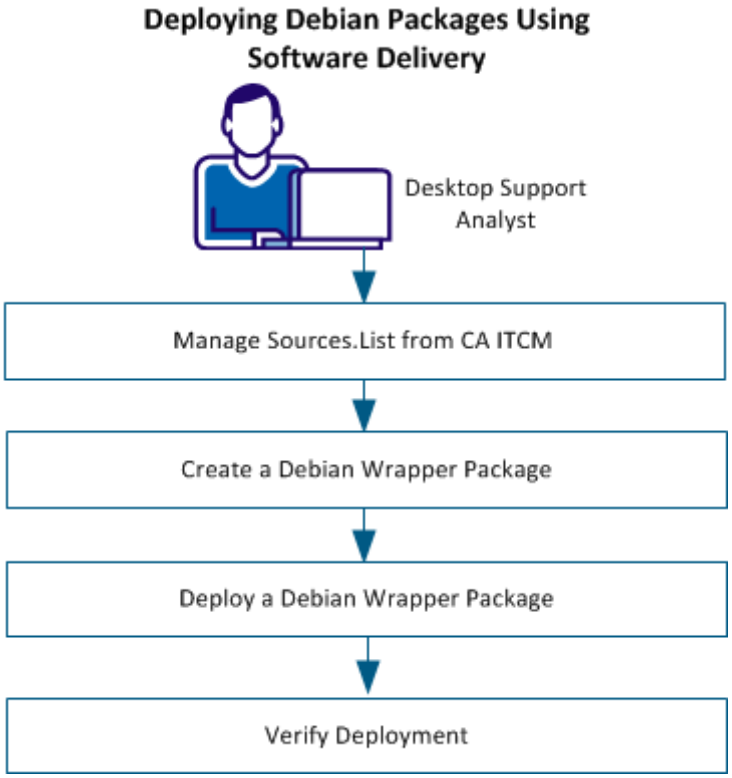
Note: If you open the repository before the extraction task completes, it is possible that you do not see all the distributions in the list.

3. Click a distribution.

A list of Debian packages in the distribution is displayed.

Deploy Debian Packages Using Software Delivery

As a desktop support analyst, you can deploy Debian software packages on target Kubuntu computers using software delivery. Software deployment through software delivery lets you send software packages to any managed Debian computer and deploy them. The native Debian packages are not physically stored in CA ITCM; they are stored in the Debian master and mirror repositories. Hence deployment of Debian packages is different from the regular SD packages. The following diagram illustrates the steps that you perform to deploy Debian packages using software delivery:



Perform the following tasks to deploy Debian packages using software delivery:

1. Manage Sources.List from CA ITCM (see page 153)
2. Create a Debian Wrapper Package (see page 155)
3. Deploy a Debian Wrapper Package (see page 156)
4. Verify Deployment (see page 157)

Manage Sources.List from CA ITCM

The Debian computers maintain a file named sources.list that contains the details of repositories, distributions, and components from which the packages can be obtained. To deploy Debian packages through software delivery, you must manage the sources.list from CA ITCM.

Follow these steps:

1. Navigate to Control Panel, Configuration, Configuration Policy, *Policy Name*, DSM, Software Delivery, Shared, External Repositories, Debian, and double-click Sources on the right pane.

   Note: This configuration policy change must be applied to computers or group of computers that use a particular source repository. For example, you have a master repository and five mirror repositories. The mirror repositories are located in different offices for faster download. You want the computers in these offices to connect to the mirrors in the respective locations. In this case, you create five configuration policies. You then open each of them and configure the sources table with the mirror repository details for that location, and apply the policy to all the computers in that location.

2. Provide the following details in the Sources table:

   Note: When the policy is applied on target computers with at least one row in the sources.list table, CA ITCM renames the original sources.list as sources.list.original.CADSM. It then creates a sources.list file and adds the information from the Sources table.

   Repository Name

   Specifies the repository name. The value in this field must match the Repository Name in the Repositories table; otherwise, software deployment can fail. Specify the details of only those repositories that the target computers must connect to.

   Repository Assignment

   Specifies how the host name for the repository is assigned.

   Static

   Specifies that the host name provided in the repository table must be used. This option is applicable only for master and mirror repositories and not to mirror templates.

   Dynamic

   Specifies that the host name of the repository is provided in the Dynamic Repository Host configuration policy under Control Panel, Configuration, Configuration Policy, Policy Name, DSM, Software Delivery, Shared, External Repositories, Debian. This option is only applicable for mirror templates.

Note: Dynamic assignment is helpful when the target computer roams or moves. In this case, the host name and URI changes, but the distributions remain the same. The management of the assigned distributions is separated from the physical locations of the mirrors.

Scalability Server

Specifies that the host name of the repository is the scalability server. The host name value in the sources.list file is dynamically updated based on the scalability server of the target computer. This option is only applicable for mirror templates.

Distribution

Specifies the distribution that contains the packages that you want to deploy.

Components

Specifies the components that contain the packages that you want to deploy.

Note: You can specify multiple components; separate the components with a space.

Repository Format

Specifies format of the Debian packages in the repository.

Binary

Specifies that the packages are in binary format. This format is equivalent to "deb" in sources.list that is.deb <URI> <DISTRIBUTIONS> <COMPONENTS>.

3. (Optional) Add additional repositories, if the target computers have more than one source repository that they will connect to.
4. (For Dynamic Repository Assignment only) Navigate back to External Debian Repository, Debian, and double-click Dynamic Repository Host. Specify the repository host name.

   Note: You can also define this parameter in the Default Configuration Policy of the domain managers. This action is helpful when the target computer moves from one manager to another. The target can automatically connect to the default repository host name configured for the new manager, without any additional configuration.
5. Save and seal the policy. Apply the policy on the target computers to which the configuration applies.

   The configuration policy is pushed to the target computers.
6. Navigate to All Computers, *Computer Name*, Configuration, Configuration Policy and verify that the policy has been applied and activated.
7. (Optional) Log in to one of the target computers and verify that the sources.list file contains the sources you configured.

   The repository details are added to the sources.list file.

Create a Debian Wrapper Package

A Debian wrapper package includes references to native Debian software packages stored in an external Debian repository. You cannot directly deploy a native Debian software package using CA ITCM; you need wrapper packages.

Note: Though you can add multiple master and mirror repositories to the Repositories table, you can create wrapper packages only from the first (alphabetically) available master repository, whose package metadata has been extracted. For more information, see Extract Package Metadata from the Repository.

You can create a Debian wrapper package in one the following ways:

- Create a Debian wrapper package.
- Create a Debian wrapper package based on an existing wrapper package. The new wrapper package contains references to Debian packages and debconf parameters from the source wrapper package.

Follow these steps:

1. Log in to DSM Web Console.
2. Navigate to Software, Packages and click the software package group under which you want to create the wrapper package.

   A list of packages in the group is displayed.
3. Click New Debian Wrapper Package in the Actions panel.

   Note: If you want to create a wrapper package based on an existing wrapper package, click New Based On on the Actions panel.

   The New Debian Wrapper Package wizard opens.
4. Follow the instructions in the wizard to specify the pre-install actions, include Debian packages, configure Debconfig parameters, and specify post-install actions.
5. Click Finish on the last page.

   The new Debian wrapper package is added to the list of registered software packages.

Note: If you want to edit the wrapper package, unseal it first and then click Edit on the Actions panel.

Deploy a Debian Wrapper Package

Deploying a Debian wrapper package on target computers sends a software job to the agent. The job then installs the software on the target computers at the scheduled time.

Verify the following prerequisites before you start the deployment:

- Verify that HTTP or FTP access is configured on computers hosting the repository. For more information about configuring the access, see Setting Up HTTP and FTP Share for Software Packages and OS Images.
- Verify that you have applied this patch on the target computer

Follow these steps to deploy a package from Web Console:

1. Open the Web Console and navigate to Express Action.
2. Click Install Software.
3. Follow the instructions in the wizard and Click Finish on the last page.

Follow these steps to deploy a package from DSM Explorer:

1. Open DSM Explorer and navigate to Computers and Users, All Computers and find the target computer on which you want to deploy the package.
2. Right-click the target computer and select Software Jobs, Deploy Software Package.

   The Deploy Software Package Wizard appears.
3. Follow the instructions in the wizard and click Finish on the last page.

The software job is sent to selected computers. At the scheduled time, the jobs download the Debian packages from the Debian repository that is defined in sources.list on the target computer and run the installer.

Debian Software Deployment Considerations

If you first install a version of a wrapper package on a target computer, and you later install another version of the same wrapper package on the same computer, the first version is uninstalled and all the packages in the second version installed.

If a native Debian package is part of more than one Debian wrapper package, and you deploy such Debian wrapper packages on the same target computer, the Debian package is installed or updated in both the deployment jobs. During the uninstallation procedure of one of the Debian Wrapper packages, the Debian packages that are uninstalled are checked. If they are referred in another Debian wrapper package, the uninstallation job completes without uninstalling the shared Debian package.

View the Configuration of Package Resource List

You can view the configuration of sources.list at the following inventory location:

Follow these steps:

1. Navigate to Computers and Users, All Computers, *debian computer*, Inventory, System Status, Package Resource List.

   The Package Resource List configuration is viewed.

Verify Deployment

Verify the deployment to help ensure that the wrapper package is deployed successfully on the target computer.

Note: The Debian software installer does not return the success or failure message to CA ITCM. The status of the SD job only reflects the status of wrapper package deployment and not of the actual Debian software package.

Follow these steps:

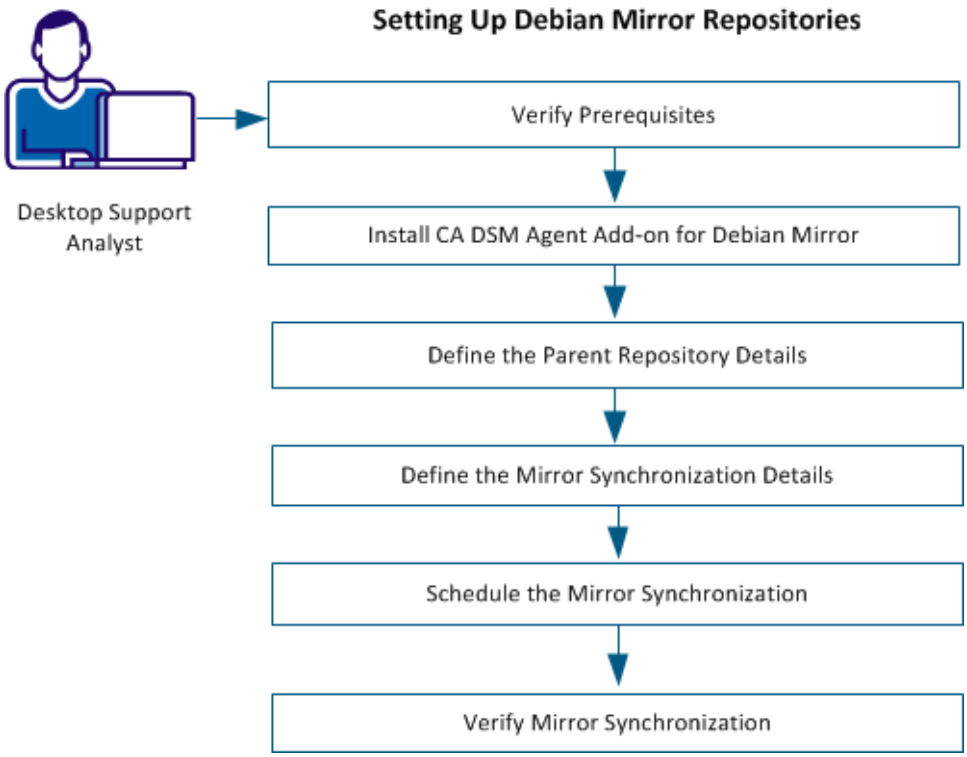
1. Open DSM Explorer and navigate to Computers and Users, All Computers and find the target computer on which you deployed the package.
2. Right-click the computer and select Jobs, Software Jobs.

   The status of the job is displayed.
3. Double-click the respective job when the status changes to SW Installed and click the Job output tab.

   The job output, and success or failure messages are displayed.

Setting Up Debian Mirror Repositories

As a desktop support analyst, you can set up mirrors of a Debian repository to help ensure easy access and faster download of the packages at the target computers. The following diagram illustrates the steps that you perform to set up Debian mirror repositories:



Perform the following tasks to set up Debian mirror repositories:

1. Verify Prerequisites (see page 159)
2. Install CA DSM Agent Add-on for Debian Mirror (see page 159)
3. Define the Parent Repository Details (see page 160)
4. Define the Mirror Synchronization Details (see page 162)
5. Schedule the Mirror Synchronization (see page 163)
6. Verify Mirror Synchronization (see page 164)

Verify Prerequisites

Verify the following prerequisites to help ensure that the mirror and synchronization work properly:

- Identify the computers on which you want to create the mirror repository.

  Note: Only Linux variants are supported for mirrors. For example, you can host the mirror repository on a Linux scalability server.

- Install DSM agent on the identified computers.
- Install the debmirror utility on the identified computers. For more information about installing debmirror, see Install debmirror Utility.
- Expose the location and the directory where you want to create the mirror repository, as both HTTP and FTP shares. For more information about setting up HTTP and FTP shares on the mirror, see Setting Up HTTP and FTP Share for Software Packages and OS Images.

Install CA DSM Agent Add-on for Debian Mirror

Install the add-on package on computers that host the mirror repository. The add-on enables the computer for mirror synchronization.

Important! Mirror synchronization fails if you do not install the add-on package.

Follow these steps:

1. Navigate to Software, Software Package Library, DSM Software Packages in DSM Explorer.
2. Right-click the package CA DSM Agent add-on for Debian Mirror 1.0 and select Deploy.
3. Follow the instructions in the wizard. Specify the following information in the wizard:
   - Select the computers on which you plan to host the mirror repository.
4. Click Finish on the last page.

   A software job is created for each computer that you selected.
5. Monitor the job status in All Computers, *computer_name*, Jobs, Software Jobs.

   When the job is completed, the job status changes to SW Installed.

Define the Parent Repository Details

Define the details of the parent repository for the mirror. A parent repository can be a master repository or a mirror repository because you can create a mirror from a master repository or from another mirror repository. You can define multiple mirrors of a parent repository depending on the network traffic, load, and sites you want to support. For example, if you decide to have two mirrors at each site and you have five different office sites, you need ten mirrors of the parent repository.

Note: The steps are the same as defining the external repository, except that you need to define whether the parent is a master or mirror.

Follow these steps:

1. Navigate to Control Panel, Configuration, Configuration Policy.
2. Right-click Default Configuration Policy and select Unseal.

   Note: The changed configuration policy must be applied to all the target computers. Hence, select the Default Configuration Policy.

   The policy becomes editable.
3. Navigate to DSM, Software Delivery, Shared, External Repository, Debian and select Repositories on the right pane.
4. Provide the following details for each repository that you want CA ITCM to connect to, in the Repositories table:

   Repository Name

   Specifies a unique repository name. You can specify any name but verify that the name is unique across the Repositories table.

   Repository Relation

   Specifies whether the repository is a master, mirror, or mirror template.

   Master

   Specifies that the repository is a master. A master repository is used while creating wrapper packages. CA ITCM cannot deploy native Debian packages directly. Create wrapper packages that include references to the native Debian packages and then deploy the wrapper packages.

   Following guidelines apply for master repositories:

   – Add at least one master repository to create and deploy Debian wrapper packages.

   – You can add multiple master repositories; however, you can create wrapper packages only from the first (alphabetically) available master.

- You can configure different master repositories at the enterprise manager and domain manager level. A master repository can be an external Debian repository or another mirror repository that acts as a master for creating wrapper packages. For example, you have an external Debian repository co-located with the enterprise manager. You created mirrors of this repository on a Linux computer that is co-located with each of your domain managers. You can configure these mirrors as the master for the respective domain managers so that you can create wrapper packages from the mirrors co-located with your domain managers.

Mirror

Specifies that the repository is a mirror that is created from a master or another mirror.

Mirror-Template

Specifies that the mirror is only a template and not a physical repository. The mirror template is only a placeholder for multiple mirror repositories that have the same configuration. When you have numerous mirrors, you can create one mirror template per parent instead of creating a row each for all the mirrors. Mirror templates are used for software deployment and repository extraction but not for mirror synchronization. The host name of the computers hosting the mirrors is dynamically replaced at run time.

Repository Type

Specifies the repository type.

Repository Method

Specifies the transfer protocol that is used for transferring the packages from the repository to the target computers. Select HTTP, FTP depending on what you have configured. For more information about this configuration, see Setting Up FTP and HTTP Share for Software Packages and OS Images.

Note: If the repository is a master and you want to browse the repository and create wrapper packages from it, configure the repository as an FTP share.

Hostname

Specifies the host name of the computer that hosts the repository. For mirror template repositories, do not specify the host name because the host name is dynamically provided at run time. Even if you specify, the host name is ignored for mirror templates.

Root

Specifies the root node of the repository.

5. Repeat step 4 to add more repositories.
6. Save and seal the policy. Verify that the policy is applied on all the target computers.

   The parent repositories information is updated on all target computers.

Define the Mirror Synchronization Details

The synchronization job requires that you define the mirror synchronization details for each mirror repository. The job uses these details to synchronize the mirrors.

Follow these steps:

1. Navigate to Control Panel, Configuration. Right-click Configuration Policy and select New Policy.

   You need a new policy for mirror synchronization so that you can apply the synchronization details only to the computers that host the mirrors.

2. Navigate to DSM, Software Delivery, Shared, External Repositories, Debian and double-click Mirror Synchronization.

3. Provide the following details for mirroring a repository in the mirror synchronization table:

   Parent Repository name

   Specifies the parent repository you want to mirror.

   Note: Verify that the parent repository name you specify in this field exactly matches the name specified in the Default Configuration Policy, DSM, Software Delivery, Shared, External Repositories, Debian, Repositories configuration table. If the names do not match, the synchronization job fails at run time.

   Distributions

   Specifies the list of the distributions from the selected repository that must be mirrored. You can specify more than one value by separating each value with a space.

   Components

   Specifies the list of the components from the selected repository that must be mirrored. You can specify more than one value by separating each value with a space.

   Architectures

   Specifies the list of the architectures from the selected repository that must be mirrored. You can specify more than one value by separating each value with a space.

Location

Specifies the location where you want to create the mirror repository.

Note: Verify that this location is exposed as both HTTP and FTP shares. For more information about setting up HTTP and FTP shares, see Setting Up HTTP and FTP Share for Software Packages and OS Images.

Additional Arguments

Specifies the additional arguments that are used while launching the debmirror utility.

Status

Specifies whether you want to synchronize the mirror or not. If you are not using a mirror repository actively, you can disable the synchronization without deleting the mirror.

4. Save and seal the policy. Apply the policy to computers that host the mirror repository.

   The mirror synchronization details are defined and the configuration is applied on the mirror computers.

Schedule the Mirror Synchronization

Schedule the mirror synchronization to automatically synchronize the mirror with its parent repository at the scheduled time. The mirror repository is created when the synchronization job runs successfully for the first time after you have defined the mirror synchronization details.

Follow these steps:

1. Navigate to Control Panel, Configuration Policy.
2. Right-click the configuration policy that you applied on computers hosting mirrors and select Unseal.
3. Navigate to DSM, Common Components, CAF, Scheduler, Run Mirrorsync from DSM Explorer.
4. Select CAF Scheduler : Enabled and set the value to true.
5. Configure the other parameters under the Run Mirrorsync node to specify the mirror synchronization schedule. For more information about the scheduling parameter, press F1.
6. Seal and apply the policy on computers that host the mirror repositories.

   The mirror synchronization is scheduled. At the scheduled time, the CAF Scheduler synchronizes the mirror with the parent repository.

Verify Mirror Synchronization

After the mirror synchronization job is executed, follow these steps to verify whether mirror synchronization was successful and CA ITCM is able to connect to the mirrors.

1. View the Status of Last Mirror Synchronization (see page 164)
2. Extract Package Metadata from the Repository (see page 150)
3. View Debian Packages from Web Console (see page 151)

View the Status of Last Mirror Synchronization

You can view the status of the last synchronization to verify whether the mirror synchronization was successful.

Follow these steps:

1. Verify the engine logs to ensure that the inventory collect task ran at least once from the time the mirror was last synchronized.
2. Navigate to Computers and Users, All Computers, *mirror computer*, Inventory, System Status, External Repositories.

   The External Repositories page appears.
3. View the value of the following parameter to know the status:

   Last Sync Result

   Specifies the result of last mirror synchronization. A successful synchronization returns 0 and a failure returns a non-zero value.

   If the synchronization failed, follow these steps:

   a. Deploy the FetchMirrorLog procedure in the CA DSM Agent add-on for Debian Mirror 1.0 package on the computer that failed the synchronization.

   b. Verify the job status under All Computers, *computer name*, Jobs, Software Jobs.

   c. Right-click the FetchMirrorLog procedure job, select Properties and click the Job Output tab.

      The mirror synchronization log is displayed.

Extract Package Metadata from the Repository

Extracting package metadata from the repository lets you view the Debian package details on DSM Web Console.

Note: The following steps apply for extracting the package metadata from both master and mirror repositories.

Follow these steps:

1. Navigate to Control Panel, Engines, All Engines, SystemEngine from DSM Explorer.

   The engine log is displayed.

2. Right-click the SystemEngine and select Add New Task.

   The New Task Wizard opens.

3. Follow the instructions and perform the following steps in the wizard:

   a. Select the task type as CA Repository Extraction, and enter a task name and description. Click Next.

      Note: Ensure that you disable the system firewall to execute the task successfully.

   b. Provide the following details:

      Note: As the repository server is on Linux, values provided in the following Distribution and Components Name fields must be case-sensitive; they must match the case in the repository server. For example, if the repository server location for ftp://172.16.0.12/ubuntu/dists/lucid/main/binary-i386/, the distribution name must be specified as lucid and not as Lucid or LUCID.

      Repository Name

      Specifies the repository name from which you want to extract the package metadata. The list displays the repositories you had defined in the Repositories configuration table.

      Note: You cannot create two engine tasks with the same repository and distribution combination.

      Host Name

      Specifies the host name of the repository. This field is enabled only for repositories of type Mirror-Template. For the master and mirror repositories, the host name is automatically taken from the Repositories configuration table.

Distribution

Specifies the distribution from which you want to extract the package details.

Note: An engine task can extract data only from a single distribution. If you want to extract data from multiple distributions, create additional engine tasks.

Components Name

Specifies the components that you want to extract. Click Add to add more components.

c. Specify scheduling options.

4. Click Finish on the last page.

   The System Engine creates the task and executes it at the schedule time. You can monitor the task by clicking the SystemEngine and review the status in the Task List section on the right pane.

   Note: You can also browse the repository from Web Console while the engine task is still in progress. The Web Console displays the distributions and packages as and when they are extracted from the repository.

Browse the Debian Repository from Web Console

You can browse the contents of a Debian repository in Web Console to know what packages are present in the repository.

Follow these steps:

1. Log in to DSM Web Console.
2. Navigate to Console, Software, External Repositories, *repository*.

   A list of distributions in the selected repository is displayed. The Synchronization Status column shows the status of the repository extraction task. You can also click View under the Synchronization Log column to view the progress of metadata extraction and errors that are encountered, if any.

   Note: If you open the repository before the extraction task completes, it is possible that you do not see all the distributions in the list.

3. Click a distribution.

   A list of Debian packages in the distribution is displayed.

Setting Up FTP or HTTP Share for Software Packages and OS Images

For Kubuntu deployments, you are required to set up FTP or HTTP share to store software packages and OS images.

See *Setting Up FTP or HTTP Share for Software Packages and OS Images* section in OSIM Administration Guide for more information.

Configuration Parameters for Managing Debian Packages

CA ITCM delivers new configuration parameters to manage Debian packages. Navigate to DSM, Software Delivery, Agent to use these parameters.

- Debian Job Check: Job execution timeout
- Debian Repository: APT commands logging level
- Debian Repository: Autoremove packages
- Debian Repository: Execution of Post-Actions
- Debian Repository: Execution of Pre-Actions
- Debian Uninstall Behavior: Reinstall the packages

For more information about a parameter description, see the configuration policy description in DSM Explorer.

Install the debmirror Utility

The debmirror utility synchronizes a Debian mirror repository from the parent repository. Install the debmirror utility on computers hosting the mirror repository to be able to synchronize the mirrors.

Install debmirror on Ubuntu OS

Execute the following command to install the debmirror utility on Ubuntu OS:

```
sudo apt-get install debmirror
```

On successful execution of the command, the debmirror utility is installed.

Install debmirror on RedHat or SUSE

This section describes how you can set up a Debian mirror on RedHat or SUSE computers. As DSM scalability servers are not supported on Debian, you can set up mirrors of the Debian system on RedHat or SUSE computers.

Verify Prerequisites

Verify the following prerequisites before you set up a Debian mirror:

- Perl 5.14 or later is installed on the target computer.
- The master server from which the repository is going to be mirrored is already configured. For example, if debmirror uses the HTTP download method, configure the master server to expose a virtual directory of the repository. Similar configurations are required for FTP, if used.

Download Perl Scripts for using Debmirror

Debmirror is a perl script that mirrors Debian repositories on RedHat or SUSE computers. Debmirror requires certain perl modules to be present.

Follow these steps:

1. Verify that the following perl modules are present:
   - LockFile::Simple;
   - Compress::Zlib;
   - Digest::MD5;
   - Digest::SHA;
   - Net::INET6Glue;
   - LWP::UserAgent

   Few of the perl modules come with default installation. If the modules are not available, install the modules using one of the following approaches:

Approach 1: Using the cpanminus tool

a. Install cpanminus tool that downloads perl modules. Do one of the following actions to install the cpanminus tool:
   - Run the cpan App::cpanminus command.
   - Run the RPM package for cpanminus, which can be downloaded from the following location:

     http://rpmfind.net/linux/rpm2html/search.php?query=cpanminus

b. Run the following command to install the required perl modules:

   ```
   cpan m <module-name>
   ```

   Examples:

   To install LockFile::Simple module, run the cpanm LockFile::Simple command.

   To install Net::INET6Glue module, run the cpanm Net::INET6Glue command.

   The command downloads the perl modules from Internet and installs the modules. This command automatically resolves dependencies.

c. Verify that the Perl modules are installed.

Approach2: Using the src packages

a. Download the perl module package tar from http://www.cpan.org/modules/index.html.

b. Extract the tar.

c. Run the perl MakeFile.PL command. This command generates a makefile.

d. Run the make command.

e. Run the make install command.

Note: Ensure that you resolve the dependencies manually. For example, Net::INET6Glue depends on the Socket6 module. Verify that you install Socket6 before installing Net::INET6Glue. You can find the dependencies at the following location:

http://deps.cpantesters.org/

f. Verify that the Perl modules are installed.

Note: For Approach 1 and Approach 2, verify that gcc is installed on the RedHat or SUSE computers.

Approach3: Using the rpm sources

a. Search for the following perl modules on the Internet and install the modules using YUM:

- perl-Compress-Zlib-1.42-1.fc6
- perl-Digest-SHA1-2.11-1.2.1.i386.rpm
- perl-LockFile-Simple-0.206-1.el5.rf.noarch.rpm
- perl-Digest-MD5-M4p-0.01-1.2.el5.rf.i386.rpm

Note: If you do not find the libnet-inet6glue-perl module on the Internet, download the source files and build the binaries manually using approach 2.

b. Verify that the Perl modules are installed.

Install debmirror

Install the debmirror utility on computers hosting the mirror repository to be able to create mirrors of the master Debian repository.

Follow these steps:

1. Get the latest debmirror (currently debmirror_2.14ubuntu1.tar.gz) src from http://archive.ubuntu.com/ubuntu/pool/universe/d/debmirror/.
2. Extract the tar file and copy the debmirror perl script to "/usr/bin" location on the RHEL/SUSE computer.
3. Run the debmirror command.

Chapter 6: Integration with Data Transport Service

Data Transport Service (DTS) is a data transfer management tool that lets you control the flow of data transfers in your software delivery environment. Using DTS, you can establish a data transport network topology that consists of machine objects and define preferred routes for data transport.

For further information about DTS functionality and settings see the *Data Transport Service Administration Guide* that is available as part of the online documentation for CA ITCM.

This section contains the following topics:

Using DTS with Software Delivery

Data Transport Service (DTS) can be used to facilitate the transfer of software delivery objects between enterprise manager and domain manager, domain manager and scalability server, domain manager and agents, and scalability server and agents.

The performance of the managed DTS file transfers has been improved by redesigning internal mechanisms and minimizing the number of processes launched.

This redesign benefits all managed file transfers between the enterprise manager and domain manager, the domain manager and scalability server, the domain manager and agent, and the scalability server and agent, as well as the deregistration of software packages from the software library of the scalability servers.

If you perform an upgrade of CA ITCM, all file transfers must be completed. If file transfers are active during an actual upgrade of a manager, they are lost.

DTS between Managers and Scalability Servers

Data Transport Service (DTS) is integrated with software delivery (SD) functionality so that you can optimize the SD usage of your network to your requirements. This is achieved through the definition of a network topology that consists of your managers and any intermediate scalability servers. The fanout role of the scalability servers, resulting in a single read with multiple sends and multiple writes, can be handled through DTS. It can also use point-to-many, which means a single read, a single send, and multiple writes can be performed. However, for fanout or point-to-many to work, the transfer objects involved must have certain property values in common. Hierarchical relationships can be established between the managers that determine how data is distributed.

DTS provides a finely tunable, unlimited fanout hierarchy. Using the enhanced fanout and routing capabilities of DTS helps you build efficient networks.

DTS between Domain Managers and Agents

Data Transport Service (DTS) can be installed on software delivery (SD) agents to enhance the connection possibilities between these agents and the domain manager.

Once DTS has been installed on an SD agent, NOS-less DTS download can be used. The SD manager supports mix and match. It can simultaneously use the SD built-in file transfer to SD agents without DTS installed, and DTS file transfer to agents with DTS installed.

The integration of software delivery functionality with DTS provides the following benefits:

- State-of-the-art multicast and broadcasting technology to reduce network congestion.
- Mobile users using intermittent connections to a corporate network can rely on the automated checkpoint and restart capabilities of DTS to ensure the integrity of the data they receive.
- Secure information transfer capabilities to enhance data integrity.

DTS Components Installed with Software Delivery

The following sections list the Data Transport Service components that are installed when you install software delivery functionality.

DTS Components on Windows

Data Transport Service (DTS) components are automatically installed on the enterprise manager, domain managers, and scalability servers on Windows, however, on the agents a different behavior applies, as follows:

- **Enterprise Manager:**

  DTS Network Object Server (NOS), Transfer Object Server (TOS), Schedule Object Server (SOS) and DTS agent are installed.

- **Domain Manager:**

  DTS Network Object Server (NOS), Transfer Object Server (TOS), Schedule Object Server (SOS), and DTS agent are installed.

- **Scalability Server:**

  DTS agent is installed.

- **Agent:**

  On Windows, the DTS functionality is not contained in the software delivery agent plug-in, but in a separate installation package. That means, if you need the DTS functionality, for example, to use the DTS download method for a specific agent, you must deploy the separate DTS installation package to that agent.

  Note: As the DTS agent is installed through a separate installation package, you need to remove it separately when you uninstall the software delivery agent.

DTS Components on Linux and UNIX

Data Transport Service (DTS) is automatically installed on the Linux or UNIX enterprise manager, domain managers, scalability servers, and agents:

Enterprise Manager:

DTS Network Object Server (NOS), Transfer Object Server (TOS), Schedule Object Server (SOS), and DTS agent are installed.

Domain Manager:

DTS Network Object Server (NOS), Transfer Object Server (TOS), Schedule Object Server (SOS) and DTS agent are installed.

Scalability Server:

DTS agent is installed.

Agent:

DTS agent is installed.

Note: The behavior of Data Transport Service is controlled by settings in a configuration policy.

Enabling and Disabling DTS

To enable or disable the DTS NOS-less download method for agents, simply right-click one or multiple agents or a group of agents in the DSM Explorer and select or deselect Software Jobs, Download Method, DTS - NOS-less. As a result of this, the software delivery (SD) functions will not use this particular download method when pushing software to be installed by the SD agent.

Another method for changing the download type from the agent is as follows: Use the command "sd_acmd SetDownloadMethod <DTS | NONE | NOS>" or set it from the advanced software delivery Properties on the agent computer (Software Delivery: Request a specific Network Operating System (NOS)).

It is not possible to disable the use of DTS between managers and scalability servers, as it is the only supported transport between those parts of the SD network.

DTS Method of Operation

When jobs are set up to agents connecting with scalability servers, the domain manager first checks if the package in question already has been stored in the Software Package Library of the scalability server. If this is the case, the copy is sent to the agent using Data Transport Service (DTS). If the package is not available in the Software Package Library on the scalability server, the package is transferred from the Software Package Library on the domain manager. Once the DTS file transfers of the software packages are completed, the job orders are sent to the scalability server for the agents execution. Once the job has completed, the files downloaded for the job are deleted.

Chapter 7: Diagnostics and Troubleshooting Software Delivery

Some of the most common questions encountered with software delivery functionality and components are considered in this chapter; and details about how to resolve potential problems are provided. Read this information before contacting CA Technologies's Technical Support.

This section contains the following topics:

Identify Build Number of CA ITCM

To identify the build number of the installed CA ITCM components run the following command from the DOS command prompt:

```
dsmver
```

Check the Application Framework Plug-ins

If you encounter software delivery problems, you should first check if all services are up and running. For this purpose run the "caf status" command.

Following is an example for a manager system:

```
caf status
Querying caf for status information...
CA DSM r12 Common Application Framework 12.xx.xx.xx

Showing running DSM services...
[1]  Asset Management manager (ammanager)
[2]  Asset Management performance agent (ampmagent)
[3]  Asset Management server (amrss)
[4]  Asset Management usage server (amms)
[5]  Certificate exchange plugin (cfcertex)
[6]  Common Server (cserver)
[7]  Common object manager (cmobjectmanager)
[8]  Configuration agent (ccnfagent)
[9]  Configuration and State Management agent (ccsmagt)
[10] Configuration and State Management agent controller (ccsmact)
[11] Configuration and State Management database api server (ccsmapi)
[12] Configuration and State Management server (ccsmsvr)
[13] DSM Service Locator plugin (cfsvclocator)
[14] Data Transport network object server (dtsnos)
[15] Data Transport schedule object server (dtssos)
[16] Data Transport transfer agent (dtsagent)
[17] Data Transport transfer object server (dtstos)
[18] Deployment Manager (dmdeploy)
[19] Engine (SystemEngine)
[20] Event notification plugin (cfnotify)
[21] File transfer server (cfftplugin) (transfers job output)
[22] Notification Server (cfnotsrvd)
[23] Port multiplexer (pmux)
[24] Registration plugin (cfregister)
[25] Remote Control host agent (rchost)
[26] Remote Control manager (rcmanager)
[27] Remote Control server (rcserver)
[28] Session messaging server (smserver)
```

```
[29] Software Delivery boot server (sdmpcserver)
[30] Software Delivery manager: api server (sdmgr_api_0)
[31] Software Delivery manager: dialog manager (sdmgr_dm)
[32] Software Delivery manager: file transfer (sdmgr_ft)
[33] Software Delivery manager: installation manager (sdmgr_im)
[34] Software Delivery manager: task manager (sdmgr_tm)
[35] Software Delivery server (sdserver)
[36] tomcat server (tomcat)
```

The CAF services in bold are software delivery-specific.

If you find a service to be down, you may start it explicitly, for example:

```
caf start sdserver
```

In this case, you should check the log file to find out why the service terminated.

RAL Extraction Task Hangs

When the firewall is enabled on the computer that runs the RAL extraction task, add java.exe file to the firewall exception list.

For example, if CA ITCM is installed in a default location, add the following path to the firewall exception list:

C:\Program Files (x86)\CA\SC\JRE\1.7.0_17\bin\java.exe

Software Deployment Jobs Occasionally Hang on Citrix XenDesktop Streamed Virtual Machines

Symptom:

When I create a software deployment job container with 15 or more jobs and deploy the container to 15 or more machines, the software deployment job hangs on some machines. The job is not completed. caf status sdagent displays *cfPluginWorkerProcess is waiting for Messages.*

Solution:

Override the default value and assign an appropriate value to the Software Delivery configuration setting, Scalability Server: "Concurrency: Maximum number of simultaneously executing agents on Scalability Server." This action ensures that the number of agents that are connected to the Scalability Server and executing jobs is optimally managed.

Use a value 10 for the above configuration parameter for a deployment job container with 15 jobs each on all 15 computers.

Note: The default value is 25 and the optimal value for this setting is dependent on external factors like network latency, memory and CPU resources available. If the jobs still hang, reduce the value further.

Log File Collection Tool dsminfo

CA Technologies provides the dsmInfo tool, which collects diagnostic information from systems that have CA ITCM installed. The data collected is compressed into a single file that contains log files, system information, directory structures, and registry and environment information. This diagnostic tool is available in the CA ITCM product installation media under the DiagnosticTools folder.

If a problem with CA ITCM is reproducible, then run the following command to change the trace level to DETAIL:

```
cftrace -c set -l DETAIL
```

Reproduce the problem and collect the diagnostic information with the dsmInfo tool.

Notes:

For more information about this tool, see the DSMInfoReadMe.txt file available under the DiagnosticTools folder in the product installation media.

The dsmInfo tool produces ".7z" files by default. These files provide better compression than zip files, so uploading to CA Technologies is easier.

Log Files for CAF Services

The common application framework (CAF) services log their activities into log files. The degree of detail depends on the trace level, which can be customized. The log files support you in analyzing problems.

The trace level is set to ERROR by default. If you need to get more trace information you may want to set the trace level, for example, for software delivery functionality or Data Transport Service to DETAIL by running the cftrace command as follows:

```
cftrace -c set -f USD -l DETAIL -s 30000
```

or

```
cftrace -c set -f DTS -l DETAIL -s 30000
```

The -s option sets the log file size to 30,000 KByte size. The default size is 2,000 KByte, which might be too small for the DETAIL trace level. (The trace file will be overwritten, when the size limit and the number of configured trace files is reached.)

Note: For the list of trace settings run the cftrace command as follows:
`cftrace list`

On Windows, the log files for all CAF services are located at *install_dir*\logs (Default: c:\Program Files\CA\DSM\logs).

Log files created during installation of CA ITCM are located under your user temp folder. Usually, the environment variable %temp% points to this directory.

On Linux, the log files for all CAF services are located at $CA_ITRM_BASEDIR/logs (Default: /opt/CA/DSM/logs).

Log files created during installation of CA ITCM are located under /opt/CA/installer/log.

Software Delivery Log Files

Software delivery-specific activities are logged in the following trace files (n is the number of the file):

Manager:

File Name	Description/Comment
TRC_USD_APISERVER_*i*_n.log	*i* is the SD API Server instance number
TRC_USD_DIALOGM_n.log	Not Applicable

File Name	Description/Comment
TRC_USD_INSTMAN_n.log	Not Applicable
TRC_USD_MPCWORKER_n.log	Not Applicable
TRC_USD_SDAGENT_n.log	Not Applicable
TRC_USD_SDMGRFT_n.log	Not Applicable
TRC_USD_SDMSIEXE_n.log	Windows only
TRC_USD_SDSERVER_n.log	On domain manager only
TRC_USD_SSCMD_n.log	On domain manager only
TRC_USD_SXP_n.log	Not Applicable
TRC_USD_TASKMAN_n.log	Not Applicable
TRC_MIGRATION_USD_n.log	Migration log file

Scalability Server:

File Name	Description/Comment
TRC_USD_SDSERVER_n.log	Not Applicable
TRC_USD_SXP_n.log	Not Applicable
TRC_USD_SSCMD_n.log	Not Applicable
TRC_USD_SDAGENT_n.log	Not Applicable
TRC_USD_SDMSIEXE_n.log	Windows only
TRC_USD_MPCWORKER_n.log	OSIM Boot Server

Agent:

File Name	Description/Comment
TRC_USD_SDAGENT_n.log	Not Applicable
TRC_USD_SDMSIEXE_n.log	Windows only
TRC_USD_SXP_n.log	Not Applicable

Data Transport Service Log Files

If you encounter problems when running Data Transport Service (DTS) transfers, there are some log files that you can check in error situations. You can also use the trace facilities.

The following DTS log files are created (*n* is the number of the file):

Manager:

File Name	Description/Comment
TRC_DtsTos_*n*.log	DTS Transfer Object Server log file
TRC_DtsNos_*n*.log	DTS Network Object Server log file
TRC_DtsSos_*n*.log	DTS Schedule Object Server log file
TRC_DTS_*n*.log	SDDTSFT log file
TRC_DtsAgent_*n*.log	DTS Master Agent log file
TRC_DtsAgent*m*_*n*.log	DTS Slave Agent log files; *m* is the number of the DTS slave agents
TRC_DtsBrowser.log	DTS browser log file

Scalability Server and Agent:

File Name	Description/Comment
TRC_DtsAgent_*n*.log	DTS Master Agent log file
TRC_DtsAgent*m*_*n*.log	DTS Slave Agent log files; *m* is the number of the DTS slave agents

Setting up DTS Transfer:

The following log files are created by software delivery functions that set up DTS transfers.

File Name	Description/Comment
TRC_USD_DTSFT_*n*.log	For deliveries to Staging Libraries

Registration of Large Software Packages in the DSM Explorer Takes a Long Time

Symptom:

When I register a large software package in the DSM Explorer, the package registration takes a long time to register the package, and the DSM Explorer session does not let me perform any other task during that period.

Solution:

While registering a large software package in the DSM Explorer, the package registration might take some time depending on the package size, server hardware configuration, remote or local DSM Explorer, and load on the server. If you want to perform any other task in the DSM Explorer when the DSM Explorer is busy performing a resource-intensive operation (such as registration of a large software package, listing numerous job containers, and so on), you can open a new DSM Explorer session and perform the required task.

Migrated Query Produces Different Results

With the attribute 'Type' (in the attributes group 'Target') and its values 'Machine' and 'Staging Server', queries behave differently in Unicenter Software Delivery 4.0 and CA ITCM. The reason is that in version 4.0 the agent on the Local Server was of the type 'Machine', whereas in CA ITCM the agent on the domain manager is of the type 'Staging Server'.

In Unicenter Software Delivery 4.0, a query "Target.Type='Machine'" would return all agents (no Staging Servers), including the Local Server's own agent. When this query is migrated to CA ITCM, it will return only standalone agents, that is, agents that have no scalability server or domain manager on the same machine.

In Unicenter Software Delivery 4.0, a query "Target.Type='Staging Server'" would return all Staging Servers. When this query is migrated to CA ITCM, it will also return the domain manager, as its agent is considered to be a Staging Server.

Software Catalog and Scalability Server Move

The Software Catalog gets the network address of the domain manager to connect to from the configuration storage (comstore) using the following configuration parameter:

itrm/agent/units/./currentmanageraddress

This parameter is populated every time the agent registers with its scalability server.

If the scalability server is moved to a new domain manager, that is, registered with a new domain manager and deregistered from the original domain manager, all agents which connect through that scalability server will have this parameter set to the address of the original manager until the agents register with the scalability server again.

As a consequence, the Software Catalog will not work properly until the agent reregistration has occurred and the above mentioned configuration parameter has been correctly populated.

How Do I Know SD Agent Bridge Is Running?

Symptom:

I need to verify that SD Agent Bridge is indeed running. How do I do this?

Solution:

The SD Agent Bridge is fully integrated with the software delivery scalability server. If the software delivery scalability server is running and the SD server policy "Backward compatibility support" is enabled, SD Agent Bridge is running.

Task Manager Fails to Run in Concurrent Mode

Symptom:

I have configured the Task Manager to run in concurrent mode, but it is still running in non-concurrent mode.

Solution:

The reason for the Task Manager to run in non-concurrent mode despite configuring it to run in concurrent mode is that the Task Manager is unable to start the Policy Manager and Replication Manager. You must restart the Task Manager plug-in (sdmgr_tm) to run the Task Manager in concurrent mode.

To restart the Task Manager using the DSM Explorer, click the Stop Engine link in the Tasks portlet (Control Panel, Engine, All Engines, System Delivery Engine) and then click the Start Engine link to restart the Task Manager. You can also use the CAF command to restart the Task Manager. You can see the detailed information about this failure in the TRC_USD_TASKMAN.log file.

However, if this issue occurs repeatedly, contact CA Technical Support.

Installation Manager Fails to Run in Concurrent Mode

Symptom:

I have configured the Installation Manager to run in concurrent mode, but it is still running in non-concurrent mode.

Solution:

The reason for the Installation Manager to run in non-concurrent mode despite configuring it to run in the concurrent mode is that the Installation Manager is unable to start the Notification Manager. You must restart the Installation Manager plug-in (sdmgr_im) to run the Installation Manager in concurrent mode. You need to use the CAF command to restart the Installation Manager. You can see the detailed information about this failure in the TRC_USD_INSTMAN.log file.

However, if this issue occurs repeatedly, contact CA Technical Support.

apt Commands Used for Deployment

To deploy the wrapper packages, CA ITCM uses the following apt commands:

- Installing the wrapper package:

  ```
  apt-get -y install <Pk1> <PK2> <PK3>
  ```

- Reinstalling the wrapper package:

  ```
  apt-get --reinstall -y install <Pk1> <PK2> <PK3>
  ```

- Uninstalling the wrapper package:

  ```
  apt-get -y purge <Pk1> <PK2> <PK3>
  ```

To deploy the add-on procedures in the CA DSM Agent Add-on for Debian Mirror package on the repository clients, CA ITCM uses the following commands:

- AutoRemove dependencies:

  ```
  apt-get -y autoremove
  ```

- Clean local cache:

  ```
  apt-get clean
  ```

- Update cache:

  ```
  apt-get update
  ```

- Upgrade Debian packages:

  ```
  apt-get -y upgrade
  ```

Purging RAL Records from MDB

To purge obsolete RAL records in MDB, invoke the RAL Purge command. This command works component-wise and purges the components listed in the command. It can also purge distribution and repository server details under the following conditions:

- When a distribution is empty after purging of components is complete
- When a repository server has no distributions after purging of distributions is complete.

For example, the Lenny distribution has two components, testing and main, which are extracted by the RAL engine task. To remove the records in the testing component, remove or disable synchronization engine tasks using DSM Explorer and invoke the purge command manually at the %RALHOME% folder as follows:

```
java -jar ral.jar -purge ftp://testing-i25361/debian/ lenny testing MASTER DEBIAN
"Enterprise Debian Repository"
```

This command has the following format:

```
java -jar ral.jar -purge -uri uri -distribution distribution -component component
-type type -format format -name repository name -desc description -log log path
```

URI

Specifies the URI of the Debian repository server.

Example:

RAL.jar -purge –uri ftp://testing-i25361/debian/ -distribution lenny –component testing –type MASTER –format DEBIAN –desc "Enterprise Debian Repository"

Distribution

Specifies the distribution that contains the component that you want to delete. You can use this parameter only if the format is DEBIAN.

Component

Specifies the component that you want to delete. Use commas to separate multiple components.

Type

Specifies the type of the repository as Master repository or Mirror.

Format

Specifies the repository format.
Valid value: DEBIAN

Name

Specifies the repository server name of the component that you want to delete. The name must match the repository name in the Repositories configuration table.

Desc

(Optional) Specifies the repository description as entered in the Repositories configuration table.

Log

(Optional) Specifies the log file path. If you do no specify the path, a log file is created in <DSM Install Path>\logs folder. The log file for purge operation would be RAL_purge_log.log.

Important! Verify that no synchronization engine tasks run during the purge operation. Also, verify that no users browse or create wrapper packages during the purge operation.

Cannot Register My Legacy Agent

Symptom:

I cannot register my legacy agent with CA ITCM after enabling the Agent Bridge.

Solution:

After enabling your Agent Bridge configuration policies, you have to wait for several minutes before you can register your legacy agent.

Cannot Start Unicenter Software Delivery Agent on HP-UX System

Symptom:

I have successfully installed a Unicenter Software Delivery 4.0 SP1 agent in an HP-UX 11.11 operating environment running CA ITCM with Agent Bridge enabled, but the sdpgm start command fails.

Solution:

The problem is that libcawinext.sl is missing from the shared components library path. To resolve this, add a link to libcawinext.sl so that it is included in SHLIB_PATH (and LD_LIBRARY_PATH):

```
cd /opt/CA/SharedComponents/lib
ln -s /opt/CA/SharedComponents/cawin/lib/libcawinext.sl.0 libcawinext.sl

SHLIB_PATH=/opt/CA/UnicenterSoftwareDelivery/usd/lib:
        /opt/CA/SharedComponents/lib:
        /opt/CA/SharedComponents/lib
```

Now you can start up the Unicenter Software Delivery agent.

RAC Container Job Fails

Symptom:

I reinstalled my legacy agent after a crash, and received an "Already installed" message when I ran the RAC container job.

Solution:

When a legacy agent is reinstalled after crashing (RAC), the execution of the jobs in the automatically-created RAC container may fail with the “Already installed” message. In this case, delete the RAC job container; the agent automatically becomes operational.

Virtual Application Software Package Deployment Fails

Symptom:

When I attempt to deploy a virtual application software package, the deployment fails and I receive the following error message: "ERROR (*number*) Install *package_name* failed." What do I do now?

Solution:

To troubleshoot an error while deploying a virtual application software package, perform the following steps:

1. Navigate to the Computers and Users, All Computers, *computer_name*, Jobs, Software Jobs folder.

   The right pane displays the available software delivery jobs.

2. Select the job that failed, right-click, and select Properties.

   The Job Properties dialog appears.

3. View the Status Message on the Computer Job tab.

4. Open the Job Output tab and view the trace information.

   Note: There is no trace information shown if the deployment is successful.

5. Scroll down to the Starting postprograms section.

   This section displays information related to virtual application package installation.

6. View the postprogram return code. The following list includes all return codes and their meanings:

   -1

   Indicates an internal error with wrong or incomplete parameters (install script not executed).

   0

   Indicates successful termination (no error).

   1

   Indicates that the process could not find the DSM installation (files, directories, registry keys, or environment were not found).

   2

   Indicates that the process could not create or remove files or folders.

3

Indicates that the process could not find required files for the package (for example, .sft files for Microsoft App-V packages).

4

Indicates that the creation or removal of net shares failed.

5

Indicates that the process could not restart App-V services.

6

Indicates that the execution of sftmime.exe (App-V) or ThinReg.exe (VMware ThinApp) failed. These required tools create or remove links (icons) on the desktop and entries in the Start > Programs menu.

7

Indicates that the process failed to connect to the ThinApp streaming server.

7. View the command line that caused the deployment failure in the Action output of installation section of the trace information. Scroll right to view the command line parameters and return code.
8. Determine the cause of the error and fix the problem.
9. Redeploy the virtual application software package.

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 and are part of a WORKGROUP rather than a domain.

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.

SD Agent Does not Start after a CAF Restart

Valid on Windows and UNIX

Symptom:

When you start CAF, the SD agent does not initiate automatically. Hence, the SD job check does not run on CAF restart.

Solution:

Do the following:

- On the CAF Scheduler, change the default value of the random now time field to 0 seconds.
- Verify that the default value of the CAF: Enable registration on start-up configuration policy is true.

Note: On UNIX, CAF register does not run all the plug-ins. Use the CAF register all command to run all the plug-ins.

Variables in debconf Parameters are not Preseeded

During deployment, the software delivery agent preseeds the debconf parameters with the values you specify during the creation of wrapper packages. The agent does not preseed debconf parameters when you assign them variables such as ${choices}.

Perform the following steps to preseed a variable with known values:

1. Navigate to DSM Explorer, Computer, Software, Software Package Library, All Software, *Debian wrapper package*, Source, *New Volume*, debWrpMetadata.wdp.
2. Double-click and edit the wdp file as required.

Installation of Debian Wrapper Package Fails

Symptom:

When I install a Debian Wrapper package, installation fails with the following error:

WARNING: The following packages cannot be authenticated!

Solution:

Perform one of the following steps:

- Create a configuration file for APT commands to allow unauthenticated packages to be installed. On the agent computer, add the following text in one of the APT configuration files or create a new file under */etc/apt/apt.conf.d*:

```
APT {
   Get {
    AllowUnauthenticated "true";
   };
}
```

- Import the public key to the agent computer using the apt-key add command. For a large-scale import of the key, create a software delivery package.

Debian Wrapper Package Fails to Install

Symptom:

I installed a Debian wrapper package but the package failed to install.

Solution:

Do the following:

- Verify that the package size or hash is not changed from the index file.
- Verify that the package is present in the repositories mentioned in sources.list.
- Verify that all package dependency is fulfilled.
- Verify that runtime errors do not appear during installation.

SD Job Hangs and the Message Is Not Displayed

Symptom:

When I deploy the Interactive DM Script SD package, the SD job check hangs and the message box is not displayed.

Solution:

You can fix this in any *one* of the following ways:

Editing *itemproc.dat* of SD Package:

If a DM script is pushed to an agent as part of SD job, which has an interactive window, add *w_dms* flag to the procedure options of the package.

1. Open the itemproc.dat file in the package and identify the procedures that are interactive.
2. Go to [Itemproc*X*] section (where *X* is the number of the procedure which is interactive).
3. Modify the Parameters key and append the value -w_dms at the end.

Using Procedure Properties from DSM Explorer:

1. In the install procedure of the package which is interactive, right click the procedure name, navigate to Properties, Embedded File tab, Parameters.
2. Add -*w_dms.*

SD job is successful and the message box is displayed.

Windows Interactive Services Detection Locks the Agent

Valid only on Windows

Symptom:

When I deploy an interactive software package using the Windows Interactive Services Detection , the agent is locked if the session is idle for more than one minute.

Solution:

This behavior is due to the limitation of Windows Vista and above Operating Systems. To continue with the deployment, login again and choose the session 0.

DebWrap Package Type is Missing in DSM Reporter

The software package type for Debian wrapper packages is identified by numerical 10 instead of DebWrap as the package type.

Abort Command Fails during Reinstallation of VDI Components

Symptom:

When I use the command line to abort a reinstallation of the VDI compoenents, the abort process does not initiate.

Solution:

You cannot initiate multiples instances of the SD agent at the same time. Abort the reinstallation by using the Abort button on the agent dialog box.

Appendix A: Non-UTF-8 Locale Support and Localization

This section contains the following topics:

UTF-8 and MBCS Encoding

UTF-8 (8-bit Unicode Transformation Format) is a way of encoding characters so that every possible character can be represented using a variable number of bytes. On UNIX, it is treated like any other multi-byte character set and is backwards compatible with the ASCII character set.

CA ITCM code on Linux and UNIX is generally operating in a UTF-8 locale. This causes problems interfacing with the operating system, if the operating system is using a non-UTF-8 locale. All code that interfaces with the operating system, such as file names, command line parameters, and so on is converting in between the system MBCS locale and UTF-8.

A multi-byte character set (MBCS) uses 1 or 2 bytes per character and is used for character sets that contain large numbers of different characters (for example, Asian language character sets).

Localization and UTF-8 Encoding

The only way that localization can work out fully is if all the involved computers use UTF-8 encoding or the exact same locale. This applies to the whole chain, from the manager to the scalability server down to the agent. It is thus preferable to use UTF-8 everywhere. Not doing so and sending out jobs containing files and directories that contain National Language Characters (NLCs), can result in failed jobs.

On Linux versions that do not support the CIFS file system, the Samba protocol may not work correctly when trying to access files and directories that contain NLCs. This means that jobs, that succeed in mounting the file shares, may fail because they cannot access files and directories that contain NLCs. The software delivery functions automatically detect, if CIFS is available and use it whenever possible.

SuSE 9 ES and RedHat 4 support CIFS, but SuSE 9 Pro and RedHat 3.x do not.

Non-UTF-8 Locale Support Feature

The non-UTF-8 locale support feature provides internal utilities that help to solve National Language Character (NLC) problems with localization on Linux and UNIX.

National Language Characters are characters that are special to a certain locale.

Scalability Server Considerations

The following list provides considerations of individual scalability server use cases:

- On a scalability server, when having a non-UTF-8 system and using Samba, it is vital that it is configured correctly (note that YaST2 in SuSE does not do this correctly). It is very important that the setting “unix charset” is set correctly (in the “global” section of smb.conf). A good value may be "iso8859–15" which works well on western locales. If you forget this setting, all the files are shown. However, if a directory name contains National Language Characters (NLCs), you are able to see it and go down into it, but you are not able to see any of the files that it contains. From the user perspective, the jobs will fail. After changing any such setting, make sure to reload Samba.
- By design, if a Linux scalability server is configured to use NFS and Samba, the agents will use Samba. On the scalability server, use the commands “sd_sscmd addshare” or “sd_sscmd removeshare” to set this up properly.
- Samba and NFS pose different problems when it comes to file and directory names. Samba has an internal mechanism that maps the file and directory names for us, if we tell Samba that we (as an agent) are using UTF-8 (or non UTF-8). The name mapping will be performed discretely. NFS, however, has no such mechanism, and this can cause problems when connecting for instance a non UTF-8 agent to a UTF-8 scalability server (or conversely) and trying to access file and directory names that contain NLCs. Unfortunately, there is no way around this (except to use Samba instead of NFS).
- On a scalability server, where Samba file share is used, it may be a good idea to set up the library access (sd_sscmd libraryaccess …) properly in order for access to the Samba file share to work for Linux agents using CIFS.

  This problem is related to the Samba security configuration setting. When the agents try to mount the share on the scalability server using CIFS, they only succeed in mounting it as guest user (which is the default when no library access has been provided), if the Samba scalability server is configured to use shared-level security.

  If however, the Samba scalability server is configured to use another security type, like user-level security, the mounting with CIFS as anonymous user will not work since it requires an explicit user, along with the correct password. Furthermore, the user must have been added to the Samba user file with the smbpasswd -a command.

The reason to enforce the use of CIFS (mount -t cifs) if possible is that it handles NLCs in a much better way than the usual SMB (smbmount).

We suggest that administrators configure their scalability servers as follows:

- sd_sscmd libraryaccess …

  This sets up the credentials for software delivery that are used when sending jobs to agents.

- smbpasswd -a …

  This sets up the credentials in Samba itself.

- Open smb.conf using an editor and remove (or comment out) the line “guest ok = Yes” on the shares “sdlibrary” and “sdmsilib”. Also, for security reasons, the security setting (in the global section), should not be set to "share" (which is the default) but to “user” (or better) instead. Refer to the manl page of smb.conf for the exact meaning of all the Samba scalability server settings.

- Reload Samba, as follows:

  /etc/init.d/smb reload

  The new settings are activated.

Note: If this configuration step is not done, the jobs will likely function anyway since the fallback solution, the Internal NOS-less transport mechanism, steps in. Internal NOS-less may not be as efficient as using Internal NOS, but it will work.

Linux systems that seem to work out-of-the-box include SuSE 9 ES; Linux systems that do not work out-of-the-box include RedHat 3 ES and RedHat 4 ES.

Appendix B: Importing Unicenter Software Delivery 4.0 Query Strings

This section contains the following topics:

Overview

CA ITCM uses Unicenter Software Delivery 4.0 formatted query strings in the following areas to support backward-compatibility:

Command Line Interface

The command to create computer groups accepts Unicenter Software Delivery 4.0 formatted query string to create a dynamic group.

Software Packages

Importing software packages containing procedure prerequisites created in Unicenter Software Delivery 4.0 accepts formatted query strings.

Software Packager

The CA ITCM Software Packager uses Unicenter Software Delivery 4.0 formatted query strings to create procedure prerequisites for software packages it creates.

Note: All the above areas create custom queries in the CA ITCM query subsystem because of certain query import limitations. In addition, queries that have been migrated from version 4.0 to Unicenter DSM r11.x using the migration tools are imported as custom queries.

Query Import Limitations

Software Delivery uses queries in a number of places to automate the management of assets. Starting with Unicenter DSM release 11, a new query mechanism that is common to all the DSM components replaces the 4.0 query sub system. The new SQL-based query mechanism gives performance improvements over the code-based legacy evaluation mechanism. Also, starting with Unicenter DSM r11, a new basic hardware inventory mechanism that is common to all of DSM replaces the inventory module of Unicenter Software Delivery 4.0. The new basic hardware inventory module offers more accurate inventory. However, some of the Unicenter Software Delivery version 4.0 attributes are not collected by the CA ITCM inventory module.

These changes have the following high-level impact on the query import:

Query Attributes

When you import a 4.0 formatted query string into CA ITCM, it is not possible to map all the query attributes to equivalent CA ITCM attributes. CA ITCM will import invalid queries with empty expressions marked as invalid for informational purposes. You must modify these queries before performing an import.

Computer Users

The CA ITCM query subsystem recognizes computers and user profiles as individual target types for queries. This means that a query can return either a set of computers or a set of user profiles but not both. In version 4.0, computers and user profiles were represented by one target type allowing a query to return both computers and user profiles. When you import a version 4.0 formatted query string into CA ITCM, the ability to return both computers and user profiles is maintained through the creation of a custom query. Custom queries are pure SQL statements that are not directly compatible with the query building functionality of the Query Designer. Therefore, you need to modify the custom queries using the Edit SQL feature of the Query Designer rather than using the Insert Argument feature.

Wildcard Characters

CA ITCM uses SQL wildcards; the LIKE operator replaces the MATCH operator in Unicenter Software Delivery 4.0 and all other wildcard characters are mapped to the SQL equivalents where possible. However, some of the wildcard characters such as '?', '+' and '|' have no equivalent in SQL; the 'set negation' [^ ….] is not supported and produces an invalid query.

Attribute Values

Some attribute values have changed in CA ITCM. In many cases, a simple mapping is possible to convert the version 4.0 values embedded in queries to the new values. In other cases, this is not possible because the number of values used in CA ITCM and version 4.0 may not match; in some cases an '=' or '<>' operator can be replaced with LIKE and some wildcards added to the literal. In this case, operators other than '=' or '<>' produce an invalid query.

This limitation specifically applies to the Target attribute group with the attribute values such as Machine, Staging Server, Domain, and UserId. It also applies to the Name attribute of attribute groups SDAttr_OS2, SDAttr_WinNT, SDAttr_WinCE, SDAttr_unix, SDAttr_Win9X, SDAttr_Netware, and SDAttr_VMS.

In the case of the attribute Type (in the Target attribute group) with the values 'Machine' and 'Staging Server', queries behave differently in Unicenter Software Delivery version 4.0 and CA ITCM. The reason for this is, in version 4.0 the agent on the Local Server was of the type 'Machine' whereas in CA ITCM the agent on the domain manager is of type 'Staging Server'.

Query Results

In Unicenter Software Delivery 4.0, a query "Target.Type='Machine'" returns all agents (no Staging Servers) including the Local Server's agent. When this query is imported to CA ITCM, it returns only standalone agents (agents that have no scalability server or domain manager on the same machine).

In Unicenter Software Delivery 4.0, a query "Target.Type='Staging Server'" returns all Staging Servers. When this query is imported to CA ITCM, it also returns the domain manager, as its agent is considered to be a Staging Server.

Import of Expressions Containing OS Security or Directory Lookups

When you import a Unicenter Software Delivery version 4.0 formatted query string that contains NTGroup source or the Directory source, authorities are added to the URI strings. These are machines names for the local authorities used with NTGroup and directory authorities used with Directory. These authorities may be incorrect in the new environment where you are using the Manager. In this case, you can edit the query after import and change the authority name.

To change the authority name, open the Properties dialog of the query, right-click the SQL fragment, and select Edit SQL. Replace the authority name with the correct one.

Import of Expressions Using IN and NOT IN Operators

The IN/NOT IN operations of Unicenter Software Delivery version 4.0 involve using a plug-in to provide a set of values instead of the single literal used for the other operations. The Unicenter Software Delivery version 4.0 plug-in sources and their equivalent functionalities in CA ITCM are as follows:

- SDGroup
- NTGroup
- AMOQuery
- DirectoryService

The SDGroup plug-in functionality is provided by standard CA ITCM queries that use computer group definitions.

NTGroup is implemented using the Directory services feature of CA ITCM queries. The allowed attribute group is Target and the allowed attributes in that group are User and UserId.

For IN/NOT IN tests against sets produced by Directory Services enquiries, the allowed attribute group is Target and the allowed attributes in that group are User, UserId, Name, Server, and Machine.

For IN/NOT IN tests against sets produced using the Unicenter Software Delivery version 4.0 query integration with Asset Management, the allowed attribute group is Target and the allowed attributes in that group are User, UserId, Name, Server, and Machine.

Import of Expressions Not Using IN and NOT IN Operators

The following table lists the supported and unsupported attributes in each attribute group that do not contain expressions using IN or NOT IN operators; the unsupported attributes will not be imported successfully:

Import of Expressions Not Using IN and NOT IN Operators

The following table lists the supported and unsupported attributes in each attribute group that do not contain expressions using IN or NOT IN operators; the unsupported attributes will not be imported successfully:

Attribute group	Supported Attribute	Unsupported Attribute
SDAttr_AgentConfig	Not Applicable	Status
SDAttr_AgentConfig	LibraryAccess	Not Applicable
SDAttr_AgentConfig	Not Applicable	PalmSupport
SDAttr_AgentConfig	Not Applicable	WinCESupport
SDAttr_AgentConfig	Not Applicable	NokiaSupport
SDAttr_AgentConfig	Not Applicable	UserAgent
SDAttr_AgentConfig	Not Applicable	LogonShield
SDAttr_AgentConfig	Not Applicable	LogoffPolicy
SDAttr_AgentConfig	Not Applicable	operationalMode
SDAttr_LogonShield	Not Applicable	Status
SDAttr_LastUpdated	Date	Not Applicable
SDAttr_LastUpdated	Not Applicable	Time
SDAttr_Win3x	Not Applicable	Name
SDAttr_Win3x	Not Applicable	Version
SDAttr_Win3x	Not Applicable	StartupFreeMem
SDAttr_Win3x	Not Applicable	Mode
SDAttr_Win3x	Not Applicable	Locale
SDAttr_Win3x	Not Applicable	ANSI_CP
SDAttr_Win3x	Not Applicable	OEM_CP
SDAttr_OS2	Name	Not Applicable
SDAttr_OS2	Version	Not Applicable
SDAttr_OS2	Not Applicable	StartingFreeMemory
SDAttr_WinNT	Name	Not Applicable
SDAttr_WinNT	Version	Not Applicable
SDAttr_WinNT	Not Applicable	StartupFreeMem

Attribute group	Supported Attribute	Unsupported Attribute
SDAttr_WinNT	Not Applicable	Locale
SDAttr_WinNT	Not Applicable	ANSI_CP
SDAttr_WinNT	Not Applicable	OEM_CP
SDAttr_WinNT	Not Applicable	Build
SDAttr_WinNT	ServicePack	Not Applicable
SDAttr_WinNT	Not Applicable	Type
SDAttr_WinCE	Name	Not Applicable
SDAttr_WinCE	Version	Not Applicable
SDAttr_WinCE	Not Applicable	StartupFreeMem
SDAttr_WinCE	Not Applicable	Locale
SDAttr_WinCE	Not Applicable	ANSI_CP
SDAttr_WinCE	Not Applicable	OEM_CP
SDAttr_WinCE	Not Applicable	Build
SDAttr_WinCE	Not Applicable	ServicePack
SDAttr_WinCE	Not Applicable	Type
SDAttr_WinCE	Not Applicable	DeviceName
SDAttr_WinCE	Not Applicable	OriginalDeviceName
SDAttr_WinCE	Not Applicable	ProxyName
SDAttr_Unix	Name	Not Applicable
SDAttr_Unix	Not Applicable	Version
SDAttr_Unix	Not Applicable	Locale
SDAttr_Unix	Not Applicable	ANSI_CP
SDAttr_Unix	Not Applicable	OEM_CP
SDAttr_Unix	PhysicalMem	Not Applicable
SDAttr_Win9x	Name	Not Applicable
SDAttr_Win9x	Version	Not Applicable
SDAttr_Win9x	Not Applicable	LoggedOnUser
SDAttr_Win9x	Not Applicable	StartupFreeMem
SDAttr_Win9x	Not Applicable	Locale

Attribute group	Supported Attribute	Unsupported Attribute
SDAttr_Win9x	Not Applicable	ANSI_CP
SDAttr_Win9x	Not Applicable	OEM_CP
SDAttr_Win9x	Not Applicable	Build
SDAttr_Win9x	ServicePack	Not Applicable
SDAttr_Netware	Name	Not Applicable
SDAttr_Netware	Version	Not Applicable
SDAttr_Netware	Not Applicable	MachineName
SDAttr_Netware	Not Applicable	NetworkNumber
SDAttr_Netware	Not Applicable	NodeAddress
SDAttr_Netware	Not Applicable	Locale
SDAttr_Netware	Not Applicable	ANSI_CP
SDAttr_Netware	Not Applicable	OEM_CP
SDAttr_VMS	Name	Not Applicable
SDAttr_VMS	Version	Not Applicable
SDAttr_VMS	Memory	Not Applicable
SDAttr_NokiaAdminSuite	Not Applicable	Name
SDAttr_NokiaAdminSuite	Not Applicable	Version
SDAttr_NokiaAdminSuite	Not Applicable	DeviceType
SDAttr_NokiaAdminSuite	Not Applicable	EPOCCommandVersion
SDAttr_NokiaAdminSuite	Not Applicable	LogFile
SDAttr_PCSystem	Not Applicable	Model
SDAttr_PCSystem	Not Applicable	SerialNumber
SDAttr_PCSystem	Not Applicable	BaseMemory
SDAttr_PCSystem	ExtendedMemory	Not Applicable
SDAttr_PCSystem	Not Applicable	BiosOEMName
SDAttr_PCSystem	Not Applicable	BiosRevision
SDAttr_PCSystem	Not Applicable	BiosDate
SDAttr_PCSystem	Processor	Not Applicable
SDAttr_PCSystem	Not Applicable	ProcessorDesc

Attribute group	Supported Attribute	Unsupported Attribute
SDAttr_PCSystem	Not Applicable	BusType
SDAttr_PCSystem	Not Applicable	DMAController
SDAttr_PCSystem	ProcessorCount	Not Applicable
SDAttr_PCSystem	ProcessorSpeed	Not Applicable
SDAttr_PCSystem	Not Applicable	MainBatteryStatus
SDAttr_PCSystem	Not Applicable	BackupBatteryStatus
SDAttr_PCSystem	Not Applicable	PowerSource
SDAttr_Unix_Processor	Not Applicable	Type
SDAttr_Unix_Processor	Not Applicable	SubType
SDAttr_Unix_Processor	Not Applicable	Description
SDAttr_Unix_Processor	ProcessorCount	Not Applicable
SDAttr_PhoneUnit	Not Applicable	Not Applicable
SDAttr_PCFloppy	Drive	Not Applicable
SDAttr_PCFloppy	Not Applicable	Capacity
SDAttr_PCFloppy	Not Applicable	Format
SDAttr_PCDisk	Drive	Not Applicable
SDAttr_PCDisk	Size	Not Applicable
SDAttr_PCDisk	Available	Not Applicable
SDAttr_PCDisk	Not Applicable	Name
SDAttr_PCDisk	Not Applicable	Type
SDAttr_PCMappedDrive	Not Applicable	Drive
SDAttr_PCCDROM	Drive	Not Applicable
SDAttr_PCDisplay	Not Applicable	DisplayAttached
SDAttr_PCDisplay	Not Applicable	SerialNumber
SDAttr_PCDisplay	Not Applicable	AdapterString
SDAttr_PCDisplay	Not Applicable	AdapterRam
SDAttr_PCDisplay	Not Applicable	AdapterBiosType
SDAttr_PCDisplay	Not Applicable	AdapterBiosDate
SDAttr_PCDisplay	Not Applicable	Resolution

Attribute group	Supported Attribute	Unsupported Attribute
SDAttr_PCDisplay	Not Applicable	Width
SDAttr_PCDisplay	Not Applicable	Height
SDAttr_PCDisplay	AdapterType	Not Applicable
SDAttr_PCKeyboard	Not Applicable	Type
SDAttr_PCKeyboard	Not Applicable	SerialNumber
SDAttr_PCSerialPorts	Not Applicable	NumberOf
SDAttr_PCParallelPorts	Not Applicable	NumberOf
SDAttr_PCMouse	Not Applicable	PointingDevice
SDAttr_PCMouse	Not Applicable	SerialNumber
SDAttr_MSNOS	Not Applicable	Name
SDAttr_MSNOS	Not Applicable	Version
SDAttr_MSNOS	Computername	Not Applicable
SDAttr_MSNOS	IPAddress	Not Applicable
SDAttr_MSNOS	Not Applicable	LoggedOnUser
SDAttr_MSNOS	Not Applicable	LoggedOnDomain
SDAttr_NovellNOS	Not Applicable	Name
SDAttr_NovellNOS	Not Applicable	VersionShell
SDAttr_NovellNOS	Not Applicable	NetworkNumber
SDAttr_NovellNOS	Not Applicable	NodeAddress
SDAttr_NovellNOS	Not Applicable	LoggedOnUser
SDAttr_IBMNOS	Not Applicable	Name
SDAttr_IBMNOS	Not Applicable	Version
SDAttr_IBMNOS	Not Applicable	Computername
SDAttr_IBMNOS	Not Applicable	LoggedOnUser
SDAttr_IBMNOS	Not Applicable	LoggedOnDomain
SDAttr_Win9xNOS	Not Applicable	Name
SDAttr_Win9xNOS	Not Applicable	LoggedOnDomain
SDAttr_PCNetworkAdapter	Not Applicable	Number
SDAttr_PCNetworkAdapter	Not Applicable	Type

Attribute group	Supported Attribute	Unsupported Attribute
SDAttr_PCNetworkAdapter	Not Applicable	Manufacturer
SDAttr_PCNetworkAdapter	Not Applicable	IDBytes
SDAttr_PCNetworkAdapter	Name	Not Applicable
SDAttr_Win9xNetworkAdapter	Not Applicable	Number
SDAttr_UnixNetworkAdapter	Name	Not Applicable
SDAttr_UnixNetworkAdapter	Not Applicable	Description
SDAttr_PCOtherAdapter	Not Applicable	Name
SDAttr_UnixVolume	Number	Not Applicable
SDAttr_UnixVolume	Capacity	Not Applicable
SDAttr_UnixVolume	Available	Not Applicable
SDAttr_UnixVolume	Label	Not Applicable
SDAttr_UnixVolume	Not Applicable	FileSystem
SDAttr_VMSVolume	Number	Not Applicable
SDAttr_VMSVolume	Capacity	Not Applicable
SDAttr_VMSVolume	Available	Not Applicable
SDAttr_VMSVolume	Label	Not Applicable
SDAttr_VMSVolume	Not Applicable	FileSystem
SDAttr_NFSLink	Not Applicable	RemoteName
SDAttr_NFSLink	Not Applicable	Capacity
SDAttr_NFSLink	Not Applicable	Available
SDAttr_NFSLink	Not Applicable	LinkName
SDAttr_VMSNFSLink	Not Applicable	RemoteName
SDAttr_VMSNFSLink	Not Applicable	Capacity
SDAttr_VMSNFSLink	Not Applicable	Available
SDAttr_VMSNFSLink	Not Applicable	LinkName
SDAttr_Win9xProtocol	Not Applicable	Name
SDAttr_Win9xProtocol	Address	Not Applicable
SDAttr_MacAddress	MACAddress	Not Applicable
Installation	ItemName	Not Applicable

Attribute group	Supported Attribute	Unsupported Attribute
Installation	ItemVersion	Not Applicable
Installation	ItemProcedure	Not Applicable
Installation	State	Not Applicable
Installation	Date	Not Applicable
Installation	Not Applicable	Time
Installation	Not Applicable	OrderedBy
StagingLibrary	ItemName	Not Applicable
StagingLibrary	ItemVersion	Not Applicable
StagingLibrary	State	Not Applicable
StagingLibrary	Date	Not Applicable
StagingLibrary	Not Applicable	Time
StagingLibrary	Not Applicable	OrderedBy
Target	Name	Not Applicable
Target	Type	Not Applicable
Target	Address	Not Applicable
Target	OS	Not Applicable
Target	Registration date	Not Applicable
Target	Not Applicable	RegistrationTime
Target	ChangedDate	Not Applicable
Target	Not Applicable	ChangedTime
Target	User	Not Applicable
Target	Phone	Not Applicable
Target	Location	Not Applicable
Target	ViaStagingServer	Not Applicable
Target	StagingServer	Not Applicable
Target	Comment	Not Applicable
Target	Calendar	Not Applicable
Target	DownloadMethod	Not Applicable

Attribute group	Supported Attribute	Unsupported Attribute
Target	SoftwareManagementSystem	Not Applicable
Target	Not Applicable	CoreName
Target	Server	Not Applicable
Target	Machine	Not Applicable
Target	Domain	Not Applicable
Target	UserId	Not Applicable
Target	UUID	Not Applicable
Target	PreviousLocalServer	Not Applicable
Target	RACPolicy	Not Applicable
Target	Not Applicable	Obsolete
SDAttr_DownloadMethod	Method	Not Applicable
SDAttr_AgentConfig	LibraryAccess	Not Applicable

Glossary

application

An *application* is a piece of software, for example, Microsoft Word.

application virtualization

Application virtualization is the encapsulation of an application, separating it from the underlying operating system on which it is executed. At runtime the application is tricked into acting as if it were directly interfacing with the original operating system and all the resources managed by it, but in reality it is not.

centrally managed environment

A *centrally managed environment* is one where the remote control domain manager controls the host settings through computer policies, global address book (GAB) items, licensing of the host agent on the domain, and user permissions. This is the default setting for CA IT Client Manager.

centrally managed host environment

A *centrally managed host environment* is one where either a remote control enterprise or domain manager is responsible for the configuration of the hosts and the authentication of viewer connections. It also manages the address book that users use to find hosts.

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.

configuration view

A *configuration view* is a customized Windows-only user interface that lets you edit configuration policies that are related to specific components or functionality. Configuration views summarize the relevant policies for a component or function independent of where they are actually located in the hierarchy and the DSM Explorer tree.

connectors

connectors are the links from products that consume connector data to external products, or *domain managers*. Each connector retrieves information from its domain manager and transmits the information through the connector framework to the consuming product for visualization and analysis. Connectors can also enact inbound operations on data in the source domain manager, such as object creation. connectors use a unified connector framework to enable integration with multiple consuming products.

desktop recompose

Desktop recompose is the process of assigning a new golden template to the virtual desktop. Operating systems and applications have to be maintained during their lifetime to fix problems resolved by hot fixes or service packs or to provide new features by new versions. For linked clones, this means the master image, or golden template, has to be updated. Once the updates are completed, the linked clone is recomposed and becomes active. During the recompose operation the related linked clones are linked to this new golden template and are refreshed.

desktop refresh

Desktop refresh is the process of resetting the virtual desktop to its original state. Linked clones track changes to the virtual machine with the clone. To control the storage allocations with the clone, VMware View offers the refresh operation that resets the clone to its baseline and releases all deltas provided for tracking changes. This means that all information stored to the system drive since the creation of clone or its last refresh or recompose is lost. Unlike desktop recompose, the same golden template continues to be used as before the refresh operation.

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.

Federal Information Processing Standard (FIPS)

Federal Information Processing Standard (FIPS) is a security standard that is issued and approved by NIST. It specifies the security requirements that must be satisfied by a cryptographic module utilized within a security system protecting sensitive but unclassified information.

FIPS-certified cryptography module

FIPS-certified cryptography module refer to RSA CryptoC BSAFE module, which is FIPS 140-2 certified.

FIPS-Compliant Cryptography

FIPS-compliant cryptography refers to the use of FIPS 140-2 certified modules, FIPS-approved, and FIPS-allowed techniques and algorithms for cryptography.

FIPS-only

FIPS-only is a mode of operation for CA ITCM wherein only FIPS-compliant cryptography is allowed. In this mode, CA ITCM is not backward compatible with the previous releases of CA ITCM.

FIPS-preferred

FIPS-preferred is a mode of operation for CA ITCM wherein bulk of cryptographic operations are FIPS-compliant, leaving few encryptions in legacy format. In this mode, CA ITCM is backward-compatible with the previous releases of CA ITCM.

golden template

In CA ITCM terminology, the *golden template* is the virtual machine from which virtual desktops are cloned.

guest

A *guest* in generic platform virtualization terminology is the virtual machine and the guest operating system.

guest operating system

The *guest operating system* is the operating system running inside a virtual machine.

health monitoring

Health Monitoring (HM) functionality lets you configure alerts, set threshold values, and monitor the overall health of the CA ITCM infrastructure.

host

A *host* in generic platform virtualization terminology is the physical machine, the host operating system, and the hypervisor.

host cluster

The *host cluster* is the aggregate computing and memory resources of a group of hosts sharing some or all of the same network and storage.

host operating system

The *host operating system* is the operating system running on a physical machine.

hosted virtual environment

A *hosted virtual environment* is the virtualization software that runs on top of a host operating system, that is, the physical machine, host OS, and the hypervisor.

hypervisor

The *hypervisor* is the virtualization software layer simulating physical hardware on behalf of the guest operating system. This term is synonymous with Virtual Machine Monitor (VMM).

instance software state database

The *instance software state database* is a part of the software state database that contains the history of all software jobs executed by the agent running on a non-golden template system, that is, any clones of the golden template.

linked clones

In VMware View, *linked clones* of a master or golden image only refer to the master or golden image but do not include it. Changes to the system during user sessions are not stored to the master image but are kept in delta files with the clone.

location awareness

Location Awareness lets DSM Agent on a computer detect the location of the computer.

master target device

In Citrix XenDesktop, a *master target device* is the base desktop with the OS and required set of applications from which a vDisk is generated.

master vDisk

In Citrix XenDesktop, a *master vDisk* is the initial vDisk generated from the golden template machine.

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.

native virtual environment

A *native virtual environment* is the virtualization software that runs directly on the physical machine, becoming or acting as a host operating system (often minimal), that is, the physical machine and the hypervisor. A synonymous term is "bare metal environment."

non-linked clones

In VMware View, *non-linked clones,* or full clones, are full copies of a master or golden image. The clone includes a copy of the image and all changes to the system during user sessions are stored to this copy.

nonpersistent clones

Nonpersistent clones are virtual desktops from the nonpersistent pool of VMware View user data that are transient out-of-the-box. Once a user logs off, the clone is refreshed and all user data at the system disk are lost.

nonpersistent linked clone virtual desktop

A *nonpersistent linked clone virtual desktop* is a virtual machine that is refreshed or recomposed every time the user logs on, with no persistence for custom installed applications, personalization, and so on.

offline patching

Offline Patching lets you export the patch content and patch files remotely and import to the CA ITCM environment using CA Patch Manager without accessing Internet.

Offline RAC

Offline RAC is a reinstall after crash (RAC) task that is driven by the agent rather than by the manager. Virtual desktops are *recomposed* frequently, that is, whenever the golden template is updated and the disk is reset, any changes to the virtual desktop since the previous reset are effectively voided. For virtual desktops, the agent and not the manager is responsible for the creation of the RAC job container. When the disk reset occurs, the agent initiates an Offline RAC to restore any software that has been deployed to the agent.

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.

package format

The *package format* is a property of a software package. Formats include regular and virtual.

package type

The *package type* is a property of a software package. Current types include Generic, MSI, SXP, PIF, and PKG. Package type is not used or altered for the purpose of supporting virtual application packages.

partition

A *partition* is an isolated instance of a host operating system. Partitions do not usually use guest operating systems because they all share the host's operating system.

partitioned virtual environment

A *partitioned virtual environment* is one where multiple instances of the host operating system can run in isolation on the same physical machine. This is not strictly a virtualization technology, but is used to solve the same type of problems.

persistent clones

Persistent clones are virtual desktops from the persistent pool that survive as they are after the user has logged off until they are refreshed or recomposed. VMware View offers out-of the box separate devices for system and user data with the persistent clones. Information stored to the user data device survives any refresh or recompose action while changes to the system disk are lost.

persistent linked clone virtual desktop

A *persistent linked clone virtual desktop* is a virtual machine that is dedicated to a specific user, and the user can request specific software to be added, customize settings, and so on. At each logon the user's customized environment is restored. This persists until the virtual desktop is refreshed or recomposed. At that point, all the software products installed on system drive are lost.

persistent non-linked clone virtual desktop

A *persistent non-linked clone virtual desktop* is a virtual machine that is dedicated to a specific user and is presented to that user at each logon with their custom installed applications, user settings, data, and so on.

platform virtualization

Platform virtualization is the encapsulation of computers or operating systems, hiding their physical characteristics from users and emulating the computing platform at runtime.

provisioned application

A *provisioned application* is an application (regular or virtual) that has been made available for execution on a target computer. The application need not be "installed" locally in order to treat it as provisioned.

regular application

A *regular application* is application software that has not been virtualized and can be installed and executed in a traditional fashion. When talking about releases, patches, and suites, regular applications are implied.

Replication

Replication is an engine task to perform the data replication from Domain Manager to Enterprise Manager and Enterprise Manager to Domain Manager.

sandbox

A sandbox is an application runtime environment that isolates the application from the computer's operating system and resources and also from other applications on the computer. The degree of isolation is usually set to allow the application some access to the operating system resources, such as the documents folder.

scalability server

A *scalability server* is the central server to enable geographical scalability for management tasks. It is a distributed process that is the primary interface for agents.

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

schema map

A *schema map* is a mapping of the attribute names associated with data objects, such as users, computers, and groups, used in an external directory to those attribute names used by corresponding CA ITCM objects. The fixed and standard set of DSM attribute names is used for querying directories and for formulating complex queries and reports.

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/.

software signature

A *software signature* defines the attributes of a software application, such as the main executable file name, other associated files, size range, version range, creation, and modification dates of the software. All these attributes of a software signature uniquely identify a software application. Software signatures in asset management are created as software definitions. You can create software definitions for a product, release, patch, suite, suite component, or virtual application image. By default, asset management provides predefined software signatures covering the most widely used software in the IT industry.

software type

The *software type* is a property of a software definition. Current types include suite, product, release, patch, and virtual application image.

staged virtual application image

A *staged virtual application image* is a virtual application image that has been discovered in the file system of a computer.

stand-alone environment

A *stand-alone environment* is one where the users of the host and viewer computers locally manage all settings, properties, and licensing of the CA ITCM remote control component. It is set by a Standalone Agent installation. To install it manually, the RC agent setup needs to be called directly.

standalone virtual application

A *standalone virtual application* is a virtual application that has been provisioned in a way where the virtual application image used as the source resides on the system to which it has been provisioned.

streamed virtual application

A *streamed virtual application* is a virtual application that has been provisioned in a way where the virtual application image used as the source resides on a remote system that is different from the system to which it has been provisioned.

streamed virtual application image

A *streamed virtual application image* is a virtual application image that has been discovered to be accessible through the network from a computer. Discovery of streamed virtual application images will usually only be possible if the virtual applications residing inside of the image have been provisioned.

vDisk

In Citrix XenDesktop, a *vDisk*, or virtual disk, is basically an image file with the OS and the required set of applications.

virtual application (VA)

A *virtual applicatio*n is software that has been virtualized.

virtual application image

A *virtual application image* contains one or more virtual applications stored inside a file, possibly with a set of supporting metadata files.

virtual application image definition

A *virtual application image definition* describes the "footprint" for discovering a virtual application image. To discover an image containing one or more included virtual applications (stored inside), regular software signatures must be associated with the virtual application image definition.

virtual application package (VAP)

A virtual application image packaged inside of one or more software delivery packages is referred to as a v*irtual application package*. These packages are used to provision computers with virtual applications.

virtual application staging package

A *virtual application staging package* is a virtual application package used to stage the virtual application image.

virtual application standalone package

A *virtual application standalone package* is a virtual application package used to provision a virtual application in standalone mode.

virtual application streaming package

A *virtual application streaming package* is a virtual application package used to provision a virtual application in streaming mode.

virtual disk

A *virtual disk* is a set of files that forms a file system that appears as a physical disk to the guest operating system.

virtual image

A *virtual image* is a file or set of of files containing the complete definition of a virtual machine, including its hardware specifications and virtual disks. It is the host's file system representation of a guest. A virtual image can be online or offline depending on the running state of the virtual machine it captures.

virtual machine (VM)

A *virtual machine* is an isolated virtualized environment simulating a physical machine. The virtual machine does by definition not include the guest operating system.

virtual patch

A *virtual patch* is the virtual equivalent of a regular patch and has the same basic meaning. The term is used when reporting software inventory for virtual applications (not virtual application images).

virtual release

A *virtual release* is the virtual equivalent of the regular release and has the same basic meaning. The term is used when reporting software inventory for virtual applications (not virtual application images). Note that a provisioned virtual application can use either a staged or streamed virtual application image as source. The virtual applications contained within the virtual application image can themselves be seen as staged but not yet provisioned.

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

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X