Microsoft

Microsoft System Center

Troubleshooting Configuration Manager

Rushi Faldu ▪ Manoj Kumar Pal ▪ Andre Della Monica ▪ Kaushal Pandey
Mitch Tulloch, Series Editor

PUBLISHED BY
Microsoft Press
A Division of Microsoft Corporation
One Microsoft Way
Redmond, Washington 98052-6399

Library of Congress Control Number: 2013952210
ISBN: 978-0-7356-8302-0

Microsoft Press books are available through booksellers and distributors worldwide. If you need support related to this book, email Microsoft Press Book Support at mspinput@microsoft.com. Please tell us what you think of this book at *http://www.microsoft.com/learning/booksurvey.*

The example companies, organizations, products, domain names, email addresses, logos, people, places, and events depicted herein are fictitious. No association with any real company, organization, product, domain name, email address, logo, person, place, or event is intended or should be inferred.

This book expresses the author’s views and opinions. The information contained in this book is provided without any express, statutory, or implied warranties. Neither the authors, Microsoft Corporation, nor its resellers, or distributors will be held liable for any damages caused or alleged to be caused either directly or indirectly by this book.

Acquisitions Editor: Anne Hamilton
Developmental Editor: Karen Szall
Project Editor: Karen Szall
Editorial Production: Diane Kohnen, S4Carlisle Publishing Services
Copyeditor: Andrew Jones
Cover Illustration: Twist Creative • Seattle
Cover Design: Microsoft Press Brand Team

Contents

Foreword

Ever since the client-server computing architecture became mainstream, IT pros around the world have been challenged and required to manage these servers and clients. As more client computers were introduced in IT environments and started playing a critical role in performing day-to-day tasks, the need to manage them became even more urgent. More importantly, these clients became an integral part of any business's productivity and started to perform more mission-critical tasks.

Today, the clients are becoming more powerful, smarter, and increasingly mobile. They have now become assets. As these assets grow in number, become more portable, and store critical business data, the risk to organizations increases. Now, more than ever before, there is a need for IT pros to manage, monitor, and secure these assets.

Windows Active Directory and Group Policy were the starting points for IT pros to secure some aspects of these assets. However, they weren't sufficient and didn't give IT pros the ability to manage the lifecycle of these assets.

In 1994, Microsoft introduced Systems Management Server (SMS) 1.0. It was the beginning of client management solution, but more in the non-Active Directory era. SMS 2003 truly ushered in an era of advanced client management that leveraged Active Directory and all of its functionality. The adoption and popularity of SMS has continued to grow since SMS 2003, and Microsoft has pushed the limits of the solution and its ability over time.

Microsoft System Center Configuration Manager 2007 changed the game with the vision of an integrated solution along with other System Center products. Microsoft introduced many new features and firsts with Configuration Manager 2007 and took client management to a whole new level with System Center 2012 Configuration Manager. Now, Configuration Manager (both 2007 and 2012) is an integral part of the IT infrastructure of many companies, and expertise with Configuration Manager has become one of the most sought after IT skills around the globe.

Microsoft Press and the authors of this book have a passion for helping IT pros working with Configuration Manager enhance their knowledge and make the most of the solution. The authors of this book are Microsoft Consultants from Microsoft Consulting Services (MCS) and Premier Field Engineers (PFE) from Microsoft Global Business Support (GBS) organizations with real field experience. The authors have come together to share their collective knowledge and experiences from both consulting and support in the field.

The authors have identified and chosen topics that are used on a daily basis by all Configuration Manager administrators around the world irrespective of the size and complexity of the solution or the industry it is deployed in. The authors have made an attempt to cover topics that are usually pain points for most Configuration Manager administrators. The authors have broken these into two books: *System Center: Configuration Manager Field Experience* and *System Center: Troubleshooting Configuration Manager.*

We hope you enjoy this book and the other one as much as the authors have enjoyed writing them, and that these resources help make the most of your System Center 2012 Configuration Manager solution.

Manish Raval

Consultant, Microsoft Consulting Services (MCS)

Introduction

As the authors of this book, we have tried provide you with insights and tips on troubleshooting System Center 2012 Configuration Manager drawn from our insider knowledge and real-world field experience. While most of you who are Configuration Manager administrators are fairly comfortable with the product and can perform common management tasks, many of you still have pain points when it comes to certain aspects of how the product works. Based on our observations and interactions with customers, the biggest knowledge gaps tend to be in the following areas:

- Troubleshooting common Configuration Manager tasks such as software distribution, software updates, and deployment.
- Understanding how the various components of Configuration Manager on both the server and client side work together when such tasks are performed.
- Dealing with the enormous number of log files that are generated on both the server and client side of Configuration Manager.

This book is our attempt to address some of these gaps and pain points. Chapter 1 provides insights into the Configuration Manager architecture and deployment principles. Chapter 2 familiarizes you with some of the key components of Configuration Manager and how they interact with each other when performing common tasks by using verbose logging for tracing the actions of various components. And Chapter 3 examines how to troubleshoot various Configuration Manager functionality including software and application deployment, site-to-site replication, software update and patching, operating system deployment, and Mac client issues.

Errata & book support

We've made every effort to ensure the accuracy of this content. Any errors that have been reported since this content was published are listed on our Microsoft Press site:

http://aka.ms/SCtrouble/errata

If you find an error that is not already listed, you can report it to us through the same page.

If you need additional support, email Microsoft Press Book Support at *mspinput@microsoft.com*.

Please note that product support for Microsoft software is not offered through the addresses above.

We want to hear from you

At Microsoft Press, your satisfaction is our top priority, and your feedback our most valuable asset. Please tell us what you think of this book at:

http://aka.ms/tellpress

The survey is short, and we read every one of your comments and ideas. Thanks in advance for your input!

Stay in touch

Let's keep the conversation going! We're on Twitter: *http://twitter.com/MicrosoftPress*.

CHAPTER 1

Configuration Manager site hierarchy and distribution points

Microsoft System Center 2012 Configuration Manager helps empower people to use the devices and applications they need to be productive, while maintaining corporate compliance and control. It accomplishes this with a unified infrastructure that acts like a single pane of glass to manage physical, virtual, and mobile clients. It also provides tools and improvements that make it easier for IT administrators to do their jobs.

A good understanding of basic Configuration Manager concepts, processes, and practices is essential for being able to effectively troubleshoot problems when they arise. This chapter provides an overview of the Configuration Manager site hierarchy including determining when to use a central administration site, primary site, and secondary site; inter-site replication; distribution points; Active Directory requirements for sites; Forest Discovery and Publishing; boundaries and boundary groups; and cross-forest scenarios. The chapter also describes some best practices for installing the central administration site, primary sites, and secondary sites; performing unattended installations of sites; and using Prerequisite Checker. The chapter then concludes with some troubleshooting tips concerning database replication and the Configuration Manager console.

Configuration Manager site hierarchy

The Configuration Manager site hierarchy consists of the following site system roles:

- Central administration site
- Primary sites
- Secondary sites

There are other Configuration Manager roles, such as management point, distribution point, and so on, but this chapter mainly focuses on these three roles.

Central administration site

When setting up a Configuration Manager hierarchy, the central administration site is the first one you must install. The central administration site is always on the top of the hierarchy and cannot be joined or moved to an existing hierarchy. You can have only one central administration site per hierarchy.

The central administration site coordinates inter-site data replication across the hierarchy by using Configuration Manager database replication. The central administration site also allows the administration of hierarchy-wide configurations for client agents, discovery performance, and other operations.

The following are some considerations when deploying a central administration site:

- Used for all administration and reporting for the hierarchy
- Used for administration purposes only
- Can support up to 25 child primary sites simultaneously
- Participates in SQL database replication
- Does not process client data and does not support client assignment
- Does not support a management point so no client can report to this site
- Not all site system roles are available

Primary sites

Primary sites can be used to manage clients in well-connected networks. Primary sites cannot be tiered below other primary sites.

The following are some considerations when deploying primary sites:

- Can be a stand-alone site or a member of a hierarchy
- Only supports a central administration site as a parent site
- Use database replication to communicate directly to their central administration site
- Automatically configures database replication with its designated central administration site
- Attached directly to the central administration site
- Only supports secondary sites as child sites
- Can support up to 250 secondary sites
- Are responsible for processing all client data from their assigned clients
- Can have up to 100,000 clients attached to them

Secondary sites

Secondary sites control content distribution for clients in remote locations across links that have limited network bandwidth. The following are some considerations when deploying secondary sites:

- Are used to host site system roles to offload WAN link traffic.
- Can only be installed (pushed) from the Configuration Manager console.
- Can communicate with clients but never have clients assigned to them. A management point and distribution point are automatically deployed during the site installation.
- Can distribute content to other secondary sites (new in Configuration Manager 2012).
- Cannot report to another secondary site.

Determining when to use a central administration site

You should install a central administration site if you plan to install multiple primary sites. Use a central administration site to configure hierarchy-wide settings and to monitor all sites and objects in the hierarchy. This site type does not manage clients directly, but it does coordinate inter-site data replication, which includes the configuration of sites and clients throughout the hierarchy.

You can manage all clients in the hierarchy and perform site management tasks for any primary site when you use a Configuration Manager console that is connected to the central administration site. The central administration site is the only place where you can see site data from all sites. This data includes information such as inventory data and status messages.

You should configure discovery operations throughout the hierarchy from the central administration site by assigning discovery methods to run at individual sites. You can manage security throughout the hierarchy by assigning different security roles, security scopes, and collections to different administrative users. These configurations apply at each site in the hierarchy. You can configure addresses to communicate between sites in the hierarchy. This includes settings that manage the schedule and bandwidth for transferring file-based data between sites.

Consider installing a central administration site for any of the following reasons:

- When more than one primary site is present in a hierarchy
- When you need to scale-up the number of clients that can be managed
- When you need to off-load reporting and administration from your primary site
- When you need to monitor and report from all sites and objects in the hierarchy

NOTE **A central administration site can be installed only as a new installation.**

Determining when to use a primary site

Consider installing a primary site for any of the following reasons:

- When you need to manage clients directly.
- When you need to increase the number of clients you can manage. Each primary site can support up to 100,000 clients.
- When you need to reduce the possible result of failure of a single primary site.
- When you need to provide load-balancing support for clients across multiple servers.
- When you need to provide a local point of connectivity for administration.
- When you need to meet organizational management requirements. For example, you might install a primary site at a remote location to manage the transfer of deployment content across a low-bandwidth network.

Determining when to use a secondary site

Consider installing a secondary site for any of the following reasons:

- When a local administrative user is not required in a location
- When you need to manage the transfer of deployment content across low-bandwidth networks
- When you need to manage the transfer of client data across low-bandwidth networks
- When you need to establish tiered content routing for deep network topologies

Understanding site-to-site replication

Site-to-site replication is running behind the scenes when you create a collection, a package, or folders on a central administration site. The central administration site replicates that information using database replication to primary sites, and then the primary sites replicate their secondary sites.

The basic concepts and components involved in the process of replication of global and site data are as follows.

- **Database replication** Performs all non-content related site-to-site transfer of information such as inventory data, status messages, and Windows Server Update Services (WSUS) metadata. When you deploy a secondary site, Microsoft SQL Server Express is installed and used for replicating Configuration Manager data. In Configuration Manager, database replication is now used for replication between sites in all cases except for when data flows from a secondary site to a primary site; for that process the file-based replication employed by Configuration Manager 2007 is still used. In addition, file-based replication is used to initialize/re-initialize database replication by copying exported SQL data to another site server.

- **Global data** Global data is replicated to all primary sites but only a subset of it is replicated to secondary sites.
- **Site data** Site data is replicated between the primary site where clients are assigned and the central administration site.
- **Content** The content replicated to child sites includes software deployment packages and software update packages.

NOTE **If a data discovery record (DDR) is newly generated by Active Directory System Discovery in a child primary site, it is sent to the central administration site in the standard way by passing the DDR record up the hierarchy. After the DDR has been added to the database at the central administration site, any updates to the DDR information will use database replication to replicate.**

Global and site data

The differences between global and site data can be summarized as follows:

- Global data objects are replicated everywhere and consist of collections and their rules, packages, CIs, software updates, deployment data, and so on.
- Site or local data is replicated only between the primary site that created it and the central administration site. Site data, in general, is the data created by the system, for example data concerning collection membership (built by Collection Evaluator component) or hardware inventory (built by the client and processed by data loader).

Database replication

Configuration Manager database replication transfers data quickly and guarantees delivery by using SQL Service Broker (SSB) and SQL Change Tracking. However, this has nothing to do directly with SQL database replication technology from a Configuration Manager standpoint.

Database replication in Configuration Manager is more reliable than the file-based replication used in Configuration Manager 2007 which is based on file transfer using the Server Message Block (SMB) protocol. Configuration Manager 2007 environments sometimes used to experience site-to-site communication issues caused by anti-virus software when the customer environment did not have the proper filter configured in their anti-virus scanning software.

Database replication in Configuration Manager has the following characteristics:

- It can be one-way (for example, site data) or bi-directional (for example, global data).
- Site data is replicated from a primary site to a central administration site.
- Global data is replicated to all site servers. For example, a collection created on one primary site will show up in another primary site because the collection rule is global data.

File-based replication

As described previously, file-based replication is still used in certain circumstances by Configuration Manager. During the file-based replication process, files are transferred using the SMB protocol and TCP port 445. Filed-based replication works like this:

1. The sending component places a file into the Replmgr's outbound folder.
2. Replmgr creates a job file and places it into the Ready folder.
3. Scheduler picks up the job file and creates the sending request file, and generates the compressed files, which will be sent to the tosend folder.
4. Based on the job priority and other settings, the scheduler triggers the sender to write the files from the tosend folder to the despooler folder on the receiving site server.

Understanding distribution points

A *distribution point* is a computer designed to deliver binary files/packages to Configuration Manager clients. Examples of such binary files can include applications, operating system deployment images, boot images, software updates, and so on.

In Configuration Manager, distribution points now use a new storage format called the content library. The content library replaces the SMSPKG shares as the default folder structure used to host content. The content library stores all content on the distribution point using single instance storage; this means each unique file is only stored once on the distribution point, regardless of how many times it is referenced by a package. In addition, the file is stored only once on the distribution point even if it is contained in multiple packages.

You should use a distribution point instead of a secondary site if:

- You are not concerned about network usage due to clients pulling policy or reporting status, inventory, or discovery to their primary site location. In this case you would use a distribution point instead of secondary site.
- You want to leverage Background Intelligent Transfer Service (BITS) access for clients, for example to use BranchCache, Operating System Deployment (OSD) multicasting, or Application Virtualization (APP-V) streaming.
- You find that client-side BITS does not provide enough bandwidth control for your WAN.

Active Directory requirements for sites

To install any Configuration Manager site, such as a central administration site, primary site, or secondary site, the server needs to be a member of an Active Directory domain. Though the Active Directory schema extension is optional, it is highly recommended that you extend the schema for Configuration Manager.

Active Directory schema extension

Extending the Active Directory schema is a forest-wide action and can only be done one time per forest. The following are some considerations for Active Directory schema extension in Configuration Manager environments:

- All Configuration Manager site systems must be members of an Active Directory domain.
- Configuration Manager Active Directory schema extensions provide many benefits for Configuration Manager sites, but they are not required for all Configuration Manager functions.
- If you have extended your Active Directory schema for Configuration Manager 2007, you do not have to update your schema for Configuration Manager.
- You can update the Active Directory schema before or after you install Configuration Manager.
- Schema updates do not interfere with an existing Configuration Manager 2007 site or clients.

Disjoint namespaces

A disjoint namespace happens when one or more domain member computers have a primary Domain Name Service (DNS) suffix that does not match the DNS name of the Active Directory domain of which the computers are members. For example, a member computer that uses a primary DNS suffix of corp.contoso.com in an Active Directory domain named na.corp.contoso.com is using a disjoint namespace.

The following are some considerations for disjoint namespaces in Configuration Manager environments:

- With the exception of out-of-band management, Configuration Manager supports installing site systems and clients in a domain that has a disjoint namespace.
- To allow a computer to access domain controllers that are disjoint, you must modify the msDS-AllowedDNSSuffixes Active Directory attribute on the domain object container. You must add both of the DNS suffixes to the attribute.
- To ensure that the DNS suffix search list contains all DNS namespaces that are deployed within the organization, you must configure the search list for each computer in a domain that is disjoint. Include in the list of namespaces the primary DNS suffix of the domain controller, the DNS domain name, and any additional namespaces for other servers with which Configuration Manager might interoperate. You can use Group Policy to configure the DNS suffix search list.

Single label domains

Single-label domain names are DNS names that do not contain a suffix such as .com, .corp, .net, or .org. For example contoso would be a single-label domain name while contoso.com, contoso.net, or contoso.local would not be single-label domain names. Configuration Manager does not support single-label domain names.

Extending the schema for Configuration Manager

You can extend the schema during setup, by using the Extadsch.exe command line tool, or by using the LDIFDE tool. The schema changes are stored in \SMSSETUP\BIN\x64\ConfigMgr_ad_schema.ldf

NOTE **The schema does not need to be extended again for Configuration Manager 2012 and later, if it has already been extended for Configuration Manager 2007.**

Forest Discovery and Publishing

In order to guarantee that clients are correctly assigned to Configuration Manager sites, and to guarantee that all software, software updates, and operating system images are available to Configuration Manager clients, it is necessary to make sure that the boundaries in Configuration Manager and Active Directory are correctly configured. Up-to-date boundary information results in efficient deployment of applications and software updates to managed client computers. Forest Discovery and Publishing helps clients not only discover the sites in the forest, but also publish existing sites that can manage clients across domains, thus eliminating the need to deploy additional sites.

Forest Discovery can discover IP subnets and sites in Active Directory and then add these as boundaries in Configuration Manager. Forest Discovery and Publishing can connect to all of your forests to build a complete map of your Configuration Manager environment. Forest Discovery and Publishing can also cross forest boundaries using specific credentials for each forest regardless of the trust type. The information obtained through Forest Discovery can be directly exported as either boundaries or boundary groups. Changes to discovered data are updated dynamically and aged out from the database when no longer present in Active Directory. The discovered data is also used when clients request a management point or distribution point to ensure they receive the best possible site for performance reasons. Credentials specified for each forest are used for both discovery and publishing and enable Configuration Manager sites to publish site information in both trusted and untrusted forests.

Publishing stores information, such as site system locations and capabilities, boundaries, and security information, required by client computers to establish trusted connections with site systems. It also stores information such as the client's trust relationship with the forest, and the management point's communication mode (HTTPS/HTTP) and the boundaries that are used to locate the most appropriate management point or distribution point to communicate with. This enables client computers to locate servers in a trusted forest to ensure user-targeted applications are successful.

IMPORTANT **As in Configuration Manager 2007, supernetting is not supported in Configuration Manager. However, when you run Active Directory Forest Discovery to discover your IP subnets it creates IP address ranges based on the subnet and mask defined in Active Directory.**

Boundaries and boundary groups

Boundaries represent network locations on the intranet where Configuration Manager clients are located. Boundary groups are logical groups of boundaries that provide clients access to resources. The sections below summarize some considerations concerning boundaries and boundary groups.

Boundaries

Each boundary represents a network location in Configuration Manager and is available from every site in your hierarchy. A boundary alone, however, does not enable you to manage clients at that network location. To manage a client, the boundary must also be a member of a boundary group. Boundaries can be any of the following:

- IP range
- IP subnet
- Active Directory site
- IPv6 prefix
- Boundary group for site assignment and/or content location

IMPORTANT **Overlapping site boundaries are supported for content location but are not supported for site assignment.**

Boundary groups

Boundary groups are used to manage your network locations. You must assign boundaries to boundary groups before you can use the boundary group. Boundary groups have the following functions:

- They enable clients to find a primary site for client assignment (automatic site assignment).
- They can provide clients with a list of available site systems that have content after you associate the distribution point and state migration point site system servers with the boundary group.
- To support site assignment, you must configure the boundary group to specify an assigned site for clients to use during automatic site assignment. To support content location, you must specify one or more site systems. You can only specify site systems with the distribution point or state migration point site system role. Both the site assignment and content location configurations are optional for boundary groups.
- When you plan for boundary groups, consider creating one set of boundary groups for content location and a second set of boundary groups for automatic site assignment. This separation can help you avoid overlapping boundaries for site assignment. When you have overlapping boundaries and use automatic site assignment, the site to which a client is assigned, might be too nondeterministic.

Cross-forest scenarios

Several cross-forest scenarios are possible when administering Configuration Manager environments:

- Simple client management in a different Active Directory forest. This scenario involves no object discovery, no added infrastructure, and manual client deployment.
- Managing clients using discovery and performing client push installations. This scenario involves cross-forest site publishing, cross-forest system discovery, and automated client installation. However, it does not add any additional infrastructure into the remote untrusted forest.
- Implementing child primary or secondary sites in a cross-forest environment. This requires a two-way forest trust.
- Installing site roles such as management point, software update point, and distribution point in a cross-forest environment.

Cross-forest tips

The following are some tips for cross-forest scenarios:

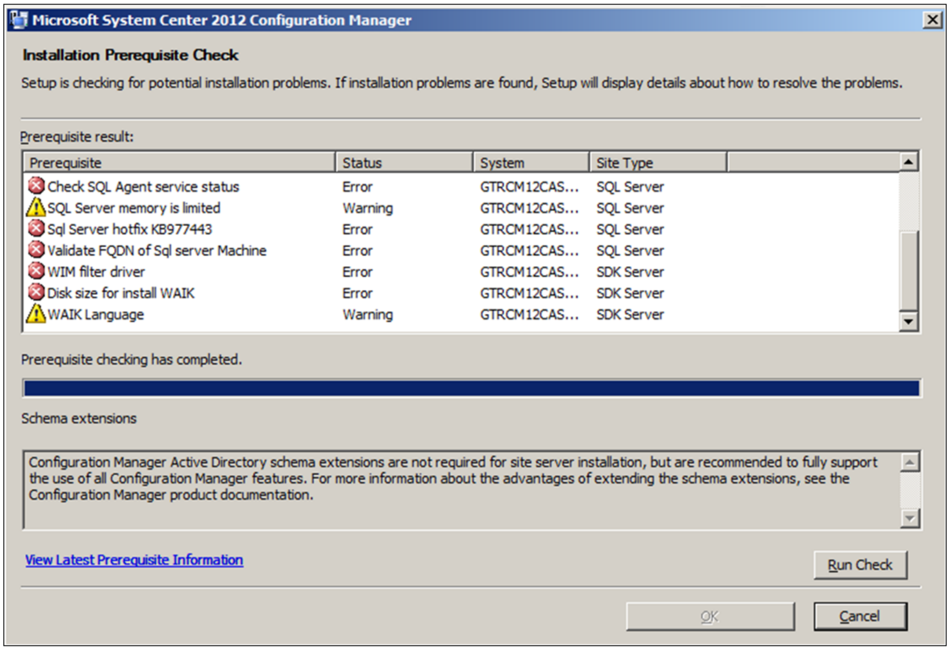
- Inner-site communication (site-to-site communication) can use both file-based replication (SMB Port 445) and database replication (TCP/IP port 4022 by default) so configure your perimeter network firewalls accordingly.
- Site system roles (management point, distribution point, and so on) with the exception of the out-of-band service point and the application catalog web service point can be deployed in an untrusted forest.
- The Server Locator Point (SLP) functionality is now performed by a management point.
- Each Configuration Manager site can only host two software update points, one for intranet located clients and one for internet located clients. This needs to be considered when designing a multiforest (non-trusted) Configuration Manager site.
- You can add the forest you need on the Configuration Manager console through the Active Directory Forest Discovery method.
- You can use Publish to publish information to the client's Active Directory forest.
- To install and configure a child site (primary or secondary), the child site server must be located in the same forest as the parent site or reside in a forest that contains a two-way trust with the forest of the parent (central administration or primary) site.

Client approval

After client installation, the client remains in an unapproved state if you are using the default setting Automatically Approve Computers In Trusted Domains. You will therefore need to approve such clients after their installation.

Using Prerequisite Checker

The Prerequisite Checker (prereqchk.exe) is a stand-alone application that verifies server readiness for a site server or specific site system roles. Before site installation, Setup runs the Prerequisite Checker (see Figure 1-1). You can manually run the Prerequisite Checker on potential site servers or site systems to verify server readiness. This allows you to remediate any issues that you find before you run Setup.



Installation Prerequisite Check

Setup is checking for potential installation problems. If installation problems are found, Setup will display details about how to resolve the problems.

Prerequisite result:

Prerequisite	Status	System	Site Type
Check SQL Agent service status	Error	GTRCM12CAS...	SQL Server
SQL Server memory is limited	Warning	GTRCM12CAS...	SQL Server
Sql Server hotfix KB977443	Error	GTRCM12CAS...	SQL Server
Validate FQDN of Sql server Machine	Error	GTRCM12CAS...	SQL Server
WIM filter driver	Error	GTRCM12CAS...	SDK Server
Disk size for install WAIK	Error	GTRCM12CAS...	SDK Server
WAIK Language	Warning	GTRCM12CAS...	SDK Server

Prerequisite checking has completed.

Schema extensions

Configuration Manager Active Directory schema extensions are not required for site server installation, but are recommended to fully support the use of all Configuration Manager features. For more information about the advantages of extending the schema extensions, see the Configuration Manager product documentation.

FIGURE 1-1 Error and warning messages are displayed in Prerequisite Checker.

When you run Prerequisite Checker without the command-line options, the local computer is scanned for an existing site server and only the checks that are applicable to the site are run. If no existing sites are detected, then all prerequisite rules are run.

You can run Prerequisite Checker from a command prompt and specify the specific command-line options to perform only checks associated with the site server or site systems specified in the command-line. When you specify another server to check, you must have Administrator rights on the server for Prerequisite Checker to complete the checks.

The following are some tips on using Prerequisite Checker:

- You must have Administrator rights on the server.
- Prerequisite Checker creates a log file ConfigMgrPrereq.log in the root of the C: drive.
- The following files are needed to run Prerequisite tool independently.
  - prereqchk.exe
  - prereqcore.dll
  - basesql.dll
  - basesvr.dll
  - baseutil.dll

  These files are located under <ConfigMgrSourceFiles>\SMSSETUP\BIN\X64\ folder.

Best practices for installing a central administration site or primary site

This section summarizes some best practices when installing a central administration site or a primary site.

Security rights

Before starting the central administration installation, verify that the administrative user who runs Setup has the following security rights:

- Local Administrator rights on the central administration site server computer
- Local Administrator rights on each computer that hosts one of the following:
  - The site database
  - An instance of the SMS Provider for the site
  - A management point for the site
  - A distribution point for the site
- Sysadmin (SA) rights on the instance of SQL Server that hosts the site database

Site naming

Be sure to plan your site codes and site names carefully before you deploy your Configuration Manager hierarchy. Configuration Manager site naming should adhere to the following guidelines:

- Site codes and site names are used to identify and manage the sites in a Configuration Manager hierarchy. In the Configuration Manager console, the site code and site name are displayed in the <*site code*> - <*site name*> format.
- Every site code that you use in your Configuration Manager hierarchy must be unique. If the Active Directory schema is extended for Configuration Manager, and sites are publishing data, the site codes used within an Active Directory forest must be unique even if they are being used in a different Configuration Manager hierarchy or if they have been used in previous Configuration Manager installations.
- During Configuration Manager Setup, you are prompted for a site code and site name for the central administration site, and each primary and secondary site installation. The site code must uniquely identify each Configuration Manager site in the hierarchy. Because the site code is used in folder names, never use Microsoft Windows reserved names for the site code, such as AUX, CON, NUL, or PRN.
- To enter the site code for a site during Configuration Manager Setup, you must enter three alphanumeric characters. Only the letters A through Z, numbers 0 through 9, or combinations of the two are allowed when specifying site codes. The sequence of letters or numbers has no effect on the communication between sites. For example, it is not necessary to name a primary site ABC and a secondary site DEF.

- The site name is a friendly name identifier for the site. Use only the standard characters A through Z, a through z, 0 through 9, and the hyphen (-) in site names.

IMPORTANT **Changing the site code or site name after installation is not supported.**

Evaluation media

If you install Configuration Manager as an evaluation edition, after 180 days the Configuration Manager console becomes read-only until you activate the product with a product key from the Site Maintenance page in Setup.

Best practices for installing a secondary site

This section summarizes some best practices when installing secondary sites.

Security rights

To create a secondary site, verify the user that runs Setup has the following security rights:

- Local Administrator rights on the secondary site computer
- Local Administrator rights on the remote site database server for the primary site (if it is remote)
- Infrastructure Administrator or Full Administrator security role on the parent primary site

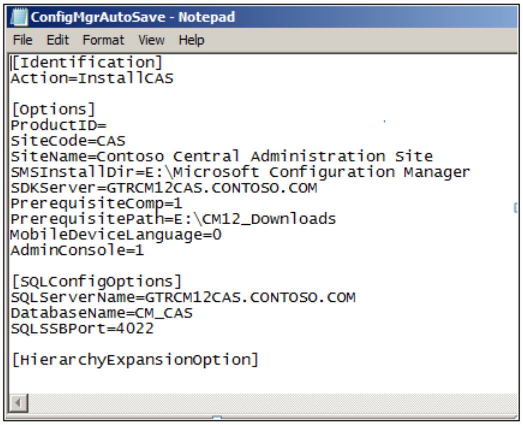
Other considerations

Some other considerations when installing secondary sites include:

- You need to specify a site code for the secondary site because it will be participating of the Configuration Manager hierarchy.
- When you choose the Use The Source Files At The Following Network Location or Use The Source Files At The Following Location On The Secondary Site Computer options, the location must contain the folder named Redist as a subfolder with the prerequisite redistributables, language packs, and the latest product updates for Setup.
- Use Setup Downloader to download the required files to the named folder Redist before you install the secondary site. Secondary site installation will fail if the files are not available in the Redist subfolder.
- Secondary site will use SQL Server Express or an existing SQL Server instance for the site database, and then configure the associated settings. Install and configure a local copy of SQL Express on the secondary site computer.

Unattended installation of a central administration site or primary site

By default, an unattended script named ConfigMgrAutoSave.ini is saved in the %TEMP% folder. Figure 1-2 shows an example of an unattended script.



```
[Identification]
Action=InstallCAS

[Options]
ProductID=
SiteCode=CAS
SiteName=Contoso Central Administration Site
SMSInstallDir=E:\Microsoft Configuration Manager
SDKServer=GTRCM12CAS.CONTOSO.COM
PrerequisiteComp=1
PrerequisitePath=E:\CM12_Downloads
MobileDeviceLanguage=0
AdminConsole=1

[SQLConfigOptions]
SQLServerName=GTRCM12CAS.CONTOSO.COM
DatabaseName=CM_CAS
SQLSSBPort=4022

[HierarchyExpansionOption]
```

FIGURE 1-2 An example of a sample unattended script.

Troubleshooting database replication and console issues

This section shares some experience gained from the field concerning troubleshooting database replication and console issues with Configuration Manager.

Troubleshooting database replication

As explained earlier in this chapter, Configuration Manager site-to-site communication uses the SSB feature to replicate data between the site databases instead of the file-based replication used in previous versions of Configuration Manager. With SQL replication, the performance and reliability is improved. However, as a result of this change, it might be a little more difficult for some Configuration Manager administrators to troubleshoot replication issues when they occur. This section provides some tips on how to troubleshoot SQL replication in Configuration Manager by using the following step-by-step approach:

1. Using Replication Link Analyzer
2. Examining the log files
3. Performing SQL queries
4. Reinitiating replication

Step 1: Using Replication Link Analyzer

Your first step for troubleshooting replication should be to use the Replication Link Analyzer. In the Configuration Manager console, start by viewing the current status of the replication links. When you have problems, the first place you should check is the Replication Link Analyzer.

1. Click Monitoring | Overview | Site Hierarchy.

   If the link icon is green, everything is fine. If it is not green, continue with this procedure to use the Replication Link Analyzer to troubleshoot.

2. Click Monitoring | Overview | Database Replication.
3. Select the link.
4. In the lower portion of the window, you can see the detailed status of this link. This information includes whether the replication is active, and the status of the global data replication link and the site data replication link.
5. Right-click the link name to open the Replication Link Analyzer Wizard.
6. Follow the wizard to remediate if necessary, and then review the result files:
   - ReplicationLinkAnalysis.log
   - ReplicationLinkAnalysis.xml

The Replication Link Analyzer works by examining both sites and checking whether:

- The SMS service is running
- The SMS Replication Configuration Monitor component is running
- The ports required for SQL replication are enabled
- The SQL version is supported
- The network is available between the two sites
- There is enough space for the SQL database
- The SSB service configuration exists
- The SSB service certificate exists
- There are any known errors in SQL log files
- There are any replication queues disabled
- Time is in sync
- The transmission of data is stuck
- A key conflict exists

The Replication Link Analyzer can find and fix most but not all database replication problems. If Replication Link Analyzer has not helped you resolve your problem, you should proceed with step 2.

Step 2: Examining the log files

If you are still having difficulties after using the Replication Link Analyzer, your next step should be to check the following two log files for all involved sites:

- rcmctrl.log
- replmgr.log

During the troubleshooting process, you might not get extra details with default logging. You need to turn on verbose logging using the following registry key:

HKEY_LOCAL_MACHINE\Software\Microsoft\SMS\Component\SMS_REPLICATION_CONFIGURATION_MONITOR\Verbose logging

- Set the Value 0 for Errors and key messages (the default value)
- Set the Value 1 for Errors, key messages, warnings and more general information
- Set the Value 2, which is Verbose, to see everything

Step 3: Performing SQL queries

If you are still unable to find the root cause of the issue, you need to run SQL queries using Microsoft SQL Server Management Studio on the central administration site or primary site to get more information. Specifically, you should:

1. Run the spDiagDRS script. The resulting output contains useful information about the general status of the database replication, the current replication link status, and the last sync time for each replication group.
2. Examine the vLogs view. These logs show more detailed information about the process. For example, when the database replication checks for changes, when it receives the BCP (bulk copy data) from the publisher, when it ProcessSyncDataXml, and when a specific table is updated.
3. Check the SSB log found at:

   C:\Program Files\Microsoft SQL Server\MSSQL10.MSSQLSERVER\MSSQL\ErrorLog

For more information on using profiler and SSB-related tables to troubleshoot service broker problems, see *http://www.sqlteam.com/article/how-to-troubleshoot-service-broker-problems*.

Step 4: Reinitiating replication

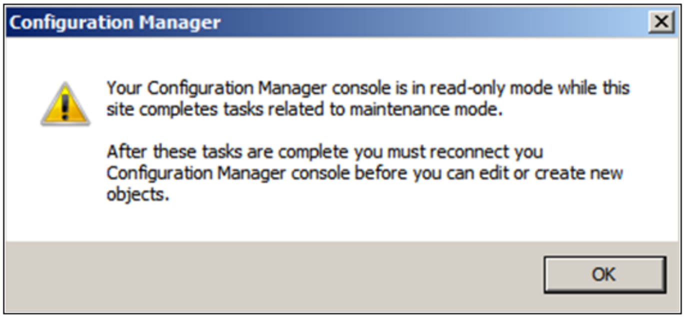
Reinitiating replication by sending a subscription invalid message should be the last step you try because it causes all the data to be re-replicated between the sites, which will generate a lot of network traffic.

To reinitiate the global data, run the following SQL command:

```
EXEC spDrsSendSubscriptionInvalid 'SiteCode', 'SiteCode', 'Configuration Data'
```

Troubleshooting the Configuration Manager console

Sometimes when you open the Configuration Manager console you will see the warning message shown in Figure 1-3.



Your Configuration Manager console is in read-only mode while this site completes tasks related to maintenance mode.

After these tasks are complete you must reconnect you Configuration Manager console before you can edit or create new objects.

FIGURE 1-3 A warning indicates when Configuration Manager sessions are read-only.

This warning message tells you that the Configuration Manager console will be opened in Read-Only mode, which means you won't be able to make any changes to your Configuration Manager console. This happens under the following circumstances:

- The primary site did not complete site installation yet.
- The primary site has inter-site replication problems.
- The primary site is running a site restoration.
- The primary site is initializing global data.

In some cases, you will need to wait until the replication site restoration or the site server installation is completed; after that you must close and reconnect the Configuration Manager console to establish a normal session.

CHAPTER 2

Understanding Configuration Manager components

Components form the basis of the architecture of System Center 2012 Configuration Manager and they work together to implement different functionality. You can install all the components on the site server or, alternatively, you can separate different components to other servers to offload some of the work from the site server to improve the performance.

This book doesn't cover all the components but focuses on the following ones which are heavily used by many administrators:

- Content distribution
- Pull distribution points
- Software update points
- Troubleshooting rotating management points and failover software update points
- Application deployment troubleshooting

A thorough understanding of how the various Configuration Manager components work together is essential for successful troubleshooting when problems arise. The goal of this chapter is to help build such an understanding.

Content distribution

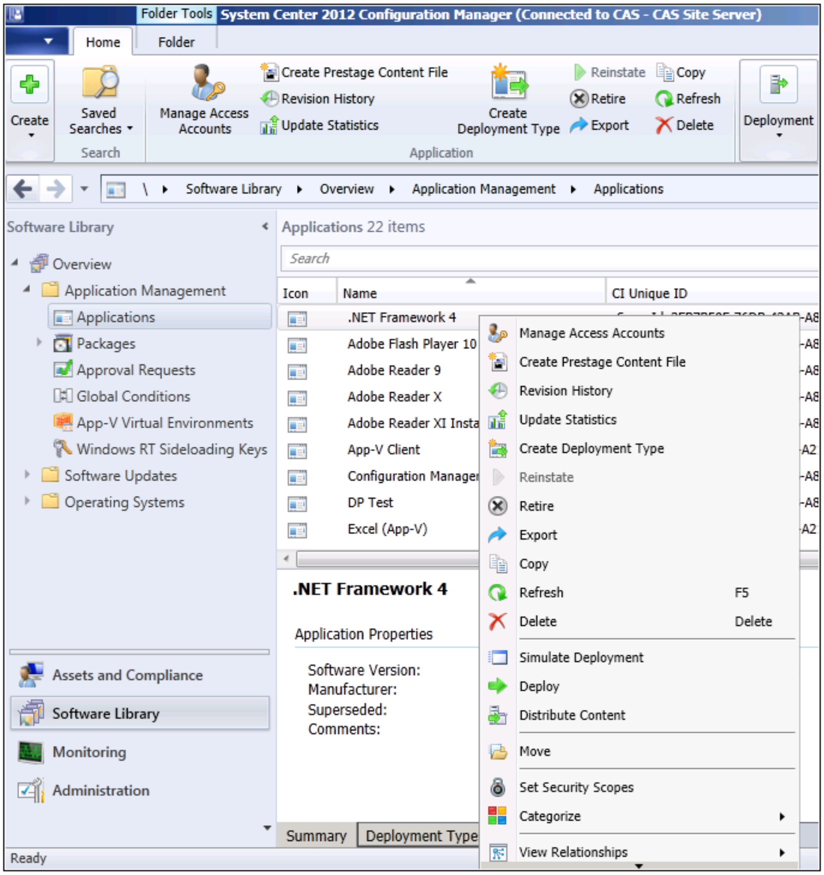
When you install the Distribution Manager role on a site server, the Site Component Manager (SMS_SITE_COMPONENT_MANAGER) triggers the installation of the role and invokes the related component for installation. This section examines the Distribution Manager and other components used when distributing content to distribution points.

Sending packages/applications to distribution points

When deploying any applications or packages, packages must be sent to a distribution point. Configuration Manager clients then download the package from the distribution point. If packages/applications are not distributed to distribution points, the clients will be unable to find the package and they won't be able to deploy that application.

The process for sending a package/application to a distribution point is as follows:

1. Open the Configuration Manager Console and click Software Library, and then Application Management.
2. Click Applications or Packages to see the list of created applications or packages.
3. Right-click one of the applications or packages and then select Distribute Content.

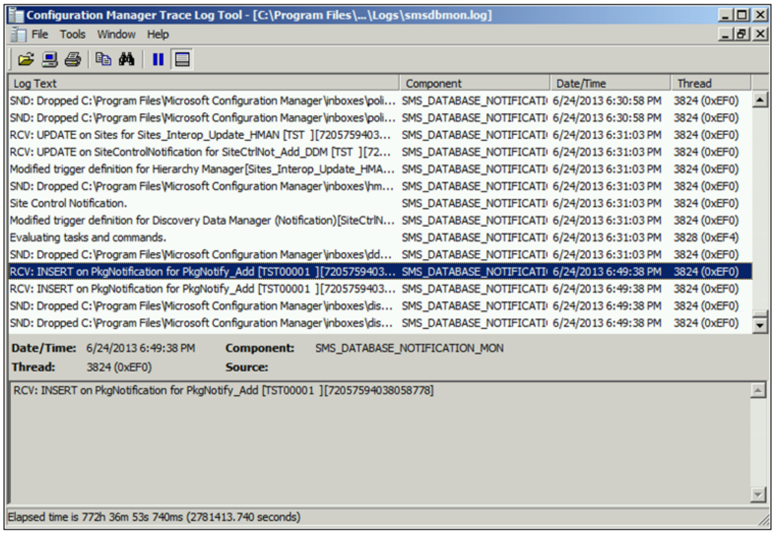


4. Follow the wizard to add the required distribution points.

Examining the log files

Understanding Configuration Manager components helps you troubleshoot issues when they arise. A good way to learn how these components work together is by reviewing the various log files that Configuration Manager uses. Verbose logging can also be configured to provide further information concerning components.

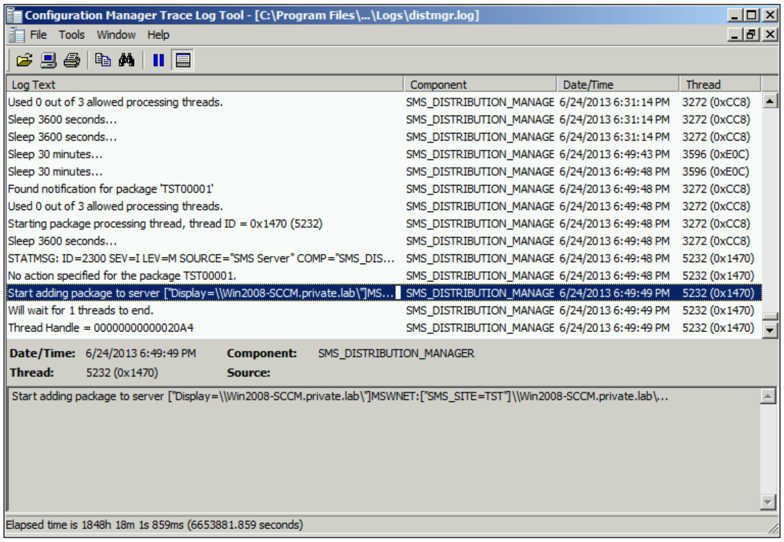
Let's look at what actually happens when you distribute content to distribution points. When you add a package or application to a distribution point, the SMS_DATABASE_NOTIFICATION component updates the database with the information and you can review the details in smsdbmon.log as shown in Figure 2-1.


Configuration Manager Trace Log Tool - [C:\Program Files\...\Logs\smsdbmon.log]
File
Tools
Window
Help

```
Log Text                                                                      Component                    Date/Time               Thread
SND: Dropped C:\Program Files\Microsoft Configuration Manager\inboxes\poli...  SMS_DATABASE_NOTIFICATI    6/24/2013 6:30:58 PM    3824 (0xEF0)
SND: Dropped C:\Program Files\Microsoft Configuration Manager\inboxes\poli...  SMS_DATABASE_NOTIFICATI    6/24/2013 6:30:58 PM    3824 (0xEF0)
RCV: UPDATE on Sites for Sites_Interop_Update_HMAN [TST ][7205759403...        SMS_DATABASE_NOTIFICATI    6/24/2013 6:31:03 PM    3824 (0xEF0)
RCV: UPDATE on SiteControlNotification for SiteCtrlNot_Add_DDM [TST ][72...   SMS_DATABASE_NOTIFICATI    6/24/2013 6:31:03 PM    3824 (0xEF0)
Modified trigger definition for Hierarchy Manager[Sites_Interop_Update_HMA...  SMS_DATABASE_NOTIFICATI    6/24/2013 6:31:03 PM    3824 (0xEF0)
SND: Dropped C:\Program Files\Microsoft Configuration Manager\inboxes\hm...    SMS_DATABASE_NOTIFICATI    6/24/2013 6:31:03 PM    3824 (0xEF0)
Site Control Notification.                                                     SMS_DATABASE_NOTIFICATI    6/24/2013 6:31:03 PM    3824 (0xEF0)
Modified trigger definition for Discovery Data Manager (Notification)[SiteCtrlN... SMS_DATABASE_NOTIFICATI 6/24/2013 6:31:03 PM    3824 (0xEF0)
Evaluating tasks and commands.                                                 SMS_DATABASE_NOTIFICATI    6/24/2013 6:31:03 PM    3828 (0xEF4)
SND: Dropped C:\Program Files\Microsoft Configuration Manager\inboxes\dd...    SMS_DATABASE_NOTIFICATI    6/24/2013 6:31:03 PM    3824 (0xEF0)
RCV: INSERT on PkgNotification for PkgNotify_Add [TST00001 ][7205759403...     SMS_DATABASE_NOTIFICATI    6/24/2013 6:49:38 PM    3824 (0xEF0)
RCV: INSERT on PkgNotification for PkgNotify_Add [TST00001 ][7205759403...     SMS_DATABASE_NOTIFICATI    6/24/2013 6:49:38 PM    3824 (0xEF0)
SND: Dropped C:\Program Files\Microsoft Configuration Manager\inboxes\dis...   SMS_DATABASE_NOTIFICATI    6/24/2013 6:49:38 PM    3824 (0xEF0)
SND: Dropped C:\Program Files\Microsoft Configuration Manager\inboxes\dis...   SMS_DATABASE_NOTIFICATI    6/24/2013 6:49:38 PM    3824 (0xEF0)

Date/Time:  6/24/2013 6:49:38 PM      Component:  SMS_DATABASE_NOTIFICATION_MON
Thread:     3824 (0xEF0)              Source:

RCV: INSERT on PkgNotification for PkgNotify_Add [TST00001 ][72057594038058778]

Elapsed time is 772h 36m 53s 740ms (2781413.740 seconds)
```

FIGURE 2-1 A package notification is inserted in the smsdbmon.log.

The Distribution Manager (SMS_DISTRIBUTION_MANAGER) component then starts the process of adding the package to the distribution point. This information is logged in the distmgr.log file as shown in Figure 2-2.


Configuration Manager Trace Log Tool - [C:\Program Files\...\Logs\distmgr.log]
File
Tools
Window
Help

```
Log Text                                                                  Component                   Date/Time               Thread
Used 0 out of 3 allowed processing threads.                               SMS_DISTRIBUTION_MANAGE    6/24/2013 6:31:14 PM    3272 (0xCC8)
Sleep 3600 seconds...                                                     SMS_DISTRIBUTION_MANAGE    6/24/2013 6:31:14 PM    3272 (0xCC8)
Sleep 3600 seconds...                                                     SMS_DISTRIBUTION_MANAGE    6/24/2013 6:31:14 PM    3272 (0xCC8)
Sleep 30 minutes...                                                       SMS_DISTRIBUTION_MANAGE    6/24/2013 6:49:43 PM    3596 (0xE0C)
Sleep 30 minutes...                                                       SMS_DISTRIBUTION_MANAGE    6/24/2013 6:49:48 PM    3596 (0xE0C)
Found notification for package 'TST00001'                                 SMS_DISTRIBUTION_MANAGE    6/24/2013 6:49:48 PM    3272 (0xCC8)
Used 0 out of 3 allowed processing threads.                               SMS_DISTRIBUTION_MANAGE    6/24/2013 6:49:48 PM    3272 (0xCC8)
Starting package processing thread, thread ID = 0x1470 (5232)             SMS_DISTRIBUTION_MANAGE    6/24/2013 6:49:48 PM    3272 (0xCC8)
Sleep 3600 seconds...                                                     SMS_DISTRIBUTION_MANAGE    6/24/2013 6:49:48 PM    3272 (0xCC8)
STATMSG: ID=2300 SEV=I LEV=M SOURCE="SMS Server" COMP="SMS_DIS...          SMS_DISTRIBUTION_MANAGE    6/24/2013 6:49:48 PM    5232 (0x1470)
No action specified for the package TST00001.                             SMS_DISTRIBUTION_MANAGE    6/24/2013 6:49:48 PM    5232 (0x1470)
Start adding package to server ["Display=\\Win2008-SCCM.private.lab\"]MS... SMS_DISTRIBUTION_MANAGE  6/24/2013 6:49:49 PM    5232 (0x1470)
Will wait for 1 threads to end.                                           SMS_DISTRIBUTION_MANAGE    6/24/2013 6:49:49 PM    5232 (0x1470)
Thread Handle = 00000000000020A4                                          SMS_DISTRIBUTION_MANAGE    6/24/2013 6:49:49 PM    5232 (0x1470)

Date/Time:  6/24/2013 6:49:49 PM      Component:  SMS_DISTRIBUTION_MANAGER
Thread:     5232 (0x1470)             Source:

Start adding package to server ["Display=\\Win2008-SCCM.private.lab\"]MSWNET:["SMS_SITE=TST"]\\Win2008-SCCM.private.lab\...

Elapsed time is 1848h 18m 1s 859ms (6653881.859 seconds)
```

FIGURE 2-2 A package is being added to distribution point.

If for any reason the Distribution Manager fails to send the package to the distribution point, it will log the resulting errors in the distmgr.log. We'll look at the distmgr.log again later in this chapter.

Package Transfer Manager

What if you have second distribution point that is remote from your primary site server? System Center 2012 Configuration Manager introduces a new component called Package Transfer Manager that is used to distribute packages to a remote distribution point.

The process of troubleshooting deployment of applications and packages to remote distribution points is similar to what was described previously except that Package Transfer Manager (not Distribution Manager) is used to transfer the application or package to the remote distribution point.

Monitoring distribution of content to remote distribution points

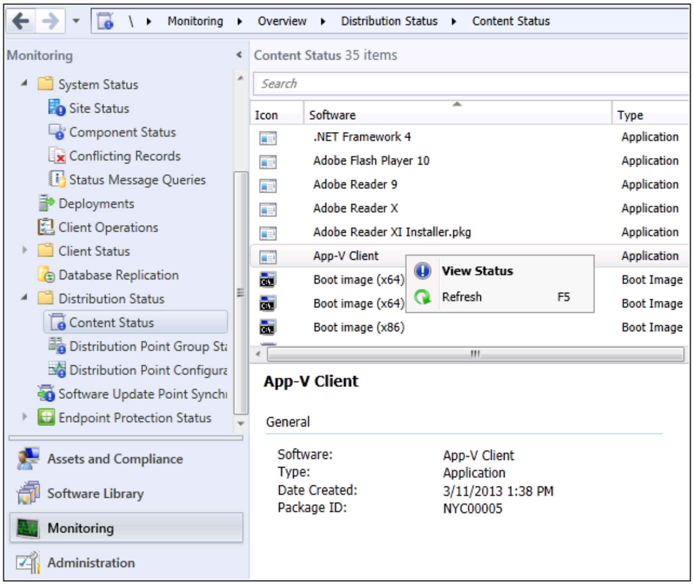
When you distribute content to a remote distribution point, there are two ways to monitor progress:

- Using the Monitoring workspace in the console
- Using the Package Transfer Manager log (PkgXferMgr.log)

Using the Monitoring workspace

To monitor progress in distributing content to remote distribution points using the Configuration Manager console, follow these steps:

1. Connect to the Console and then select Monitoring | Distribution Status | Content Status. Highlight the application you want to monitor and review the Completion Statistics in the lower half of the window. Click View Status for additional details.



\ ▸ Monitoring ▸ Overview ▸ Distribution Status ▸ Content Status

Monitoring

- System Status
  - Site Status
  - Component Status
  - Conflicting Records
  - Status Message Queries
- Deployments
- Client Operations
- Client Status
- Database Replication
- Distribution Status
  - Content Status
  - Distribution Point Group Sta
  - Distribution Point Configura
- Software Update Point Synchi
- Endpoint Protection Status

Assets and Compliance

Software Library

Monitoring

Administration

Content Status 35 items

Search

Icon	Software	Type
	.NET Framework 4	Application
	Adobe Flash Player 10	Application
	Adobe Reader 9	Application
	Adobe Reader X	Application
	Adobe Reader XI Installer.pkg	Application
	App-V Client	Application
	Boot image (x64)	Boot Image
	Boot image (x64)	Boot Image
	Boot image (x86)	Boot Image

App-V Client

General

Software: App-V Client
Type: Application
Date Created: 3/11/2013 1:38 PM
Package ID: NYC00005

2. Click the various tabs such as Success, In Progress, Error, and Unknown and review the details. For example, click the Error tab to review errors on why distribution of content is failing.
3. Under Asset Details, review the data and click More Details to view the description of the errors.

Using PkgXferMgr.log

Sometimes the Monitoring workspace might not provide you with enough information to troubleshoot an issue relating to the distribution of content to a remote distribution point. In such cases, your next step should be to examine the Package Transfer Manager log (PkgXferMgr.log) for further details concerning the process.

For example, if the Content Status indicates that the server's computer account does not have access to the package source or the distribution point doesn't have enough disk space, what should you do? First, review your environment to make sure that the computer account has proper access and that there is enough disk space on the remote distribution point.

If the problem persists, review the PkgXFerMgr.log on the primary site server. The following log entry is a potential error for the application:

```
ExecStaticMethod failed (80041001) SMS_DistributionPoint, AddFile
        SMS_PACKAGE_TRANSFER_MANAGER       7/26/2013 2:07:43 PM       5152 (0x1420)
CSendFileAction::AddFile failed; 0x80041001    SMS_PACKAGE_TRANSFER_MANAGER   7/26/2013
2:07:43 PM       5152 (0x1420)
```

```
CSendFileAction::SendFiles failed; 0x80041001  SMS_PACKAGE_TRANSFER_MANAGER   7/26/2013
2:07:44 PM       5152 (0x1420)
CSendFileAction::SendFiles failed; 0x80041001  SMS_PACKAGE_TRANSFER_MANAGER   7/26/2013
2:07:44 PM       5152 (0x1420)
Notifying pkgXferJobMgr  SMS_PACKAGE_TRANSFER_MANAGER                         7/26/2013
2:07:44 PM       5152 (0x1420)
Sending failed. Failure count = 7, Restart time = 7/26/2013 2:37:44 PM Eastern Daylight
Time    SMS_PACKAGE_TRANSFER_MANAGER       7/26/2013 2:07:44 PM      5152 (0x1420)
Sent status to the distribution manager for pkg LA100005, version 2, status 4 and
distribution point

["Display=\\Cm12PRINA.Contoso.com\"]MSWNET:["SMS_SITE=LA1"]\\Cm12PRINA.Contoso.com\
         SMS_PACKAGE_TRANSFER_MANAGER      7/26/2013 2:07:44 PM     5152 (0x1420)
```

What does this log tell you? It has an error code 0x80041001 which means “Generic Failure – Source: WMI.” It is not giving you any information other than that it is a generic failure.

Next, review the smsdbprov.log on the remote distribution point. The following log excerpt shows that an error is being thrown:

```
Error Code 0x80040154 means "Class not registered"
Remote DP – smsdpprov.log: (located on remote DP under C:\SMS_DP$\sms\logs folder):
[1608][Fri 07/26/2013 15:46:18]:Failed to add file 'ccmsetup.cab' to content library.
Error code: 0X80040154
[1920][Fri 07/26/2013 15:52:46]:CFileLibrary::AddFile failed; 0x80040154
[1920][Fri 07/26/2013 15:52:46]:CFileLibrary::AddFile failed; 0x80040154
[1920][Fri 07/26/2013 15:52:46]:CContentDefinition::AddFile failed; 0x80040154
[1920][Fri 07/26/2013 15:52:46]:Failed to add file 'ccmsetup.exe' to content library.
Error code: 0X80040154
Remote DP – smsdpprov.log:
[10DC][Fri 07/26/2013 16:10:42]:Content 'Content_e89f02f4-6fa0-41d8-b9da-2cdaadf6b82f.1'
for package 'LA100005' has been added to content library successfully
[E64][Fri 07/26/2013 16:18:38]:Content 'CAS00001.3' for package 'CAS00001' has been
added to content library successfully
[564][Fri 07/26/2013 16:23:04]:Content 'CAS00002.3' for package 'CAS00002' has been
added to content library successfully
```

The error code 0x80040154, which is explained as “Class not registered,” indicates that there might be some class or component missing on the remote distribution point. Your next step would be to review the prerequisites for distribution points as listed on Microsoft TechNet at *http://technet.microsoft.com/en-us/library/gg682077.aspx* to ensure all the prerequisites have been met. First on the list of prerequisites is the Remote Differential Compression (RDC) component which you discover is missing on a remote distribution point running Windows Server 2008 R2. In this case, you go ahead and install the RDC component on your remote distribution point. After the RDC component has been installed, the content distribution process finishes and the application is successfully installed on the remote distribution point.

As you can see in this example, one of the error codes (0x80041001) was not useful but the second one (0x80040154) at least provided you with a hint. So the lesson learned here is to always check all of the appropriate logs before spending too much time looking for other possible causes of your problem.

Pull distribution points

Microsoft System Center 2012 Configuration Manager SP1 introduces a new type of distribution point called a *pull distribution point*. The task of distributing content to a large number of distribution points puts a huge load on a site server, especially the Distribution Manager (distmgr) and Package Transfer Manager (pkgxfermgr) components of the site server. Basically, the Distribution Manager becomes a bottleneck, and this is why the previous recommendation in the RTM release of System Center 2012 Configuration Manager was to have not more than 250 distribution points per site.

You can examine this problem in more detail with the help of some diagrams. In Figure 2-3 you can see a primary site connected to three distribution points. Two of them are connected with 100 Mbps links and one is connected with a 2 Mbps link. All of these distribution points are under same distribution group.

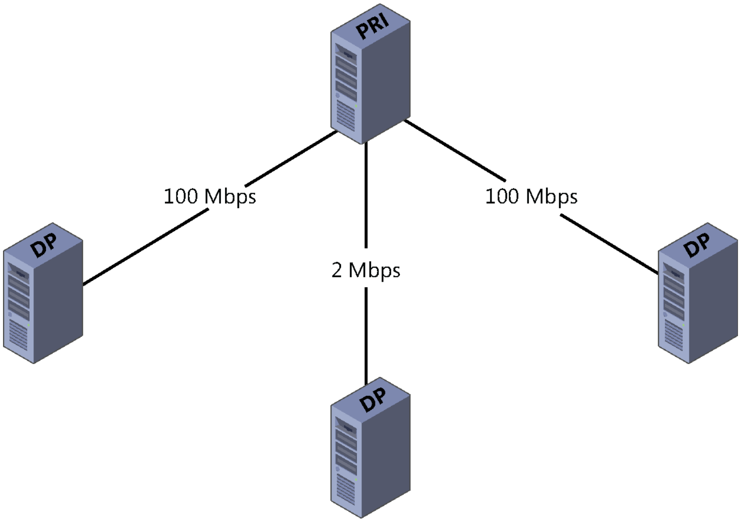


FIGURE 2-3 Three distribution points complete this content distribution scenario.

Once you start distributing content from the primary site, the content will route to all the distribution points via Distribution Manager. However, since the originating source is the same in all the distribution points, the Distribution Manager and Package Transfer Manager components are under heavy load.

Figure 2-4 shows the new pull distribution scenario supported by System Center 2012 Configuration Manager SP1. Instead of having to get the content from the primary site, a distribution point can pull the content from the nearest distribution point. Pull distribution points still allow you to specify where each distribution point resides in the hierarchy but also gives you the flexibility of defining the source distribution point. The result also allows you to overcome the previous limitation of a maximum of 250 distribution points and helps reduce the load of content distribution on primary sites.

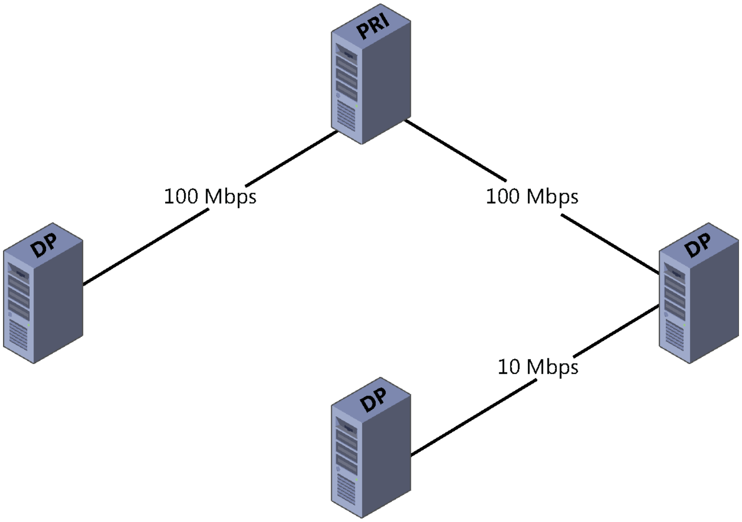


FIGURE 2-4 An example of a pull distribution scenario.

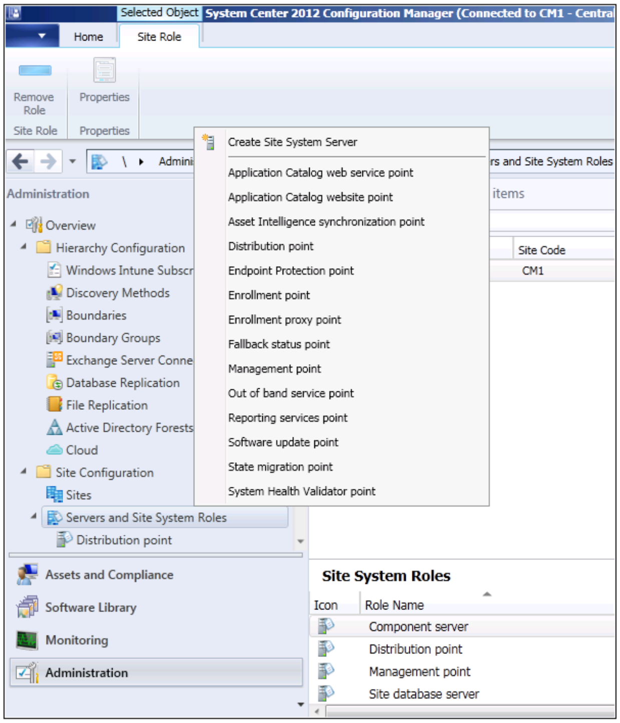
IMPORTANT **Background Intelligent Transfer Service (BITS) is used for transferring content to pull distribution points. This means you can configure BITS throttling using Group Policy to throttle downloads.**

Installing a pull distribution point

This section describes how to install a pull distribution point. It also shows how to verify installation with the help of the relevant log files.

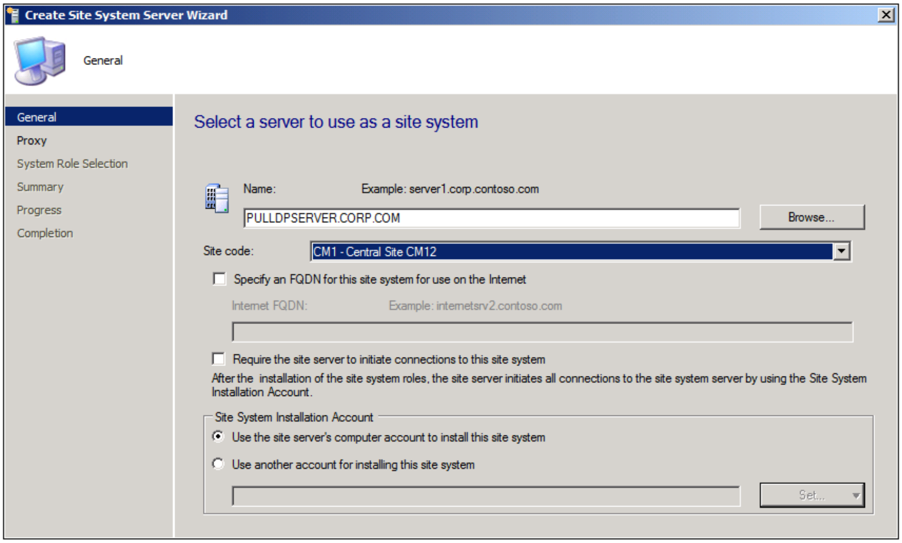
Follow these steps to install a pull distribution point:

1. In the Configuration Manager console, select the Administration workspace, Site Configuration, right-click Servers And Site System Roles, and then select Create Site System Server:



Icon	Role Name
	Component server
	Distribution point
	Management point
	Site database server

2. On the General page of the Create Site System Server Wizard, specify the name of the server you want to designate as a pull distribution point:



Select a server to use as a site system

Name: Example: server1.corp.contoso.com

PULLDPSERVER.CORP.COM

Site code: CM1 - Central Site CM12

□ Specify an FQDN for this site system for use on the Internet

Internet FQDN: Example: internetsrv2.contoso.com

□ Require the site server to initiate connections to this site system

After the installation of the site system roles, the site server initiates all connections to the site system server by using the Site System Installation Account.

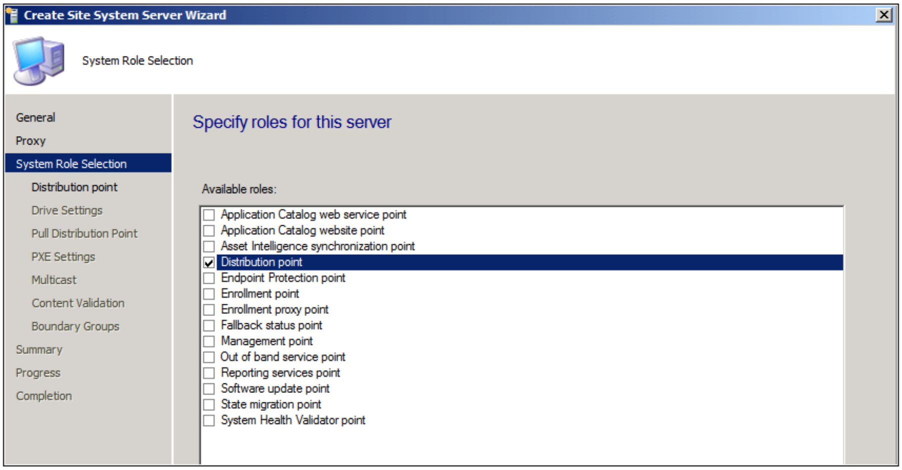
Site System Installation Account

● Use the site server's computer account to install this site system

○ Use another account for installing this site system

3. Click Next and then Next again on the Proxy page.

4. On the System Role Selection page, select Distribution Point as the role and then click Next:

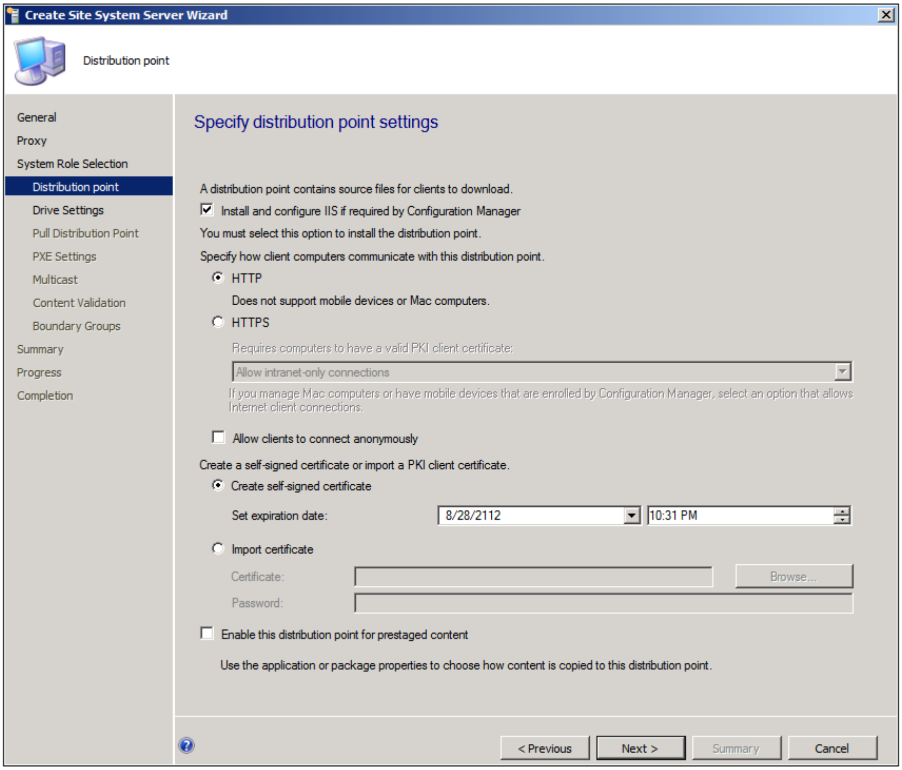


Specify roles for this server

Available roles:

☐ Application Catalog web service point
☐ Application Catalog website point
☐ Asset Intelligence synchronization point
☑ Distribution point
☐ Endpoint Protection point
☐ Enrollment point
☐ Enrollment proxy point
☐ Fallback status point
☐ Management point
☐ Out of band service point
☐ Reporting services point
☐ Software update point
☐ State migration point
☐ System Health Validator point

5. On the Distribution Point page, select the Install And Configure IIS If Required By Configuration Manager check box and then click Next:



Specify distribution point settings

A distribution point contains source files for clients to download.

☑ Install and configure IIS if required by Configuration Manager

You must select this option to install the distribution point.

Specify how client computers communicate with this distribution point.

● HTTP

Does not support mobile devices or Mac computers.

○ HTTPS

Requires computers to have a valid PKI client certificate:

Allow intranet-only connections

If you manage Mac computers or have mobile devices that are enrolled by Configuration Manager, select an option that allows Internet client connections.

☐ Allow clients to connect anonymously

Create a self-signed certificate or import a PKI client certificate.

● Create self-signed certificate

Set expiration date: 8/28/2112 10:31 PM

○ Import certificate

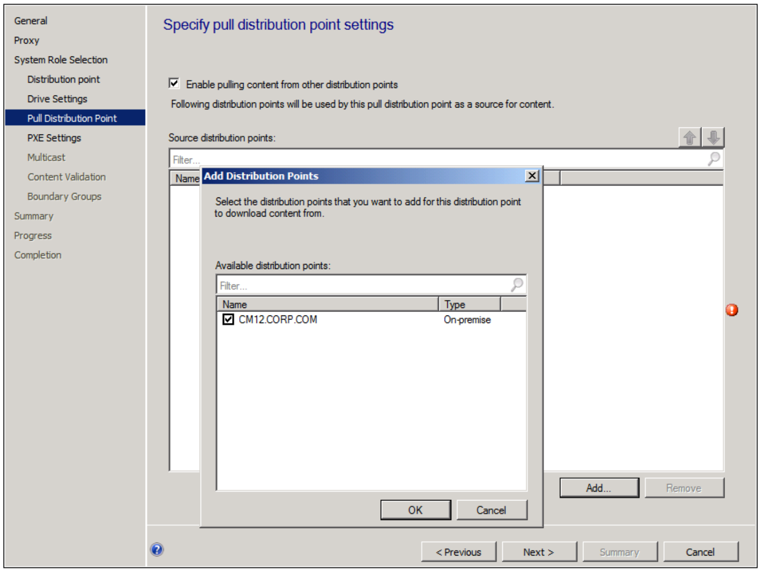
Certificate:

Password:

☐ Enable this distribution point for prestaged content

Use the application or package properties to choose how content is copied to this distribution point.

6. On the Pull Distribution Point page, select the Enable Pulling Content From Other Distribution Points check box. Then, under Source Distribution Points, click Add and use the Add Distribution Points dialog box to add the distribution point you want to act as the source distribution point:



Specify pull distribution point settings

☑ Enable pulling content from other distribution points

Following distribution points will be used by this pull distribution point as a source for content.

Source distribution points:

Filter...

Add Distribution Points

Select the distribution points that you want to add for this distribution point to download content from.

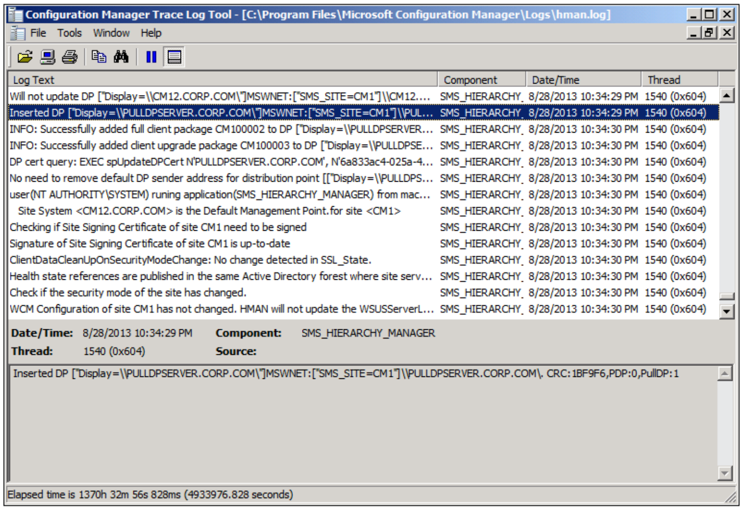
Available distribution points:

Filter...

Name	Type
☑ CM12.CORP.COM	On-premise

7. Click OK and then click Next and complete the remaining wizard pages.

8. After installation of the pull distribution point is finished, you will see the following entry in the hman.log :



Configuration Manager Trace Log Tool - [C:\Program Files\Microsoft Configuration Manager\Logs\hman.log]

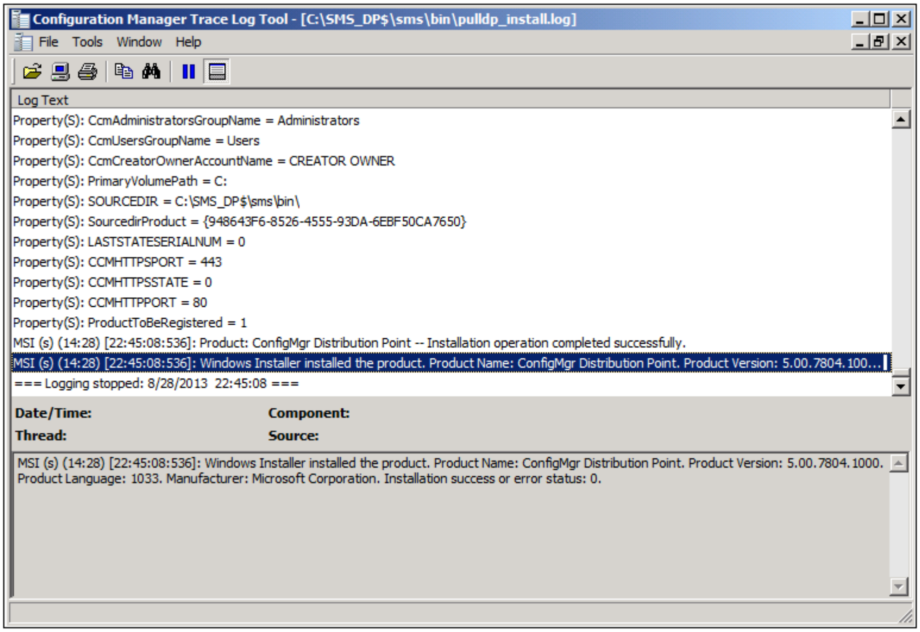
```
Log Text                                                                        Component        Date/Time             Thread
Will not update DP ["Display=\\CM12.CORP.COM\"]MSWNET:["SMS_SITE=CM1"]\\CM12....  SMS_HIERARCHY_  8/28/2013 10:34:29 PM  1540 (0x604)
Inserted DP ["Display=\\PULLDPSERVER.CORP.COM\"]MSWNET:["SMS_SITE=CM1"]\\PUL...   SMS_HIERARCHY_  8/28/2013 10:34:29 PM  1540 (0x604)
INFO: Successfully added full client package CM100002 to DP ["Display=\\PULLDPSERVER...  SMS_HIERARCHY_  8/28/2013 10:34:30 PM  1540 (0x604)
INFO: Successfully added client upgrade package CM100003 to DP ["Display=\\PULLDPSE...   SMS_HIERARCHY_  8/28/2013 10:34:30 PM  1540 (0x604)
DP cert query: EXEC spUpdateDPCert N'PULLDPSERVER.CORP.COM', N'6a833ac4-025a-4...  SMS_HIERARCHY_  8/28/2013 10:34:30 PM  1540 (0x604)
No need to remove default DP sender address for distribution point [["Display=\\PULLDPS...  SMS_HIERARCHY_  8/28/2013 10:34:30 PM  1540 (0x604)
user(NT AUTHORITY\SYSTEM) runing application(SMS_HIERARCHY_MANAGER) from mac...  SMS_HIERARCHY_  8/28/2013 10:34:30 PM  1540 (0x604)
  Site System <CM12.CORP.COM> is the Default Management Point.for site <CM1>      SMS_HIERARCHY_  8/28/2013 10:34:30 PM  1540 (0x604)
Checking if Site Signing Certificate of site CM1 need to be signed               SMS_HIERARCHY_  8/28/2013 10:34:30 PM  1540 (0x604)
Signature of Site Signing Certificate of site CM1 is up-to-date                  SMS_HIERARCHY_  8/28/2013 10:34:30 PM  1540 (0x604)
ClientDataCleanUpOnSecurityModeChange: No change detected in SSL_State.          SMS_HIERARCHY_  8/28/2013 10:34:30 PM  1540 (0x604)
Health state references are published in the same Active Directory forest where site serv...  SMS_HIERARCHY_  8/28/2013 10:34:30 PM  1540 (0x604)
Check if the security mode of the site has changed.                              SMS_HIERARCHY_  8/28/2013 10:34:30 PM  1540 (0x604)
WCM Configuration of site CM1 has not changed. HMAN will not update the WSUSServerL...  SMS_HIERARCHY_  8/28/2013 10:34:30 PM  1540 (0x604)
```

Date/Time: 8/28/2013 10:34:29 PM **Component:** SMS_HIERARCHY_MANAGER
Thread: 1540 (0x604) **Source:**

```
Inserted DP ["Display=\\PULLDPSERVER.CORP.COM\"]MSWNET:["SMS_SITE=CM1"]\\PULLDPSERVER.CORP.COM\. CRC:1BF9F6,PDP:0,PullDP:1
```

Elapsed time is 1370h 32m 56s 828ms (4933976.828 seconds)

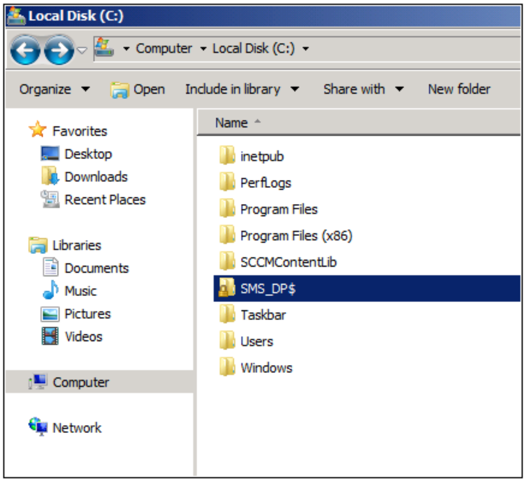
The distmgr.log on the primary site server will look like this:


Configuration Manager Trace Log Tool - [C:\SMS_DP$\sms\bin\pulldp_install.log]
File
Tools
Window
Help
Log Text
Date/Time:
Component:
Thread:
Source:

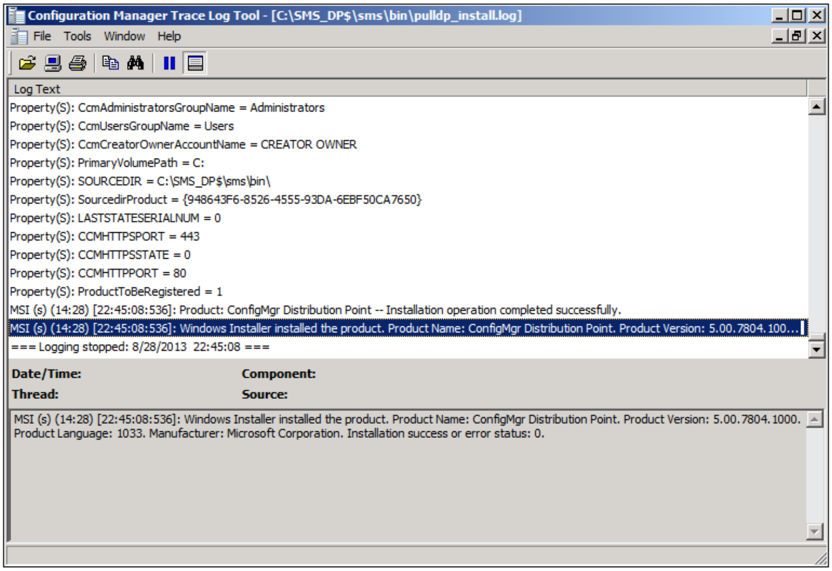
```
Property(S): CcmAdministratorsGroupName = Administrators
Property(S): CcmUsersGroupName = Users
Property(S): CcmCreatorOwnerAccountName = CREATOR OWNER
Property(S): PrimaryVolumePath = C:
Property(S): SOURCEDIR = C:\SMS_DP$\sms\bin\
Property(S): SourcedirProduct = {948643F6-8526-4555-93DA-6EBF50CA7650}
Property(S): LASTSTATESERIALNUM = 0
Property(S): CCMHTTPSPORT = 443
Property(S): CCMHTTPSSTATE = 0
Property(S): CCMHTTPPORT = 80
Property(S): ProductToBeRegistered = 1
MSI (s) (14:28) [22:45:08:536]: Product: ConfigMgr Distribution Point -- Installation operation completed successfully.
MSI (s) (14:28) [22:45:08:536]: Windows Installer installed the product. Product Name: ConfigMgr Distribution Point. Product Version: 5.00.7804.100...
=== Logging stopped: 8/28/2013  22:45:08 ===
```

```
MSI (s) (14:28) [22:45:08:536]: Windows Installer installed the product. Product Name: ConfigMgr Distribution Point. Product Version: 5.00.7804.1000.
Product Language: 1033. Manufacturer: Microsoft Corporation. Installation success or error status: 0.
```

9. If you now open Windows Explorer on the server where the pull distribution point has been created, you will see that the following folder structure has been created.



10. To further verify the installation of the pull distribution point, review the log files under \SMS_DP$\SMS\BIN\pulldp_Install.log on the server where the pull distribution point resides:

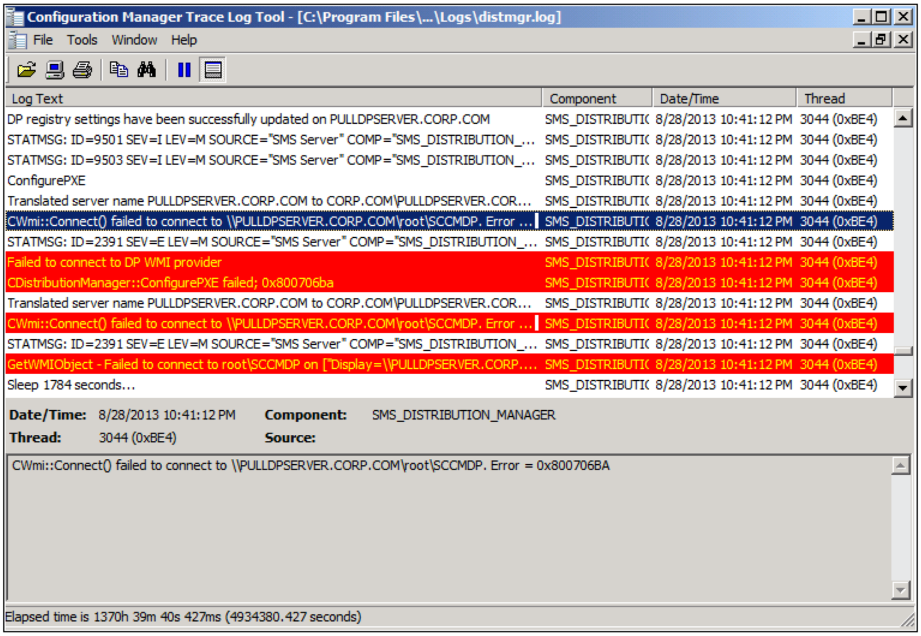


Configuration Manager Trace Log Tool - [C:\SMS_DP$\sms\bin\pulldp_install.log]
File
Tools
Window
Help

```
Log Text
Property(S): CcmAdministratorsGroupName = Administrators
Property(S): CcmUsersGroupName = Users
Property(S): CcmCreatorOwnerAccountName = CREATOR OWNER
Property(S): PrimaryVolumePath = C:
Property(S): SOURCEDIR = C:\SMS_DP$\sms\bin\
Property(S): SourcedirProduct = {948643F6-8526-4555-93DA-6EBF50CA7650}
Property(S): LASTSTATESERIALNUM = 0
Property(S): CCMHTTPSPORT = 443
Property(S): CCMHTTPSSTATE = 0
Property(S): CCMHTTPPORT = 80
Property(S): ProductToBeRegistered = 1
MSI (s) (14:28) [22:45:08:536]: Product: ConfigMgr Distribution Point -- Installation operation completed successfully.
MSI (s) (14:28) [22:45:08:536]: Windows Installer installed the product. Product Name: ConfigMgr Distribution Point. Product Version: 5.00.7804.100...
=== Logging stopped: 8/28/2013  22:45:08 ===

Date/Time:                              Component:
Thread:                                 Source:

MSI (s) (14:28) [22:45:08:536]: Windows Installer installed the product. Product Name: ConfigMgr Distribution Point. Product Version: 5.00.7804.1000.
Product Language: 1033. Manufacturer: Microsoft Corporation. Installation success or error status: 0.
```

Troubleshooting pull distribution point installation

You can use the log files to troubleshoot issues involving installation of pull distribution points. As an example of how to do this, let's say that while installing a pull distribution point in a lab environment you encounter the error shown in Figure 2-5.



Configuration Manager Trace Log Tool - [C:\Program Files\...\Logs\distmgr.log]
File
Tools
Window
Help

```
Log Text                                                                    Component          Date/Time               Thread
DP registry settings have been successfully updated on PULLDPSERVER.CORP.COM SMS_DISTRIBUTI(   8/28/2013 10:41:12 PM   3044 (0xBE4)
STATMSG: ID=9501 SEV=I LEV=M SOURCE="SMS Server" COMP="SMS_DISTRIBUTION_...  SMS_DISTRIBUTI(   8/28/2013 10:41:12 PM   3044 (0xBE4)
STATMSG: ID=9503 SEV=I LEV=M SOURCE="SMS Server" COMP="SMS_DISTRIBUTION_...  SMS_DISTRIBUTI(   8/28/2013 10:41:12 PM   3044 (0xBE4)
ConfigurePXE                                                                 SMS_DISTRIBUTI(   8/28/2013 10:41:12 PM   3044 (0xBE4)
Translated server name PULLDPSERVER.CORP.COM to CORP.COM\PULLDPSERVER.COR...  SMS_DISTRIBUTI(   8/28/2013 10:41:12 PM   3044 (0xBE4)
CWmi::Connect() failed to connect to \\PULLDPSERVER.CORP.COM\root\SCCMDP. Error ...  SMS_DISTRIBUTI(   8/28/2013 10:41:12 PM   3044 (0xBE4)
STATMSG: ID=2391 SEV=E LEV=M SOURCE="SMS Server" COMP="SMS_DISTRIBUTION_...  SMS_DISTRIBUTI(   8/28/2013 10:41:12 PM   3044 (0xBE4)
Failed to connect to DP WMI provider                                         SMS_DISTRIBUTI(   8/28/2013 10:41:12 PM   3044 (0xBE4)
CDistributionManager::ConfigurePXE failed; 0x800706ba                        SMS_DISTRIBUTI(   8/28/2013 10:41:12 PM   3044 (0xBE4)
Translated server name PULLDPSERVER.CORP.COM to CORP.COM\PULLDPSERVER.COR...  SMS_DISTRIBUTI(   8/28/2013 10:41:12 PM   3044 (0xBE4)
CWmi::Connect() failed to connect to \\PULLDPSERVER.CORP.COM\root\SCCMDP. Error ...  SMS_DISTRIBUTI(   8/28/2013 10:41:12 PM   3044 (0xBE4)
STATMSG: ID=2391 SEV=E LEV=M SOURCE="SMS Server" COMP="SMS_DISTRIBUTION_...  SMS_DISTRIBUTI(   8/28/2013 10:41:12 PM   3044 (0xBE4)
GetWMIObject - Failed to connect to root\SCCMDP on ["Display=\\PULLDPSERVER.CORP....  SMS_DISTRIBUTI(   8/28/2013 10:41:12 PM   3044 (0xBE4)
Sleep 1784 seconds...                                                        SMS_DISTRIBUTI(   8/28/2013 10:41:12 PM   3044 (0xBE4)

Date/Time:   8/28/2013 10:41:12 PM        Component:   SMS_DISTRIBUTION_MANAGER
Thread:      3044 (0xBE4)                 Source:

CWmi::Connect() failed to connect to \\PULLDPSERVER.CORP.COM\root\SCCMDP. Error = 0x800706BA

Elapsed time is 1370h 39m 40s 427ms (4934380.427 seconds)
```

FIGURE 2-5 The distmgr.log displays a pull distribution point error.

In addition, during your troubleshooting of this issue you checked the pull distribution point server and discovered that none of the expected folders were created on it.

The distmgr.log excerpt shown in Figure 2-5 shows that Distribution Manager has failed to connect with the Windows Management Instrumentation (WMI) provider on the pull distribution point. When you get a WMI error like this, you should perform the following steps to troubleshoot:

1. Check Windows Firewall on the pull distribution point server to see if the connection to the remote WMI provider is being blocked.
2. Check to see if an anti-virus program might be blocking the communication.
3. Verify that the site server's computer account (for example, PrimaryServer$ if PrimaryServer is the name of the server) is part of the local Administrator group on the pull distribution point server.

For example, you might discover that the site server's computer account is not a member of the local Administrator group on the pull distribution point server. In this case, your problem will be solved as soon as you add the site server computer account to the pull distribution point local Administrator group.

Software update points

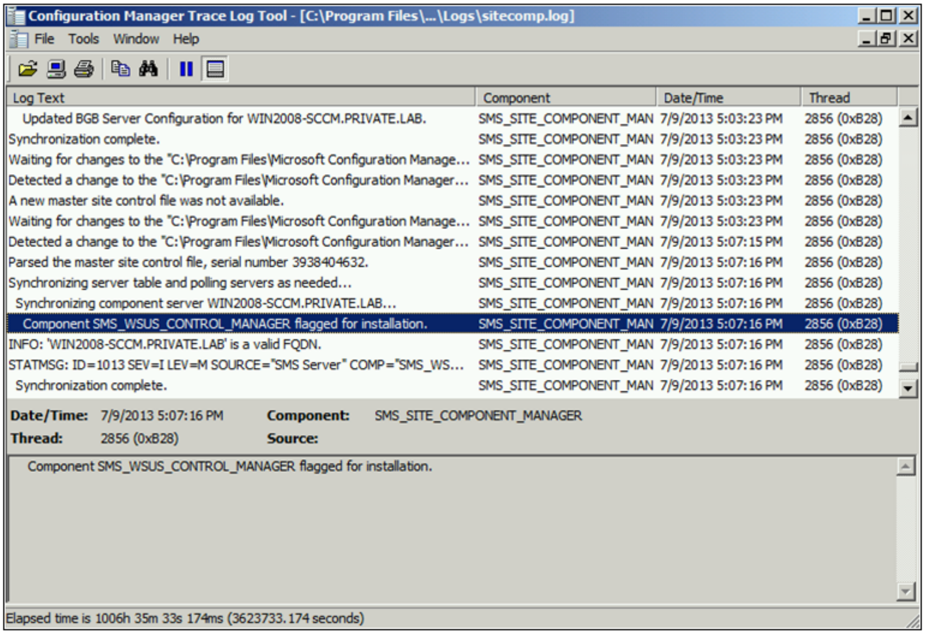
Software update point (SUP) in Configuration Manager is a required component for software updates on primary sites and an optional component for software updates on secondary sites. It is installed as a site system role using the Configuration Manager console.

The SUP site system role must be created on a server that has Windows Server Update Services (WSUS) 3.0 SP2 installed. The SUP interacts with the WSUS services to configure update settings and to request synchronization to the upstream update source. It also interacts with the central site to synchronize software updates from the WSUS database to the site server database.

Beginning with System Center 2012 Configuration Manager SP1, you can have multiple software update points in your Configuration Manager environment to support clients in an untrusted forest. In addition, if you configure multiple SUPs at a site and one fails or becomes unavailable, clients will switch to another SUP. This behavior is called software update point switching or failover. We will discuss more about SUP switching and troubleshooting process related to switching later in the section.

Troubleshooting installation of software update points

When you add a SUP as a site system role, the sitecomp.log file shows that the SMS_WSUS_CONTROL_MANAGER has been flagged for installation (see Figure 2-6). It also shows the installation process for the SUP on the server. If the installation of the role fails for any reason, you'll find detailed information in the sitecomp.log.



Configuration Manager Trace Log Tool - [C:\Program Files\...\Logs\sitecomp.log]

Log Text	Component	Date/Time	Thread
Updated BGB Server Configuration for WIN2008-SCCM.PRIVATE.LAB.	SMS_SITE_COMPONENT_MAN	7/9/2013 5:03:23 PM	2856 (0xB28)
Synchronization complete.	SMS_SITE_COMPONENT_MAN	7/9/2013 5:03:23 PM	2856 (0xB28)
Waiting for changes to the "C:\Program Files\Microsoft Configuration Manage...	SMS_SITE_COMPONENT_MAN	7/9/2013 5:03:23 PM	2856 (0xB28)
Detected a change to the "C:\Program Files\Microsoft Configuration Manager...	SMS_SITE_COMPONENT_MAN	7/9/2013 5:03:23 PM	2856 (0xB28)
A new master site control file was not available.	SMS_SITE_COMPONENT_MAN	7/9/2013 5:03:23 PM	2856 (0xB28)
Waiting for changes to the "C:\Program Files\Microsoft Configuration Manage...	SMS_SITE_COMPONENT_MAN	7/9/2013 5:03:23 PM	2856 (0xB28)
Detected a change to the "C:\Program Files\Microsoft Configuration Manager...	SMS_SITE_COMPONENT_MAN	7/9/2013 5:07:15 PM	2856 (0xB28)
Parsed the master site control file, serial number 3938404632.	SMS_SITE_COMPONENT_MAN	7/9/2013 5:07:16 PM	2856 (0xB28)
Synchronizing server table and polling servers as needed...	SMS_SITE_COMPONENT_MAN	7/9/2013 5:07:16 PM	2856 (0xB28)
Synchronizing component server WIN2008-SCCM.PRIVATE.LAB...	SMS_SITE_COMPONENT_MAN	7/9/2013 5:07:16 PM	2856 (0xB28)
Component SMS_WSUS_CONTROL_MANAGER flagged for installation.	SMS_SITE_COMPONENT_MAN	7/9/2013 5:07:16 PM	2856 (0xB28)
INFO: 'WIN2008-SCCM.PRIVATE.LAB' is a valid FQDN.	SMS_SITE_COMPONENT_MAN	7/9/2013 5:07:16 PM	2856 (0xB28)
STATMSG: ID=1013 SEV=I LEV=M SOURCE="SMS Server" COMP="SMS_WS...	SMS_SITE_COMPONENT_MAN	7/9/2013 5:07:16 PM	2856 (0xB28)
Synchronization complete.	SMS_SITE_COMPONENT_MAN	7/9/2013 5:07:16 PM	2856 (0xB28)

Date/Time: 7/9/2013 5:07:16 PM **Component:** SMS_SITE_COMPONENT_MANAGER
Thread: 2856 (0xB28) **Source:**

Component SMS_WSUS_CONTROL_MANAGER flagged for installation.

Elapsed time is 1006h 35m 33s 174ms (3623733.174 seconds)

FIGURE 2-6 Software update point installation can be seen in sitecomp.log

Certain prerequisites must be met before installing a SUP. For example, you need to install Windows Server Update Services (WSUS) 3.0 SP2 with KB2734608 on Windows Server 2008 in System Center 2012 Configuration Manager SP1. When you go through the WSUS installation and reach the configuration part of the WSUS, you want to cancel and exit at that point. You should not configure WSUS because the software update point will take over WSUS after it is installed. Once WSUS 3.0 SP2 plus KB 2734608 are installed, you can start installation of the software update point and configure it the way you want with categories and products. You can also review the SUPsetup.log, which provides additional details on the software update point installation process.

If you run into problems, make sure the following items have been implemented correctly:

- The port settings configured for the active SUP must be the same as the port settings configured for the WSUS website in Internet Information Services (IIS) (that is, port 8530).
- The computer and local Administrator accounts must be able to access virtual directories under the WSUS website in IIS from the site server.

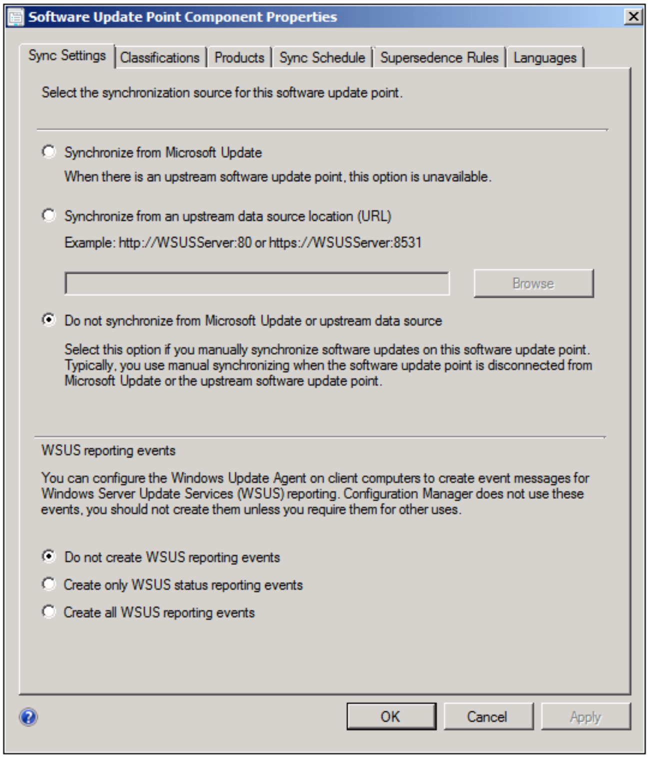
To sum up, you should review the following two logs when troubleshooting SUP installation:

- Sitecomp.log
- SUPsetup.log

Synchronizing software update points with Microsoft Update

In a Configuration Manager environment, the first step in deploying software updates to systems is to configure the SUP. From the central administration site, there are three ways to sync with a SUP (see Figure 2-7):

- **Synchronize From Microsoft Update** This option synchronizes updates directly from the Microsoft Update.
- **Synchronize From An Upstream Data Source Location (URL)** This is a new feature in Configuration Manager.
- **Do Not Synchronize From Microsoft Update Or Upstream Data Source** This option can be used to synchronize manually when the central administration site does not have access to the Internet.



Select the synchronization source for this software update point.

○ Synchronize from Microsoft Update

When there is an upstream software update point, this option is unavailable.

○ Synchronize from an upstream data source location (URL)

Example: http://WSUSServer:80 or https://WSUSServer:8531

● Do not synchronize from Microsoft Update or upstream data source

Select this option if you manually synchronize software updates on this software update point. Typically, you use manual synchronizing when the software update point is disconnected from Microsoft Update or the upstream software update point.

WSUS reporting events

You can configure the Windows Update Agent on client computers to create event messages for Windows Server Update Services (WSUS) reporting. Configuration Manager does not use these events, you should not create them unless you require them for other uses.

● Do not create WSUS reporting events

○ Create only WSUS status reporting events

○ Create all WSUS reporting events

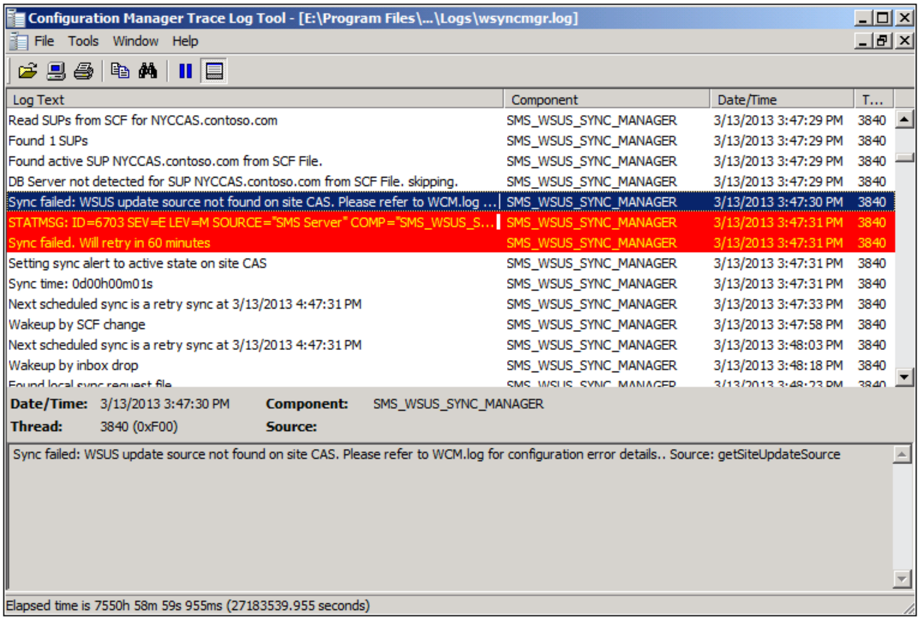
FIGURE 2-7 There are a few synchronization options for a software update point.

Troubleshooting synchronization with Microsoft Update

When you configure your software update point to synchronize with Microsoft Update, you can monitor or troubleshoot any issues by using the following logs:

- **WsynMgr.log** The wsyncmgr.log is located on the site server in the <ConfigMgrInstallationPath>\Logs folder. When there are any issues with synchronizations, it will be logged here.
- **WCM.log** The WCM.log file is located on the site server in the <ConfigMgrInstallationPath>\Logs folder. WSUS Configuration Manager connects to WSUS running on the active SUP once every hour. If there are any issues with ports or connectivity, it will log the errors.
- **WSUSCtrl.log** The WSUSCtrl.log file is located on the site server in the <ConfigMgrInstallationPath>\Logs folder. Where there are configuration or database connectivity issues, they will be logged in this log file.

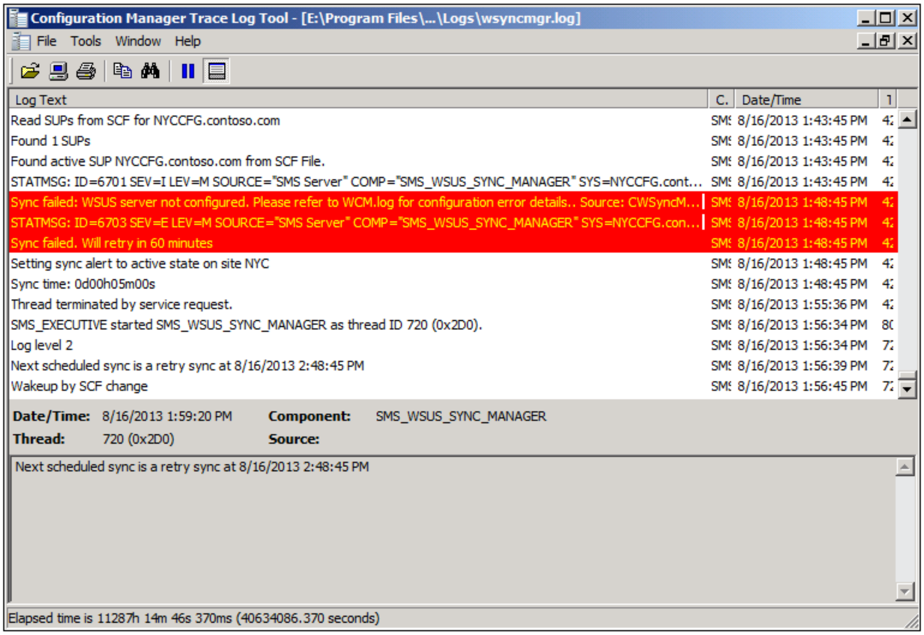
For example, you might see the errors shown in Figure 2-8 if the minimum requirement of WSUS are not detected (that is, WSUS 3.0 SP2 with KB2734608) or when the port configuration is incorrect (that is, port 80 compared to 8530).


Configuration Manager Trace Log Tool - [E:\Program Files\...\Logs\wsyncmgr.log]
File
Tools
Window
Help

```
Log Text                                                                   Component                 Date/Time               T...
Read SUPs from SCF for NYCCAS.contoso.com                                  SMS_WSUS_SYNC_MANAGER     3/13/2013 3:47:29 PM    3840
Found 1 SUPs                                                               SMS_WSUS_SYNC_MANAGER     3/13/2013 3:47:29 PM    3840
Found active SUP NYCCAS.contoso.com from SCF File.                         SMS_WSUS_SYNC_MANAGER     3/13/2013 3:47:29 PM    3840
DB Server not detected for SUP NYCCAS.contoso.com from SCF File. skipping. SMS_WSUS_SYNC_MANAGER     3/13/2013 3:47:29 PM    3840
Sync failed: WSUS update source not found on site CAS. Please refer to WCM.log ... SMS_WSUS_SYNC_MANAGER  3/13/2013 3:47:30 PM  3840
STATMSG: ID=6703 SEV=E LEV=M SOURCE="SMS Server" COMP="SMS_WSUS_S...       SMS_WSUS_SYNC_MANAGER     3/13/2013 3:47:31 PM    3840
Sync failed. Will retry in 60 minutes                                      SMS_WSUS_SYNC_MANAGER     3/13/2013 3:47:31 PM    3840
Setting sync alert to active state on site CAS                             SMS_WSUS_SYNC_MANAGER     3/13/2013 3:47:31 PM    3840
Sync time: 0d00h00m01s                                                     SMS_WSUS_SYNC_MANAGER     3/13/2013 3:47:31 PM    3840
Next scheduled sync is a retry sync at 3/13/2013 4:47:31 PM                SMS_WSUS_SYNC_MANAGER     3/13/2013 3:47:33 PM    3840
Wakeup by SCF change                                                       SMS_WSUS_SYNC_MANAGER     3/13/2013 3:47:58 PM    3840
Next scheduled sync is a retry sync at 3/13/2013 4:47:31 PM                SMS_WSUS_SYNC_MANAGER     3/13/2013 3:48:03 PM    3840
Wakeup by inbox drop                                                       SMS_WSUS_SYNC_MANAGER     3/13/2013 3:48:18 PM    3840
Found local sync request file                                              SMS_WSUS_SYNC_MANAGER     3/13/2013 3:48:23 PM    3840

Date/Time:  3/13/2013 3:47:30 PM        Component:  SMS_WSUS_SYNC_MANAGER
Thread:     3840 (0xF00)                Source:

Sync failed: WSUS update source not found on site CAS. Please refer to WCM.log for configuration error details.. Source: getSiteUpdateSource

Elapsed time is 7550h 58m 59s 955ms (27183539.955 seconds)
```

FIGURE 2-8 A synchronization failed error is displayed in wsyncmgr.log.

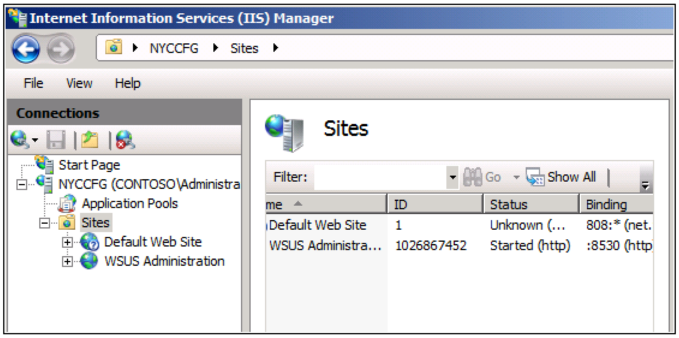
In the case of port misconfiguration, the wsyncmgr.log will report a "WSUS server not configured" message as shown in Figure 2-9. In this case, the question arises: How do you find out which port WSUS is trying to use? To find out, you should review the WCM.log file for an entry that says "Attempting connection to WSUS Server: <SiteServerName, port: <portnumber>, useSSL:<True or False>." As an example of this, if *portnumber* is listed as 80 and you configured WSUS to use the custom port 8530, then you would run into this issue.


Configuration Manager Trace Log Tool - [E:\Program Files\...\Logs\wsyncmgr.log]
File
Tools
Window
Help

```
Log Text                                                                                        C.   Date/Time              T
Read SUPs from SCF for NYCCFG.contoso.com                                                       SMS  8/16/2013 1:43:45 PM   42
Found 1 SUPs                                                                                    SMS  8/16/2013 1:43:45 PM   42
Found active SUP NYCCFG.contoso.com from SCF File.                                              SMS  8/16/2013 1:43:45 PM   42
STATMSG: ID=6701 SEV=I LEV=M SOURCE="SMS Server" COMP="SMS_WSUS_SYNC_MANAGER" SYS=NYCCFG.cont... SMS  8/16/2013 1:43:45 PM   42
Sync failed: WSUS server not configured. Please refer to WCM.log for configuration error details.. Source: CWSyncM... SMS  8/16/2013 1:48:45 PM   42
STATMSG: ID=6703 SEV=E LEV=M SOURCE="SMS Server" COMP="SMS_WSUS_SYNC_MANAGER" SYS=NYCCFG.con... SMS  8/16/2013 1:48:45 PM   42
Sync failed. Will retry in 60 minutes                                                           SMS  8/16/2013 1:48:45 PM   42
Setting sync alert to active state on site NYC                                                  SMS  8/16/2013 1:48:45 PM   42
Sync time: 0d00h05m00s                                                                          SMS  8/16/2013 1:48:45 PM   42
Thread terminated by service request.                                                           SMS  8/16/2013 1:55:36 PM   42
SMS_EXECUTIVE started SMS_WSUS_SYNC_MANAGER as thread ID 720 (0x2D0).                           SMS  8/16/2013 1:56:34 PM   80
Log level 2                                                                                     SMS  8/16/2013 1:56:34 PM   72
Next scheduled sync is a retry sync at 8/16/2013 2:48:45 PM                                     SMS  8/16/2013 1:56:39 PM   72
Wakeup by SCF change                                                                            SMS  8/16/2013 1:56:45 PM   72

Date/Time:  8/16/2013 1:59:20 PM        Component:  SMS_WSUS_SYNC_MANAGER
Thread:     720 (0x2D0)                 Source:

Next scheduled sync is a retry sync at 8/16/2013 2:48:45 PM

Elapsed time is 11287h 14m 46s 370ms (40634086.370 seconds)
```

FIGURE 2-9 A synchronization failed error is displayed in wsyncmgr.log.

Now let's say you check the IIS configuration for WSUS and you determine that it is using port 8530 as shown in Figure 2-10. If this is the case, you would also want to check the SUP properties to make sure WSUS is configured to use port 8530 and not port 80.



me	ID	Status	Binding
Default Web Site	1	Unknown (...	808:* (net.
WSUS Administra...	1026867452	Started (http)	:8530 (http

FIGURE 2-10 An example of WSUS port configuration in IIS.

If you have determined that both configurations are set to use port 8530 (or only the SUP is configured to use 8530 but not WSUS in IIS), you might want to run the following command to make sure WSUS is actually using port 8530.

```
C:\Program Files\Update Services\Tools\wsusutil.exe usecustomwebsite true
```

IMPORTANT **Sometimes, even though WSUS is shown as using 8530 in IIS Manager, it is not really using 8530 because the initial default setting (that is, port 80) is still being used.**

For the sync process to work properly, the SUP and the WSUS server must be able to communicate using the correct port (that is, 80 or 8530). A frequent experience of Microsoft Support is that even after fixing this issue (that is, port configuration, connectivity, or WSUS installation), synchronization fails at the first retry but succeeds at subsequent reties, so you might want to wait until the next retry before spending more time in troubleshooting the problem. Note also that the initial synchronization process normally takes longer than any subsequent synchronization.

NOTE **The client side workflow for software updates is covered in Chapter 3.**

Troubleshooting rotating management point and SUP failover

System Center 2012 Configuration Manager SP1 introduces several new features to support clients in an untrusted forest:

- Allowing multiple management points (MPs) so that a management point in an untrusted forest can support clients in an untrusted forest.
- Allowing multiple software update points so that a software update point in an untrusted forest can support clients in an untrusted forest.

This section examines some of the issues you need be aware of when deploying an MP or SUP in a remote forest.

Management point rotating behavior

If you have multiple MPs assigned to your primary site, clients can pick either one. However, there are number of factors involve in this process:

1. If one of the MPs is set up as HTTPS with PKI and a client has the proper PKI certificate, MP with HTTPS will be the first preference and will use that over other HTTP MPs.
2. The next preference is forest affinity for domain-joined clients where the MPs have published their information to Active Directory. If clients are in the same forest as the MP, the client would prefer that MP over other HTTP MPs assigned to the same primary site.
3. Now assume the real world scenario where you have the clients in different forests (that is, Forest C) where there is no MP but there are MPs in other forests (that is, Forest A and B). In this case, you have to be very careful when setting up remote MPs as if there is a firewall between the forests and clients in the forest that are not allowed

to communicate with any other MP but one particular forest (that is, Forest B). There is no way to guarantee that during rotating behavior a client will pick the MP from the forest (that is, Forest B) that the client is allowed to communicate with. In this scenario, you either want to have MP in the Forest C or set up one of the MPs from other Forests as HTTPS with proper PKI certificates. If this is not an option, an unsupported method that might work is using a host file to point to the specific MP.

Software update point switching/failover behavior

Multiple SUPs provide fault tolerance through failover. The way SUP failover works is that a list of SUPs is given to the client and the client chooses one from that list randomly. If the SUP it chooses cannot be reached, the client retries a minimum of four times at 30 minute intervals and after the fourth failure, it waits an additional two minutes and then tries to connect to the next SUP on the list. However, this failover behavior depends on the retry error codes received by the client when the scan fails. The WSUS component has a list of retry error codes and if the client gets the error code which is not part of this list, it will not failover to different SUP. You can find additional details around SUP switching behavior on Microsoft TechNet at *http://technet.microsoft.com/en-us/library/bcf8ed65-3bea-4bec-8bc5-22d9e54f5a6d*.

The list of error codes which would trigger a retry can be found using the following SQL query:

```
Select ID, SiteServerName, Name, Value2 as WSUSErrorCodes
from SC_Component_Property SCPROP
Join SC_SiteDefinition SCSITEDEF on SCSITEDEF.SiteNumber = SCProp.SiteNumber
where SCProp.Name = 'WSUS Scan Retry Error Codes' and SCSITEDEF.SiteCode = '<sitecode>'
'replace <sitecode> with your Primary site's site code
```

Review the list of error codes under the 'WSUSErrorCodes' column.

Application deployment troubleshooting

Application Management in Configuration Manager provides administrators with tools to manage applications in the enterprise. A new feature of Configuration Manager allows administrators to specify dependencies, supersedence, and other criteria within Application Management instead of creating different collections to deploy applications. This new functionality is much more robust than the old method of deploying legacy packages used in Configuration Manager 2007. This section examines the workflow and troubleshooting process for application deployment using Configuration Manager.

Enabling verbose logging

Before you begin troubleshooting for application deployment, always start by enabling verbose logging on the Configuration Manager client. Without verbose logging, many of the relevant log entries might not be recorded in the logs.

Client-side logging

By default, the client-side logging level is set to the value 1 in the registry. This means that Configuration Manager logs only Information, Warning, and Error messages. To enable verbose logging for those Configuration Manager logs that support it, do the following:

1. Open Registry Editor and find:

   HKLM\Software\Microsoft\CCM\Logging\@GLOBAL\LogLevel

2. Change the value of LogLevel from 1 to 0 (note that you will need to change the permissions for Administrators to have Full Control in order to change this value).
3. Restart the SMS Agent Host service.

Client-side debug logging

For even greater detail, you can enable debug logging. To enable debug logging for Configuration Manager logs, do the following:

1. Open Registry Editor and find:

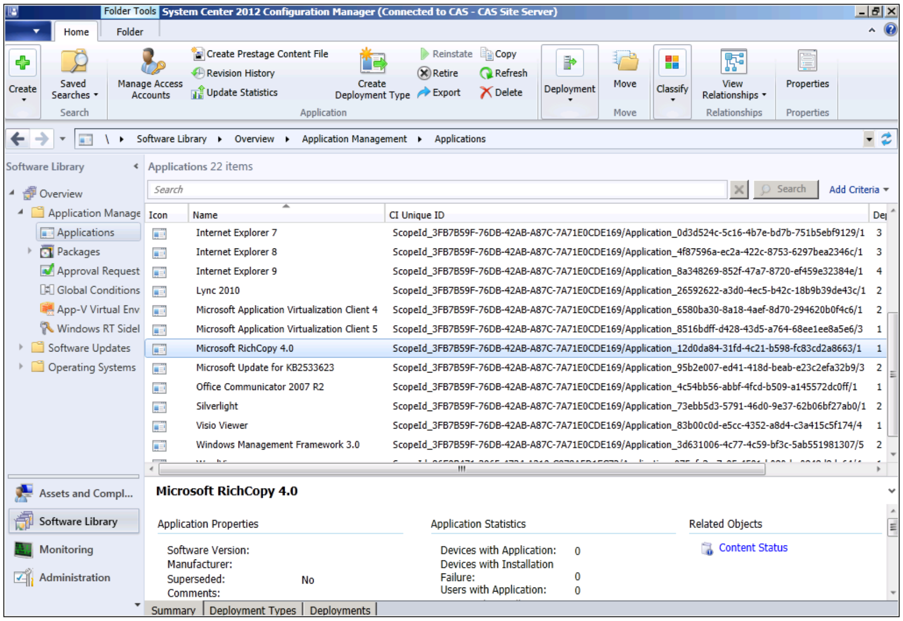
   HKLM\Software\Microsoft\CC\Logging

2. Create a new key called DebugLogging.
3. Create a new value of type REG_SZ under this key and name it Enabled.
4. Set the Enabled value to True.
5. Restart the SMS Agent Host service.

Troubleshooting application deployment

Once you enable verbose logging on the client computer, you can use the additional information the log files provide to help you troubleshoot application deployment problems. The following walkthrough demonstrates how you might do this with an example of a problem deploying Microsoft RichCopy 4.0 using Configuration Manager. Here are the steps you might follow in troubleshooting this issue:

1. Open the Configuration Manager console, select the Software Library workspace, select Applications, right-click the Name column, and add the column CI Unique ID.
2. Write down the entry shown for ScopeID_*xxxxx*/Application_*xxxx* for the problem application as shown in Figure 2-11.



Applications 22 items

Icon	Name	CI Unique ID	De
	Internet Explorer 7	ScopeId_3FB7B59F-76DB-42AB-A87C-7A71E0CDE169/Application_0d3d524c-5c16-4b7e-bd7b-751b5ebf9129/1	3
	Internet Explorer 8	ScopeId_3FB7B59F-76DB-42AB-A87C-7A71E0CDE169/Application_4f87596a-ec2a-422c-8753-6297bea2346c/1	3
	Internet Explorer 9	ScopeId_3FB7B59F-76DB-42AB-A87C-7A71E0CDE169/Application_8a348269-852f-47a7-8720-ef459e32384e/1	4
	Lync 2010	ScopeId_3FB7B59F-76DB-42AB-A87C-7A71E0CDE169/Application_26592622-a3d0-4ec5-b42c-18b9b39de43c/1	2
	Microsoft Application Virtualization Client 4	ScopeId_3FB7B59F-76DB-42AB-A87C-7A71E0CDE169/Application_6580ba30-8a18-4aef-8d70-294620b0f4c6/1	2
	Microsoft Application Virtualization Client 5	ScopeId_3FB7B59F-76DB-42AB-A87C-7A71E0CDE169/Application_8516bdff-d428-43d5-a764-68ee1ee8a5e6/3	1
	Microsoft RichCopy 4.0	ScopeId_3FB7B59F-76DB-42AB-A87C-7A71E0CDE169/Application_12d0da84-31fd-4c21-b598-fc83cd2a8663/1	1
	Microsoft Update for KB2533623	ScopeId_3FB7B59F-76DB-42AB-A87C-7A71E0CDE169/Application_95b2e007-ed41-418d-beab-e23c2efa32b9/3	2
	Office Communicator 2007 R2	ScopeId_3FB7B59F-76DB-42AB-A87C-7A71E0CDE169/Application_4c54bb56-abbf-4fcd-b509-a145572dc0ff/1	1
	Silverlight	ScopeId_3FB7B59F-76DB-42AB-A87C-7A71E0CDE169/Application_73ebb5d3-5791-46d0-9e37-62b06bf27ab0/1	2
	Visio Viewer	ScopeId_3FB7B59F-76DB-42AB-A87C-7A71E0CDE169/Application_83b00c0d-e5cc-4352-a8d4-c3a415c5f174/4	1
	Windows Management Framework 3.0	ScopeId_3FB7B59F-76DB-42AB-A87C-7A71E0CDE169/Application_3d631006-4c77-4c59-bf3c-5ab551981307/5	2

Microsoft RichCopy 4.0

Application Properties

Software Version:
Manufacturer:
Superseded: No
Comments:

Application Statistics

Devices with Application: 0
Devices with Installation Failure: 0
Users with Application: 0

Related Objects

Content Status

FIGURE 2-11 Determining the application CI unique ID from the console.

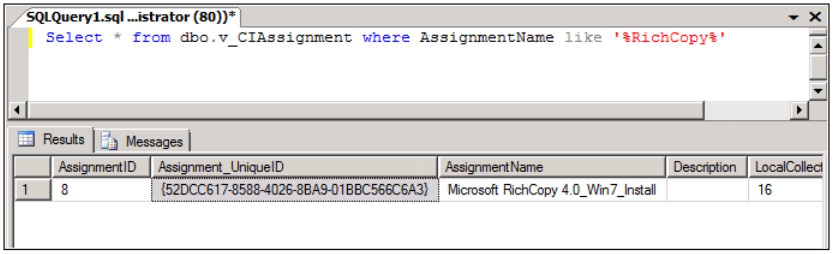
3. Use either Microsoft SQL Server Management Studio or the Configuration Manager console to get the Deployment ID. For example, using SQL Server Management Studio, you would connect to the database and run the following query to retrieve Assignment_UniqueID:

```
Select * from dbo.v_CIAssignment where AssignmentName like '%<name of the
application>%'
```

In the example here, this would be:

```
Select * from dbo.v_CIAssignment where AssignmentName like '%RichCopy%'
```

Figure 2-12 shows the results of running the above query:



```
Select * from dbo.v_CIAssignment where AssignmentName like '%RichCopy%'
```

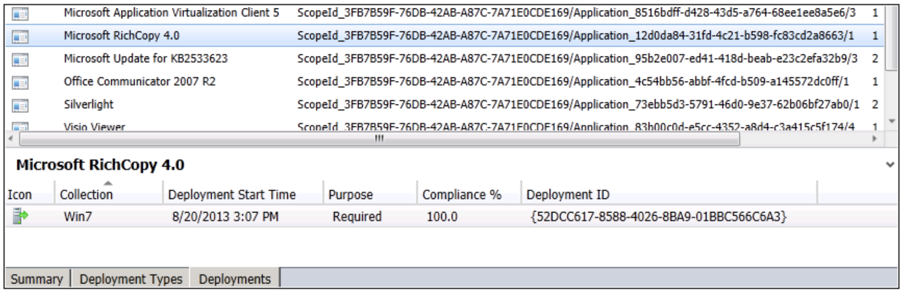
	AssignmentID	Assignment_UniqueID	AssignmentName	Description	LocalCollect
1	8	{52DCC617-8588-4026-8BA9-01BBC566C6A3}	Microsoft RichCopy 4.0_Win7_Install		16

FIGURE 2-12 Determining the PolicyID using SQL Server Management Studio.

4. Write down the Assignment_UniqueID, which in the example here is:

```
{52DCC617-8588-4026-8BA9-01BBC566C6A3}
```

5. With Applications still selected in the Configuration Manager console, add the column Deployment ID. Then highlight the application (Microsoft RichCopy 4.0) and in the lower portion of the window, click Deployments and add a Deployment ID column to get the Deployment ID for the application as shown in Figure 2-13.



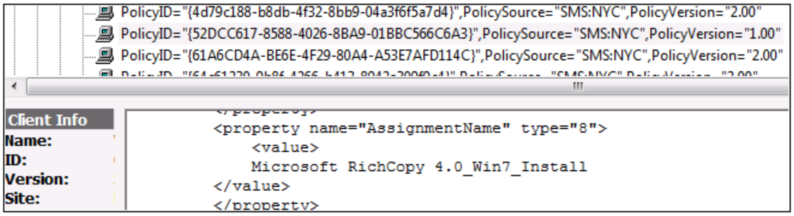
Microsoft Application Virtualization Client 5	ScopeId_3FB7B59F-76DB-42AB-A87C-7A71E0CDE169/Application_8516bdff-d428-43d5-a764-68ee1ee8a5e6/3	1
Microsoft RichCopy 4.0	ScopeId_3FB7B59F-76DB-42AB-A87C-7A71E0CDE169/Application_12d0da84-31fd-4c21-b598-fc83cd2a8663/1	1
Microsoft Update for KB2533623	ScopeId_3FB7B59F-76DB-42AB-A87C-7A71E0CDE169/Application_95b2e007-ed41-418d-beab-e23c2efa32b9/3	2
Office Communicator 2007 R2	ScopeId_3FB7B59F-76DB-42AB-A87C-7A71E0CDE169/Application_4c54bb56-abbf-4fcd-b509-a145572dc0ff/1	1
Silverlight	ScopeId_3FB7B59F-76DB-42AB-A87C-7A71E0CDE169/Application_73ebb5d3-5791-46d0-9e37-62b06bf27ab0/1	2
Visio Viewer	ScopeId_3FB7B59F-76DB-42AB-A87C-7A71E0CDE169/Application_83b00c0d-e5cc-4352-a8d4-c3a415c5f174/4	1

Microsoft RichCopy 4.0

Icon	Collection	Deployment Start Time	Purpose	Compliance %	Deployment ID
	Win7	8/20/2013 3:07 PM	Required	100.0	{52DCC617-8588-4026-8BA9-01BBC566C6A3}

FIGURE 2-13 The Console displays the Deployment ID.

The Assignment_UniqueID and Deployment ID are the same as PolicyID for this particular application (RichCopy). This means that you can use either of these IDs to track the policy on the system using PolicyAgent and other components as shown in later steps in this example. You can also use PolicySpy tool to get the PolicyID as shown in Figure 2-14.



```
PolicyID="{4d79c188-b8db-4f32-8bb9-04a3f6f5a7d4}",PolicySource="SMS:NYC",PolicyVersion="2.00"
PolicyID="{52DCC617-8588-4026-8BA9-01BBC566C6A3}",PolicySource="SMS:NYC",PolicyVersion="1.00"
PolicyID="{61A6CD4A-BE6E-4F29-80A4-A53E7AFD114C}",PolicySource="SMS:NYC",PolicyVersion="2.00"
```

Client Info
Name:
ID:
Version:
Site:

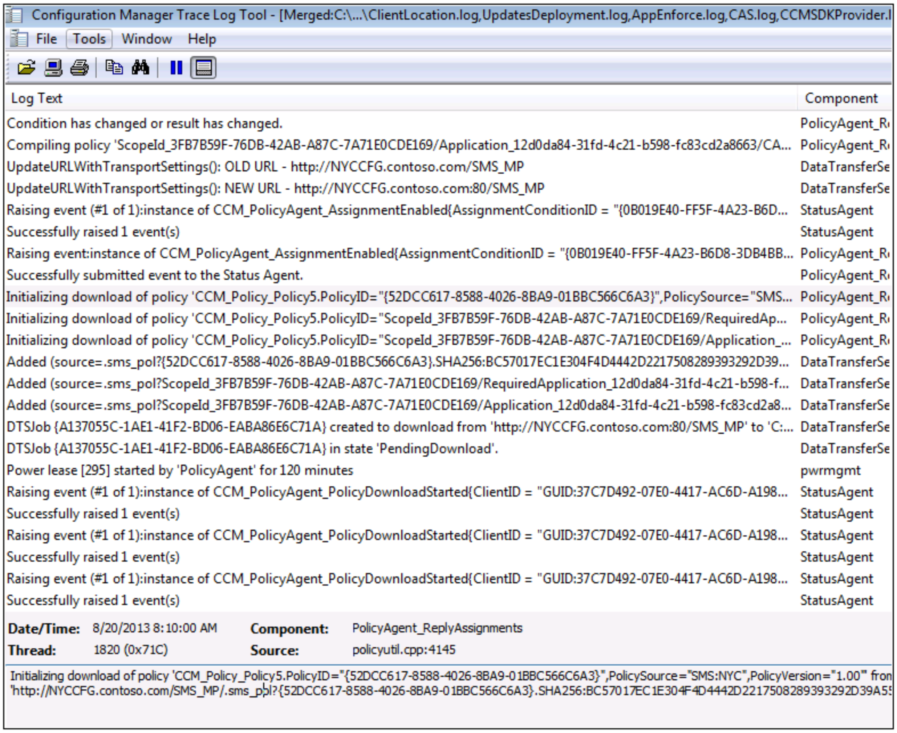
```
</property>
<property name="AssignmentName" type="8">
    <value>
    Microsoft RichCopy 4.0_Win7_Install
</value>
</property>
```

FIGURE 2-14 Determining the PolicyID using PolicySpy.

6. Open the PolicyAgent.log in the CM Trace Tool and select the policy ID determined in Figure 2-13. Look for the following entries in the
PolicyAgent.log:

```
Compiling Policy '{<policyID>}…
Initializing download of policy…
```

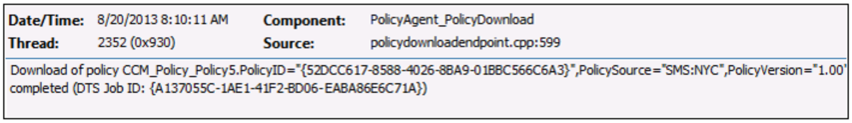
See Figure 2-15 for an example of what these entries might look like.


Configuration Manager Trace Log Tool - [Merged:C:\...\ClientLocation.log,UpdatesDeployment.log,AppEnforce.log,CAS.log,CCMSDKProvider.l
File
Tools
Window
Help

```
Log Text                                                                                                Component
Condition has changed or result has changed.                                                            PolicyAgent_R
Compiling policy 'ScopeId_3FB7B59F-76DB-42AB-A87C-7A71E0CDE169/Application_12d0da84-31fd-4c21-b598-fc83cd2a8663/CA...   PolicyAgent_R
UpdateURLWithTransportSettings(): OLD URL - http://NYCCFG.contoso.com/SMS_MP                            DataTransferSe
UpdateURLWithTransportSettings(): NEW URL - http://NYCCFG.contoso.com:80/SMS_MP                         DataTransferSe
Raising event (#1 of 1):instance of CCM_PolicyAgent_AssignmentEnabled{AssignmentConditionID = "{0B019E40-FF5F-4A23-B6D...   StatusAgent
Successfully raised 1 event(s)                                                                          StatusAgent
Raising event:instance of CCM_PolicyAgent_AssignmentEnabled{AssignmentConditionID = "{0B019E40-FF5F-4A23-B6D8-3DB4BB...   PolicyAgent_R
Successfully submitted event to the Status Agent.                                                       PolicyAgent_R
Initializing download of policy 'CCM_Policy_Policy5.PolicyID="{52DCC617-8588-4026-8BA9-01BBC566C6A3}",PolicySource="SMS...   PolicyAgent_R
Initializing download of policy 'CCM_Policy_Policy5.PolicyID="ScopeId_3FB7B59F-76DB-42AB-A87C-7A71E0CDE169/RequiredAp...   PolicyAgent_R
Initializing download of policy 'CCM_Policy_Policy5.PolicyID="ScopeId_3FB7B59F-76DB-42AB-A87C-7A71E0CDE169/Application_...   PolicyAgent_R
Added (source=.sms_pol?{52DCC617-8588-4026-8BA9-01BBC566C6A3}.SHA256:BC57017EC1E304F4D4442D2217508289393292D39...   DataTransferSe
Added (source=.sms_pol?ScopeId_3FB7B59F-76DB-42AB-A87C-7A71E0CDE169/RequiredApplication_12d0da84-31fd-4c21-b598-f...   DataTransferSe
Added (source=.sms_pol?ScopeId_3FB7B59F-76DB-42AB-A87C-7A71E0CDE169/Application_12d0da84-31fd-4c21-b598-fc83cd2a8...   DataTransferSe
DTSJob {A137055C-1AE1-41F2-BD06-EABA86E6C71A} created to download from 'http://NYCCFG.contoso.com:80/SMS_MP' to 'C:...   DataTransferSe
DTSJob {A137055C-1AE1-41F2-BD06-EABA86E6C71A} in state 'PendingDownload'.                               DataTransferSe
Power lease [295] started by 'PolicyAgent' for 120 minutes                                              pwrmgmt
Raising event (#1 of 1):instance of CCM_PolicyAgent_PolicyDownloadStarted{ClientID = "GUID:37C7D492-07E0-4417-AC6D-A198...   StatusAgent
Successfully raised 1 event(s)                                                                          StatusAgent
Raising event (#1 of 1):instance of CCM_PolicyAgent_PolicyDownloadStarted{ClientID = "GUID:37C7D492-07E0-4417-AC6D-A198...   StatusAgent
Successfully raised 1 event(s)                                                                          StatusAgent
Raising event (#1 of 1):instance of CCM_PolicyAgent_PolicyDownloadStarted{ClientID = "GUID:37C7D492-07E0-4417-AC6D-A198...   StatusAgent
Successfully raised 1 event(s)                                                                          StatusAgent

Date/Time:   8/20/2013 8:10:00 AM      Component:   PolicyAgent_ReplyAssignments
Thread:      1820 (0x71C)              Source:      policyutil.cpp:4145

Initializing download of policy 'CCM_Policy_Policy5.PolicyID="{52DCC617-8588-4026-8BA9-01BBC566C6A3}",PolicySource="SMS:NYC",PolicyVersion="1.00" fron
'http://NYCCFG.contoso.com/SMS_MP/.sms_pol?{52DCC617-8588-4026-8BA9-01BBC566C6A3}.SHA256:BC57017EC1E304F4D4442D2217508289393292D39A5
```

FIGURE 2-15 The initializing download of the policy is displayed.

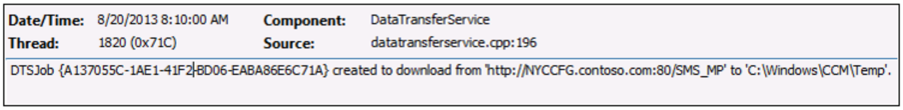
7. During the application deployment process, PolicyAgent will hand over the task to the DataTransferService component and it will create DTSJob to download the policy. So your next task is to determine the DTS Job ID. In this example, you would search for the phrase “Download of policy CCM_Policy” in the PolicyAgent.log. Once you’ve found this log entry, you can determine the DTS Job ID as shown in Figure 2-16.



```
Date/Time:   8/20/2013 8:10:11 AM      Component:   PolicyAgent_PolicyDownload
Thread:      2352 (0x930)              Source:      policydownloadendpoint.cpp:599

Download of policy CCM_Policy_Policy5.PolicyID="{52DCC617-8588-4026-8BA9-01BBC566C6A3}",PolicySource="SMS:NYC",PolicyVersion="1.00'
completed (DTS Job ID: {A137055C-1AE1-41F2-BD06-EABA86E6C71A})
```

FIGURE 2-16 You can monitor the DTSJob download process.

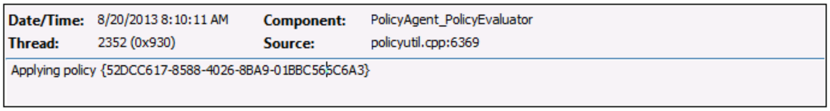
8. Now you can trace the DTS Job (that is, A137055C-41F2-BD06-EABA86E6C71A) in the DataTransferService.log and you can also find out which MP it is downloading from (this is important if you have more than one MP per site). If there are any issues with that particular MP, you might want to first fix that MP because all of the clients using that MP might also fail to download any policies (see Figure 2-17).



```
Date/Time:  8/20/2013 8:10:00 AM     Component:  DataTransferService
Thread:     1820 (0x71C)             Source:     datatransferservice.cpp:196
DTSJob {A137055C-1AE1-41F2-BD06-EABA86E6C71A} created to download from 'http://NYCCFG.contoso.com:80/SMS_MP' to 'C:\Windows\CCM\Temp'.
```

FIGURE 2-17 You can track the DTSJob ID.

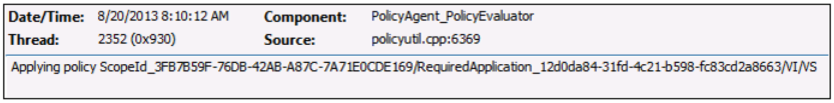
Once download of the policy has successfully completed, PolicyAgent will hand over the task of updating and applying the policy to the system to the Policy Evaluator component as shown in Figure 2-18.



```
Date/Time:  8/20/2013 8:10:11 AM     Component:  PolicyAgent_PolicyEvaluator
Thread:     2352 (0x930)             Source:     policyutil.cpp:6369
Applying policy {52DCC617-8588-4026-8BA9-01BBC566C6A3}
```

FIGURE 2-18 The policy is being applied.

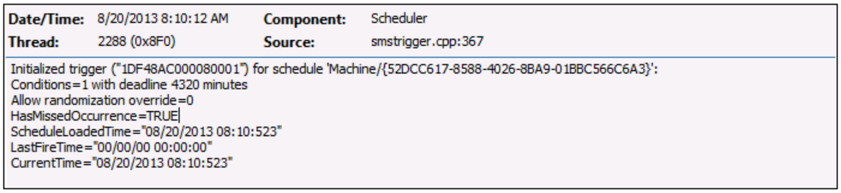
The Policy Evaluator will also compile and apply the deployment associated with the policy as shown in Figure 2-19.



```
Date/Time:  8/20/2013 8:10:12 AM     Component:  PolicyAgent_PolicyEvaluator
Thread:     2352 (0x930)             Source:     policyutil.cpp:6369
Applying policy ScopeId_3FB7B59F-76DB-42AB-A87C-7A71E0CDE169/RequiredApplication_12d0da84-31fd-4c21-b598-fc83cd2a8663/VI/VS
```

FIGURE 2-19 You can apply policy trace for deployment in PolicyEvaluator log.

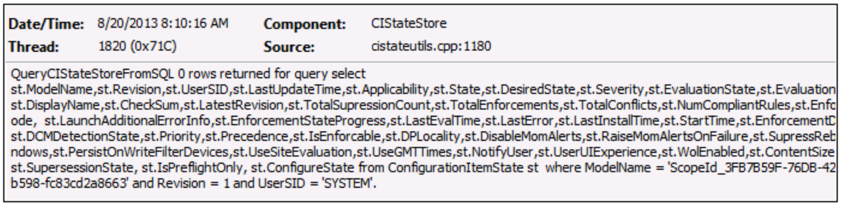
9. The PolicyEvaluator component will then update WMI (root\ccm\policy\machine\actualconfig) and you can then either use PolicySpy (under the Actual tab) or directly connect to the WMI namespace and review CCM_ApplicationCIAssignment and CCM_CIVersionInfo using the appropriate AssignmentID and ScopeId. The Schedule component will then take over and initialize the trigger for the deployment as shown in Figure 2-20. There are also a few other components, such as CIStore, CIStateStore, CIDownloader, CITaskMgr, and DCMAgent, that work together throughout this process, but we won't go into details for those components because we are focusing on the ones that are useful when troubleshooting.



```
Date/Time:  8/20/2013 8:10:12 AM     Component:  Scheduler
Thread:     2288 (0x8F0)             Source:     smstrigger.cpp:367
Initialized trigger ("1DF48AC000080001") for schedule 'Machine/{52DCC617-8588-4026-8BA9-01BBC566C6A3}':
Conditions=1 with deadline 4320 minutes
Allow randomization override=0
HasMissedOccurrence=TRUE
ScheduleLoadedTime="08/20/2013 08:10:523"
LastFireTime="00/00/00 00:00:00"
CurrentTime="08/20/2013 08:10:523"
```

FIGURE 2-20 An example of tracking a deadline trigger with Scheduler.

You can also see in the CIStateStore logs that the CIStateStore component is querying something using an SQL query as shown in Figure 2-21.



```
Date/Time:  8/20/2013 8:10:16 AM      Component:  CIStateStore
Thread:     1820 (0x71C)              Source:     cistateutils.cpp:1180

QueryCIStateStoreFromSQL 0 rows returned for query select
st.ModelName,st.Revision,st.UserSID,st.LastUpdateTime,st.Applicability,st.State,st.DesiredState,st.Severity,st.EvaluationState,st.Evaluation
st.DisplayName,st.CheckSum,st.LatestRevision,st.TotalSupressionCount,st.TotalEnforcements,st.TotalConflicts,st.NumCompliantRules,st.Enfc
ode,  st.LaunchAdditionalErrorInfo,st.EnforcementStateProgress,st.LastEvalTime,st.LastError,st.LastInstallTime,st.StartTime,st.EnforcementD
st.DCMDetectionState,st.Priority,st.Precedence,st.IsEnforcable,st.DPLocality,st.DisableMomAlerts,st.RaiseMomAlertsOnFailure,st.SupressReb
ndows,st.PersistOnWriteFilterDevices,st.UseSiteEvaluation,st.UseGMTTimes,st.NotifyUser,st.UserUIExperience,st.WolEnabled,st.ContentSize
st.SupersessionState, st.IsPreflightOnly, st.ConfigureState from ConfigurationItemState st  where ModelName = 'ScopeId_3FB7B59F-76DB-42
b598-fc83cd2a8663' and Revision = 1 and UserSID = 'SYSTEM'.
```

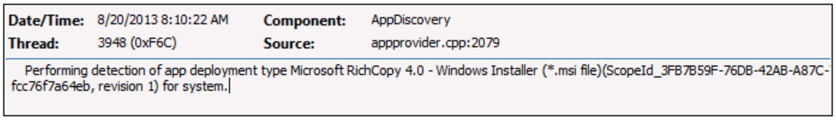
FIGURE 2-21 A view of CIStateStore log and the SQL query.

As you can see, a SQL query is being run that uses the following:

```
ModelName = 'ScopeId_3FB7xxxxx/Application_12d0da84xxxx'.
```

The ScopeID indicates that this is the same application that we are tracking (RichCopy). Since the Configuration Manager Client doesn't access the primary site database directly, the question is: Which SQL database does the CIStateStore component issue its query against? The answer is that the Configuration Manager Client has the Microsoft SQL Compact edition file located under the CCM folder (that is, CIStateDB, CIStoreDB, etc.) and it is running the query against that file, trying to determine if it has a configuration item (CI) related to the application downloaded locally. Notice in Figure 2-21 that it returned 0 rows initially.

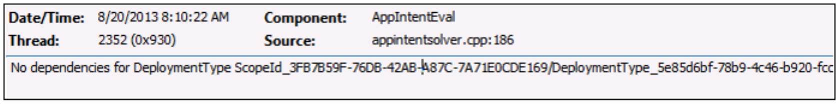
Next, the CIAgent will go through all of the dependencies of the policy CI and will work with CIAgent, CIStateStore, and CIDownloader to download them and run the SQL query again. It will then hand over the task to the AppDiscovery component to find out if this application exists (see Figure 2-22).



```
Date/Time:  8/20/2013 8:10:22 AM      Component:  AppDiscovery
Thread:     3948 (0xF6C)              Source:     appprovider.cpp:2079

  Performing detection of app deployment type Microsoft RichCopy 4.0 - Windows Installer (*.msi file)(ScopeId_3FB7B59F-76DB-42AB-A87C-
fcc76f7a64eb, revision 1) for system.
```

FIGURE 2-22 The AppDiscovery determines if the application exists.

If the application is not detected, the AppDiscovery component will hand over the task to the AppIntentEval component to find out if there are any dependencies associated with the application deployment (see Figure 2-23). If there are any dependencies, it will download and install them first.

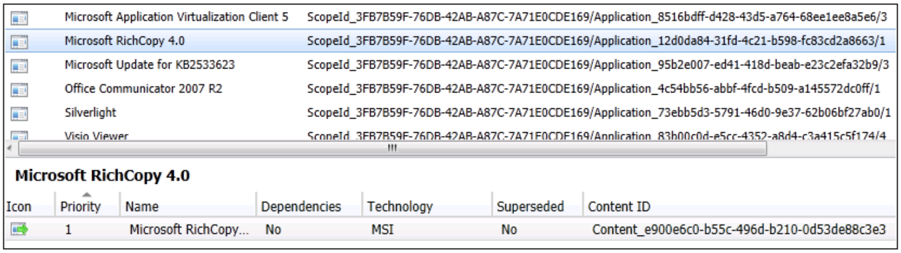


```
Date/Time:  8/20/2013 8:10:22 AM      Component:  AppIntentEval
Thread:     2352 (0x930)              Source:     appintentsolver.cpp:186

No dependencies for DeploymentType ScopeId_3FB7B59F-76DB-42AB-A87C-7A71E0CDE169/DeploymentType_5e85d6bf-78b9-4c46-b920-fcc
```

FIGURE 2-23 The AppIntentEval component identifies dependencies.

The ContentAccess component (CAS logs) will then request the content with ID Content_xxxxx together with its size and priority. The ContentTransferManager component then creates a CTM job with an ID for the download of the application to the local Configuration Manager client cache. When you are reviewing these logs (CAS and ContentTransferManager), they will now indicate the name of the application. This raises the question of how to determine which content is being requesting for download. You'll determine this next.

10. In the Configuration Manager console, select the Software Library workspace | Application Manager | Applications. Select the application (RichCopy) and in the lower portion of the window, click the Deployment Types tab to determine Content ID (that is, Content_e900e6c0-b55c-496d-b210-0d53de88c3e3) as shown in Figure 2-24.



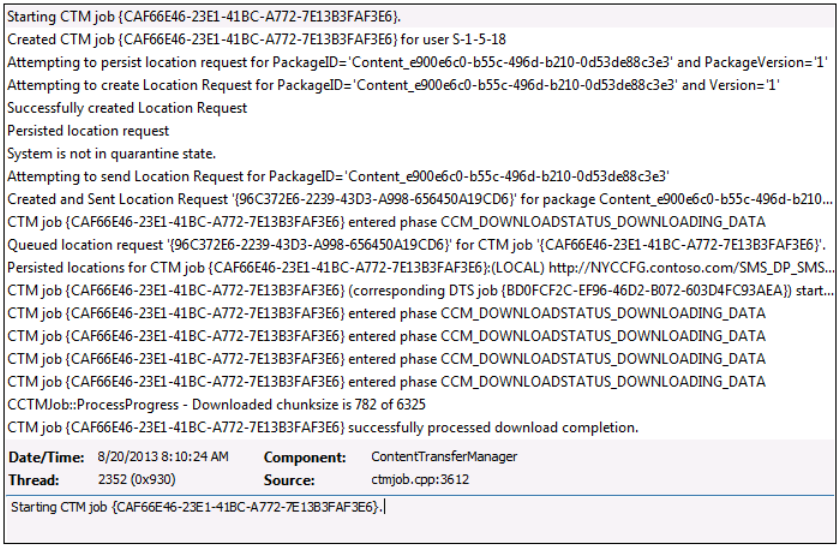
	Microsoft Application Virtualization Client 5	ScopeId_3FB7B59F-76DB-42AB-A87C-7A71E0CDE169/Application_8516bdff-d428-43d5-a764-68ee1ee8a5e6/3
	Microsoft RichCopy 4.0	ScopeId_3FB7B59F-76DB-42AB-A87C-7A71E0CDE169/Application_12d0da84-31fd-4c21-b598-fc83cd2a8663/1
	Microsoft Update for KB2533623	ScopeId_3FB7B59F-76DB-42AB-A87C-7A71E0CDE169/Application_95b2e007-ed41-418d-beab-e23c2efa32b9/3
	Office Communicator 2007 R2	ScopeId_3FB7B59F-76DB-42AB-A87C-7A71E0CDE169/Application_4c54bb56-abbf-4fcd-b509-a145572dc0ff/1
	Silverlight	ScopeId_3FB7B59F-76DB-42AB-A87C-7A71E0CDE169/Application_73ebb5d3-5791-46d0-9e37-62b06bf27ab0/1
	Visio Viewer	ScopeId_3FB7B59F-76DB-42AB-A87C-7A71E0CDE169/Application_83b00c0d-e5cc-4352-a8d4-c3a415c5f174/4

Microsoft RichCopy 4.0

Icon	Priority	Name	Dependencies	Technology	Superseded	Content ID
	1	Microsoft RichCopy...	No	MSI	No	Content_e900e6c0-b55c-496d-b210-0d53de88c3e3

FIGURE 2-24 A display of the Content ID from the console.

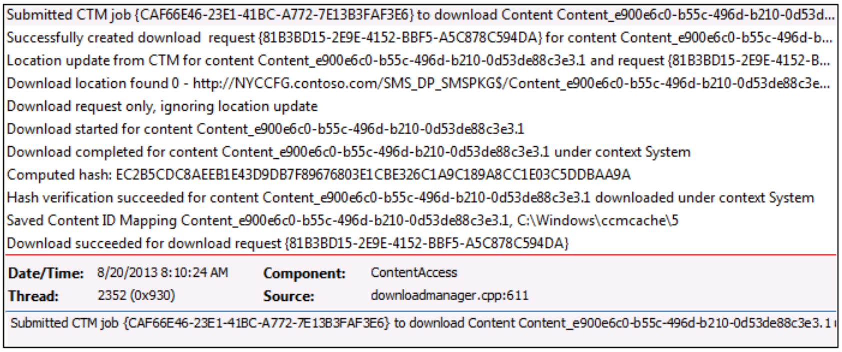
11. When you review the ContentTransferManager.log, notice that the CTM job is starting (see Figure 2-25).



```
Starting CTM job {CAF66E46-23E1-41BC-A772-7E13B3FAF3E6}.
Created CTM job {CAF66E46-23E1-41BC-A772-7E13B3FAF3E6} for user S-1-5-18
Attempting to persist location request for PackageID='Content_e900e6c0-b55c-496d-b210-0d53de88c3e3' and PackageVersion='1'
Attempting to create Location Request for PackageID='Content_e900e6c0-b55c-496d-b210-0d53de88c3e3' and Version='1'
Successfully created Location Request
Persisted location request
System is not in quarantine state.
Attempting to send Location Request for PackageID='Content_e900e6c0-b55c-496d-b210-0d53de88c3e3'
Created and Sent Location Request '{96C372E6-2239-43D3-A998-656450A19CD6}' for package Content_e900e6c0-b55c-496d-b210...
CTM job {CAF66E46-23E1-41BC-A772-7E13B3FAF3E6} entered phase CCM_DOWNLOADSTATUS_DOWNLOADING_DATA
Queued location request '{96C372E6-2239-43D3-A998-656450A19CD6}' for CTM job '{CAF66E46-23E1-41BC-A772-7E13B3FAF3E6}'.
Persisted locations for CTM job {CAF66E46-23E1-41BC-A772-7E13B3FAF3E6}:(LOCAL) http://NYCCFG.contoso.com/SMS_DP_SMS...
CTM job {CAF66E46-23E1-41BC-A772-7E13B3FAF3E6} (corresponding DTS job {BD0FCF2C-EF96-46D2-B072-603D4FC93AEA}) start...
CTM job {CAF66E46-23E1-41BC-A772-7E13B3FAF3E6} entered phase CCM_DOWNLOADSTATUS_DOWNLOADING_DATA
CTM job {CAF66E46-23E1-41BC-A772-7E13B3FAF3E6} entered phase CCM_DOWNLOADSTATUS_DOWNLOADING_DATA
CTM job {CAF66E46-23E1-41BC-A772-7E13B3FAF3E6} entered phase CCM_DOWNLOADSTATUS_DOWNLOADING_DATA
CTM job {CAF66E46-23E1-41BC-A772-7E13B3FAF3E6} entered phase CCM_DOWNLOADSTATUS_DOWNLOADING_DATA
CCTMJob::ProcessProgress - Downloaded chunksize is 782 of 6325
CTM job {CAF66E46-23E1-41BC-A772-7E13B3FAF3E6} successfully processed download completion.

Date/Time:  8/20/2013 8:10:24 AM      Component:  ContentTransferManager
Thread:     2352 (0x930)              Source:     ctmjob.cpp:3612

Starting CTM job {CAF66E46-23E1-41BC-A772-7E13B3FAF3E6}.
```

FIGURE 2-25 The ContentTransferManager.log shows that the CTM job is starting.

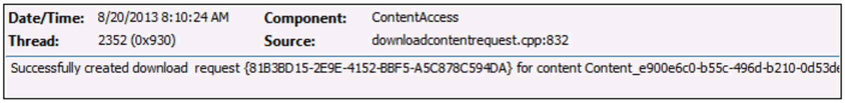
12. The question now arises: How can you determine which CTM job is being referred to by the log entry shown in Figure 2-25? The answer is that you need to find that CTM job in the CAS.log as shown in Figure 2-26.



```
Submitted CTM job {CAF66E46-23E1-41BC-A772-7E13B3FAF3E6} to download Content Content_e900e6c0-b55c-496d-b210-0d53d...
Successfully created download  request {81B3BD15-2E9E-4152-BBF5-A5C878C594DA} for content Content_e900e6c0-b55c-496d-b...
Location update from CTM for content Content_e900e6c0-b55c-496d-b210-0d53de88c3e3.1 and request {81B3BD15-2E9E-4152-B...
Download location found 0 - http://NYCCFG.contoso.com/SMS_DP_SMSPKG$/Content_e900e6c0-b55c-496d-b210-0d53de88c3e...
Download request only, ignoring location update
Download started for content Content_e900e6c0-b55c-496d-b210-0d53de88c3e3.1
Download completed for content Content_e900e6c0-b55c-496d-b210-0d53de88c3e3.1 under context System
Computed hash: EC2B5CDC8AEEB1E43D9DB7F89676803E1CBE326C1A9C189A8CC1E03C5DDBAA9A
Hash verification succeeded for content Content_e900e6c0-b55c-496d-b210-0d53de88c3e3.1 downloaded under context System
Saved Content ID Mapping Content_e900e6c0-b55c-496d-b210-0d53de88c3e3.1, C:\Windows\ccmcache\5
Download succeeded for download request {81B3BD15-2E9E-4152-BBF5-A5C878C594DA}

Date/Time:  8/20/2013 8:10:24 AM      Component:  ContentAccess
Thread:     2352 (0x930)              Source:     downloadmanager.cpp:611

Submitted CTM job {CAF66E46-23E1-41BC-A772-7E13B3FAF3E6} to download Content Content_e900e6c0-b55c-496d-b210-0d53de88c3e3.1
```

FIGURE 2-26 The Cas.log shows that the CTM job has been submitted.

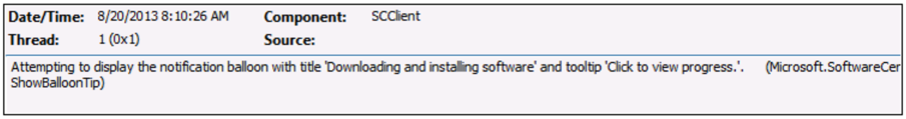
13. The ContentAccess component will also create a download request with a completely different ID for the same content ID. You can track that download request in the CAS.log to make sure the content was successfully downloaded as shown in Figure 2-27. You can then follow it through ContentTransferManager.log, CAS.log and DataTransferService.log which will provide all the details around downloading the contents, hash verification, and cache location.



```
Date/Time:  8/20/2013 8:10:24 AM      Component:  ContentAccess
Thread:     2352 (0x930)              Source:     downloadcontentrequest.cpp:832

Successfully created download  request {81B3BD15-2E9E-4152-BBF5-A5C878C594DA} for content Content_e900e6c0-b55c-496d-b210-0d53de
```

FIGURE 2-27 The download request has been successfully created.

14. You can also monitor the SCClient component by using the. _SCNotify_<username>. log which provides information around displaying notification balloons with other details such as downloading and installing software. Once the download completes, ServiceWindowManager will check to see if there are any maintenance windows specified for the system. If there are no maintenance windows specified for the system, the AppEnforce component will begin installation of the application as shown in Figure 2-28. It will also display the actual command line being executed on the client as well as the exit-code.

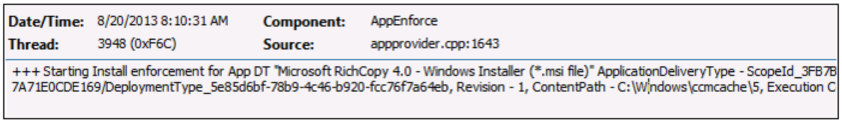


```
Date/Time:  8/20/2013 8:10:26 AM      Component:  SCClient
Thread:     1 (0x1)                   Source:

Attempting to display the notification balloon with title 'Downloading and installing software' and tooltip 'Click to view progress.'.     (Microsoft.SoftwareCer
ShowBalloonTip)
```

FIGURE 2-28 The client is attempting to display a notification balloon.

> ***IMPORTANT*** **Please note that the application installation activity is no longer logged in execmgr.log. If you use legacy software distribution process, the installation activity is logged in execmgr.log.**

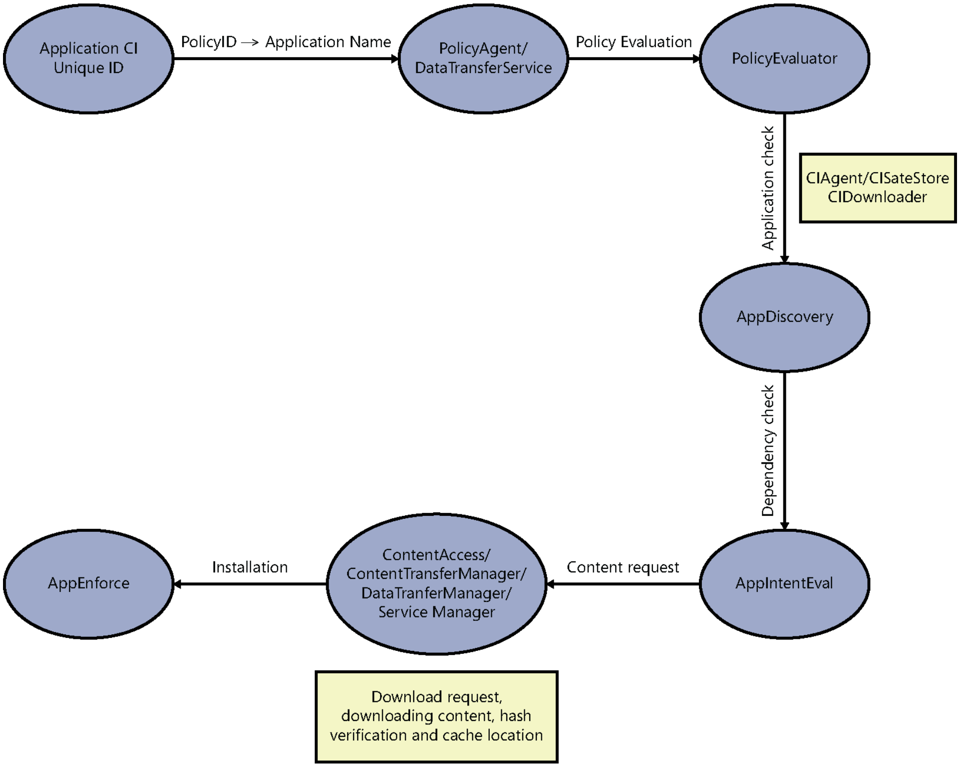
15. Finally, at the end of the installation, the AppEnforce component will perform the check again to see if application has been detected on the system (see Figure 2-29).



```
Date/Time:  8/20/2013 8:10:31 AM     Component:  AppEnforce
Thread:     3948 (0xF6C)             Source:     appprovider.cpp:1643

+++ Starting Install enforcement for App DT "Microsoft RichCopy 4.0 - Windows Installer (*.msi file)" ApplicationDeliveryType - ScopeId_3FB7B
7A71E0CDE169/DeploymentType_5e85d6bf-78b9-4c46-b920-fcc76f7a64eb, Revision - 1, ContentPath - C:\Windows\ccmcache\5, Execution C
```

FIGURE 2-29 An example of application installation tracking.

So here you have it: the end-to-end process of troubleshooting application deployment using Configuration Manager. The diagram in Figure 2-30 shows the overall application deployment process and how the various Configuration Manager components work together. The diagram does not include all of the components involved in the process, just the main ones that are useful for troubleshooting application deployment issues.



Application CI Unique ID
PolicyID → Application Name
PolicyAgent/ DataTransferService
Policy Evaluation
PolicyEvaluator
Application check
CIAgent/CISateStore CIDownloader
AppDiscovery
Dependency check
AppIntentEval
Content request
ContentAccess/ ContentTransferManager/ DataTranferManager/ Service Manager
Installation
AppEnforce
Download request, downloading content, hash verification and cache location

FIGURE 2-30 The application deployment process contains various components.

CHAPTER 3

Configuration Manager log files and troubleshooting scenarios

In Microsoft System Center 2012 Configuration Manager, client and site server components record information about the tasks and processes that take place in various log files. This client and server component logging is enabled by default and you can use these log files to help troubleshoot any issues that might occur in your Configuration Manager environment.

This chapter provides more information about some of these different log files. You can use this information when you need to examine these logs for operational details, interpreting errors, and various other troubleshooting purposes.

Software updates

Software updates in System Center 2012 Configuration Manager provide a set of tools and resources that can help manage the complex task of tracking and applying software updates to client computers in the enterprise. An effective software update management process is necessary to maintain operational efficiency, overcome security issues, and maintain the stability of the network infrastructure. However, because of the changing nature of technology and the continual appearance of new security threats, effective software update management requires consistent and continual attention.

Software update log files

Table 3-1 lists the log files that contain information related to software update points. Later in this section we'll examine how to troubleshoot various issues by using these log files.

TABLE 3-1 Log files for software update points

Log name	Description	Computer with log file
objreplmgr.log	Records details about the replication of software updates notification files from a parent to child sites.	Site server
PatchDownloader.log	Records details about the process of downloading software updates from the update source to the download destination on the site server.	The computer hosting the Configuration Manager console from which downloads are initiated
ruleengine.log	Records details about automatic deployment rules for the identification, content download, and software update group and deployment creation.	Site server
SUPSetup.log	Records details about the software update point installation. When the software update point installation completes, Installation was successful is written to this log file.	Site system server
WCM.log	Records details about the software update point configuration and connections to the Windows Server Update Services (WSUS) server for subscribed update categories, classifications, and languages.	Site server that connects to the WSUS server
WSUSCtrl.log	Records details about the configuration, database connectivity and health of the WSUS server for the site.	Site system server
wsyncmgr.log	Records details about the software updates synchronization process.	Site system server
WindowsUpdate.log	Records details about when the Windows Update Agent connects to the WSUS server and retrieves the software updates for compliance assessment and whether there are updates to the agent components.	Client

Software update workflow

The workflow for deploying software updates using Configuration Manager should follow a dynamic, interactive content model approach. The diagrams in this section provide the detailed steps to plan and configure software updates at a site.

Step 1: Prepare for software update deployment

To prepare for software update deployment, you must verify the prerequisites for software update deployment, create deployment templates, manage deployment collections, and configure maintenance windows.

Figure 3-1 shows the process flow for creating a deployment template. The SMS Provider creates the deployment template in the Configuration Manager database.

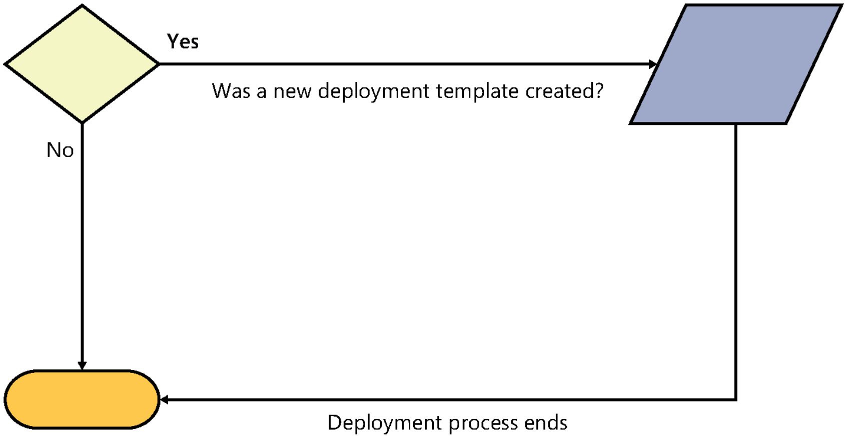


FIGURE 3-1 The process for creating a deployment template.

Step 2: Add software updates to an update list and download the update files

In this step, you create a search folder to find software updates, add software updates to an update list, and download the update files to a deployment package. The process is shown in Figure 3-2 and can be described as follows:

1. The SMS Provider creates a new configuration item for the update list in the Configuration Manager database and associates the software updates to the update list. SQL triggers create table change notifications.
2. Database notification monitors create notification files and object replication manager processes the configuration items.

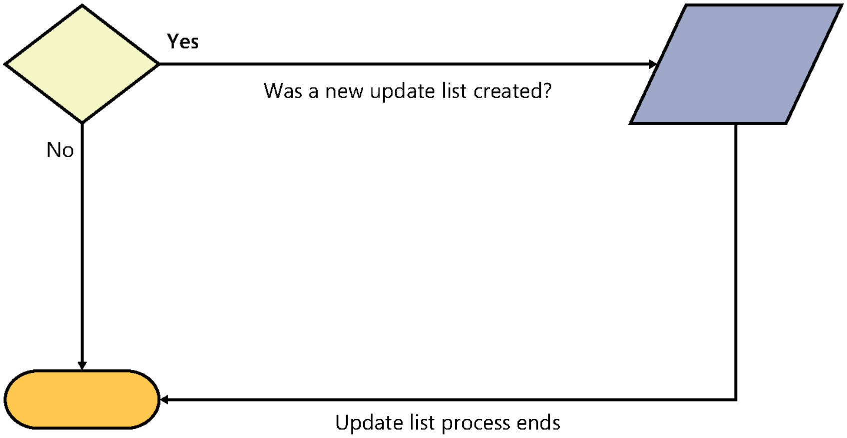


FIGURE 3-2 The process for creating an update list.

The process then continues, as shown in Figure 3-3, and can be described as follows:

1. The SMS Provider creates the deployment package in the site database and determines which software update files need to be downloaded to the source location. SQL triggers add table change notifications in the site database.
2. Database Notification Monitor then creates the deployment packages, copies the software updates to the distribution points specified in the deployment package, and creates policy notification files. Policy provider updates any associated assignment policies.
3. The SMS Provider updates the deployment packages in the database and determines which software update files need to be downloaded to the source location.
4. Software updates patch downloader downloads the update file from the configured download location, verifies the file hash, checks for certification revocation, and moves the update files to the package source share.
5. Once all the software update files that need to be downloaded have been downloaded, the SMS Provider updates the deployment packages in the database and initiates a package refresh. A SQL trigger adds a table change notification in the site database.
6. Database Notification Monitor creates a package notification file.
7. Distribution Manager updates the deployment package, copies software updates to the distribution points specified in the deployment package, and creates a policy notification file.
8. Policy Provider updates any associated assignment policies.

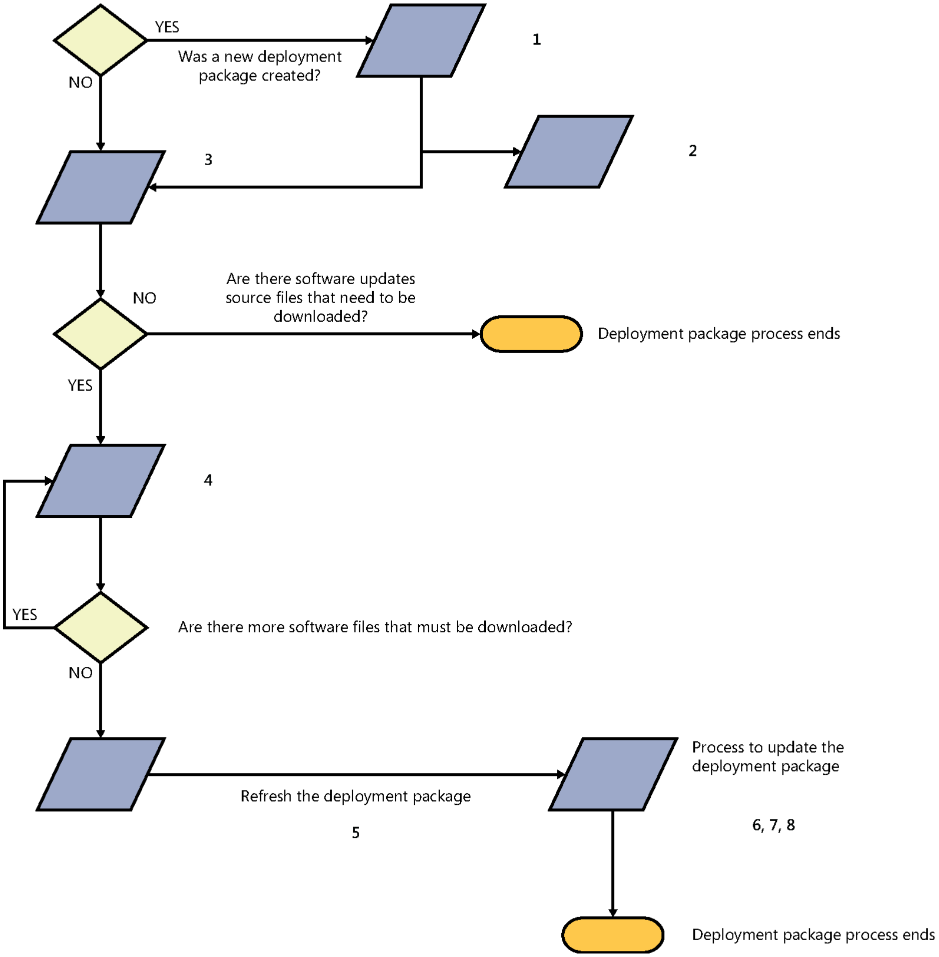

YES
Was a new deployment package created?
NO
1
2
3
Are there software updates source files that need to be downloaded?
NO
Deployment package process ends
YES
4
YES
Are there more software files that must be downloaded?
NO
Process to update the deployment package
Refresh the deployment package
5
6, 7, 8
Deployment package process ends

FIGURE 3-3 The process continues by downloading the update files.

Step 3: Create the software update deployment

In this step, you use the update list and deployment template to initiate software update deployment and create the deployment using the Deploy Software Updates Wizard. The process is shown in Figure 3-4 and can be described as follows:

1. The SMS Provider retrieves information about the update list, determines what software updates are in the update list, whether there are software updates that require license terms approval, and retrieves information about the deployment template and the settings stored in the template.
2. The SMS Provider inserts the deployment (assignment) information into the Configuration Manager site database. An SQL trigger adds a table change notification to the site database.

3. If Network Access Protection (NAP) evaluation is enabled in the deployment, the SMS Provider updates the software updates (configuration items) in the deployment with the NAP effective date and creates the software update deployment assignment policy.
4. If NAP evaluation is not enabled, the Database Notification Monitor creates a file notification, CI Assignment Manager creates the deployment assignment in the Configuration Manager site database, and Policy Provider creates the policy for the deployment assignment. Status message ID 5800 is created when the process completes.

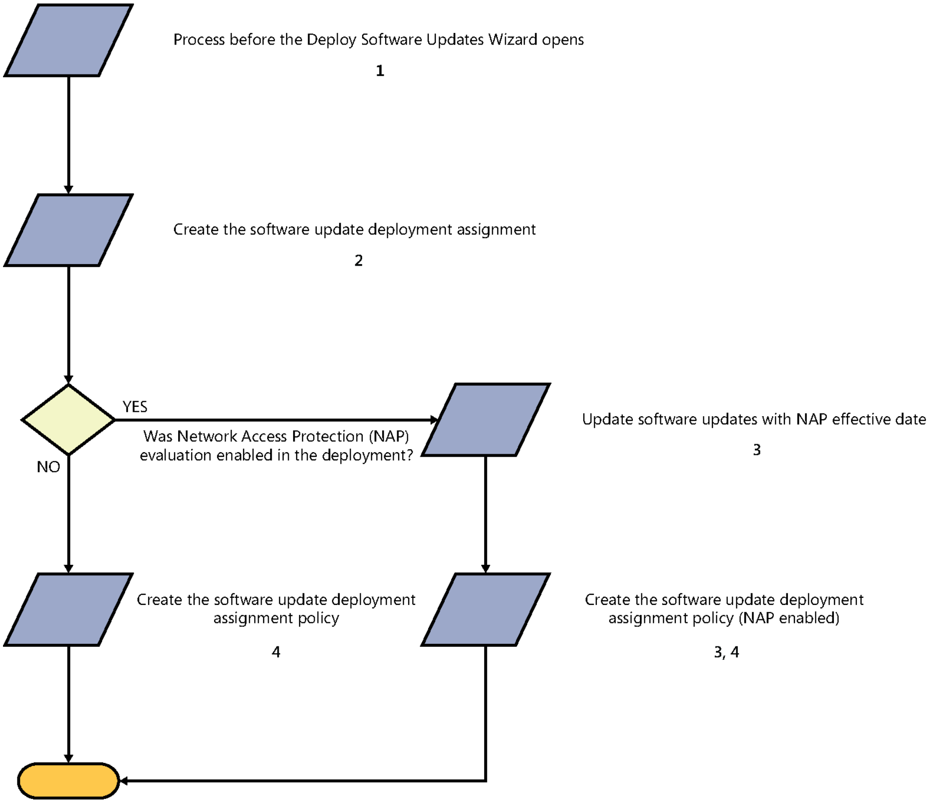

Process before the Deploy Software Updates Wizard opens
1
Create the software update deployment assignment
2
YES
Was Network Access Protection (NAP) evaluation enabled in the deployment?
NO
Update software updates with NAP effective date
3
Create the software update deployment assignment policy
4
Create the software update deployment assignment policy (NAP enabled)
3, 4

FIGURE 3-4 Software update deployment follows this process.

Troubleshooting software update issues

Errors might occur during the process of installing and configuring a software update point. This typically happens when any of the following are not configured properly:

- When the active software update point is installed on a remote site system server, the WSUS Administration console must be installed on the site server.

- The port settings configured for the active software update point must be the same as the port settings configured for the WSUS website in Internet Information Services (IIS).
- The computer and Administrator accounts must be able to access virtual directories under the WSUS website in IIS from the site server.
- When the site is running in native mode or when the software update point is configured to communicate by using SSL, the HTTPS port setting must be set correctly, specific WSUS virtual directories must be configured to require SSL, a web server signing certificate must be configured, and the WSUSUtil command-line tool must be run on the software update point.

Keeping software updated is essential in any networked, distributed computing environment. An effective software update management process is important to help maintain operational efficiency, prevent security problems, and maintain the stability of the infrastructure. However, because of the changing nature of technology and the continual appearance of new security threats, the task of effective software update management can often be challenging.

The software updates capabilities included in System Center 2012 Configuration Manager SP1 provide a set of tools and resources that can help you manage the complex task of tracking and applying software updates to client computers in the enterprise.

Troubleshooting the server side

The Configuration Manager component that takes care of software updates is called the software update point. The first step in troubleshooting software update issues is therefore to check whether your software update point is properly installed. If it is installed correctly you will see entries in your SUPSetup.log similar to those shown in this section. Specifically, you should see “SMSWSUS Setup Started” and “Installing the SMSWSUS” entries to indicate that installation of the software update point has commenced, and an “Installation was successful” entry to indicate that installation of the software update point has succeeded.

SUPSETUP.LOG

The SUPsetup.log file records details about the installation of the software update point. When the software update point installation has completed, the entry “Installation was successful” is written to the log as shown here.

```
<04-27-2013 23:51:04> =================================================================
<04-27-2013 23:51:04> SMSWSUS Setup Started....
<04-27-2013 23:51:04> Parameters: C:\PROGRA~1\MICROS~1\bin\i386\ROLESE~1.EXE /install /
siteserver:SCCM SMSWSUS
<04-27-2013 23:51:04> Installing Pre Reqs for SMSWSUS
<04-27-2013 23:51:04>   ======== Installing Pre Reqs for Role SMSWSUS ========
<04-27-2013 23:51:04> Found 0 Pre Reqs for Role SMSWSUS
```

```
<04-27-2013 23:51:04>   ======== Completed Installion of Pre Reqs for Role SMSWSUS
========
<04-27-2013 23:51:04> Installing the SMSWSUS
<04-27-2013 23:51:04> Correct and supported WSUS Server version is installed.
<04-27-2013 23:51:04> Invoking process
"C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe" "C:\Program Files\Microsoft
Configuration Manager\bin\i386\wsusmsp.dll"
<04-27-2013 23:51:30> Registered DLL C:\Program Files\Microsoft Configuration Manager\
bin\i386\wsusmsp.dll
<04-27-2013 23:51:30> Installation was successful.
```

WSUSCTRL.LOG

The WSUSctrl.log file records details about the configuration, database connectivity, and health of the WSUS server for the site. Once the software installation point has been installed, you need to make sure that it is configured properly. The logs that can be of help concerning this are WCM.log and WSUSctrl.log. If you find errors in these logs, make sure that WSUS is working properly as well. If WSUS is configured properly, the logs should display information about the WSUS role registry key information as shown here in the log excerpt for WSUSctrl.log. This log will also display information about the WSUS admin DDL, successful connection to the local WSUS server and Configuration Manager database, and the health of the WSUS server.

```
SMS_EXECUTIVE started SMS_WSUS_CONTROL_MANAGER as thread ID 3432 (0xD68).
SMS_WSUS_CONTROL_MANAGER   4/27/2013 11:51:33 PM   3216 (0x0C90)
This is a WSUS Role as WSUS registry key exists.   SMS_WSUS_CONTROL_MANAGER   4/27/2013
11:51:33 PM   3432 (0x0D68)
Found WSUS Admin dll of assembly version Microsoft.UpdateServices.Administration,
Version=3.0.6000.273, Major Version = 0x30000, Minor Version = 0x17700111
SMS_WSUS_CONTROL_MANAGER   4/27/2013 11:51:33 PM   3432 (0x0D68)
Found WSUS Admin dll of assembly version Microsoft.UpdateServices.Administration,
Version=3.1.6001.1, Major Version = 0x30001, Minor Version = 0x17710001
SMS_WSUS_CONTROL_MANAGER   4/27/2013 11:51:33 PM   3432 (0x0D68)
Found WSUS Admin dll of assembly version Microsoft.UpdateServices.Administration,
Version=2.0.0.0, Major Version = 0x20000, Minor Version = 0x0   SMS_WSUS_CONTROL_MANAGER
4/27/2013 11:51:33 PM   3432 (0x0D68)
The installed WSUS build has the valid and supported WSUS Administration DLL assembly
version (3.1.7600.226)   SMS_WSUS_CONTROL_MANAGER   4/27/2013 11:51:33 PM   3432
(0x0D68)
Successfully connected to local WSUS server   SMS_WSUS_CONTROL_MANAGER   4/27/2013
11:51:33 PM   3432 (0x0D68)
Local WSUS Server Proxy settings are correctly configured as Proxy Name  and Proxy Port
80   SMS_WSUS_CONTROL_MANAGER   4/27/2013 11:51:35 PM   3432 (0x0D68)
Waiting for changes for 0 minutes   SMS_WSUS_CONTROL_MANAGER   4/27/2013 11:51:35 PM
3432 (0x0D68)
```

```
Timed Out...   SMS_WSUS_CONTROL_MANAGER   4/27/2013 11:51:35 PM   3432 (0x0D68)
……………………..
……………………..
……………………..
   SMS_WSUS_CONTROL_MANAGER   4/27/2013 11:51:35 PM   3432 (0x0D68)
There are no unhealthy WSUS Server components on WSUS Server SCCM
SMS_WSUS_CONTROL_MANAGER   4/27/2013 11:51:35 PM   3432 (0x0D68)
Successfully checked database connection on WSUS server SCCM   SMS_WSUS_CONTROL_MANAGER
4/27/2013 11:51:38 PM   3432 (0x0D68)
```

WCM.LOG

The WCM.log file records details about the software update point configuration and its connections to the WSUS server for subscribed update categories, classifications, and languages.

```
This SCCM system is the Top Site where WSUS Server is configured to Sync from Microsoft
Update (WU/MU) OR do not Sync.   SMS_WSUS_CONFIGURATION_MANAGER   4/27/2013 11:50:36 PM
5992 (0x1768)
Found WSUS Admin dll of assembly version Microsoft.UpdateServices.Administration,
Version=3.0.6000.273, Major Version = 0x30000, Minor Version = 0x17700111
SMS_WSUS_CONFIGURATION_MANAGER   4/27/2013 11:50:37 PM   5992 (0x1768)
Found WSUS Admin dll of assembly version Microsoft.UpdateServices.Administration,
Version=3.1.6001.1, Major Version = 0x30001, Minor Version = 0x17710001
SMS_WSUS_CONFIGURATION_MANAGER   4/27/2013 11:50:37 PM   5992 (0x1768)
Found WSUS Admin dll of assembly version Microsoft.UpdateServices.Administration,
Version=2.0.0.0, Major Version = 0x20000, Minor Version = 0x0
SMS_WSUS_CONFIGURATION_MANAGER   4/27/2013 11:50:37 PM   5992 (0x1768)
The installed WSUS build has the valid and supported WSUS Administration DLL assembly
version (3.1.7600.226)   SMS_WSUS_CONFIGURATION_MANAGER   4/27/2013 11:50:37 PM   5992
(0x1768)
Successfully connected to server: SCCM.MYLAB.IN, port: 80, useSSL: False   SMS_WSUS_
CONFIGURATION_MANAGER   4/27/2013 11:51:23 PM   5992 (0x1768)
Verify Upstream Server settings on the Active WSUS Server
SMS_WSUS_CONFIGURATION_MANAGER   4/27/2013 11:51:23 PM   5992 (0x1768)
Successfully configured WSUS Server settings and Upstream Server to Microsoft Update
SMS_WSUS_CONFIGURATION_MANAGER   4/27/2013 11:51:34 PM   5992 (0x1768)
Successfully connected to server: SCCM.MYLAB.IN, port: 80, useSSL: False
SMS_WSUS_CONFIGURATION_MANAGER   4/27/2013 11:51:39 PM   5992 (0x1768)
……………………….
……………………….
STATMSG: ID=6617 SEV=E LEV=M SOURCE="SMS Server" COMP="SMS_WSUS_CONFIGURATION_MANAGER"
SYS=SCCM SITE=LAB PID=3040 TID=5992 GMTDATE=Tue Apr 27 18:23:49.259 2010 ISTR0=""
ISTR1="" ISTR2="" ISTR3="" ISTR4="" ISTR5="" ISTR6="" ISTR7="" ISTR8="" ISTR9=""
NUMATTRS=0   SMS_WSUS_CONFIGURATION_MANAGER   4/27/2013 11:53:49 PM   5992 (0x1768)
```

```
completed unpublishing previous clients   SMS_WSUS_CONFIGURATION_MANAGER   4/27/2013
11:53:49 PM   5992 (0x1768)
completed checking for client deployment   SMS_WSUS_CONFIGURATION_MANAGER   4/27/2013
11:53:49 PM   5992 (0x1768)
Successfully inserted the WSUS Enterprise Update Source object {A36F27F1-F657-437E-9EBF-
8531FE189A6B}   SMS_WSUS_CONFIGURATION_MANAGER   4/27/2013 11:54:03 PM   5992 (0x1768)
```

WSUSSYNCMGR.LOG

The WSUSsyncmgr.log file tracks the details of the software updates synchronization process. Once you have confirmed that WSUS has been configured properly, you next need to ensure that the software update point is able to synchronize with the Microsoft Update Catalog website. The WSUSsyncmgr.log can be used for this purpose.

```
Performing sync on local request   SMS_WSUS_SYNC_MANAGER   4/27/2013 11:59:54 PM   6112
(0x17E0)
STATMSG: ID=6701 SEV=I LEV=M SOURCE="SMS Server" COMP="SMS_WSUS_SYNC_MANAGER" SYS=SCCM
SITE=LAB PID=3040 TID=6112 GMTDATE=Tue Apr 27 18:29:54.530 2010 ISTR0="" ISTR1=""
ISTR2="" ISTR3="" ISTR4="" ISTR5="" ISTR6="" ISTR7="" ISTR8="" ISTR9="" NUMATTRS=0
SMS_WSUS_SYNC_MANAGER   4/27/2013 11:59:54 PM   6112 (0x17E0)
STATMSG: ID=6704 SEV=I LEV=M SOURCE="SMS Server" COMP="SMS_WSUS_SYNC_MANAGER" SYS=SCCM
SITE=LAB PID=3040 TID=6112 GMTDATE=Tue Apr 27 18:30:18.547 2010 ISTR0="" ISTR1=""
ISTR2="" ISTR3="" ISTR4="" ISTR5="" ISTR6="" ISTR7="" ISTR8="" ISTR9="" NUMATTRS=0
SMS_WSUS_SYNC_MANAGER   4/28/2013 12:00:18 AM   6112 (0x17E0)
Synchronizing WSUS server SCCM   SMS_WSUS_SYNC_MANAGER   4/28/2013 12:00:18 AM   6112
(0x17E0)
Synchronizing WSUS server sccm.mylab.in ...   SMS_WSUS_SYNC_MANAGER   4/28/2013 12:02:16
AM   5220 (0x1464)
sync: Starting WSUS synchronization   SMS_WSUS_SYNC_MANAGER   4/28/2013 12:02:16 AM
5220 (0x1464)
sync: WSUS synchronizing categories   SMS_WSUS_SYNC_MANAGER   4/28/2013 12:02:44 AM
5220 (0x1464)

Synchronizing update e6d5e961-e5c4-4816-b414-648feba450b7   SMS_WSUS_SYNC_MANAGER
28/04/2013 5:53:10 PM   4380 (0x111C)
Synchronizing update 35a0b603-61ce-4f1e-b2dd-3cc36cdf8b31   SMS_WSUS_SYNC_MANAGER
28/04/2013 5:53:11 PM   4380 (0x111C)
Synchronizing update 333bf753-7abb-4fce-a15f-a1862ecf838b   SMS_WSUS_SYNC_MANAGER
28/04/2013 5:53:11 PM   4380 (0x111C)
Synchronizing update 136df562-d188-4e79-8879-8d8082c97614:  Definition Update for
Windows Defender - KB915597 (Definition 1.81.438.0)   SMS_WSUS_SYNC_MANAGER   28/04/2013
5:53:12 PM   4380 (0x111C)
Done synchronizing SMS with WSUS Server sccmcen.scs.in   SMS_WSUS_SYNC_MANAGER
28/04/2013 5:53:13 PM   4380 (0x111C)
STATMSG: ID=6702 SEV=I LEV=M SOURCE="SMS Server" COMP="SMS_WSUS_SYNC_MANAGER"
```

```
SYS=SCCMCEN SITE=CEN PID=1880 TID=3256 GMTDATE=Wed Apr 28 12:23:13.745 2010 ISTR0=""
ISTR1="" ISTR2="" ISTR3="" ISTR4="" ISTR5="" ISTR6="" ISTR7="" ISTR8="" ISTR9=""
NUMATTRS=0   SMS_WSUS_SYNC_MANAGER   28/04/2013 5:53:13 PM   3256 (0x0CB8)
Updated 3072 items in SMS database, new update source content version is 2
SMS_WSUS_SYNC_MANAGER   28/04/2013 5:53:13 PM   3256 (0x0CB8)
```

Once synchronization has been successfully completed, updates should be available in the update repository. At this point you can go ahead and create your deployment template and schedule for installation. Once this has been done, and you check the status messages for your created update packages, you should find the status messages such as “Distribution Manager successfully processed package - Package name” as shown here:

```
Severity   Type   Site code   Date / Time   System   Component   Message ID
Description
Information   Milestone   CEN   28/04/2013 4:21:28 PM   SCCMCEN
SMS_DISTRIBUTION_MANAGER   2301   SMS Distribution Manager successfully processed
package "TEST" (package ID = CEN00003).
Information   Milestone   CEN   28/04/2013 4:21:27 PM   SCCMCEN
SMS_DISTRIBUTION_MANAGER   2300   SMS Distribution Manager is beginning to process
package "TEST" (package ID = CEN00003).
Information   Milestone   CEN   28/04/2013 4:21:21 PM   SCCMCEN
SMS_DISTRIBUTION_MANAGER   2330   SMS Distribution Manager successfully distributed
package "CEN00003" to distribution point
"["Display=\\SCCMCEN\"]MSWNET:["SMS_SITE=CEN"]\\SCCMCEN\".
Info
 Distribution Manager is beginning to process package "TEST" (package ID = CEN00003).
Information   Audit   CEN   28/04/2013 4:20:59 PM   SCCMCEN
Microsoft.ConfigurationManagement.dll   30068   User "SCS\Administrator" updated a
package named " TEST  " (CEN00003) to the site distribution points.
Information   Milestone   CEN   28/04/2013 4:12:14 PM   SCCMCEN
SMS_DISTRIBUTION_MANAGER   2300   SMS Distribution Manager is beginning to process
package "TEST" (package ID = CEN00003).
Information   Milestone   CEN   28/04/2013 4:12:08 PM   SCCMCEN
SMS_DISTRIBUTION_MANAGER   2301   SMS Distribution Manager successfully processed
package "TEST" (package ID = CEN00003).
Information   Milestone   CEN   28/04/2013 4:12:06 PM   SCCMCEN
SMS_DISTRIBUTION_MANAGER   2330   SMS Distribution Manager successfully distributed
package "CEN00003" to distribution point
Distribution Manager is beginning to process package "TEST" (package ID = CEN00003).
Information   Audit   CEN   28/04/2013 4:11:21 PM   SCCMCEN
Microsoft.ConfigurationManagement.dll   30125   User "SCS\Administrator" added new
distribution points to a package named " TEST  " (CEN00003).
Information   Audit   CEN   28/04/2013 4:11:20 PM   SCCMCEN
Microsoft.ConfigurationManagement.dll   30000   User "SCS\Administrator" created a
package named " TEST  " (CEN00003).
```

Once all these steps have completed, the remainder of the process happens in the client.

Troubleshooting the client side

The Software Updates Client Agent is heavily dependent upon the default software update components on the client system. Thus the Software Updates Client Agent often faces similar challenges as those seen for WSUS deployments. There are a number of log files you can use in Configuration Manager to help you troubleshoot client issues. These log files are located on both the client computer and on the site server. On the client side, the first thing you should check is the LocationServices.log to make sure that the correct software update point has been detected by the client. After that, you need to make sure that the client is correctly reporting to the site server and that the software update point has been enabled. Make sure also that the server name and port are specified correctly.

LOCATIONSERVICES.LOG

The LocationServices.log file can be used to identify client activity for locating management points, software update points, and distribution points. The LocationServices.log also shows information about which client is reporting to which management point/distribution point as shown by the entry “WSUS Path / Distribution Point path” here:

```
Calling back with the following WSUS locations LocationServices   4/29/2013 10:39:40 AM
2844 (0x0B1C)
WSUS Path='https://SCCMCEN.SCS.IN:443', Server='SCCMCEN', Version='2'   LocationServices
4/29/2013 10:39:40 AM   2844 (0x0B1C)
Calling back with locations for WSUS request {10066528-1C1B-4A0C-958B-F29ACBEDBBDF}
LocationServices   4/29/2013 10:41:31 AM  2844 (0x0B1C)
Calling back with the following distribution points   LocationServices   4/29/2013
11:27:23 AM  2552 (0x09F8)
Distribution Point='\\SCCMCEN.SCS.IN\SMSPKGC$\CEN00003\4ea80bd5-c8ac-4f98-
be8a-1c18f24a34e4', Locality='LOCAL', DPType='SERVER', Version='6487',
Capabilities='<Capabilities SchemaVersion="1.0"><Property Name="SSL"
Version="1"/></Capabilities>', Signature=''   LocationServices   4/29/2013 11:27:23 AM
2552 (0x09F8)
```

WUAHANDLER.LOG

Once the policy agent has triggered the scan cycle, the Windows Update Agent on the client will contact the WSUS server, which in the example shown here is also a software update point. Once scanning has successfully completed, a state message is sent to the site server. This can be verified in the WindowsUpdate.log or you can check the WUAhandler.log as shown here:

```
Async searching of updates using WUAgent started.   WUAHandler   4/29/2013 10:42:20 AM
3488 (0x0DA0)
```

```
Async searching completed.   WUAHandler   4/29/2013 11:24:21 AM  1496 (0x05D8)
Successfully completed scan.   WUAHandler   4/29/2013 11:24:25 AM  2752 (0x0AC0)
Its a WSUS Update Source type ({D4F72DDB-F6C4-4B05-835F-A8C23098857A}), adding it.
WUAHandler   4/29/2013 11:25:24 AM   2752 (0x0AC0)
Existing WUA Managed server was already set (https://SCCMCEN.SCS.IN:443), skipping Group
Policy registration.   WUAHandler   4/29/2013 11:25:25 AM  2752 (0x0AC0)
Added Update Source ({D4F72DDB-F6C4-4B05-835F-A8C23098857A}) of content type: 2
WUAHandler   4/29/2013 11:25:25 AM   2752 (0x0AC0)
Async searching of updates using WUAgent started.   WUAHandler   4/29/2013 11:25:25 AM
2752 (0x0AC0)
Async searching completed.   WUAHandler   4/29/2013 11:26:28 AM  2396 (0x095C)
Successfully completed scan.   WUAHandler   4/29/2013 11:26:32 AM  3756 (0x0EAC)
```

Completion of scanning is important; when the policy agent triggers the software update deployment cycle, the scan result is compared with the catalog so that only the required updates will be downloaded and installed according to schedule. More information concerning this process can be found in the updatestore.log, updatedeploymemt.log, and windowsupdate.log log files as shown in this section.

> ***TIP*** **If scanning is not successful, you can use the information in this blog post on WSUS troubleshooting for hints on troubleshooting any error codes you find: *http://blogs.technet.com/b/sus/archive/2009/11/17/tips-for-troubleshooting-wsus-agents-that-are-not-reporting-to-the-wsus-server.aspx*.**

UPDATEDEPLOYMENT.LOG

The UpdateDeployment.log file provides information about deployment on the client, including software update activation, evaluation, and enforcement. Verbose logging will show additional information about the interaction with the client user interface.

```
Service startup system task   UpdatesDeploymentAgent   4/28/2013 7:49:39 PM   3468
(0x0D8C)
Software Updates client configuration policy has not been received.
UpdatesDeploymentAgent   4/28/2013 7:49:39 PM   3468 (0x0D8C)
Software updates functionality will not be enabled until the configuration policy has
been received. If this issue persists please check client/server policy communication.
UpdatesDeploymentAgent   4/28/2013 7:49:39 PM   3468 (0x0D8C)
Software Updates feature is disabled   UpdatesDeploymentAgent   4/28/2013 7:49:39 PM
3468 (0x0D8C)
Software Updates client configuration policy has not been received.
UpdatesDeploymentAgent   4/28/2013 7:49:39 PM   3468 (0x0D8C)
Software updates functionality will not be enabled until the configuration policy has
been received. If this issue persists please check client/server policy
communication.   UpdatesDeploymentAgent   4/28/2013 7:49:39 PM   3468 (0x0D8C)
```

```
…………………….
……………………
Evaluation initiated for (1) assignments.   UpdatesDeploymentAgent   4/29/2013 10:39:20
AM   336 (0x0150)
Deadline received for assignment ({3B1C5820-953D-4EFB-BDB7-3ABEE4C9788D})
UpdatesDeploymentAgent   4/29/2013 10:39:20 AM   3344 (0x0D10)
Enforcement trigger will be effective when the current action completes
UpdatesDeploymentAgent   4/29/2013 10:39:20 AM   3344 (0x0D10)
Message received: '<?xml version='1.0' ?><SoftwareUpdatesMessage
MessageType='EvaluateAssignments'><UseCachedResults>True</UseCachedResults></
SoftwareUpdatesMessage>'   UpdatesDeploymentAgent   4/29/2013 10:39:30 AM   3940 (0x0F64)
Evaluation initiated for (0) assignments.   UpdatesDeploymentAgent   4/29/2013 11:01:55
AM   4064 (0x0FE0)
…………………………………….
DetectJob completion received for assignment ({3B1C5820-953D-4EFB-BDB7-3ABEE4C9788D})
UpdatesDeploymentAgent   4/29/2013 11:26:59 AM   3856 (0x0F10)
………………………..
Added update (Site_D4F72DDB-F6C4-4B05-835F-A8C23098857A/SUM_9fb3050e-26f2-4ccc-b9b0-
b453ff58aaa9) to the targeted list   UpdatesDeploymentAgent   4/29/2013 11:26:59 AM
3856 (0x0F10)
Added update (Site_D4F72DDB-F6C4-4B05-835F-A8C23098857A/SUM_de919dec-2021-474a-8a7f-
d632c2068146) to the targeted list   UpdatesDeploymentAgent   4/29/2013 11:26:59 AM
3856 (0x0F10)
Added update (Site_D4F72DDB-F6C4-4B05-835F-A8C23098857A/SUM_d2e84b36-f0fd-4434-825d-
a753a338b0bd) to the targeted list   UpdatesDeploymentAgent   4/29/2013 11:26:59 AM
3856 (0x0F10)
……………………..
………………………
Update (Site_D4F72DDB-F6C4-4B05-835F-A8C23098857A/SUM_de919dec-2021-474a-8a7f-
d632c2068146) Progress: Status = ciStateDownloading, PercentComplete = 83, Result = 0x0
UpdatesDeploymentAgent   4/29/2013 11:27:36 AM   1068 (0x042C)
Progress received for assignment ({3B1C5820-953D-4EFB-BDB7-3ABEE4C9788D})
UpdatesDeploymentAgent   4/29/2013 11:27:38 AM   12 (0x000C)
DownloadJob completion received for assignment ({3B1C5820-953D-4EFB-BDB7-3ABEE4C9788D})
UpdatesDeploymentAgent   4/29/2013 11:27:38 AM   12 (0x000C)
EnumerateUpdates for action (UpdateActionInstall) - Total visible updates = 3
UpdatesDeploymentAgent   4/29/2013 11:27:38 AM   2960 (0x0B90)
Starting install for assignment ({3B1C5820-953D-4EFB-BDB7-3ABEE4C9788D})
UpdatesDeploymentAgent   4/29/2013 11:27:38 AM   12 (0x000C)

…………………….
Update (Site_D4F72DDB-F6C4-4B05-835F-A8C23098857A/SUM_de919dec-2021-474a-8a7f-d632c2068146)
Progress: Status = ciStateInstalling, PercentComplete = 100, DownloadSize = 0,
Result = 0x0   UpdatesDeploymentAgent   4/29/2013 11:31:26 AM   440 (0x01B8)
Update (Site_D4F72DDB-F6C4-4B05-835F-A8C23098857A/SUM_de919dec-2021-474a-8a7f-
d632c2068146) Progress: Status = ciStatePendingSoftReboot, PercentComplete = 0,
DownloadSize = 0, Result = 0x0   UpdatesDeploymentAgent   4/29/2013 11:31:31 AM   3568
(0x0DF0)
CTargetedUpdatesManager - Job completion received.   UpdatesDeploymentAgent   4/29/2013
11:31:32 AM   496 (0x01F0)
Job Id = {A807D023-9E41-4FE5-A528-6120C46C1134}   UpdatesDeploymentAgent   4/29/2013
11:31:32 AM   496 (0x01F0)
No pending install assignment   UpdatesDeploymentAgent   4/29/2013 11:31:33 AM   440
(0x01B8)
EnumerateUpdates for action (UpdateActionInstall) - Total visible updates = 3
UpdatesDeploymentAgent   4/29/2013 11:31:33 AM   2236 (0x08BC)
No installations in pipeline, notify reboot.   UpdatesDeploymentAgent   4/29/2013
11:31:33 AM   440 (0x01B8)
Notify reboot with deadline = Thursday, Apr 29, 2010. - 11:31:33, Ignore reboot Window =
False   UpdatesDeploymentAgent   4/29/2013 11:31:33 AM   440 (0x01B8)
```

EXECMGR.LOG

The Execmgr.log file displays information for all deployed packages (old-style) and associated programs and policies. The following log excerpt shows an advertisement and program executing for deploying software updates:

```
Mandatory execution requested for program Software Updates Program and advertisement
{3D49D216-341B-4456-B52C-A0A480C06BEC}   execmgr   4/29/2013 11:27:50 AM   2188 (0x088C)
Creating mandatory request for advert {3D49D216-341B-4456-B52C-A0A480C06BEC}, program
Software Updates Program, package {3D49D216-341B-4456-B52C-A0A480C06BEC}   execmgr
4/29/2013 11:27:50 AM   2188 (0x088C)
CExecutionRequest::Overriding Service Windows as per policy.   execmgr   4/29/2013
11:27:50 AM   2188 (0x088C)
Execution Manager timer has been fired.   execmgr   4/29/2013 11:27:50 AM   3256
(0x0CB8)
Executing program  in Admin context   execmgr   4/29/2013 11:27:50 AM   2188 (0x088C)
Execution Request for package {3D49D216-341B-4456-B52C-A0A480C06BEC} program Software
Updates Program state change from NotExist to NotifyExecution   execmgr   4/29/2013
11:27:50 AM   2188 (0x088C)
Executing program as an update.   execmgr   4/29/2013 11:27:51 AM   2188 (0x088C)
Executing Update Program   execmgr   4/29/2013 11:27:51 AM   2188 (0x088C)
Updates Installation started for the passed command line   execmgr   4/29/2013 11:27:51
AM   2188 (0x088C)
Looking for MIF file to get program status   execmgr   4/29/2013 11:31:31 AM   440
(0x01B8)
Script for  Package:{3D49D216-341B-4456-B52C-A0A480C06BEC}, Program: Software Updates
Program succeeded with exit code 0   execmgr   4/29/2013 11:31:31 AM   440 (0x01B8)
Execution is complete for program Software Updates Program. The exit code is 0, the
execution status is Success   execmgr   4/29/2013 11:31:31 AM   440 (0x01B8)
The user has logged off.   execmgr   4/29/2013 11:38:13 AM   2788 (0x0AE4)
```

REBOOTCOORDINATOR.LOG

Once the software updates have been installed, then depending on the reboot setting the system might be rebooted. You can view information about possible reboots in the RebootCoordinator.log file which provides information about the process for coordinating system restarts on client computers after software update installations:

```
Shutdown is already in progress   RebootCoordinator   4/29/2013 11:38:10 AM   3792
(0x0ED0)
Reboot initiated   RebootCoordinator   4/29/2013 11:38:10 AM   3792 (0x0ED0)
User logoff notification received   RebootCoordinator   4/29/2013 11:38:13 AM   2788
(0x0AE4)
Shutdown is already in progress   RebootCoordinator   4/29/2013 11:38:17 AM   2788
(0x0AE4)
Reboot initiated   RebootCoordinator   4/29/2013 11:38:17 AM   2788 (0x0AE4)
```

MORE INFO **For information about the other logs you can use for troubleshooting, see** ***http://technet.microsoft.com/en-us/library/hh427342.aspx*****.**

Software distribution

The software distribution feature of Configuration Manager provides a set of tools and resources that help you create and manage packages and advertisements used to distribute software to client and server systems within your enterprise. The software distribution process advertises packages, which contain programs, to members of a collection. The client then installs the software from the specified distribution points. The order in which you create the components that make up the software distribution process is important.

Software distribution log files

Table 3-2 lists the log files that contain information related to software distribution. Later in this section we'll examine how to troubleshoot various issues by using these log files.

TABLE 3-2 Log files for software distribution

Log name	Description	Computer with log file
DataTransferService.log	Records all BITS communication for policy or package access. This log is also used for content management by pull-distribution points.	A computer that is configured as a pull-distribution point
PulllIDP.log	Records details about content that the pull-distribution point transfers from source distribution points. Note: This log file is for System Center 2012 Configuration Manager SP1 only.	A computer that is configured as a pull-distribution point

Log name	Description	Computer with log file
PrestageContent.log	Records the details about the use of the ExtractContent.exe tool on a remote prestaged distribution point. This tool extracts content that has been exported to a file. Note: This log file is for System Center 2012 Configuration Manager SP1 only.	Site system role
SMSdpmon.log	Records details about the distribution point health monitoring scheduled tasks that are configured on a distribution point.	Site system role
smsdpprov.log	Records details about the extraction of compressed files received from a primary site. This log is generated by the WMI Provider of the remote distribution point.	A distribution point computer that is not co-located with the site server.

Troubleshooting software distribution

This section examines the server and client sides of software distribution separately for troubleshooting purposes.

Troubleshooting the server side

When you create a package, you need to check the status messages to see whether the package has been created. Look for entries in the logs that say "SMS Distribution Manager successfully processed package" as shown here:

```
Status ID : 30000 => User "Domain\User" created a package named " Test Package  "
(LAB00003).
Status ID : 2301 => SMS Distribution Manager successfully processed package "Test
Package" (package ID = LAB00003).
```

You will see a message ID of 2300 for the starting of packages once you add the distribution point:

```
Status ID : 30125 User "Domain\User" added new distribution points to a package named "
Test Package  " (LAB00003).
Severity   Type   Site code   Date / Time   System   Component   Message ID
Description   Thread ID   Process ID
Information   Milestone   LAB   4/26/2013 10:28:51 PM   SCCM   SMS_DISTRIBUTION_MANAGER
   2330   SMS Distribution Manager successfully distributed package "LAB00003" to
distribution point "["Display=\\SCCM\"]MSWNET:["SMS_SITE=LAB"]\\SCCM\".   4412   3040
Information   Milestone   LAB   4/26/2013 10:28:51 PM   SCCM   SMS_DISTRIBUTION_MANAGER
2329   SMS Distribution Manager copied package "LAB00003" from "C:\SOFTDUMP\" to
"MSWNET:["SMS_SITE=LAB"]\\SCCM\SMSPKGC$\LAB00003\".   4412   3040
```

```
Information   Milestone   LAB   4/26/2013 10:28:29 PM   SCCM   SMS_DISTRIBUTION_MANAGER
2342   SMS Distribution Manager is starting to distribute package "Test Package" to
distribution point "["Display=\\SCCM\"]MSWNET:["SMS_SITE=LAB"]\\SCCM\".   4412   3040
```

If you see errors, you can check the distmgr.log for error information. The distmgr.log should have the package information, package ID, and source version:

```
STATMSG: ID=2300 SEV=I LEV=M SOURCE="SMS Server" COMP="SMS_DISTRIBUTION_MANAGER"
SYS=SCCM SITE=LAB PID=3040 TID=3276 GMTDATE=Mon Apr 26 16:59:00.772 2010 ISTR0="Test
Package" ISTR1="LAB00003" ISTR2="" ISTR3="" ISTR4="" ISTR5="" ISTR6="" ISTR7="" ISTR8=""
ISTR9="" NUMATTRS=1 AID0=400 AVAL0="LAB00003"   SMS_DISTRIBUTION_MANAGER   4/26/2013
10:29:00 PM   3276 (0x0CCC)
No action specified for the package LAB00003.   SMS_DISTRIBUTION_MANAGER   4/26/2013
10:29:00 PM   3276 (0x0CCC)
No action specified for the package on server
["Display=\\SCCM\"]MSWNET:["SMS_SITE=LAB"]\\SCCM\.   SMS_DISTRIBUTION_MANAGER
4/26/2013 10:29:00 PM   3276 (0x0CCC)
Updating package info for package LAB00003   SMS_DISTRIBUTION_MANAGER   4/26/2013
10:29:00 PM   3276 (0x0CCC)
Package LAB00003 does not have a preferred sender.   SMS_DISTRIBUTION_MANAGER
4/26/2013 10:29:00 PM   3276 (0x0CCC)
The package and/or program properties for package LAB00003 have not changed,  need
to determine which site(s) need updated package info.   SMS_DISTRIBUTION_MANAGER
4/26/2013 10:29:00 PM   3276 (0x0CCC)
StoredPkgVersion (0) of package LAB00003. StoredPkgVersion in database is 0.
SMS_DISTRIBUTION_MANAGER   4/26/2013 10:29:00 PM   3276 (0x0CCC)
SourceVersion (1) of package LAB00003. SourceVersion in database is 1.
SMS_DISTRIBUTION_MANAGER   4/26/2013 10:29:00 PM   3276 (0x0CCC)
STATMSG: ID=2301 SEV=I LEV=M SOURCE="SMS Server" COMP="SMS_DISTRIBUTION_MANAGER"
SYS=SCCM SITE=LAB PID=3040 TID=3276 GMTDATE=Mon Apr 26 16:59:01.073 2010 ISTR0="Test
Package" ISTR1="LAB00003" ISTR2="" ISTR3="" ISTR4="" ISTR5="" ISTR6="" ISTR7="" ISTR8=""
ISTR9="" NUMATTRS=1 AID0=400 AVAL0="LAB00003"   SMS_DISTRIBUTION_MANAGER   4/26/2013
10:29:01 PM   3276 (0x0CCC)
Exiting package processing thread.   SMS_DISTRIBUTION_MANAGER   4/26/2013 10:29:01 PM
3276 (0x0CCC)
```

If you find any anomalies in the logs, make sure that:

- There is network connectivity between the server and the distribution point server.
- There are no DNS name resolution issues.
- The SMSPKG<DriveLettre>$ share has been successfully created and the package has been updated to the distribution point.
- The SMSPKG<DriveLettre>$ share also has the required permissions (that is, the machine account for the distribution point should belong to the ConfigMgr group which has write permission to the distribution point).

Once this has all been verified, your next step would be to verify if the advertisement has been created. When the new advertisement is ready, you can check the status of the newly created advertisement like this:

```
Information   Milestone   LAB   4/26/2013 10:44:36 PM   SCCM   SMS_OFFER_MANAGER   3900
SMS Offer Manager successfully processed new advertisement Test Advr.
Information   Audit   LAB   4/26/2013 10:44:24 PM   SCCM
Microsoft.ConfigurationManagement.dll   30006   User "MYLAB\Administrator" created an
advertisement named "Test Advr" (LAB20000) advertising program "Test Program".
```

Once the newly created advertisement (here "Test Advr") has been received by the client, you should see the following status message:

```
Severity   Type   Site code   Date / Time   System   Component   Message ID
Description
Information   Milestone   LAB   4/26/2013 10:44:36 PM   SCCM   SMS_OFFER_MANAGER   3900
SMS Offer Manager successfully processed new advertisement Test Advr.
Information   Audit   LAB   4/26/2013 10:44:24 PM   SCCM
Microsoft.ConfigurationManagement.dll   30006   User "MYLAB\Administrator" created an
advertisement named "Test Advr" (LAB20000) advertising program "Test Program".
```

At this point, if you still haven't resolved your issue, you should check the client logs as described next.

Troubleshooting the client side

When you make a change in the Configuration Manager console, the site server creates a policy to communicate the change to the client. The site server sends the policy to the management point and the client polls for policy at the interval configured in the Computer Client Agent properties.

Policies are created and accessed in two ways: policy assignments and policy bodies. Policy assignments can contain applicability rules so that clients download only the policy assignments that apply to them. If there is no applicability rule in a policy, the policy applies to all clients. Policy assignments contain pointers to the actual policy, which is contained in the policy body. This pointer is actually a URL to the policy body on the management point. Such URLs in a policy assignment do not actually contain the name of the management point, just a variable that the client replaces with the name of the assigned management point, or, if this is a secondary site, the proxy management point.

POLICYAGNET.LOG

The PolicyAgnet.log records requests for policies made by using the Data Transfer service. Here is an example with related information from the PolicyEvaluvator.log:

```
Download of policy CCM_Policy_Policy4.PolicyID="LAB20000-LAB00003-
9785047B",PolicySource="SMS:LAB",PolicyVersion="1.00" completed (DTS Job ID: {231E2AE2-
7ED2-4AA3-84F4-81CA1712217E})   PolicyAgent_PolicyDownload   4/26/2013 10:47:12 PM
1944 (0x0798)
Raising event:
 instance of CCM_PolicyAgent_PolicyDownloadSucceeded
{
   ClientID = "GUID:76B6D180-F0B6-4689-B294-6CCE9033D7EB";
   DateTime = "20100426171712.258000+000";
   DownloadMethod = "BITS";
   DownloadSource = "http://SCCM.MYLAB.IN/SMS_MP/.sms_pol?LAB20000-LAB00003-
9785047B.1_00";
   PolicyNamespace = "\\\\SQL\\ROOT\\ccm\\Policy\\Machine\\RequestedConfig";
   PolicyPath = "CCM_Policy_Policy4.PolicyID=\"LAB20000-LAB00003-9785047B\",
PolicySource=\"SMS:LAB\",PolicyVersion=\"1.00\"";
   ProcessID = 3568;
   ThreadID = 1944;
};
   PolicyAgent_PolicyDownload   4/26/2013 10:47:12 PM   1944 (0x0798)
```

POLICYEVALUVATOR.LOG

```
Raising event:
 instance of CCM_PolicyAgent_PolicyEvaluationComplete
{
   ClientID = "GUID:76B6D180-F0B6-4689-B294-6CCE9033D7EB";
   DateTime = "20100426171716.924000+000";
   PolicyNamespace = "\\\\SQL\\ROOT\\ccm\\Policy\\Machine\\RequestedConfig";
   PolicyPath = "CCM_Policy_Policy4.PolicyID=\"LAB20000-LAB00003-9785047B\",PolicySource
=\"SMS:LAB\",PolicyVersion=\"1.00\"";
   ProcessID = 3568;
   ThreadID = 1944;
};
   PolicyAgent_PolicyEvaluator   4/26/2013 10:47:16 PM   1944 (0x0798)
Policy state for [CCM_Policy_Policy4.PolicyID="LAB20000-LAB00003-
9785047B",PolicyVersion="1.00",PolicySource="SMS:LAB"] is currently [Active]
PolicyAgent_PolicyEvaluator   4/26/2013 10:47:16 PM   3488 (0x0DA0)
Updating settings in \\sql\root\ccm\policy\machine\actualconfig
PolicyAgent_PolicyEvaluator   4/26/2013 10:47:16 PM   3488 (0x0DA0)
Raising event:

instance of CCM_PolicyAgent_SettingsEvaluationComplete
```

```
{
   ClientID = "GUID:76B6D180-F0B6-4689-B294-6CCE9033D7EB";
   DateTime = "20100426171718.827000+000";
   PolicyNamespace = "\\\\sql\\root\\ccm\\policy\\machine\\actualconfig";
   ProcessID = 3568;
   ThreadID = 3488;
};
   PolicyAgent_PolicyEvaluator   4/26/2013 10:47:18 PM   3488 (0x0DA0)
```

EXECMGR.LOG

The Execmgr log file should include the entry “Policy arrived for parent package <Package Id and Name>”. The presence of such an entry helps you determine whether you have the latest policy for the new package populating the client:

```
Policy arrived for parent package LAB00003 program Test Program   execmgr   4/26/2013
10:47:19 PM   2004 (0x07D4)
Raising event:
[SMS_CodePage(437), SMS_LocaleID(1033)]
instance of SoftDistProgramOfferReceivedEvent
{
   AdvertisementId = "LAB20000";
   ClientID = "GUID:76B6D180-F0B6-4689-B294-6CCE9033D7EB";
   DateTime = "20100426171720.299000+000";
   MachineName = "SQL";
   ProcessID = 3568;
   SiteCode = "LAB";
   ThreadID = 2004;
};
   execmgr   4/26/2013 10:47:20 PM   2004 (0x07D4)
Requesting content from CAS for package LAB00003 version 1   execmgr   4/26/2013
10:47:25 PM   1944 (0x0798)
Successfully created a content request handle {80539F34-D400-4978-95F2-9D26151C9BF8} for
the package LAB00003 version 1   execmgr   4/26/2013 10:47:29 PM   1944 (0x0798)
```

DATATRANSFERSERVICES.LOG

The DataTransferServices.log records all Background Intelligent Transfer Service (BITS) communication for policy or package access. Once the client receives the new policy for the package that needs to be installed, the package needs to be downloaded as part of the deployment. The entry “Request content from the DP” signifies the start of the download process. After a period of time has elapsed, you can see the software being downloaded in the DataTransferServices.log as shown here:

```
UpdateURLWithTransportSettings(): OLD URL -
http://SCCM.MYLAB.IN/SMS_MP/.sms_pol?LAB20000-LAB00003-9785047B.1_00
DataTransferService   4/26/2013 10:47:06 PM   3208 (0x0C88)
UpdateURLWithTransportSettings(): NEW URL -
http://SCCM.MYLAB.IN:80/SMS_MP/.sms_pol?LAB20000-LAB00003-9785047B.1_00
DataTransferService   4/26/2013 10:47:06 PM   3208 (0x0C88)
DTSJob {231E2AE2-7ED2-4AA3-84F4-81CA1712217E} created to download from
'http://SCCM.MYLAB.IN/SMS_MP/.sms_pol?LAB20000-LAB00003-9785047B.1_00' to
'C:\WINDOWS\system32\CCM\Temp\{55C3178E-C27D-4C29-AC2D-439C6E87D53D}.tmp'.
DataTransferService   4/26/2013 10:47:06 PM   3208 (0x0C88)
DTSJob {231E2AE2-7ED2-4AA3-84F4-81CA1712217E} in state 'PendingDownload'.
DataTransferService   4/26/2013 10:47:06 PM   1944 (0x0798)
DTS::AddTransportSecurityOptionsToBITSJob - Failed to QueryInterface for
IBackgroundCopyJobHttpOptions. BITS 2.5+ may not be installed properly.
DataTransferService   4/26/2013 10:47:09 PM   1944 (0x0798)
DTSJob {231E2AE2-7ED2-4AA3-84F4-81CA1712217E} in state 'DownloadingData'.
DataTransferService   4/26/2013 10:47:09 PM   1944 (0x0798)
DTSJob {231E2AE2-7ED2-4AA3-84F4-81CA1712217E} in state 'RetrievedData'.
DataTransferService   4/26/2013 10:47:11 PM   2004 (0x07D4)
DTSJob {B40BBB03-0BA0-460A-B822-3DB2535AFCF1} successfully completed download.
DataTransferService   4/26/2013 10:48:10 PM   3208 (0x0C88)
DTSJob {B40BBB03-0BA0-460A-B822-3DB2535AFCF1} in state 'NotifiedComplete'.
DataTransferService   4/26/2013 10:48:11 PM   3488 (0x0DA0)
DTS job {B40BBB03-0BA0-460A-B822-3DB2535AFCF1} has completed:
   Status : SUCCESS
   Start time : 04/26/2013 22:48:07
   Completion time : 04/26/2013 22:48:10
   Elapsed time : 3 seconds   DataTransferService   4/26/2013 10:48:11 PM   3488
(0x0DA0)
```

EXECMGR.LOG

The Execmgr.log shows download progress and completed execution of the process. If the package fails to download, make sure that the distribution point is available and that BITS is working (you can open Services.msc to check whether BITS is started or stopped). Here is an excerpt showing what the Execmgr.log should display:

```
Program Test Program change to state STATE_ADVANCED_DOWNLOAD content in progress
execmgr   4/26/2013 10:47:29 PM   1944 (0x0798)
Execution Request for package LAB00003 program Test Program state change from NotExist
to AdvancedDownload   execmgr   4/26/2013 10:47:29 PM   1944 (0x0798)
Mandatory execution requested for program Test Program and advertisement LAB20000
execmgr   4/26/2013 10:47:29 PM   3208 (0x0C88)
Creating mandatory request for advert LAB20000, program Test Program, package LAB00003
execmgr   4/26/2013 10:47:29 PM   3208 (0x0C88)
```

```
Raising event:
[SMS_CodePage(437), SMS_LocaleID(1033)]
instance of SoftDistWaitingContentEvent
{
   AdvertisementId = "LAB20000";
   ClientID = "GUID:76B6D180-F0B6-4689-B294-6CCE9033D7EB";
   DateTime = "20100426171731.545000+000";
   MachineName = "SQL";
   PackageName = "LAB00003";
   PackageVersion = "1";
   ProcessID = 3568;
   ProgramName = "Test Program";
   SiteCode = "LAB";
   ThreadID = 3208;
};
   execmgr   4/26/2013 10:47:31 PM   3208 (0x0C88)
Successfully raised SoftDistWaitingContentEvent event for program Test Program   execmgr
4/26/2013 10:47:31 PM   3208 (0x0C88)
Execution Request for package LAB00003 program Test Program state change from
WaitingDependency to WaitingContent   execmgr   4/26/2013 10:47:31 PM   3208 (0x0C88)
Content is available for program Test Program.   execmgr   4/26/2013 10:48:18 PM   3488
(0x0DA0)
CExecutionRequest::Service Windows Manager has allowed us to run.   execmgr   4/26/2013
10:48:18 PM   3488 (0x0DA0)
Execution Request for package LAB00003 program Test Program state change from
WaitingContent to NotifyExecution   execmgr   4/26/2013 10:48:18 PM   3488 (0x0DA0)
Notify user mandatory program Test Program is about to run   execmgr   4/26/2013
10:48:18 PM   3488 (0x0DA0)
Execution Manager timer has been fired.   execmgr   4/26/2013 10:53:18 PM   2184
(0x0888)
Executing program test.bat in Admin context   execmgr   4/26/2013 10:53:19 PM   2184
(0x0888)
Execution Manager timer has been fired.   execmgr   4/26/2013 10:53:19 PM   3752
(0x0EA8)
Execution Request for package LAB00003 program Test Program state change from Running to
NotifyExecution   execmgr   4/26/2013 10:53:19 PM   2184 (0x0888)
Checking content location C:\WINDOWS\system32\CCM\Cache\LAB00003.1.System for use
execmgr   4/26/2013 10:53:19 PM   2184 (0x0888)
Successfully selected content location C:\WINDOWS\system32\CCM\Cache\LAB00003.1.System
execmgr   4/26/2013 10:53:19 PM   2184 (0x0888)
Executing program as a script   execmgr   4/26/2013 10:53:19 PM   2184 (0x0888)
Successfully prepared command line
"C:\WINDOWS\system32\CCM\Cache\LAB00003.1.System\test.bat"   execmgr   4/26/2013
10:53:19 PM   2184 (0x0888)
Command line = "C:\WINDOWS\system32\CCM\Cache\LAB00003.1.System\test.bat", Working
Directory = C:\WINDOWS\system32\CCM\Cache\LAB00003.1.System\   execmgr   4/26/2013
```

```
10:53:19 PM   2184 (0x0888)
Created Process for the passed command line   execmgr   4/26/2013 10:53:20 PM   2184
(0x0888)
Raising event:
[SMS_CodePage(437), SMS_LocaleID(1033)]
instance of SoftDistProgramStartedEvent
{
   AdvertisementId = "LAB20000";
   ClientID = "GUID:76B6D180-F0B6-4689-B294-6CCE9033D7EB";
   CommandLine = "\"C:\\WINDOWS\\system32\\CCM\\Cache\\LAB00003.1.System\\test.bat\"";
   DateTime = "20100426172320.000000+000";
   MachineName = "SQL";
   PackageName = "LAB00003";
   ProcessID = 3568;
   ProgramName = "Test Program";
   SiteCode = "LAB";
   ThreadID = 2184;
   UserContext = "NT AUTHORITY\\SYSTEM";
   WorkingDirectory = "C:\\WINDOWS\\system32\\CCM\\Cache\\LAB00003.1.System\\";
};
   execmgr   4/26/2013 10:53:20 PM   2184 (0x0888)
Raised Program Started Event for Ad:LAB20000, Package:LAB00003, Program: Test Program
execmgr   4/26/2013 10:53:20 PM   2184 (0x0888)
Program exit code 0   execmgr   4/26/2013 10:53:24 PM   3752 (0x0EA8)
Looking for MIF file to get program status   execmgr   4/26/2013 10:53:24 PM   3752 (0x0EA8)
Script for  Package:LAB00003, Program: Test Program succeeded with exit code 0   execmgr
4/26/2013 10:53:24 PM   3752 (0x0EA8)
Raising event:
[SMS_CodePage(437), SMS_LocaleID(1033)]
instance of SoftDistProgramCompletedSuccessfullyEvent
{
   AdvertisementId = "LAB20000";
   ClientID = "GUID:76B6D180-F0B6-4689-B294-6CCE9033D7EB";
   DateTime = "20100426172324.741000+000";
   MachineName = "SQL";
   PackageName = "LAB00003";
   ProcessID = 3568;
   ProgramName = "Test Program";
   SiteCode = "LAB";
   ThreadID = 3752;
   UserContext = "NT AUTHORITY\\SYSTEM";
};
   execmgr   4/26/2013 10:53:24 PM   3752 (0x0EA8)
Raised Program Success Event for Ad:LAB20000, Package:LAB00003, Program: Test Program
execmgr   4/26/2013 10:53:24 PM   3752 (0x0EA8)
Execution is complete for program Test Program. The exit code is 0, the execution status
```

```
is Success   execmgr   4/26/2013 10:53:24 PM   2184 (0x0888)
Execution Manager timer has been fired.   execmgr   4/26/2013 10:55:29 PM   2184 (0x0888)
```

If there are any errors here you should verify the program command line and determine whether you can execute the command manually on your system. The software distribution functionality of Configuration Manager is merely a command carrier and will execute any command you specify with the specified set of files. If there is an execution error relating to a particular application, you will need to discuss the problem with the application owner or your User Acceptance Testing (UAT) team administrator.

Data replication

Replication Link Analyzer is a new feature in Configuration Manager 2012 you use to analyze and repair replication issues. Replication Link Analyzer can be used to remediate replication link failures when replication has failed or when replication stops working but has not yet been reported as failed. Replication Link Analyzer can also be used to remediate replication issues between a site server and the site database server in the Configuration Manager hierarchy and between the site database server in one site and a site database server in another site (intersite replication).

Troubleshooting data replication issues

If replication is failing to re-initialize, you will need to take steps to troubleshoot. The log excerpts in this section walk through the flow of re-initialization for a particular group. The walkthrough uses the replication group hardware_inventory_8 as an example. There are various methods you can use for re-initiating a specific group, but the safest method is to put *<Groupname>*-*<SITECODE>*.pub (for example, hardware_inventory_8-PR1.pub) in RCM.BOX on the site server.

To get more information that can be helpful for troubleshooting purposes, you can start by enabling enhanced/verbose logging by making the following registry changes.

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SMS\Components\SMS_REPLICATION_CONFIGURATION_MONITOR

  Verbose Logging = 2
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SMS\Tracing

  Sqlenabled = 1

Configuration Manager logs information in two ways: in .log files and in the database. For troubleshooting data replication services initialization, you can use the rcmctrl.log as shown in the next section. For troubleshooting from inside the database, you can use the vLogs view. For example, you might use a query like the following:

```
Select * from vLogs where LogTime >GETDATE()-1 and ProcedureName <>
'spDRSSendChangesForGroup' ORDER BY LogTime DESC
```

RCMCTRL.LOG

To re-initialize the group, you put the .pub file in \Microsoft Configuration Manager\inboxes\RCM.BOX. After a period of time has elapsed, you should see the file vanishing from the box. Once this occurs, you should see entries like the following in the rcmctrl.log on the central administration site server:

```
Processing replication group Hardware_Inventory_8.
SMS_REPLICATION_CONFIGURATION_MONITOR   20-10-2012 02:02:24   1820 (0x071C)
Current status is Active.   SMS_REPLICATION_CONFIGURATION_MONITOR   20-10-2012 02:02:24
1820 (0x071C)
Requesting initialization for replication group Hardware_Inventory_8.
SMS_REPLICATION_CONFIGURATION_MONITOR   20-10-2012 02:02:24   1820 (0x071C)
Checking if initialization request is needed for replication group Hardware_Inventory_8
from site PR1.   SMS_REPLICATION_CONFIGURATION_MONITOR   20-10-2012 02:02:27   1820
(0x071C)
```

In rcmctrl.log on the primary site server, you should then see entries like the ones that follow which provide information concerning requests going out to global/site groups for replication:

```
Processing replication role: DrsReplicationSite, child
SMS_REPLICATION_CONFIGURATION_MONITOR   20-10-2012 02:03:03   3364 (0x0D24)
Processing replication group Hardware_Inventory_8.
SMS_REPLICATION_CONFIGURATION_MONITOR   20-10-2012 02:03:03   3364 (0x0D24)
Current status is PendingCreation.
SMS_REPLICATION_CONFIGURATION_MONITOR   20-10-2012 02:03:03   3364 (0x0D24)
Checking if we need to create an initialization package for replication group
Hardware_Inventory_8 for site CAS. SMS_REPLICATION_CONFIGURATION_MONITOR   20-10-2012
02:03:04   3364 (0x0D24)
STATMSG: ID=7802 SEV=I LEV=M SOURCE="SMS Server"
COMP="SMS_REPLICATION_CONFIGURATION_MONITOR" SYS=CMLABPRI.CMLAB.COM SITE=PR1 PID=5060
TID=3364 GMTDATE=Sat Oct 20 09:03:04.342 2012 ISTR0="CAS" ISTR1="Hardware_Inventory_8"
ISTR2="" ISTR3="" ISTR4="" ISTR5="" ISTR6="" ISTR7="" ISTR8="" ISTR9="" NUMATTRS=0
SMS_REPLICATION_CONFIGURATION_MONITOR   20-10-2012 02:03:04   3364 (0x0D24)
Flushing DRS queue messages coming from CAS for replication group Hardware_Inventory_8.
SMS_REPLICATION_CONFIGURATION_MONITOR   20-10-2012 02:03:04   3364 (0x0D24)
Changed the status of ConfigMgrDRSSiteQueue to OFF if it exists.
SMS_REPLICATION_CONFIGURATION_MONITOR   20-10-2012 02:03:04   3364 (0x0D24)
Changed the status of ConfigMgrDRSSiteQueue to ON if it exists.
SMS_REPLICATION_CONFIGURATION_MONITOR   20-10-2012 02:03:07   3364 (0x0D24)
Files will be copied to directory C:\Program Files\Microsoft Configuration Manager\
inboxes\rcm.box\a4ba357d-1cb4-408c-9e89-681686974194.
SMS_REPLICATION_CONFIGURATION_MONITOR   20-10-2012 02:03:07   3364 (0x0D24)
Cab File to be sent will be copied to directory C:\Program Files\Microsoft Configuration
Manager\inboxes\rcm.box\CabFiles.   SMS_REPLICATION_CONFIGURATION_MONITOR   20-10-2012
02:03:07   3364 (0x0D24)
XML CreateTime: 20-10-2012 09:02:31 LastModifyTime: 20-10-2012 09:02:31
```

```
SMS_REPLICATION_CONFIGURATION_MONITOR   20-10-2012 02:03:07   3364 (0x0D24)
Creating version file C:\Program Files\Microsoft Configuration
Manager\inboxes\rcm.box\a4ba357d-1cb4-408c-9e89-681686974194\781708.version
SMS_REPLICATION_CONFIGURATION_MONITOR   20-10-2012 02:03:07   3364 (0x0D24)
Creating trackingGuid file C:\Program Files\Microsoft Configuration
Manager\inboxes\rcm.box\a4ba357d-1cb4-408c-9e89-681686974194\d74dc244-a526-4387-86b0-
efacf67df680.trackingGuid   SMS_REPLICATION_CONFIGURATION_MONITOR   20-10-2012 02:03:07
3364 (0x0D24)
Creating pubName file C:\Program Files\Microsoft Configuration
Manager\inboxes\rcm.box\a4ba357d-1cb4-408c-9e89-681686974194\Hardware_Inventory_8-PR1.
pubName   SMS_REPLICATION_CONFIGURATION_MONITOR   20-10-2012 02:03:07   3364 (0x0D24)
…………………………..
………………………….
 Calling BCP out with SELECT BINFILEVERSION00, BINPRODUCTVERSION00, DESCRIPTION00,
FILENAME00, FILEPROPERTIESHASH00, FILEPROPERTIESHASHEX00, FILEVERSION00, LOCATION00,
PRODUCT00, PRODUCTVERSION00, PUBLISHER00, STARTUPTYPE00, STARTUPVALUE00, MACHINEID,
INSTANCEKEY, TIMEKEY, REVISIONID, AGENTID, ROWVERSION~FROM AUTOSTART_SOFTWARE_HIST where
(MachineID between 16777216 and 33554431), C:\Program Files\Microsoft Configuration
Manager\inboxes\rcm.box\a4ba357d-1cb4-408c-9e89-681686974194\AUTOSTART_SOFTWARE_HIST.
bcp, C:\Program Files\Microsoft Configuration Manager\inboxes\rcm.box\a4ba357d-1cb4-
408c-9e89-681686974194\bcpErrors.errors.   SMS_REPLICATION_CONFIGURATION_MONITOR
20-10-2012 02:03:07   3364 (0x0D24)
…………………………………..
…………………………………….
Successfully created BCP file [C:\Program Files\Microsoft Configuration Manager\inboxes\
rcm.box\a4ba357d-1cb4-408c-9e89-681686974194\AUTOSTART_SOFTWARE_DATA.bcp] with rows
[6] based on SQL query [SELECT BINFILEVERSION00, BINPRODUCTVERSION00, DESCRIPTION00,
FILENAME00, FILEPROPERTIESHASH00, FILEPROPERTIESHASHEX00, FILEVERSION00, LOCATION00,
PRODUCT00, PRODUCTVERSION00, PUBLISHER00, STARTUPTYPE00, STARTUPVALUE00, MACHINEID,
INSTANCEKEY, TIMEKEY, REVISIONID, AGENTID, ROWVERSION~FROM AUTOSTART_SOFTWARE_DATA where
(MachineID between 16777216 and 33554431) ]   SMS_REPLICATION_CONFIGURATION_MONITOR
20-10-2012 02:03:07   3364 (0x0D24)
BCP out result is 0.   SMS_REPLICATION_CONFIGURATION_MONITOR   20-10-2012 02:03:07
3364 (0x0D24)
Table XML: <TABLE NAME="AUTOSTART_SOFTWARE_HIST"><COLUMN COLUMN_ID="1"
NAME="BINFILEVERSION00" TYPENAME="nvarchar" TYPEID="231" MAX_LENGTH="510" IS_
NULLABLE="1" HAS_DEFAULTVALUE="0" /><
…………………………..
……………………………
SMS_REPLICATION_CONFIGURATION_MONITOR   20-10-2012 02:03:07   3364 (0x0D24)
```

The log excerpt shows the BCP out commands being fired. It also lets you see the version file, trackinguid file, errors file, pubname file, and for each table in the group, the .bcp file and .row count file.

Once the BCP out commands have completed, compression takes place and the .pub file is stored in the CABFiles folder. The rcmctrl.log should display entries like the following:

```
Calling drs_init_send method now with parameters C:\Program Files\Microsoft
Configuration Manager\inboxes\rcm.box\a4ba357d-1cb4-408c-9e89-681686974194 and CAS.
SMS_REPLICATION_CONFIGURATION_MONITOR   20-10-2012 02:03:08   3364 (0x0D24)
Starting to compress files under folder [C:\Program Files\Microsoft Configuration
Manager\inboxes\rcm.box\a4ba357d-1cb4-408c-9e89-681686974194\] to [C:\Program
Files\Microsoft Configuration Manager\inboxes\rcm.box\CabFiles\CAS_4C7EB459-2631-455B-
93C1-8C08926BAD07.cab] ...   SMS_REPLICATION_CONFIGURATION_MONITOR   20-10-2012 02:03:08
3364 (0x0D24)
Deleting all files under folder [C:\Program Files\Microsoft Configuration
Manager\inboxes\rcm.box\a4ba357d-1cb4-408c-9e89-681686974194].
SMS_REPLICATION_CONFIGURATION_MONITOR   20-10-2012 02:03:08   3364 (0x0D24)
Created minijob to send compressed copy of DRS INIT BCP Package to site CAS. Tranfer
root = C:\Program Files\Microsoft Configuration
Manager\inboxes\rcm.box\CabFiles\CAS_4C7EB459-2631-455B-93C1-8C08926BAD07.cab.
SMS_REPLICATION_CONFIGURATION_MONITOR   20-10-2012 02:03:08   3364 (0x0D24)
drs_init_send returned 0.   SMS_REPLICATION_CONFIGURATION_MONITOR   20-10-2012 02:03:08
3364 (0x0D24)
STATMSG: ID=7803 SEV=I LEV=M SOURCE="SMS Server"
COMP="SMS_REPLICATION_CONFIGURATION_MONITOR" SYS=CMLABPRI.CMLAB.COM SITE=PR1 PID=5060
TID=3364 GMTDATE=Sat Oct 20 09:03:08.373 2012 ISTR0="Hardware_Inventory_8" ISTR1="CAS"
ISTR2="" ISTR3="" ISTR4="" ISTR5="" ISTR6="" ISTR7="" ISTR8="" ISTR9="" NUMATTRS=0
SMS_REPLICATION_CONFIGURATION_MONITOR   20-10-2012 02:03:08   3364 (0x0D24)
Current status is PackageCreated.
SMS_REPLICATION_CONFIGURATION_MONITOR   20-10-2012 02:03:08   3364 (0x0D24)
Found 1 replication roles.   SMS_REPLICATION_CONFIGURATION_MONITOR   20-10-2012 02:03:08
3364 (0x0D24)
```

Once this is done, the sender will then send the files to the central administration site server:

SENDER.LOG

```
Passed the xmit file test, use the existing connection   SMS_LAN_SENDER   20-10-2012
02:03:33   5012 (0x1394)
Package file = C:\Program Files\Microsoft Configuration
Manager\inboxes\rcm.box\CabFiles\CAS_4C7EB459-2631-455B-93C1-8C08926BAD07.cab
SMS_LAN_SENDER   20-10-2012 02:03:33   5012 (0x1394)
Instruction file = C:\Program Files\Microsoft Configuration
Manager\inboxes\schedule.box\tosend\00000085.I59 SMS_LAN_SENDER   20-10-2012 02:03:33
5012 (0x1394)
Checking for remote file \\CMLABCAS.CMLAB.COM\SMS_SITE\1003PPR1.PCK   SMS_LAN_SENDER
20-10-2012 02:03:33   5012 (0x1394)
Checking for remote file \\CMLABCAS.CMLAB.COM\SMS_SITE\1003PPR1.SNI   SMS_LAN_SENDER
20-10-2012 02:03:33   5012 (0x1394)
```

```
Checking for remote file \\CMLABCAS.CMLAB.COM\SMS_SITE\1003PPR1.TMP   SMS_LAN_SENDER
20-10-2012 02:03:33   5012 (0x1394)
Attempt to create/open the remote file \\CMLABCAS.CMLAB.COM\SMS_SITE\1003PPR1.PCK
SMS_LAN_SENDER   20-10-2012 02:03:33   5012 (0x1394)
Created/opened the remote file \\CMLABCAS.CMLAB.COM\SMS_SITE\1003PPR1.PCK
SMS_LAN_SENDER   20-10-2012 02:03:33   5012 (0x1394)
Attempt to create/open the remote file \\CMLABCAS.CMLAB.COM\SMS_SITE\1003PPR1.PCK
SMS_LAN_SENDER   20-10-2012 02:03:33   5012 (0x1394)
Created/opened the remote file \\CMLABCAS.CMLAB.COM\SMS_SITE\1003PPR1.PCK
SMS_LAN_SENDER   20-10-2012 02:03:33   5012 (0x1394)
Sending Started [C:\Program Files\Microsoft Configuration
Manager\inboxes\rcm.box\CabFiles\CAS_4C7EB459-2631-455B-93C1-8C08926BAD07.cab]
SMS_LAN_SENDER   20-10-2012 02:03:33   5012 (0x1394)
Attempt to write 1024 bytes to \\CMLABCAS.CMLAB.COM\SMS_SITE\1003PPR1.PCK at position 0
SMS_LAN_SENDER   20-10-2012 02:03:33   5012 (0x1394)
……………………….
……………………….
S.CMLAB.COM\SMS_SITE\1003PPR1.TMP   SMS_LAN_SENDER   20-10-2012 02:03:33   5012 (0x1394)
Created/opened the remote file \\CMLABCAS.CMLAB.COM\SMS_SITE\1003PPR1.TMP
SMS_LAN_SENDER   20-10-2012 02:03:33   5012 (0x1394)
Sending Started [C:\Program Files\Microsoft Configuration
Manager\inboxes\schedule.box\tosend\00000085.I59]   SMS_LAN_SENDER   20-10-2012 02:03:33
5012 (0x1394)
Attempt to write 650 bytes to \\CMLABCAS.CMLAB.COM\SMS_SITE\1003PPR1.TMP at position 0
SMS_LAN_SENDER   20-10-2012 02:03:33   5012 (0x1394)
Wrote 650 bytes to \\CMLABCAS.CMLAB.COM\SMS_SITE\1003PPR1.TMP at position 0
SMS_LAN_SENDER   20-10-2012 02:03:33   5012 (0x1394)
Sending completed [C:\Program Files\Microsoft Configuration
Manager\inboxes\schedule.box\tosend\00000085.I59]   SMS_LAN_SENDER   20-10-2012 02:03:33
5012 (0x1394)
Renaming remote file \\CMLABCAS.CMLAB.COM\SMS_SITE\1003PPR1.TMP to
\\CMLABCAS.CMLAB.COM\SMS_SITE\1003PPR1.SNI   SMS_LAN_SENDER   20-10-2012 02:03:33   5012
(0x1394)
Rename completed [\\CMLABCAS.CMLAB.COM\SMS_SITE\1003PPR1.TMP]   SMS_LAN_SENDER   20-10-
2012 02:03:33   5012 (0x1394)
Sending completed successfully   SMS_LAN_SENDER   20-10-2012 02:03:33   5012 (0x1394)
COutbox::TakeNextToSend(pszSiteCode)   SMS_LAN_SENDER   20-10-2012 02:03:33   5012
(0x1394)
We have 0 active connections  SMS_LAN_SENDER   20-10-2012 02:03:38   4784 (0x12B0)
Checking for sending capacity.  Used 0 out of 5.   SMS_LAN_SENDER   20-10-2012 02:03:38
4784 (0x12B0)
Connecting to C:\Program Files\Microsoft Configuration
Manager\inboxes\schedule.box\outboxes\LAN.   SMS_LAN_SENDER   20-10-2012 02:03:38   4784
(0x12B0)
COutbox::TakeNextToSend(pszSiteCode)   SMS_LAN_SENDER   20-10-2012 02:03:38   4784
(0x12B0)
```

```
No (more) send requests found to process.   SMS_LAN_SENDER   20-10-2012 02:03:38   4784
(0x12B0)
Waiting for new/rescheduled send requests, Maximum Sleep Time = 60 minutes
SMS_LAN_SENDER   20-10-2012 02:03:38   4784 (0x12B0)
```

Once the central administration site server has received the files, the despooler will start processing the files inside RCM.BOX\<GUID> just like on the primary site server. The despooler.log will show information about the receiving files:

DESPOOLR.LOG

```
Waiting for ready instruction file....   SMS_DESPOOLER   20-10-2012 02:03:38   3972
(0x0F84)
Decompressed C:\Program Files\Microsoft Configuration
Manager\inboxes\despoolr.box\receive\ds_fl24a.pkg to C:\Program Files\Microsoft
Configuration Manager\inboxes\rcm.box\DBAF3A0C-9FE0-4A93-B771-E2DD3784E755\  SMS_
DESPOOLER   20-10-2012 02:03:38   3376 (0x0D30)
Despooler successfully executed one instruction.   SMS_DESPOOLER   20-10-2012 02:03:38
3376 (0x0D30)
```

Once decompression has taken place, the delta records are compared with the tracking GUID. If publication matches, the old data in BCP is deleted after verifying the rowcount files:

RCMCTRL.LOG

```
Processing replication group Hardware_Inventory_8.
SMS_REPLICATION_CONFIGURATION_MONITOR   20-10-2012 02:03:41   1820 (0x071C)
Current status is PackageCreated.   SMS_REPLICATION_CONFIGURATION_MONITOR   20-10-2012
02:03:41   1820 (0x071C)
Checking if initialization request is needed for replication group Hardware_Inventory_8
from site PR1.   SMS_REPLICATION_CONFIGURATION_MONITOR   20-10-2012 02:03:41   1820
(0x071C)
Checking if there are bcp file to apply for replication group Hardware_Inventory_8 from
site PR1.   SMS_REPLICATION_CONFIGURATION_MONITOR   20-10-2012 02:03:41   1820 (0x071C)
found a tracking guid, searching through .init files.
SMS_REPLICATION_CONFIGURATION_MONITOR   20-10-2012 02:03:41   1820 (0x071C)
Checking bcpDirectory C:\Program Files\Microsoft Configuration
Manager\inboxes\rcm.box\DBAF3A0C-9FE0-4A93-B771-E2DD3784E755
SMS_REPLICATION_CONFIGURATION_MONITOR   20-10-2012 02:03:41   1820 (0x071C)
Found files for publication Hardware_Inventory_8-PR1.
SMS_REPLICATION_CONFIGURATION_MONITOR   20-10-2012 02:03:41   1820 (0x071C)
Publication names match. Checking vesrion.   SMS_REPLICATION_CONFIGURATION_MONITOR   20-
10-2012 02:03:41   1820 (0x071C)
Found our tracking guid   SMS_REPLICATION_CONFIGURATION_MONITOR   20-10-2012 02:03:41
1820 (0x071C)
Setting deadlock priority level to high.   SMS_REPLICATION_CONFIGURATION_MONITOR   20-
10-2012 02:03:41   1820 (0x071C)
```

```
Initializing to version number 781708.   SMS_REPLICATION_CONFIGURATION_MONITOR   20-10-
2012 02:03:41   1820 (0x071C)
Publication Hardware_Inventory_8 has ID 30.   SMS_REPLICATION_CONFIGURATION_MONITOR
20-10-2012 02:03:41   1820 (0x071C)
Flushing DRS queue messages coming from PR1 for replication group Hardware_Inventory_8.
SMS_REPLICATION_CONFIGURATION_MONITOR   20-10-2012 02:03:41   1820 (0x071C)
Executing pre-snapshot stored procedures for group Hardware_Inventory_8.   SMS_
REPLICATION_CONFIGURATION_MONITOR   20-10-2012 02:03:42   1820 (0x071C)
Pre-snapshot stored procedures for group Hardware_Inventory_8 finished. Applying bcp
files.   SMS_REPLICATION_CONFIGURATION_MONITOR   20-10-2012 02:03:42   1820 (0x071C)
Removing old data for site table ... [EXEC spSMSTruncatePartitionTable 'AUTOSTART_
SOFTWARE_DATA', 1;]   SMS_REPLICATION_CONFIGURATION_MONITOR   20-10-2012 02:03:42   1820
(0x071C)
Rowcount from file [C:\Program Files\Microsoft Configuration
Manager\inboxes\rcm.box\DBAF3A0C-9FE0-4A93-B771-
E2DD3784E755\AUTOSTART_SOFTWARE_DATA.bcp.rowcount] is [6].   SMS_REPLICATION_
CONFIGURATION_MONITOR   20-10-2012 02:03:42   1820 (0x071C)
Successfully bulk copied file [C:\Program Files\Microsoft Configuration
Manager\inboxes\rcm.box\DBAF3A0C-9FE0-4A93-B771-E2DD3784E755\AUTOSTART_SOFTWARE_
DATA.bcp] into table [AUTOSTART_SOFTWARE_DATA] with rows [6].   SMS_REPLICATION_
CONFIGURATION_MONITOR   20-10-2012 02:03:43   1820 (0x071C)
Removing old data for site table ... [EXEC spSMSTruncatePartitionTable 'AUTOSTART_
SOFTWARE_HIST', 1;]   SMS_REPLICATION_CONFIGURATION_MONITOR   20-10-2012 02:03:43   1820
(0x071C)
Rowcount from file [C:\Program Files\Microsoft Configuration
Manager\inboxes\rcm.box\DBAF3A0C-9FE0-4A93-B771-E2DD3784E755\AUTOSTART_SOFTWARE_HIST.
bcp.rowcount] is [0].   SMS_REPLICATION_CONFIGURATION_MONITOR   20-10-2012 02:03:43
1820 (0x071C)
'''''''''''''''''''''''
'''''''''''''''''''''''
Setting deadlock priority level to normal.   SMS_REPLICATION_CONFIGURATION_MONITOR   20-
10-2012 02:03:45   1820 (0x071C)
Current status is Active.   SMS_REPLICATION_CONFIGURATION_MONITOR   20-10-2012 02:03:45
1820 (0x071C)
--------------
```

Once replication has completed, the status changes from initialization to active in the monitoring phase.

Using Replication Link Analyzer

Replication Link Analyzer can be launched either within the Configuration Manager console or from the command line. Launching Replication Link Analyzer through the console is easy:

1. In the Monitoring workspace, click the Database Replication node.
2. Select the replication link that you want to analyze.
3. In the Database Replication group on the Home tab, select Replication Link Analyzer.

To launch Replication Link Analyzer Wizard from the command line, use the following syntax:

```
%path%\Microsoft Configuration
Manager\AdminConsole\bin\Microsoft.ConfigurationManager.ReplicationLinkAnalyzer.Wizard.exe
<source site server FQDN> <destination site server FQDN>
```

Replication Link Analyzer saves its results in the following XML-based report file and log file on the desktop of the user who runs the tool:

- ReplicationAnalysis.xml
- ReplicationLinkAnalysis.log

Understanding the replication process

When a site is first installed, it establishes an initial synchronization with the sending site so that subsequent data changes are applied to a data set identical to the one at the sending site. By default, the first replication group processed is the Replication Configuration group—this group effectively bootstraps the receiving site with the remaining configuration for other replication groups.

The site initializes by sending an init request to the sending site for the desired replication group. When the sending site receives the init request, it uses the BCP application to extract all of the data from the tables that make up the replication group being initialized. At the same time, a rowcount of the number of exported rows is also taken and stored in a .rowcount file. This allows the receiving site to ensure it has imported the same number of rows as the sending site exported for import.

The sending site then sets the receiving site as a subscriber to the replication group and replication configuration management/monitoring begins sending any changes to tables in the replication group to the receiving site. The BCP files are replicated to the receiving site via the standard content sender. Once the BCP files have arrived at the receiving site, replication configuration management/monitoring on the receiving site is notified of the files in its inbox folder and begins a cycle of actions for each table in the replication group:

1. Any existing data in the destination table that overlaps with the received data from the sending site is deleted from the table.
2. BCP is used to import the data from the sending site into the receiving site database.
3. After the import has completed, the rowcount from the BCP process is compared to the row count in the .rowcount file. If the values match, the next table is processed.
4. Once all the tables have been processed, the group status is changed to active and the site begins processing any messages in the queue.
5. Re-initialization will be attempted if any error is returned on any specific group.

When you run Replication Link Analyzer, it will try auto-remediate once so that the particular group will be re-initialized. You can also re-initialize replication anytime by copying and pasting a .pub file into the RCM.BOX on the site server. The file <*replicationgroupname*>.

pub will work fine for this purpose for global data, in which case you would copy/paste the file into the RCM.BOX on the primary server. For site data where the central administration site is the subscriber however, you must also add the sitecode to the file name so that it looks like *<replicationgroupname>*-*<sitecode>*.pub in order for the central administration site to know which primary site to re-initialize from. For example, the file hardware_inventory_8-PR1.pub for site data would be copied/pasted into the RCM.BOX on the central administration site server.

Operating system deployment

Configuration Manager provides several methods that you can use to deploy an operating system. Regardless of the deployment method that you use, there are several actions that you must take. These actions include the following:

- Identify any Windows device drivers that are required to run the boot image or the operating system image that you have to deploy.
- Identify the boot image that you want to use to start the destination computer. Configuration Manager provides two default boot images.
- Capture an image of the operating system that you want to deploy by using a task sequence.
- Distribute the boot image, operating system image, and any related content to a distribution point.
- Create a task sequence that deploys the boot image and the operating system image.
- Deploy the task sequence to the collection that contains the destination computer. If there are multiple computers in the collection, the task sequence is deployed to each computer in the collection.

Operating system deployment log files

Table 3-3 lists the log files that contain information related to operating system deployment.

TABLE 3-3 Operating system deployment log files

Log name	Description	Computer with log file
CAS.log	Records details when distribution points are found for referenced content.	Client
ccmsetup.log	Records ccmsetup tasks for client setup, client upgrade, and client removal. Can be used to troubleshoot client installation problems.	Client
CreateTSMedia.log	Records details for task sequence media creation.	The computer that runs the Configuration Manager console
Dism.log	Records driver installation actions or update apply actions for offline servicing.	Site system server

Log name	Description	Computer with log file
Distmgr.log	Records details about the configuration of enabling a distribution point for pre-boot execution environment (PXE).	Site system server
DriverCatalog.log	Records details about device drivers that have been imported into the driver catalog.	Site system server
mcsisapi.log	Records information for multicast package transfer and client request responses.	Site system server
mcsexec.log	Records health check, namespace, session creation, and certificate check actions.	Site system server
mcsmgr.log	Records changes to configuration, security mode, and availability.	Site system server
mcsprv.log	Records multicast provider interaction with Windows Deployment Services (WDS).	Site system server
MCSSetup.log	Records details about multicast server role installation.	Site system server
MCSMSI.log	Records details about multicast server role installation.	Site system server
Mcsperf.log	Records details about multicast performance counter updates.	Site system server
MP_ClientIDManager.log	Records management point responses to the client ID requests task sequences initiated from PXE or boot media.	Site system server
MP_DriverManager.log	Records management point responses to Auto Apply Driver task sequence action requests.	Site system server
OfflineServicingMgr.log	Records details of offline servicing schedules and update apply actions on operating system .wim files.	Site system server
Setupact.log	Records details about Windows Sysprep and setup logs.	Client
Setupapi.log	Records details about Windows Sysprep and setup logs.	Client
Setuperr.log	Records details about Windows Sysprep and setup logs.	Client
smpisapi.log	Records details about the client state capture and restore actions, and threshold information.	Client
Smpmgr.log	Records details about the results of state migration point health checks and configuration changes.	Site system server
smpmsi.log	Records installation and configuration details about the state migration point.	Site system server
smpperf.log	Records the state migration point performance counter updates.	Site system server
smspxe.log	Records details about the responses to clients that PXE boot and details about the expansion of boot images and boot files.	Site system server
smssmpsetup.log	Records installation and configuration details about the state migration point.	Site system server
Smsts.log	Records task sequence activities.	Client
TSAgent.log	Records the outcome of task sequence dependencies before starting a task sequence.	Client

Log name	Description	Computer with log file
TaskSequenceProvider.log	Records details about task sequences when they are imported, exported, or edited.	Site system server
loadstate.log	Records details about the User State Migration Tool (USMT) and restoring user state data.	Client
scanstate.log	Records details about the User State Migration Tool (USMT) and capturing user state data.	Client

When you begin deploying any Microsoft operating system using Configuration Manager, you soon learn that things often go wrong and you don't know why. Worse still, Configuration Manager simply confronts you with arcane task-sequence errors, advising you to "please contact your system administrator or helpdesk." Since that is you, it's not much help. Fortunately, Microsoft also provides plenty of help through log files. There are two minor challenges here: First, there are lots of different log files, and second, Configuration Manager puts them in different paths depending on what phase the deployment is in.

Since the core thread of deployment is the task-sequence, you need to find the log for that. The name betrays its age: it is called smsts.log. Examining this log should always be your first step in troubleshooting any deployment issue. Unfortunately, Configuration Manager can save the smsts.log in one of seven different places, depending on the stage of the build and the architecture of the operating system. Table 3-4 shows the possible locations for the smsts.log file.

TABLE 3-4 Location of deployment log files for different phases of deployment

Phase	Path
WinPE, before HDD format	x:\windows\temp\smstslog\smsts.log
WinPE, after HDD format	copied to c:_SMSTaskSequence\Logs\Smstslog\smsts.log
Full version Windows, before Configuration Manager agent installed	c:_SMSTaskSequence\Logs\Smstslog\smsts.log
Full operating system, after Configuration Manager agent	%windir%\system32\ccm\logs\Smstslog\smsts.log or %windir%\sysWOW64\ccm\logs\Smstslog\smsts.log (64-bit)
Full operating system, build complete	%windir%\system32\ccm\logs\smsts.log or %windir%\sysWOW64\ccm\logs\smsts.log (64-bit)

Using error messages for troubleshooting

This section summarizes some of the possible pop-up error messages you might encounter when problems arise during operating system deployment using Configuration Manager. These error messages have been grouped into different categories such as disk, network, XML, and media issues.

Troubleshooting disk issues

Occasionally, you might see errors caused by disk issues when you are using Configuration Manager for operating system deployment.

Error: Failed to run task-sequence 0×80070032

CAUSE: There is no valid file system either because the target is corrupt, encrypted, or unformatted. The task requires Configuration Manager to copy the WinPE files to C: that is, you must have an NTFS partition as a prerequisite.

FIX: Quick format the disk with **echo y | format c: /q** or recreate the disk partitions using diskpart.exe

One other possibility we have seen for this error is that the disk you are targeting has gone “offline” (as seen by diskpart). The solution is to just make it online by using this command:

```
sel dis 0
```

Error: Failed to stage WinPE. Code(0×80070032)

The cause and resolution of this error is usually similar to the resolution of the error previously described.

Troubleshooting network issues

Network issues can be another source of problems when you are using Configuration Manager for operating system deployment. This section describes some of the errors you might encounter and how to handle them.

Failed to run Task Sequence (unknown host). Error: 0x80072EE7

The most common error we have seen occurs before the task-sequence even starts. Fundamentally, they are down to networking. You normally have a clue something is wrong before this error appears, such as when Configuration Manager displays “Retrieving policy....”

CAUSE: The machine cannot talk to the Configuration Manager server because of a network issue of some kind.

FIX: Plug in the Ethernet cable (it happens), and check the subnet settings or add the correct Windows network drivers to your WinPE boot image.

> ***NOTE*** **WinPE needs Windows 7 or Windows 8 network drivers.**

The system cannot find the file specified. Error: 0×80070002

SYMPTOM: Unknown host (gethostbyname failed) repeatedly appears in the log file.

CAUSE: Configuration Manager can't find any source path to a file because there's no network driver loaded/installed in the WinPE boot image.

FIX: If "restart computer (reboot to WinPE)" stops responding, or hangs, it's also because there's no network driver. It's waiting for WinPE to download but it can't so it just sits there.

The specified domain either does not exist or could not be contacted. Error: 0x8007054B

CAUSE: Failed to join the domain

FIX: Check the user account or the domain or that you installed network drivers.

Failed to run command line Error: 0x8007010B

CAUSE: A file/dir is bad or missing. (The directory name is invalid.)

FIX: Rebuild your build media because a write error or crash has resulted in not all packages being correct.

Troubleshooting XML errors

Occasionally, Configuration Manager will report errors related to the XML files that it uses when deploying operating systems.

Error: 0×800700002

CAUSE: Configuration Manager can't read the file in sms\data\policy.xml.

FIX: Rebuild the build media or copy policy.xml from known good media (USB/DVD) or set in tsbootstrap.ini's mediatype=Bootmedia if you only want to boot and build from LAN.

Error: Prompts for #1 media then errors 0×800700002

CAUSE: You've created split media and the wrong volume label is in <boot:>VOLUMEID.XML.

FIX: Copy the right one to the root of the media and retry.

Troubleshooting media issues

Finally, here are some tips on troubleshooting common media issues when deploying operating systems using Configuration Manager.

Error: 0×80070007 = The storage control blocks were destroyed.

CAUSE: Your USB media is too small and Configuration Manager is trying to span to more!

FIX: Get a bigger USB pen-drive or write to a dual-layer DVD instead.

Error: 0×80070017

SYMPTOM: Building from DVD fails. Clue: the DVD spins and spins for ages, with the light blinking urgently until eventually you get a task sequence error.

CAUSE: Error 80070017 is a CRC failure, meaning the DVD/USB source media is corrupt. This happens when the task sequence tries to copy the content for package XYZ from the DVD. So, either the package XYZ is corrupt or there's a problem with the DVD itself (bad ISO or bad physical media). Try recreating the full media ISO then re-burn the DVD.

FIX: Burn another DVD or use a USB (or build from the network instead).

Application management

Application management in System Center 2012 Configuration Manager provides both administrative users and client device users with tools for managing applications in the enterprise.

Application deployments are regularly reconfigured by Configuration Manager. For example:

- A deployed application is uninstalled by the user. At the next evaluation cycle, Configuration Manager detects that the application is not present and reinstalls it.
- An application was not installed on a device because it failed to meet the requirements. Later, a change is made to the device and it now meets the requirements. Configuration Manager detects this change and the application is installed.

Application management log files

Table 3-5 lists the log files that contain information related to application management.

TABLE 3-5 Application management log files

Log name	Description	Computer with log file
AppIntentEval.log	Records details about the current and intended state of applications, their applicability, whether requirements were met, deployment types, and dependencies.	Client
AppDiscovery.log	Records details about the discovery or detection of applications on client computers.	Site system server
AppEnforce.log	Records details about enforcement actions (install and uninstall) taken for applications on the client.	Site system server
awebsctl.log	Records the monitoring activities for the Application Catalog web service point site system role.	Site system server

Log name	Description	Computer with log file
awebsvcMSI.log	Records detailed installation information for the Application Catalog web service point site system role.	Site system server
Ccmsdkprovider.log	Records the activities of the application management SDK.	Client
colleval.log	Records details about when collections are created, changed, and deleted by the Collection Evaluator.	Site system server
ConfigMgrSoftwareCatalog.log	Records the activity of the Application Catalog, which includes its use of Microsoft Silverlight.	Client
portlctl.log	Records the monitoring activities for the Application Catalog website point site system role.	Site system server
portlwebMSI.log	Records the MSI installation activity for the Application Catalog website role.	Site system server
PrestageContent.log	Records the details about the use of the ExtractContent.exe tool on a remote prestaged distribution point. This tool extracts content that has been exported to a file.	Site system server
ServicePortalWebService.log	Records the activity of the Application Catalog web service.	Site system server
ServicePortalWebSite.log	Records the activity of the Application Catalog website.	Site system server
SMSdpmon.log	Records details about the distribution point health monitoring scheduled task that is configured on a distribution point.	Site server
SoftwareCatalogUpdateEndpoint.log	Records the activities for managing the URL for the Application Catalog shown in Software Center.	Client
SoftwareCenterSystemTasks.log	Records the activities for Software Center prerequisite component validation.	Client

Troubleshooting application deployment

This section does not describe the workflow of application deployment. Instead, it highlights a couple of common issues you might run into during application deployment.

Application download failures

Symptoms:

- Client stuck downloading an application
- Client failed to download application
- Client stuck at 0 percent while downloading software

Possible solutions and troubleshooting information: missing or misconfigured boundaries and boundary groups.

- If the client is on the intranet and is not configured for Internet-only client management, the client's network location must be in a configured boundary and there must be a boundary group assigned to this boundary for the client to be able to download content.
- Content might not be distributed to the distribution points yet, which is why it is not available for clients to download. Use the in-console monitoring facilities to monitor content distribution to the distribution points.
- If you cannot configure a boundary for the client or if specific boundary groups cannot be a member of other boundary groups, you can configure the Deployment Type properties, Content tab, and Deployment options for the option "Download content from distribution point and run locally."

Application deployment compliance stuck at 0 percent

Possible solution and troubleshooting information: check the Deployments node in the Monitoring workplace for the deployment status of the application:

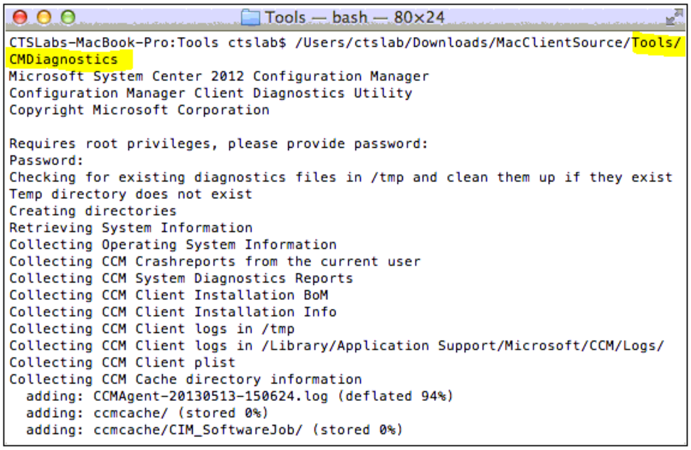
- **In progress** The client could be stuck downloading content. Check problem 1, discussed previously.
- **Error** For more information about this status, see the following blog post: *http://blogs.technet.com/b/configmgrteam/archive/2012/03/23/tips-and-tricks-how-to-take-action-on-assets-that-report-a-failed-deployment-in-system-center-2012-configuration-manager.aspx*
- **Unknown** This implies that the client has not received policy. Try manually initiating client policy and if this does not work, use client status to help verify client functionality. For more information, see the following on Microsoft TechNet: "How to Initiate Policy Retrieval for a Configuration Manager Client" at *http://technet.microsoft.com/en-us/library/bb633207.aspx*. Also see, "Monitoring the Status of Client Computers in Configuration Manager" at *http://technet.microsoft.com/en-us/library/gg682132.aspx#BKMK_ClientHealth*

Workflow of application deployment for Macintosh clients

This section demonstrates the workflow of application deployment on Mac clients by walking you through a scenario of deploying Adobe Reader to a Mac computer running Mac Book Pro with OS X Mountain Lion 10.8.

Macintosh computers have a tool called CMDiagnostics that is located under the Tools folder in your Mac client software. If you run CMDiagnostics without any switches, it will start collecting all the information shown here in the screenshot and zip it and store it in a directory named cmdiag-<MacMachineName>-<Date>.zip for example:

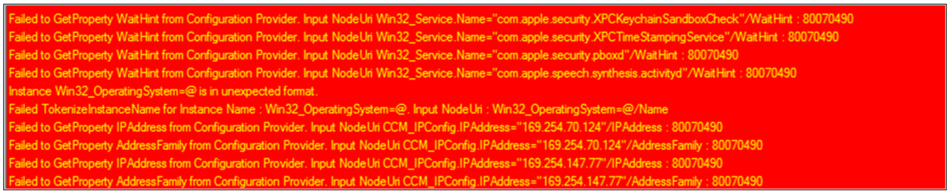
```
cmdiag-CTSLabs-MacBook-Pro.local-2013-06-07-151751.zip
```



```
CTSLabs-MacBook-Pro:Tools ctslab$ /Users/ctslab/Downloads/MacClientSource/Tools/
CMDiagnostics
Microsoft System Center 2012 Configuration Manager
Configuration Manager Client Diagnostics Utility
Copyright Microsoft Corporation

Requires root privileges, please provide password:
Password:
Checking for existing diagnostics files in /tmp and clean them up if they exist
Temp directory does not exist
Creating directories
Retrieving System Information
Collecting Operating System Information
Collecting CCM Crashreports from the current user
Collecting CCM System Diagnostics Reports
Collecting CCM Client Installation BoM
Collecting CCM Client Installation Info
Collecting CCM Client logs in /tmp
Collecting CCM Client logs in /Library/Application Support/Microsoft/CCM/Logs/
Collecting CCM Client plist
Collecting CCM Cache directory information
  adding: CCMAgent-20130513-150624.log (deflated 94%)
  adding: ccmcache/ (stored 0%)
  adding: ccmcache/CIM_SoftwareJob/ (stored 0%)
```

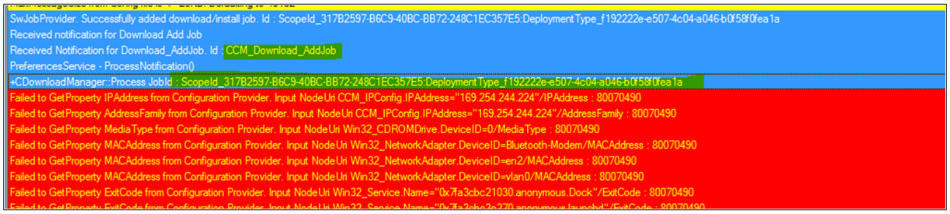
Copy this log to a Windows computer that has CMTrace for easier viewing. Browse to the ccmlogs directory and open CCMClient-<date>.log (that is, CCMClient-20130513-130117.log)

You might see many errors like the following but you can safely ignore them because they are either not related to the workflow being discussed here or are thrown because of a property not existing on the Mac computer:



```
Failed to GetProperty WaitHint from Configuration Provider. Input NodeUri Win32_Service.Name="com.apple.security.XPCKeychainSandboxCheck"/WaitHint : 80070490
Failed to GetProperty WaitHint from Configuration Provider. Input NodeUri Win32_Service.Name="com.apple.security.XPCTimeStampingService"/WaitHint : 80070490
Failed to GetProperty WaitHint from Configuration Provider. Input NodeUri Win32_Service.Name="com.apple.security.pboxd"/WaitHint : 80070490
Failed to GetProperty WaitHint from Configuration Provider. Input NodeUri Win32_Service.Name="com.apple.speech.synthesis.activityd"/WaitHint : 80070490
Instance Win32_OperatingSystem=@ is in unexpected format.
Failed TokenizeInstanceName for Instance Name : Win32_OperatingSystem=@. Input NodeUri : Win32_OperatingSystem=@/Name
Failed to GetProperty IPAddress from Configuration Provider. Input NodeUri CCM_IPConfig.IPAddress="169.254.70.124"/IPAddress : 80070490
Failed to GetProperty AddressFamily from Configuration Provider. Input NodeUri CCM_IPConfig.IPAddress="169.254.70.124"/AddressFamily : 80070490
Failed to GetProperty IPAddress from Configuration Provider. Input NodeUri CCM_IPConfig.IPAddress="169.254.147.77"/IPAddress : 80070490
Failed to GetProperty AddressFamily from Configuration Provider. Input NodeUri CCM_IPConfig.IPAddress="169.254.147.77"/AddressFamily : 80070490
```

You want to look for an entry that says CCM_Download_AddJob as shown here. Again, ignore any errors that start with Failed to GetProperty.



```
SwJobProvider. Successfully added download/install job. Id : ScopeId_317B2597-B6C9-40BC-BB72-248C1EC357E5:DeploymentType_f192222e-e507-4c04-a046-b0f58f0fea1a
Received notification for Download Add Job
Received Notification for Download_AddJob. Id : CCM_Download_AddJob
PreferencesService - ProcessNotification()
+CDownloadManager::Process JobId : ScopeId_317B2597-B6C9-40BC-BB72-248C1EC357E5:DeploymentType_f192222e-e507-4c04-a046-b0f58f0fea1a
Failed to GetProperty IPAddress from Configuration Provider. Input NodeUri CCM_IPConfig.IPAddress="169.254.244.224"/IPAddress : 80070490
Failed to GetProperty AddressFamily from Configuration Provider. Input NodeUri CCM_IPConfig.IPAddress="169.254.244.224"/AddressFamily : 80070490
Failed to GetProperty MediaType from Configuration Provider. Input NodeUri Win32_CDROMDrive.DeviceID=0/MediaType : 80070490
Failed to GetProperty MACAddress from Configuration Provider. Input NodeUri Win32_NetworkAdapter.DeviceID=Bluetooth-Modem/MACAddress : 80070490
Failed to GetProperty MACAddress from Configuration Provider. Input NodeUri Win32_NetworkAdapter.DeviceID=en2/MACAddress : 80070490
Failed to GetProperty MACAddress from Configuration Provider. Input NodeUri Win32_NetworkAdapter.DeviceID=vlan0/MACAddress : 80070490
Failed to GetProperty ExitCode from Configuration Provider. Input NodeUri Win32_Service.Name="0x7fa3cbc21030.anonymous.Dock"/ExitCode : 80070490
Failed to GetProperty ExitCode from Configuration Provider. Input NodeUri Win32_Service.Name="0x7fa3cbc2c270.anonymous.launchd"/ExitCode : 80070490
```

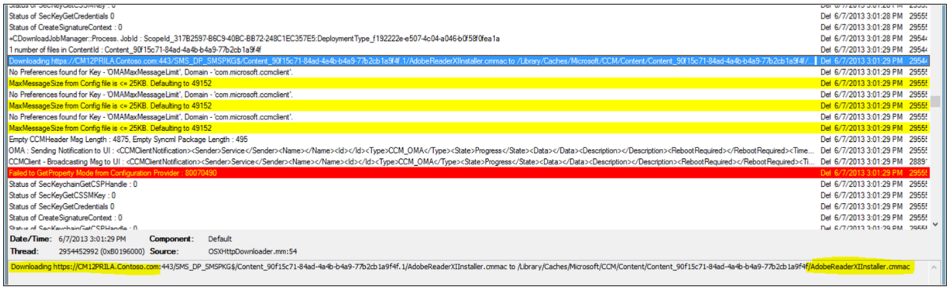
If you continue to scroll down these logs, you will see that the Configuration Manager client has successfully added the job for the Adobe Reader application.

```
SwJobProvider. Successfully added download/install job. Id : ScopeId_317B2597-B6C9-
40BC-BB72-248C1EC357E5:DeploymentType_f192222e-e507-4c04-a046-b0f58f0fea1a   Default
6/7/2013 3:01:28 PM   2955517952 (0xB029A000)
Received notification for Download Add Job   Default   6/7/2013 3:01:28 PM   2955517952
(0xB029A000)
Received Notification for Download_AddJob. Id : CCM_Download_AddJob   Default   6/7/2013
3:01:28 PM   2954452992 (0xB0196000)
PreferencesService - ProcessNotification()    Default   6/7/2013 3:01:28 PM   2956050432
(0xB031C000)
+CDownloadManager::Process JobId : ScopeId_317B2597-B6C9-40BC-BB72-
248C1EC357E5:DeploymentType_f192222e-e507-4c04-a046-b0f58f0fea1a   Default   6/7/2013
3:01:28 PM   2954452992 (0xB0196000)
```

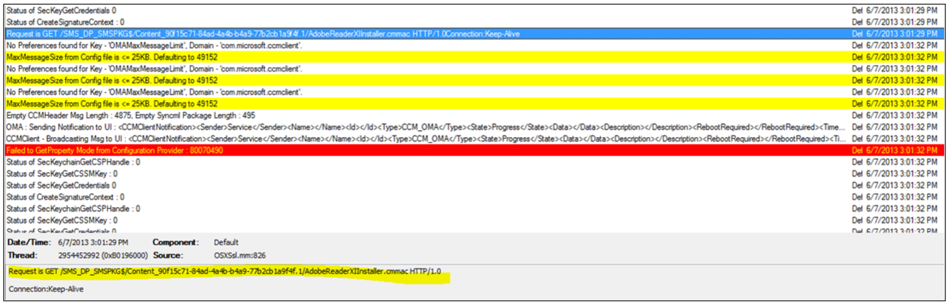
Reviewing some additional entries in the log finds some log entries like this:

```
Downloading https://<servername>:443/SMS_DP_SMSPKG$/Content_<id>/<application>.cmmac
```

This is shown in the following two screenshots:

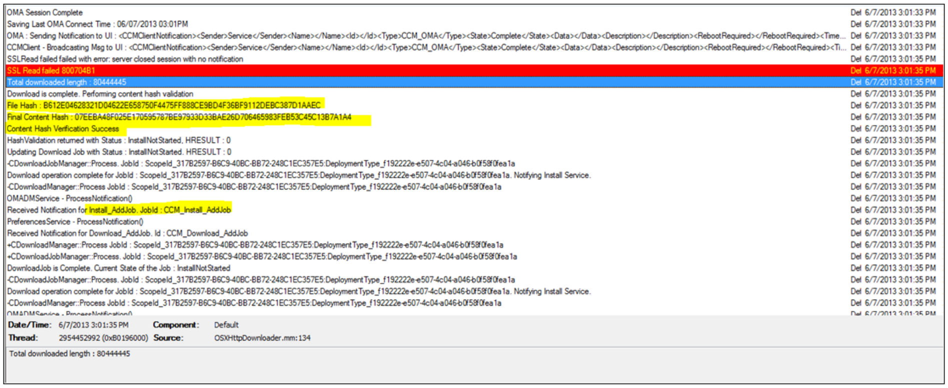


```
Status of SecKeyGetCSSMKey : 0
Status of SecKeyGetCredentials 0                                                              Del 6/7/2013 3:01:28 PM 2955
Status of CreateSignatureContext : 0                                                          Del 6/7/2013 3:01:28 PM 2955
+CDownloadJobManager::Process. JobId : ScopeId_317B2597-B6C9-40BC-BB72-248C1EC357E5:DeploymentType_f192222e-e507-4c04-a046-b0f58f0fea1a   Del 6/7/2013 3:01:28 PM 2954
1 number of files in ContentId : Content_90f15c71-84ad-4a4b-b4a9-77b2cb1a9f4f                 Del 6/7/2013 3:01:29 PM 2954
Downloading https://CM12PRILA.Contoso.com:443/SMS_DP_SMSPKG$/Content_90f15c71-84ad-4a4b-b4a9-77b2cb1a9f4f.1/AdobeReaderXIInstaller.cmmac to /Library/Caches/Microsoft/CCM/Content/Content_90f15c71-84ad-4a4b-b4a9-77b2cb1a9f4f/...   Del 6/7/2013 3:01:29 PM 2954
No Preferences found for Key - 'OMAMaxMessageLimit', Domain - 'com.microsoft.ccmclient'.      Del 6/7/2013 3:01:29 PM 2955
MaxMessageSize from Config file is <= 25KB. Defaulting to 49152                               Del 6/7/2013 3:01:29 PM 2955
No Preferences found for Key - 'OMAMaxMessageLimit', Domain - 'com.microsoft.ccmclient'.      Del 6/7/2013 3:01:29 PM 2955
MaxMessageSize from Config file is <= 25KB. Defaulting to 49152                               Del 6/7/2013 3:01:29 PM 2955
No Preferences found for Key - 'OMAMaxMessageLimit', Domain - 'com.microsoft.ccmclient'.      Del 6/7/2013 3:01:29 PM 2955
MaxMessageSize from Config file is <= 25KB. Defaulting to 49152                               Del 6/7/2013 3:01:29 PM 2955
Empty CCMHeader Msg Length : 4875, Empty Syncml Package Length : 495                          Del 6/7/2013 3:01:29 PM 2955
OMA : Sending Notification to UI : <CCMClientNotification><Sender>Service</Sender><Name></Name><Id></Id><Type>CCM_OMA</Type><State>Progress</State><Data></Data><Description></Description><RebootRequired></RebootRequired><Time...   Del 6/7/2013 3:01:29 PM 2955
CCMClient - Broadcasting Msg to UI : <CCMClientNotification><Sender>Service</Sender><Name></Name><Id></Id><Type>CCM_OMA</Type><State>Progress</State><Data></Data><Description></Description><RebootRequired></RebootRequired><Ti...   Del 6/7/2013 3:01:29 PM 2889
Failed to GetProperty Mode from Configuration Provider : 80070490                             Del 6/7/2013 3:01:29 PM 2955
Status of SecKeychainGetCSPHandle : 0                                                         Del 6/7/2013 3:01:29 PM 2955
Status of SecKeyGetCSSMKey : 0                                                                Del 6/7/2013 3:01:29 PM 2955
Status of SecKeyGetCredentials 0                                                              Del 6/7/2013 3:01:29 PM 2955
Status of CreateSignatureContext : 0                                                          Del 6/7/2013 3:01:29 PM 2955
Status of SecKeychainGetCSPHandle : 0                                                         Del 6/7/2013 3:01:29 PM 2955

Date/Time:  6/7/2013 3:01:29 PM          Component:  Default
Thread:     2954452992 (0xB0196000)      Source:     OSXHttpDownloader.mm:54

Downloading https://CM12PRILA.Contoso.com:443/SMS_DP_SMSPKG$/Content_90f15c71-84ad-4a4b-b4a9-77b2cb1a9f4f.1/AdobeReaderXIInstaller.cmmac to /Library/Caches/Microsoft/CCM/Content/Content_90f15c71-84ad-4a4b-b4a9-77b2cb1a9f4f/AdobeReaderXIInstaller.cmmac
```



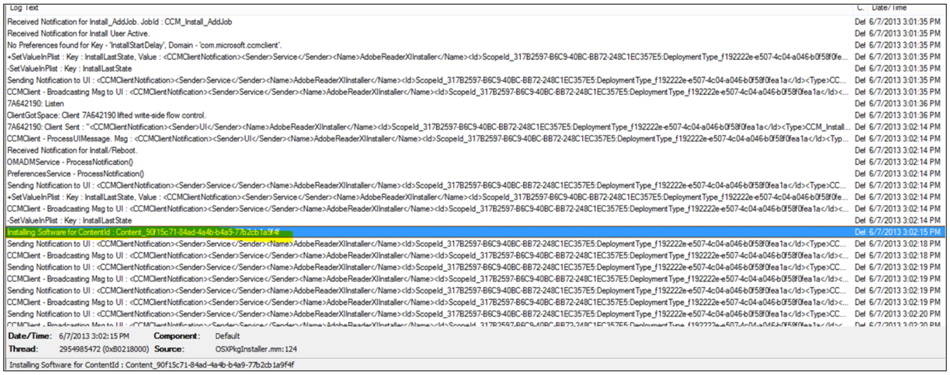
```
Status of SecKeyGetCredentials 0                                                              Del 6/7/2013 3:01:29 PM
Status of CreateSignatureContext : 0                                                          Del 6/7/2013 3:01:29 PM
Request is GET /SMS_DP_SMSPKG$/Content_90f15c71-84ad-4a4b-b4a9-77b2cb1a9f4f.1/AdobeReaderXIInstaller.cmmac HTTP/1.0Connection:Keep-Alive   Del 6/7/2013 3:01:29 PM
No Preferences found for Key - 'OMAMaxMessageLimit', Domain - 'com.microsoft.ccmclient'.      Del 6/7/2013 3:01:32 PM
MaxMessageSize from Config file is <= 25KB. Defaulting to 49152                               Del 6/7/2013 3:01:32 PM
No Preferences found for Key - 'OMAMaxMessageLimit', Domain - 'com.microsoft.ccmclient'.      Del 6/7/2013 3:01:32 PM
MaxMessageSize from Config file is <= 25KB. Defaulting to 49152                               Del 6/7/2013 3:01:32 PM
No Preferences found for Key - 'OMAMaxMessageLimit', Domain - 'com.microsoft.ccmclient'.      Del 6/7/2013 3:01:32 PM
MaxMessageSize from Config file is <= 25KB. Defaulting to 49152                               Del 6/7/2013 3:01:32 PM
Empty CCMHeader Msg Length : 4875, Empty Syncml Package Length : 495                          Del 6/7/2013 3:01:32 PM
OMA : Sending Notification to UI : <CCMClientNotification><Sender>Service</Sender><Name></Name><Id></Id><Type>CCM_OMA</Type><State>Progress</State><Data></Data><Description></Description><RebootRequired></RebootRequired><Time...   Del 6/7/2013 3:01:32 PM
CCMClient - Broadcasting Msg to UI : <CCMClientNotification><Sender>Service</Sender><Name></Name><Id></Id><Type>CCM_OMA</Type><State>Progress</State><Data></Data><Description></Description><RebootRequired></RebootRequired><Ti...   Del 6/7/2013 3:01:32 PM
Failed to GetProperty Mode from Configuration Provider : 80070490                             Del 6/7/2013 3:01:32 PM
Status of SecKeychainGetCSPHandle : 0                                                         Del 6/7/2013 3:01:32 PM
Status of SecKeyGetCSSMKey : 0                                                                Del 6/7/2013 3:01:32 PM
Status of SecKeyGetCredentials 0                                                              Del 6/7/2013 3:01:32 PM
Status of CreateSignatureContext : 0                                                          Del 6/7/2013 3:01:32 PM
Status of SecKeychainGetCSPHandle : 0                                                         Del 6/7/2013 3:01:32 PM
Status of SecKeyGetCSSMKey : 0                                                                Del 6/7/2013 3:01:32 PM
Status of SecKeyGetCredentials 0                                                              Del 6/7/2013 3:01:32 PM

Date/Time:  6/7/2013 3:01:29 PM          Component:  Default
Thread:     2954452992 (0xB0196000)      Source:     OSXSsl.mm:826

Request is GET /SMS_DP_SMSPKG$/Content_90f15c71-84ad-4a4b-b4a9-77b2cb1a9f4f.1/AdobeReaderXIInstaller.cmmac HTTP/1.0

Connection:Keep-Alive
```

Review the file hash and final content hash values as shown next. This information can be useful information because when the hash match is failing, you can update the content on distribution point to see if the problem is on server side. Then if the hash values match, the problem is solved.



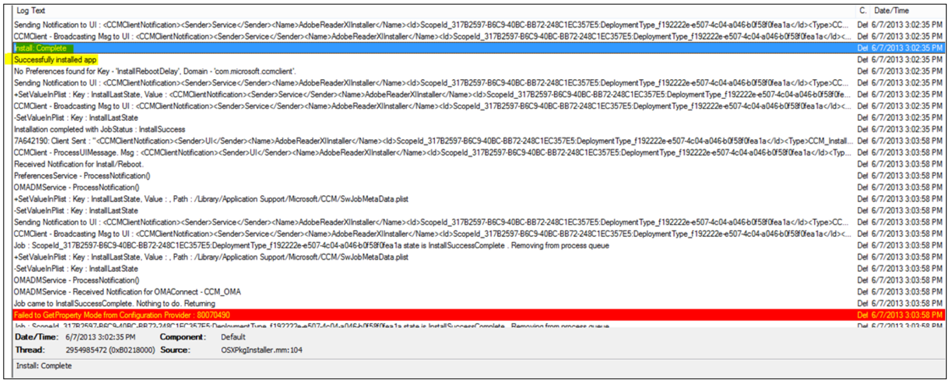
```
OMA Session Complete                                                                                     Del 6/7/2013 3:01:33 PM
Saving Last OMA Connect Time : 06/07/2013 03:01PM                                                        Del 6/7/2013 3:01:33 PM
OMA : Sending Notification to UI : <CCMClientNotification><Sender>Service</Sender><Name></Name><Id></Id><Type>CCM_OMA</Type><State>Complete</State><Data></Data><Description></Description><RebootRequired></RebootRequired><Time...  Del 6/7/2013 3:01:33 PM
CCMClient - Broadcasting Msg to UI : <CCMClientNotification><Sender>Service</Sender><Name></Name><Id></Id><Type>CCM_OMA</Type><State>Complete</State><Data></Data><Description></Description><RebootRequired></RebootRequired><Ti...  Del 6/7/2013 3:01:33 PM
SSLRead failed failed with error: server closed session with no notification                            Del 6/7/2013 3:01:35 PM
SSL Read failed 800704B1                                                                                 Del 6/7/2013 3:01:35 PM
Total downloaded length : 80444445                                                                       Del 6/7/2013 3:01:35 PM
Download is complete. Performing content hash validation                                                 Del 6/7/2013 3:01:35 PM
File Hash : B612E04628321D04622E658750F4475FF888CE9BD4F36BF9112DEBC387D1AAEC                             Del 6/7/2013 3:01:35 PM
Final Content Hash : 07EEBA48F025E170595787BE97933D33BAE26D706465983FEB53C45C13B7A1A4                    Del 6/7/2013 3:01:35 PM
Content Hash Verfication Success                                                                         Del 6/7/2013 3:01:35 PM
HashValidation returned with Status : InstallNotStarted, HRESULT : 0                                     Del 6/7/2013 3:01:35 PM
Updating Download Job with Status : InstallNotStarted. HRESULT : 0                                       Del 6/7/2013 3:01:35 PM
-CDownloadJobManager::Process. JobId : ScopeId_317B2597-B6C9-40BC-BB72-248C1EC357E5:DeploymentType_f192222e-e507-4c04-a046-b0f58f0fea1a  Del 6/7/2013 3:01:35 PM
Download operation complete for JobId : ScopeId_317B2597-B6C9-40BC-BB72-248C1EC357E5:DeploymentType_f192222e-e507-4c04-a046-b0f58f0fea1a. Notifying Install Service.  Del 6/7/2013 3:01:35 PM
-CDownloadManager::Process JobId : ScopeId_317B2597-B6C9-40BC-BB72-248C1EC357E5:DeploymentType_f192222e-e507-4c04-a046-b0f58f0fea1a  Del 6/7/2013 3:01:35 PM
OMADMService - ProcessNotification()                                                                     Del 6/7/2013 3:01:35 PM
Received Notification for Install_AddJob. JobId : CCM_Install_AddJob                                     Del 6/7/2013 3:01:35 PM
PreferencesService - ProcessNotification()                                                               Del 6/7/2013 3:01:35 PM
Received Notification for Download_AddJob. Id : CCM_Download_AddJob                                      Del 6/7/2013 3:01:35 PM
+CDownloadManager::Process JobId : ScopeId_317B2597-B6C9-40BC-BB72-248C1EC357E5:DeploymentType_f192222e-e507-4c04-a046-b0f58f0fea1a  Del 6/7/2013 3:01:35 PM
+CDownloadJobManager::Process. JobId : ScopeId_317B2597-B6C9-40BC-BB72-248C1EC357E5:DeploymentType_f192222e-e507-4c04-a046-b0f58f0fea1a  Del 6/7/2013 3:01:35 PM
DownloadJob is Complete. Current State of the Job : InstallNotStarted                                    Del 6/7/2013 3:01:35 PM
-CDownloadJobManager::Process. JobId : ScopeId_317B2597-B6C9-40BC-BB72-248C1EC357E5:DeploymentType_f192222e-e507-4c04-a046-b0f58f0fea1a  Del 6/7/2013 3:01:35 PM
Download operation complete for JobId : ScopeId_317B2597-B6C9-40BC-BB72-248C1EC357E5:DeploymentType_f192222e-e507-4c04-a046-b0f58f0fea1a. Notifying Install Service.  Del 6/7/2013 3:01:35 PM
-CDownloadManager::Process JobId : ScopeId_317B2597-B6C9-40BC-BB72-248C1EC357E5:DeploymentType_f192222e-e507-4c04-a046-b0f58f0fea1a  Del 6/7/2013 3:01:35 PM
OMADMService - ProcessNotification()                                                                     Del 6/7/2013 3:01:35 PM

Date/Time:  6/7/2013 3:01:35 PM          Component:  Default
Thread:     2954452992 (0xB0196000)      Source:     OSXHttpDownloader.mm:134

Total downloaded length : 80444445
```

Review the installation progress as shown next. If there are any errors during installation, you will find these after the following entries.



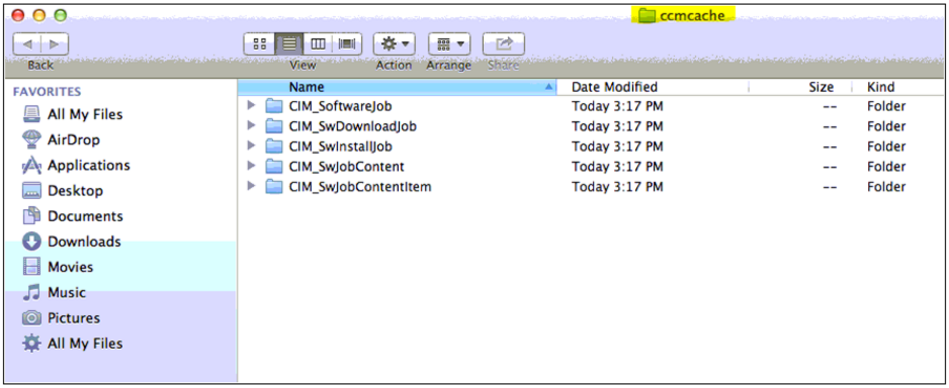
```
Log Text                                                                                                 C.  Date/Time
Received Notification for Install_AddJob. JobId : CCM_Install_AddJob                                     Del 6/7/2013 3:01:35 PM
Received Notification for Install User Active.                                                           Del 6/7/2013 3:01:35 PM
No Preferences found for Key - 'InstallStartDelay', Domain - 'com.microsoft.ccmclient'.                  Del 6/7/2013 3:01:35 PM
+SetValueInPlist : Key : InstallLastState, Value : <CCMClientNotification><Sender>Service</Sender><Name>AdobeReaderXIInstaller</Name><Id>ScopeId_317B2597-B6C9-40BC-BB72-248C1EC357E5:DeploymentType_f192222e-e507-4c04-a046-b0f58f0fe...  Del 6/7/2013 3:01:35 PM
-SetValueInPlist : Key : InstallLastState                                                                Del 6/7/2013 3:01:35 PM
Sending Notification to UI : <CCMClientNotification><Sender>Service</Sender><Name>AdobeReaderXIInstaller</Name><Id>ScopeId_317B2597-B6C9-40BC-BB72-248C1EC357E5:DeploymentType_f192222e-e507-4c04-a046-b0f58f0fea1a</Id><Type>CC...  Del 6/7/2013 3:01:35 PM
CCMClient - Broadcasting Msg to UI : <CCMClientNotification><Sender>Service</Sender><Name>AdobeReaderXIInstaller</Name><Id>ScopeId_317B2597-B6C9-40BC-BB72-248C1EC357E5:DeploymentType_f192222e-e507-4c04-a046-b0f58f0fea1a</Id><...  Del 6/7/2013 3:01:35 PM
7A642190: Listen                                                                                         Del 6/7/2013 3:01:36 PM
ClientGotSpace: Client 7A642190 lifted write-side flow control.                                          Del 6/7/2013 3:01:36 PM
7A642190: Client Sent : "<CCMClientNotification><Sender>UI</Sender><Name>AdobeReaderXIInstaller</Name><Id>ScopeId_317B2597-B6C9-40BC-BB72-248C1EC357E5:DeploymentType_f192222e-e507-4c04-a046-b0f58f0fea1a</Id><Type>CCM_Install...  Del 6/7/2013 3:02:14 PM
CCMClient - ProcessUIMessage. Msg : <CCMClientNotification><Sender>UI</Sender><Name>AdobeReaderXIInstaller</Name><Id>ScopeId_317B2597-B6C9-40BC-BB72-248C1EC357E5:DeploymentType_f192222e-e507-4c04-a046-b0f58f0fea1a</Id><Typ...  Del 6/7/2013 3:02:14 PM
Received Notification for Install/Reboot.                                                                Del 6/7/2013 3:02:14 PM
OMADMService - ProcessNotification()                                                                     Del 6/7/2013 3:02:14 PM
PreferencesService - ProcessNotification()                                                               Del 6/7/2013 3:02:14 PM
Sending Notification to UI : <CCMClientNotification><Sender>Service</Sender><Name>AdobeReaderXIInstaller</Name><Id>ScopeId_317B2597-B6C9-40BC-BB72-248C1EC357E5:DeploymentType_f192222e-e507-4c04-a046-b0f58f0fea1a</Id><Type>CC...  Del 6/7/2013 3:02:14 PM
+SetValueInPlist : Key : InstallLastState, Value : <CCMClientNotification><Sender>Service</Sender><Name>AdobeReaderXIInstaller</Name><Id>ScopeId_317B2597-B6C9-40BC-BB72-248C1EC357E5:DeploymentType_f192222e-e507-4c04-a046-b0f58f0fe...  Del 6/7/2013 3:02:14 PM
CCMClient - Broadcasting Msg to UI : <CCMClientNotification><Sender>Service</Sender><Name>AdobeReaderXIInstaller</Name><Id>ScopeId_317B2597-B6C9-40BC-BB72-248C1EC357E5:DeploymentType_f192222e-e507-4c04-a046-b0f58f0fea1a</Id><...  Del 6/7/2013 3:02:14 PM
-SetValueInPlist : Key : InstallLastState                                                                Del 6/7/2013 3:02:14 PM
Installing Software for ContentId : Content_90f15c71-84ad-4a4b-b4a9-77b2cb1a9f4f                         Del 6/7/2013 3:02:15 PM
Sending Notification to UI : <CCMClientNotification><Sender>Service</Sender><Name>AdobeReaderXIInstaller</Name><Id>ScopeId_317B2597-B6C9-40BC-BB72-248C1EC357E5:DeploymentType_f192222e-e507-4c04-a046-b0f58f0fea1a</Id><Type>CC...  Del 6/7/2013 3:02:18 PM
CCMClient - Broadcasting Msg to UI : <CCMClientNotification><Sender>Service</Sender><Name>AdobeReaderXIInstaller</Name><Id>ScopeId_317B2597-B6C9-40BC-BB72-248C1EC357E5:DeploymentType_f192222e-e507-4c04-a046-b0f58f0fea1a</Id><...  Del 6/7/2013 3:02:18 PM
Sending Notification to UI : <CCMClientNotification><Sender>Service</Sender><Name>AdobeReaderXIInstaller</Name><Id>ScopeId_317B2597-B6C9-40BC-BB72-248C1EC357E5:DeploymentType_f192222e-e507-4c04-a046-b0f58f0fea1a</Id><Type>CC...  Del 6/7/2013 3:02:19 PM
CCMClient - Broadcasting Msg to UI : <CCMClientNotification><Sender>Service</Sender><Name>AdobeReaderXIInstaller</Name><Id>ScopeId_317B2597-B6C9-40BC-BB72-248C1EC357E5:DeploymentType_f192222e-e507-4c04-a046-b0f58f0fea1a</Id><...  Del 6/7/2013 3:02:19 PM
Sending Notification to UI : <CCMClientNotification><Sender>Service</Sender><Name>AdobeReaderXIInstaller</Name><Id>ScopeId_317B2597-B6C9-40BC-BB72-248C1EC357E5:DeploymentType_f192222e-e507-4c04-a046-b0f58f0fea1a</Id><Type>CC...  Del 6/7/2013 3:02:19 PM
CCMClient - Broadcasting Msg to UI : <CCMClientNotification><Sender>Service</Sender><Name>AdobeReaderXIInstaller</Name><Id>ScopeId_317B2597-B6C9-40BC-BB72-248C1EC357E5:DeploymentType_f192222e-e507-4c04-a046-b0f58f0fea1a</Id><...  Del 6/7/2013 3:02:19 PM
Sending Notification to UI : <CCMClientNotification><Sender>Service</Sender><Name>AdobeReaderXIInstaller</Name><Id>ScopeId_317B2597-B6C9-40BC-BB72-248C1EC357E5:DeploymentType_f192222e-e507-4c04-a046-b0f58f0fea1a</Id><Type>CC...  Del 6/7/2013 3:02:20 PM
CCMClient - Broadcasting Msg to UI : <CCMClientNotification><Sender>Service</Sender><Name>AdobeReaderXIInstaller</Name><Id>ScopeId_317B2597-B6C9-40BC-BB72-248C1EC357E5:DeploymentType_f192222e-e507-4c04-a046-b0f58f0fea1a</Id><...  Del 6/7/2013 3:02:20 PM

Date/Time:  6/7/2013 3:02:15 PM          Component:  Default
Thread:     2954985472 (0xB0218000)      Source:     OSXPkgInstaller.mm:124

Installing Software for ContentId : Content_90f15c71-84ad-4a4b-b4a9-77b2cb1a9f4f
```

Look for an entry that says Install:Complete in the logs. The presence of such an entry in this stage of the workflow indicates that the application Adobe Reader has been successfully installed on the Mac computer.



```
Log Text                                                                                                 C.  Date/Time
Sending Notification to UI : <CCMClientNotification><Sender>Service</Sender><Name>AdobeReaderXIInstaller</Name><Id>ScopeId_317B2597-B6C9-40BC-BB72-248C1EC357E5:DeploymentType_f192222e-e507-4c04-a046-b0f58f0fea1a</Id><Type>CC...  Del 6/7/2013 3:02:35 PM
CCMClient - Broadcasting Msg to UI : <CCMClientNotification><Sender>Service</Sender><Name>AdobeReaderXIInstaller</Name><Id>ScopeId_317B2597-B6C9-40BC-BB72-248C1EC357E5:DeploymentType_f192222e-e507-4c04-a046-b0f58f0fea1a</Id><...  Del 6/7/2013 3:02:35 PM
Install: Complete                                                                                        Del 6/7/2013 3:02:35 PM
Successfully installed app                                                                               Del 6/7/2013 3:02:35 PM
No Preferences found for Key - 'InstallRebootDelay', Domain - 'com.microsoft.ccmclient'.                 Del 6/7/2013 3:02:35 PM
Sending Notification to UI : <CCMClientNotification><Sender>Service</Sender><Name>AdobeReaderXIInstaller</Name><Id>ScopeId_317B2597-B6C9-40BC-BB72-248C1EC357E5:DeploymentType_f192222e-e507-4c04-a046-b0f58f0fea1a</Id><Type>CC...  Del 6/7/2013 3:02:35 PM
+SetValueInPlist : Key : InstallLastState, Value : <CCMClientNotification><Sender>Service</Sender><Name>AdobeReaderXIInstaller</Name><Id>ScopeId_317B2597-B6C9-40BC-BB72-248C1EC357E5:DeploymentType_f192222e-e507-4c04-a046-b0f58f0fe...  Del 6/7/2013 3:02:35 PM
CCMClient - Broadcasting Msg to UI : <CCMClientNotification><Sender>Service</Sender><Name>AdobeReaderXIInstaller</Name><Id>ScopeId_317B2597-B6C9-40BC-BB72-248C1EC357E5:DeploymentType_f192222e-e507-4c04-a046-b0f58f0fea1a</Id><...  Del 6/7/2013 3:02:35 PM
-SetValueInPlist : Key : InstallLastState                                                                Del 6/7/2013 3:02:35 PM
Installation completed with JobStatus : InstallSuccess                                                   Del 6/7/2013 3:02:35 PM
7A642190: Client Sent : "<CCMClientNotification><Sender>UI</Sender><Name>AdobeReaderXIInstaller</Name><Id>ScopeId_317B2597-B6C9-40BC-BB72-248C1EC357E5:DeploymentType_f192222e-e507-4c04-a046-b0f58f0fea1a</Id><Type>CCM_Install...  Del 6/7/2013 3:03:58 PM
CCMClient - ProcessUIMessage. Msg : <CCMClientNotification><Sender>UI</Sender><Name>AdobeReaderXIInstaller</Name><Id>ScopeId_317B2597-B6C9-40BC-BB72-248C1EC357E5:DeploymentType_f192222e-e507-4c04-a046-b0f58f0fea1a</Id><Typ...  Del 6/7/2013 3:03:58 PM
Received Notification for Install/Reboot.                                                                Del 6/7/2013 3:03:58 PM
PreferencesService - ProcessNotification()                                                               Del 6/7/2013 3:03:58 PM
OMADMService - ProcessNotification()                                                                     Del 6/7/2013 3:03:58 PM
+SetValueInPlist : Key : InstallLastState, Value : , Path : /Library/Application Support/Microsoft/CCM/SwJobMetaData.plist  Del 6/7/2013 3:03:58 PM
-SetValueInPlist : Key : InstallLastState                                                                Del 6/7/2013 3:03:58 PM
Sending Notification to UI : <CCMClientNotification><Sender>Service</Sender><Name>AdobeReaderXIInstaller</Name><Id>ScopeId_317B2597-B6C9-40BC-BB72-248C1EC357E5:DeploymentType_f192222e-e507-4c04-a046-b0f58f0fea1a</Id><Type>CC...  Del 6/7/2013 3:03:58 PM
CCMClient - Broadcasting Msg to UI : <CCMClientNotification><Sender>Service</Sender><Name>AdobeReaderXIInstaller</Name><Id>ScopeId_317B2597-B6C9-40BC-BB72-248C1EC357E5:DeploymentType_f192222e-e507-4c04-a046-b0f58f0fea1a</Id><...  Del 6/7/2013 3:03:58 PM
Job : ScopeId_317B2597-B6C9-40BC-BB72-248C1EC357E5:DeploymentType_f192222e-e507-4c04-a046-b0f58f0fea1a state is InstallSuccessComplete . Removing from process queue  Del 6/7/2013 3:03:58 PM
+SetValueInPlist : Key : InstallLastState, Value : , Path : /Library/Application Support/Microsoft/CCM/SwJobMetaData.plist  Del 6/7/2013 3:03:58 PM
-SetValueInPlist : Key : InstallLastState                                                                Del 6/7/2013 3:03:58 PM
OMADMService - ProcessNotification()                                                                     Del 6/7/2013 3:03:58 PM
OMADMService - Received Notification for OMAConnect - CCM_OMA                                            Del 6/7/2013 3:03:58 PM
Job came to InstallSuccessComplete. Nothing to do. Returning                                             Del 6/7/2013 3:03:58 PM
Failed to GetProperty Mode from Configuration Provider : 80070490                                        Del 6/7/2013 3:03:58 PM
Job : ScopeId_317B2597-B6C9-40BC-BB72-248C1EC357E5:DeploymentType_f192222e-e507-4c04-a046-b0f58f0fea1a state is InstallSuccessComplete . Removing from process queue  Del 6/7/2013 3:03:58 PM

Date/Time:  6/7/2013 3:02:35 PM          Component:  Default
Thread:     2954985472 (0xB0218000)      Source:     OSXPkgInstaller.mm:104

Install: Complete
```

Under CCMCache folder on the Mac computer, review the different folders for the application that was downloaded. The presence of these folders is another indicator that application deployment is working as expected.



Name	Date Modified	Size	Kind
CIM_SoftwareJob	Today 3:17 PM	--	Folder
CIM_SwDownloadJob	Today 3:17 PM	--	Folder
CIM_SwInstallJob	Today 3:17 PM	--	Folder
CIM_SwJobContent	Today 3:17 PM	--	Folder
CIM_SwJobContentItem	Today 3:17 PM	--	Folder

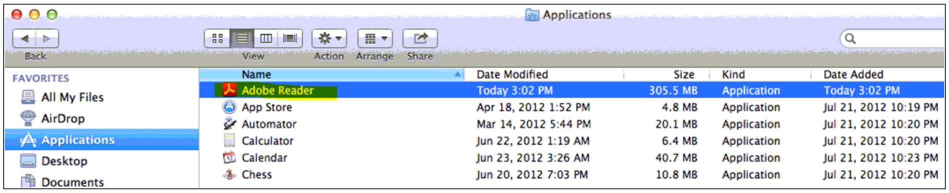
Open the CIM_SwInstallJob folder shown in the previous screenshot, then open the ScopeId_*xxxx* file and review the information it contains to verify that Adobe Reader is listed. This can be helpful when you need to determine which applications have been downloaded and which have not when you are troubleshooting the installation of multiple applications.

```
<CIM_SwInstallJob><JobId>ScopeId_317B2597-B6C9-40BC-BB72-248C1EC357E5:DeploymentType_
f192222e-e507-4c04-a046-b0f58f0fea1a</JobId><Name>AdobeReaderXIInstaller</Name><Desc
/><JobType>Software</JobType><AssociativeId>Content_90f15c71-84ad-4a4b-b4a9-
77b2cb1a9f4f</AssociativeId><PkgType>pkg</PkgType><Priority>1</Priority><CommandLine>/
usr/sbin/installer -pkg "Adobe Reader XI Installer.pkg"  -target "/" -verboseR</CommandL
ine><ActionType>Install</ActionType></CIM_SwInstallJob>
```

Open the CIM_SwJobContent folder located under CCMCache and review the information in the Content_*xxxx* file, looking for the following entry that has additional details concerning the application including its content hash. This can help when you need to troubleshoot hash mismatch issues.

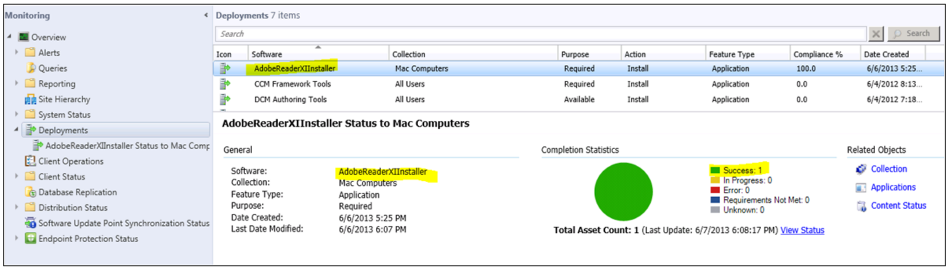
```
<CIM_SwJobContent><ContentId>Content_90f15c71-84ad-4a4b-b4a9-77b2cb1a9f4f</Content
Id><FileList><File>AdobeReaderXIInstaller.cmmac</File></FileList><FileSizeList><Fi
le>80444445</File></FileSizeList><ContentHash>07EEBA48F025E170595787BE97933D33BAE26D7064
65983FEB53C45C13B7A1A4</ContentHash></CIM_SwJobContent>
```

Under Applications on the Mac computer, make sure Adobe Reader is installed:



Name	Date Modified	Size	Kind	Date Added
Adobe Reader	Today 3:02 PM	305.5 MB	Application	Today 3:02 PM
App Store	Apr 18, 2012 1:52 PM	4.8 MB	Application	Jul 21, 2012 10:19 PM
Automator	Mar 14, 2012 5:44 PM	20.1 MB	Application	Jul 21, 2012 10:20 PM
Calculator	Jun 22, 2012 1:19 AM	6.4 MB	Application	Jul 21, 2012 10:20 PM
Calendar	Jun 23, 2012 3:26 AM	40.7 MB	Application	Jul 21, 2012 10:23 PM
Chess	Jun 20, 2012 7:03 PM	10.8 MB	Application	Jul 21, 2012 10:20 PM

One other method for checking whether application deployment was successful is to review the status in the Configuration Manager console under Deployments in the Monitoring workspace:



Deployments 7 items

Icon	Software	Collection	Purpose	Action	Feature Type	Compliance %	Date Created
	AdobeReaderXIInstaller	Mac Computers	Required	Install	Application	100.0	6/6/2013 5:25...
	CCM Framework Tools	All Users	Required	Install	Application	0.0	6/4/2012 8:13...
	DCM Authoring Tools	All Users	Available	Install	Application	0.0	6/4/2012 7:18...

AdobeReaderXIInstaller Status to Mac Computers

General

Software:	AdobeReaderXIInstaller
Collection:	Mac Computers
Feature Type:	Application
Purpose:	Required
Date Created:	6/6/2013 5:25 PM
Last Date Modified:	6/6/2013 6:07 PM

Completion Statistics

- 🟩 Success: 1
- 🟨 In Progress: 0
- 🟥 Error: 0
- 🟦 Requirements Not Met: 0
- ⬜ Unknown: 0

Total Asset Count: 1 (Last Update: 6/7/2013 6:08:17 PM) View Status

Related Objects

As you can see from the preceding walkthrough, the overall workflow for application deployment on a Mac client is a little different than for a Windows client. This section and its logs and screenshots can help you find the root cause of application deployment issues to Mac clients by enabling you to compare the logs for successful deployment shown here against the logs collected in your environment.

About the authors

Rushi Faldu

Rushi Faldu, a Senior Premier Field Engineer supporting System Center Configuration Manager, has been with Microsoft for eight years. He has been working with the product since SMS 2.0. He is a lead for the System Center Concepts & Administration workshop which is delivered to many premier customers throughout the world. He is also an author of *Microsoft System Center: Configuration Manager Field Experience* (Microsoft Press, 2013). Rushi resides in New Jersey and enjoys P90X and Insanity workouts in his free time. He loves hiking, camping, and playing tennis with his daughters.

Manoj Kumar Pal

Manoj is a consultant with Microsoft Consulting Services and has more than 10 years of IT experience. His areas of expertise are the System Center suite of products and client management. He is passionate about technology and in his free time he loves to play games on Xbox. Manoj earned his computing degree in India and is now based out of Chicago, Illinois, with his wife and son.

Andre Della Monica

Andre Della Monica, Premier Field Engineer for Microsoft, has been working with System Center Configuration Manager since it was known as SMS. Before becoming a Premier Field Engineer, he was also awarded as a top Support Engineer on the CTS for the Microsoft Platform products.

Andre attended college at Sao Paulo, Brazil, and earned his technology degree in Computer Network Management. He resides in Houston, Texas, and in his free time enjoys playing electric guitar, piano, and bass, as well as being an Xbox gamer.

Kaushal Pandey

Kaushal works as consultant with Microsoft Consulting Services and has more than 8 years of IT experience. He started his career working with SMS 2003 and since then he has seen the technology evolve into System Center Configuration Manager. He is passionate about the technology and in his free time he loves to play cricket or swim.

Manish Raval (contributing author)

Manish is a consultant with Microsoft Consulting Services based out of Calgary, Canada. He has 8+ years of experience in IT and started his career at Microsoft in the support group supporting Active Directory and later SMS 2003 and System Center Configuration Manager 2007, both as a Support Engineer and a Trainer and Technical Lead.

Manish is passionate about working with customers. He specializes in Windows Server Active Directory, Virtualization, Desktop Deployment, and the System Center suite of products with a special emphasis on System Center Configuration Manager. He has also spoken at TechEd India. In his free time, he enjoys seasonal sports like skiing, biking, hiking, swimming, and so on.

Deepak Sidhpura (contributing author)

Deepak is a consultant with Microsoft Consulting Services. He has over 8 years of IT experience and works on System Center products and Windows deployment. Before joining Consulting Services, he worked as a Support Engineer with Microsoft Support Services supporting Domain Services and System Center products. He likes spending his free time with his family.

About the Series Editor

MITCH TULLOCH is a well-known expert on Windows Server administration and virtualization. He has published hundreds of articles on a wide variety of technology sites and has written or contributed to over two dozen books, including the *Windows 7 Resource Kit* (Microsoft Press, 2009), for which he was lead author*; Understanding Microsoft Virtualization Solutions: From the Desktop to the Datacenter* (Microsoft Press, 2010); and *Introducing Windows Server 2012* (Microsoft Press, 2012), a free e-book that has been downloaded almost three quarters of a million times.

Mitch has been repeatedly awarded Most Valuable Professional (MVP) status by Microsoft for his outstanding contributions to supporting the global IT community. He is a nine-time MVP in the technology area of Windows Server Software Packaging, Deployment & Servicing. You can find his MVP Profile page at *http://mvp.microsoft.com/en-us/mvp/Mitch%20Tulloch-21182*.

Mitch is also Senior Editor of WServerNews (*http://www.wservernews.com*), a weekly newsletter focused on system admin and security issues for the Windows Server platform. With more than 100,000 IT Pro subscribers worldwide, WServerNews is the largest Windows Server–focused newsletter in the world.

Mitch runs an IT content development business based in Winnipeg, Canada that produces white papers and other collateral for the business decision maker (BDM) and technical decision maker (TDM) audiences. His published content ranges from white papers about Microsoft cloud technologies to reviews of third-party products designed for the Windows Server platform. Before starting his own business in 1998, Mitch worked as a Microsoft Certified Trainer (MCT) for Productivity Point.

For more information about Mitch, visit his website at *http://www.mtit.com*.

You can also follow Mitch on Twitter at *http://twitter.com/mitchtulloch* or like him on Facebook at *http://www.facebook.com/mitchtulloch*.