Understanding Configuration Manager components

C omponents 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.

Folder Tools System	Center 2012 Configuration Man	ager (Connected to CAS - CAS Site Server)
Home Folder Home Folder Create Saved Searches - Search Searches - Search Software Librar	Create Prestage Content File Revision History Update Statistics Dep Application y • Overview • Application	Reinstate Copy Create Ioyment Type Export Delete Management > Applications
Software Library <	Applications 22 items	
Overview	Search	
Application Management	Icon Name	CI Unique ID
Applications	.NET Framework 4	BA-FAR STREET
 Packages Approval Requests Global Conditions App-V Virtual Environments Windows RT Sideloading Keys Software Updates Operating Systems 	Adobe Flash Player 10 Adobe Reader 9 Adobe Reader 9 Adobe Reader X Adobe Reader XI Insta App-V Client Configuration Manager DP Test Excel (App-V)	Image Access Accounts -AE Image Access
Assets and Compliance Software Library Monitoring Administration	Software Version: Manufacturer: Superseded: Comments:	Image: Simulate Deployment Deploy Distribute Content Move Set Security Scopes Categorize
Ready	Summary Deployment Type	🕅 View Relationships

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.

Image: Tools Window Help Image: Tools Window Help Image: Tools Image: Tools Image: Tools Image: Tools Thread Image: Tools Image: Tools Image: Tools Image: Tools Thread Store Image: Tools Image: Tools Image: Tools Image: Tools Thread Store Store <th>Configura</th> <th>tion Manager Trace Log</th> <th>g Tool - [C:\Progr</th> <th>ram Files\\Logs</th> <th>s\smsdbmon.log]</th> <th></th> <th></th> <th></th>	Configura	tion Manager Trace Log	g Tool - [C:\Progr	ram Files\\Logs	s\smsdbmon.log]			
Component Date/Time Thread Log Text Component Date/Time Thread SND: Dropped C: (Program Files/Wicrosoft Configuration Manager (Inboxes/polSMS_DATABASE_NOTTFICATT) 6/24/2013 6:30:58 PM 3324 (0xEP0) A SND: Dropped C: (Program Files/Wicrosoft Configuration Manager (Inboxes/polSMS_DATABASE_NOTTFICATT) 6/24/2013 6:31:03 PM 3324 (0xEP0) A RCV: UPDATE on Sites for Sites_Interop_Lipdate_HMA.W [TST][7205759403 SMS_DATABASE_NOTTFICATT 6/24/2013 6:31:03 PM 3324 (0xEP0) SND: Dropped C: (Program Files/Wicrosoft Configuration Manager (Inboxes/polSMS_DATABASE_NOTTFICATT) 6/24/2013 6:31:03 PM 3324 (0xEP0) SND: Dropped C: (Program Files/Wicrosoft Configuration Manager (Inboxes/PMSMS_DATABASE_NOTTFICATT) 6/24/2013 6:31:03 PM 3324 (0xEP0) SND: Dropped C: (Program Files/Wicrosoft Configuration Manager (Inboxes/PMSMS_DATABASE_NOTTFICATT) 6/24/2013 6:31:03 PM 3324 (0xEP0) SND: Dropped C: (Program Files/Wicrosoft Configuration Manager (Inboxes/pdSMS_DATABASE_NOTFICATT) 6/24/2013 6:31:03 PM 3324 (0xEP0) SND: Dropped C: (Program Files/Wicrosoft Configuration Manager (Inboxes/pdSMS_DATABASE_NOTFICATT) 6/24/2013 6:31:03 PM 3324 (0xEP0) SND: Dropped C: (Program Files/Wicrosoft Configuration Manager (Inboxes/pdSMS_DATABASE_NOTFICATT) 6/24/2013 6:49:38 PM 324 (0xEP0) SND SND: Dropped C: (Program Files/Wicrosoft Configuration Manager (File Tool	ls Window Help					_ 6	e ×
Log Text Date Time Date/Time Thread Date/Time Thread Date/Time Thread Discourses/polSMS_DATABASE_NOTTFICATTI 6/24/2013 6:30:58 PM 3324 (0xEP0) RCV: UPDATE on Sites for Sites_Interop_Lipdate_HMAN [TST][7205759403 SMS_DATABASE_NOTTFICATTI 6/24/2013 6:31:03 PM 324 (0xEP0) SND: Dropped Ci (Program Files/Microsoft Configuration Manager (Inboxes)pol SMS_DATABASE_NOTTFICATTI 6/24/2013 6:31:03 PM 324 (0xEP0) SND: Dropped Ci (Program Files/Microsoft Configuration Manager (Inboxes)pol SMS_DATABASE_NOTTFICATTI 6/24/2013 6:31:03 PM 324 (0xEP0) SND: Dropped Ci (Program Files/Microsoft Configuration Manager (Inboxes)pol SMS_DATABASE_NOTTFICATTI 6/24/2013 6:31:03 PM 324 (0xEP0) SND: Dropped Ci (Program Files/Microsoft Configuration Manager (Inboxes)pol SMS_DATABASE_NOTTFICATTI 6/24/2013 6:31:03 PM 324 (0xEP0) SND: Dropped Ci (Program Files/Microsoft Configuration Manager (Inboxes)pol SMS_DATABASE_NOTTFICATTI 6/24/2013 6:31:03 PM 324 (0xEP0) SND: Dropped Ci (Program Files/Microsoft Configuration Manager (Inboxes)pol SMS_DATABASE_NOTTFICATTI 6/24/2013 6:31:03 PM 324 (0xEP0) SND: Dropped Ci (Program Files/Microsoft Configuration Manager (Inboxes)pol SMS_DATABASE_NOTTFICATTI 6/24/2013 6:31:03 PM 324 (0xEP0) SND: Dropped Ci (Program Files/Microsoft Configuration Manager (Inboxes)pol SMS_DATABASE_NOTTFICATTI 6/24/2013 6:31:03 PM 324 (0xEP0) SND: Dropped Ci (Program Files/Microsoft Configuration Manager (Inboxes)pol SMS_DATABASE_NOTTFICATTI 6/24/2013 6:49:38 PM 324 (0xEP0) SND: Dropped Ci (Program Files/Microsoft Configuration Manager (Inboxes)pol SMS_DATABASE_NOTTFICATTI 6/24/2013 6:49:38 PM 324 (0xEP0) SND: Dropped Ci (Program Files/Microsoft Configuration Manager (Inboxes)pol SMS_DATABASE_NOTTFICATTI 6/24/2013 6:49:38 PM 324 (0xEP0) SND: Dropped Ci (Program Files/Microsoft Configuration Manager (Inboxes)pol SMS_DATABASE_NOTTFICATTI 6/24/2013 6:49:38 PM 324 (0xEP0) SND: Dropped Ci (Program Files/Microsoft Configuration Manager (Inboxes)pol SMS_DATABASE_NOTTFICATTI 6/24/2013 6:49:38 P	6	🖻 🗛 🔢 🗖						
SND: Dropped C: (Program Files/Microsoft Configuration Manager (Inboxes) pol SMS_DATABASE_NOTIFICATE 6/24/2013 6:30:58 PM 3824 (0xEP0) SND: Dropped C: (Program Files/Microsoft Configuration Manager (Inboxes) pol SMS_DATABASE_NOTIFICATE 6/24/2013 6:30:58 PM 3824 (0xEP0) RCV: UPDATE on Sites for Sites_Interop_Update_HMAI [TST] [20:5799403 SMS_DATABASE_NOTIFICATE 6/24/2013 6:31:03 PM 3824 (0xEP0) Modified trigger definition for Hierarchy Manager [Sites_Interop_Update_HMA SMS_DATABASE_NOTIFICATE 6/24/2013 6:31:03 PM 3824 (0xEP0) SND: Dropped C: (Program Files/Microsoft Configuration Manager (Inboxes) f/m SMS_DATABASE_NOTIFICATE 6/24/2013 6:31:03 PM 3824 (0xEP0) SND: Dropped C: (Program Files/Microsoft Configuration Manager (Inboxes) f/m SMS_DATABASE_NOTIFICATE 6/24/2013 6:31:03 PM 3824 (0xEP0) SND: Dropped C: (Program Files/Microsoft Configuration Manager (Notification)[SiteCtriN SMS_DATABASE_NOTIFICATE 6/24/2013 6:31:03 PM 3824 (0xEP0) SND: Dropped C: (Program Files/Microsoft Configuration Manager (Notification)[SiteCtriN SMS_DATABASE_NOTIFICATE 6/24/2013 6:31:03 PM 3824 (0xEP0) SND: Dropped C: (Program Files/Microsoft Configuration Manager (Inboxes) f/m SMS_DATABASE_NOTIFICATE 6/24/2013 6:31:03 PM 3824 (0xEP0) SND: Dropped C: (Program Files/Microsoft Configuration Manager/Inboxes) f/m SMS_DATABASE_NOTIFICATE 6/24/2013 6:31:03 PM 3824 (0xEP0) SND: Dropped C: (Program Files/Microsoft Configuration Manager/Inboxes) f/m SMS_DATABASE_NOTIFICATE 6/24/2013 6:49:38 PM 3824 (0xEP0) SND: Dropped C: (Program Files/Microsoft Configuration Manager/Inboxes) f/m SMS_DATABASE_NOTIFICATE 6/24/2013 6:49:38 PM 3824 (0xEP0) SND: Dropped C: (Program Files/Microsoft Configuration Manager/Inboxes) f/m SMS_DATABASE_NOTIFICATE 6/24/2013 6:49:38 PM 3824 (0xEP0) SND: Dropped C: (Program Files/Microsoft Configuration Manager/Inboxes) f/m SMS_DATABASE_NOTIFICATE 6/24/2013 6:49:38 PM 3824 (0xEP0) SND: Dropped C: (Program Files/Microsoft Configuration Manager/Inboxes) f/m SMS_DATABASE_NOTIFICATE 6/	Log Text				Component	Date/Time	Thread	T
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]	SND: Dropped SND: Dropped RCV: UPDATE RCV: UPDATE RCV: UPDATE Modified trigge Evaluating tasi SND: Dropped SND: Dropped SND: Dropped SND: Dropped	C: Yrogram Files Wicrosoft C: Yrogram Files Wicrosoft O: Stes for Stess Interop_1 on Site ControlNotification of stecOntrolNotification (C: Yrogram Files Wicrosoft othication. c: Yrogram Files Wicrosoft O: Roglosoftication for Right C: Yrogram Files Wicrosoft C: Yrogram Files Wicrosoft C: Yrogram Files Wicrosoft	Configuration Mana Configuration Mana Jpdate_HMAN (TST or SileCtriNot_Add_ anager[Sites_Interc Configuration Mana ata Manager (Notifi Configuration Mana Stry_Add [TST0000 Strfy_Add [TST0000 Configuration Mana Configuration Mana	ger Vnboxes (pol ger Vnboxes (pol) [7205759403) [7205759403 poly [72]. poly [72]. poly [72]. ger Vnboxes (val 1] [7205759403 1] [7205759	SMS_DATABASE_NOTIFICATI SMS_DATABASE_NOTIFICATI SMS_DATABASE_NOTIFICATI SMS_DATABASE_NOTIFICATI SMS_DATABASE_NOTIFICATI SMS_DATABASE_NOTIFICATI SMS_DATABASE_NOTIFICATI SMS_DATABASE_NOTIFICATI SMS_DATABASE_NOTIFICATI SMS_DATABASE_NOTIFICATI SMS_DATABASE_NOTIFICATI SMS_DATABASE_NOTIFICATI SMS_DATABASE_NOTIFICATI SMS_DATABASE_NOTIFICATI	042/1116 5:30:58 PM 6[24/2013 5:30:58 PM 6[24/2013 5:30:59 PM 6[24/2013 5:31:03 PM 6[24/2013 5:49:38 PM 6[24/2013 5:49:38 PM	3824 (0xEF0) 3824 (0xEF0)	
RCV: INSERT on PkgNotification for PkgNotify_Add [TST00001][72057594038058778]	Date/Time: Thread:	6/24/2013 6:49:38 PM 3824 (0xEF0)	Component: Source:	SMS_DATABASE	NOTIFICATION_MON			
Tapsed time is 772h 36m 53s 740ms (2781413.740 seconds)	RCV: INSERT	on PkgNotification for PkgN	otify_Add [TST0000	01][72057594038	J58778]			*
	Flapsed time is	772h 36m 53s 740ms (278	1413.740 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.



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:

 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.



- 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:

 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:



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:

🚏 Create Site System Sei	rver Wizard	×
General General		
General Proxy	Select a server to use as a site system	
System Role Selection Summary Progress	Name: Example: server1.corp.contoso.com	1
Completion	PULLDPSERVER.CURP.COM erowse Site code: CM1-Central Site CM12	1
	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 mules the site server initiates all connections to the site system server by using the Site. Syste	m
	Installation Account.	
	Use the site server's computer account to install this site system Use another account for installing this site system	
	Set]

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:

🚏 Create Site System Ser	ver Wizard	×
System Role Se	ection	
General Proxy System Role Selection	Specify roles for this server	
Drive Settings Pull Dishbution Point PXE Settings Multicast Content Validation Boundary Groups Summary Progress Completion	Available frees: Application Catalog webster point Application Catalog webster point Asset Intelligence synchronization point Endpoint Protection point Frollment point Frollment proxy point Fallback status point Out of band service point Cut of band service point Software update point Software update point State migration point	

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

🚏 Create Site System Ser	ver Wizard			x
Distribution poin	it			
General	Specify distribution point	settings		
Proxy				
System Role Selection				
Distribution point	A distribution point contains source	files for clients to download.		
Drive Settings	Install and configure IIS if requi	red by Configuration Manager		
Pull Distribution Point	You must select this option to instal	the distribution point.		
PXE Settings	Specify how client computers comm	nunicate with this distribution point.		
Multicast	HTTP			
Content Validation	Does not support mobile dev	ices or Mac computers.		
Boundary Groups	C HTTPS			
Summary	Requires computers to have	a valid PKI client certificate:		
Progress	Allow intranet-only connection	วกร		¥
Completion	If you manage Mac computer Internet client connections.	s or have mobile devices that are enro nymously	Illed by Configuration Manager, select an	option that allows
	Create a self-signed certificate or im	port a PKI client certificate.		
	 Create self-signed certificate 			
	Set expiration date:	8/28/2112	▼ 10:31 PM	<u>*</u>
	C Import certificate			
	Certificate:			Browse
	Password:			
	Enable this distribution point for	prestaged content		
	Use the application or package	properties to choose how content is	copied to this distribution point.	
	0	< Previo	us Next > Summary	Cancel

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:

General Proxy System Role Selection Distribution point Drive Settings Pull Distribution Point	Specify pull distribution point settings	
PXE Settings	Source distribution points:	+
Multicast	Filer	2
Content Validation	Name Add Distribution Points	
Boundary Groups	Select the distribution points that you want to add for this distribution point	
Summary	to download content from.	
Progress		
Completion	Available distribution points:	
	Fiter	
	Name Type	
	CM12.CORP.COM On-premise	•
	OK Cancel	
		ncel

- 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 :

The Tools	Million and a state of the last		am Files (riicrosoft Configu	ration manager	logs (nman.log)		
i 🚔 🗐 🎒 🛛							12
Log Text	1 1			Component	Date/Time	Thread	
Will not update DP	["Display=\\CM12.COR	P.COM\"]MSWNET:	["SMS_SITE=CM1"]\\CM12	SMS_HIERARCHY	8/28/2013 10:34:29 PM	1540 (0x604)	
Inserted DP ["Disp	play=\\PULLDPSERVER.C	ORP.COM\"]MSWN	ET:["SMS_SITE=CM1"]\\PUL	SMS_HIERARCHY	8/28/2013 10:34:29 PM	1540 (0x604)	
INFO: Successfully	y added full client packag	e CM100002 to DF	["Display=\\PULLDPSERVER	SMS_HIERARCHY	8/28/2013 10:34:30 PM	1540 (0x604)	
INFO: Successfully	y added client upgrade p	ackage CM100003	to DP ["Display=\\PULLDPSE	SMS_HIERARCHY	8/28/2013 10:34:30 PM	1540 (0x604)	
DP cert query: EX	EC spUpdateDPCert N'PL	JLLDPSERVER.COR	P.COM', N'6a833ac4-025a-4	SMS_HIERARCHY	8/28/2013 10:34:30 PM	1540 (0x604)	
No need to remov	e default DP sender add	ress for distribution	point [["Display=\\PULLDPS	SMS_HIERARCHY	8/28/2013 10:34:30 PM	1540 (0x604)	
user(NT AUTHORI	TTY\SYSTEM) runing appli	cation(SMS_HIERA	RCHY_MANAGER) from mac	SMS_HIERARCHY	8/28/2013 10:34:30 PM	1540 (0x604)	
Site System <cm< td=""><td>M12.CORP.COM> is the I</td><td>Default Manageme</td><td>nt Point.for site <cm1></cm1></td><td>SMS_HIERARCHY</td><td>8/28/2013 10:34:30 PM</td><td>1540 (0x604)</td><td></td></cm<>	M12.CORP.COM> is the I	Default Manageme	nt Point.for site <cm1></cm1>	SMS_HIERARCHY	8/28/2013 10:34:30 PM	1540 (0x604)	
Checking if Site Sig	gning Certificate of site C	CM1 need to be sig	ned	SMS_HIERARCHY	8/28/2013 10:34:30 PM	1540 (0x604)	
Signature of Site S	Signing Certificate of site	CM1 is up-to-date		SMS_HIERARCHY	8/28/2013 10:34:30 PM	1540 (0x604)	
ClientDataCleanUp	pOnSecurityModeChange	: No change detec	ted in SSL_State.	SMS_HIERARCHY	8/28/2013 10:34:30 PM	1540 (0x604)	
Health state refer	ences are published in th	e same Active Dire	ctory forest where site serv	SMS_HIERARCHY	8/28/2013 10:34:30 PM	1540 (0x604)	
Check if the secur	ity mode of the site has	changed.		SMS_HIERARCHY	8/28/2013 10:34:30 PM	1540 (0x604)	
WCM Configuratio	on of site CM1 has not ch	anged. HMAN will r	ot 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: 15	540 (0x604)	Source:					

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



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.

🏝 Local Disk (C:)	
🕞 🕤 ~ 🦾 🗸 Computer	
Organize 🔻 📜 Open Ir	ndude in library 🔻 Share with 👻 New folder
🔶 Favorites	Name ^
🧾 Desktop	鷆 inetpub
Downloads	\mu PerfLogs
🔛 Recent Places	鷆 Program Files
📜 Libraries	鷆 Program Files (x86)
Documents	SCCMContentLib
🁌 Music	🍓 SMS_DP\$
Pictures	鷆 Taskbar
Videos	🍌 Users
📜 Computer	🕌 Windows
Network	

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:



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 Man	ager Trace Log T	ool - [C:\Progra	m Files\\Logs\dist	:mgr.k	og]		_ 🗆	l ×
File Tools Windov	v Help						_ 8	L X
) 🖻 🗏 🎒 🖻 🖊								
Log Text					Component	Date/Time	Thread	
DP registry settings have	been successfully u	updated on PULLD	PSERVER.CORP.COM		SMS_DISTRIBUTIC	8/28/2013 10:41:12 PM	3044 (0xBE4)	
STATMSG: ID=9501 SEV=	I LEV=M SOURCE=	"SMS Server" CO	MP="SMS_DISTRIBUTIO	DN	SMS_DISTRIBUTIC	8/28/2013 10:41:12 PM	3044 (0xBE4)	
STATMSG: ID=9503 SEV=	I LEV=M SOURCE=	SMS Server" CO	MP="SMS_DISTRIBUTIC	DN	SMS_DISTRIBUTIC	8/28/2013 10:41:12 PM	3044 (0xBE4)	
ConfigurePXE					SMS_DISTRIBUTIC	8/28/2013 10:41:12 PM	3044 (0xBE4)	
Translated server name P	ULLDPSERVER.COF	P.COM to CORP.	COM\PULLDPSERVER.CO	DR	SMS_DISTRIBUTIC	8/28/2013 10:41:12 PM	3044 (0xBE4)	
CWmi::Connect() failed to	o connect to \\PULL	DPSERVER.CORP	.COM/root/SCCMDP, Err	or	SMS_DISTRIBUTIC	8/28/2013 10:41:12 PM	3044 (0xBE4)	
STATMSG: ID=2391 SEV=	E LEV=M SOURCE	="SMS Server" CC	MP="SMS_DISTRIBUTIO	DN	SMS_DISTRIBUTIC	8/28/2013 10:41:12 PM	3044 (0xBE4)	
Failed to connect to DP W	/MI provider				SMS_DISTRIBUTIC	8/28/2013 10:41:12 PM	3044 (0xBE4)	
CDistributionManager::Co	onfigurePXE failed; (0x800706ba			SMS_DISTRIBUTIC	8/28/2013 10:41:12 PM	3044 (0xBE4)	
Translated server name P	ULLDPSERVER.COF	P.COM to CORP.	COM/PULLDPSERVER.CO	DR	SMS_DISTRIBUTIC	8/28/2013 10:41:12 PM	3044 (0xBE4)	
CWmi::Connect() failed to	connect to \\PULL	DPSERVER.CORP	COM/root\SCCMDP. Err	or	SMS_DISTRIBUTIC	8/28/2013 10:41:12 PM	3044 (0xBE4)	
STATMSG: ID=2391 SEV=	E LEV =M SOURCE	="SMS Server" CC	MP="SMS_DISTRIBUTIO	DN	SMS_DISTRIBUTIC	8/28/2013 10:41:12 PM	3044 (0xBE4)	- 1
GetWMIObject - Failed to	connect to root\SC	CMDP on ["Displa	y=\\PULLDPSERVER.CO	RP	SMS_DISTRIBUTIC	8/28/2013 10:41:12 PM	3044 (0xBE4)	
Sleep 1784 seconds					SMS_DISTRIBUTIC	8/28/2013 10:41:12 PM	3044 (0xBE4)	-
Date/Time: 8/28/2013 Thread: 3044 (0x8)	3 10:41:12 PM 3E4)	Component: Source:	SMS_DISTRIBUTION_N	1ANAGE	ER			
CWmi::Connect() failed I	to connect to \\PULI	LDPSERVER.CORF	COM/root/SCCMDP. Er	ror = 0	x800706BA			×
Elapsed time is 1370h 39m	n 40s 427ms (49343	80.427 seconds)						11

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.
- 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.

File Tools	s Window Help				_ 6	1×
6 📃 🖨	🖻 🚧 📕 🔲					
Log Text			Component	Date/Time	Thread	
Updated BGR	B Server Configuration for	WIN2008-SCCM.PRIVATE.LAB.	SMS_SITE_COMPONENT_MAN	7/9/2013 5:03:23 PM	2856 (0x828)	
Synchronization	n complete.		SMS_SITE_COMPONENT_MAN	7/9/2013 5:03:23 PM	2856 (0xB28)	
Waiting for cha	inges to the "C:\Program F	Files Wicrosoft Configuration Manage	SMS_SITE_COMPONENT_MAN	7/9/2013 5:03:23 PM	2856 (0x828)	
Detected a cha	inge to the "C:\Program Fi	les Microsoft Configuration Manager	SMS_SITE_COMPONENT_MAN	7/9/2013 5:03:23 PM	2856 (0x828)	
A new master :	site control file was not av	ailable.	SMS_SITE_COMPONENT_MAN	7/9/2013 5:03:23 PM	2856 (0xB28)	
Waiting for cha	inges to the "C:\Program F	Files Wicrosoft Configuration Manage	SMS_SITE_COMPONENT_MAN	7/9/2013 5:03:23 PM	2856 (0x828)	
Detected a cha	inge to the "C:\Program Fi	les Microsoft Configuration Manager	SMS_SITE_COMPONENT_MAN	7/9/2013 5:07:15 PM	2856 (0x828)	
Parsed the master site control file, serial number 3938404632.			SMS_SITE_COMPONENT_MAN	7/9/2013 5:07:16 PM	2856 (0xB28)	
Synchronizing s	server table and polling se	rvers as needed	SMS_SITE_COMPONENT_MAN	7/9/2013 5:07:16 PM	2856 (0xB28)	
Synchronizing	component server WIN20	08-SCCM.PRIVATE.LAB	SMS_SITE_COMPONENT_MAN	7/9/2013 5:07:16 PM	2856 (0x828)	
Component	SMS_WSUS_CONTROL_M/	ANAGER flagged for installation.	SMS_SITE_COMPONENT_MAN	7/9/2013 5:07:16 PM	2856 (0xB28)	
INFO: WIN200	8-SCCM.PRIVATE.LAB' is a	a valid FQDN.	SMS_SITE_COMPONENT_MAN	7/9/2013 5:07:16 PM	2856 (0x828)	
STATMSG: ID=	1013 SEV=I LEV=M SOUR	CE="SMS Server" COMP="SMS_WS	SMS_SITE_COMPONENT_MAN	7/9/2013 5:07:16 PM	2856 (0xB28)	
Synchronizatio	on complete.		SMS_SITE_COMPONENT_MAN	7/9/2013 5:07:16 PM	2856 (0xB28)	-
Date/Time: Thread:	7/9/2013 5:07:16 PM 2856 (0x828)	Component: SMS_SITE_COMP Source:	PONENT_MANAGER			
Component	SMS_WSUS_CONTROL_M	ANAGER flagged for installation.				*
						1000

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.

nc Sel	Settings Classifications Products Sync Schedule Supersedence Rules Languages ect the synchronization source for this software update point.
с	Synchronize from Microsoft Update
	When there is an upstream software update point, this option is unavailable.
Ċ.	Synchronize from an upstream data source location (URL)
	Example: http://WSUSServer:80 or https://WSUSServer:8531
	Browse
•	Do not synchronize from Microsoft Update or upstream data source
•	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.
(°	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 fror Microsoft Update or the upstream software update point.
(WS You Wir eve	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. SUS reporting events u can configure the Windows Update Agent on client computers to create event messages for ndows Server Update Services (WSUS) reporting. Configuration Manager does not use these ents, you should not create them unless you require them for other uses.
(€ WS Wir eve	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. SUS reporting events u can configure the Windows Update Agent on client computers to create event messages for ndows Server Update Services (WSUS) reporting. Configuration Manager does not use these ents, you should not create them unless you require them for other uses. Do not create WSUS reporting events
WS You Wireve	Do not synchronize from Microsoft Update or upstream data source Select this option if you manually synchronize software update point is oftware update point Typically, you use manual synchronizing when the software update point is disconnected from Microsoft Update or the upstream software update point. SUS reporting events u can configure the Windows Update Agent on client computers to create event messages for ndows Server Update Services (WSUS) reporting. Configuration Manager does not use these ents, you should not create them unless you require them for other uses. Do not create WSUS reporting events Create only WSUS status reporting events
VS Vol Vir eve	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. SUS reporting events u can configure the Windows Update Agent on client computers to create event messages for ndows Server Update Services (WSUS) reporting. Configuration Manager does not use these ris, you should not create them unless you require them for other uses. Do not create WSUS reporting events Create all WSUS status 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).

👔 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 38	40 🔺				
Found 1 SUPs SMS_WSUS_SYNC_MANAGER 3/13/2013 3:47:29 PM 38	40				
Found active SUP NYCCAS.contoso.com from SCF File. SMS_WSUS_SYNC_MANAGER 3/13/2013 3:47:29 PM 38	40 💻				
DB Server not detected for SUP NYCCAS.contoso.com from SCF File. skipping. SMS_WSUS_SYNC_MANAGER 3/13/2013 3:47:29 PM 38	40				
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 38	40				
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 38	40				
Sync failed. Will retry in 60 minutes SMS_WSUS_SYNC_MANAGER 3/13/2013 3:47:31 PM 38	40				
Setting sync alert to active state on site CAS SMS_WSUS_SYNC_MANAGER 3/13/2013 3:47:31 PM 38	40				
Sync time: 0d00h00m01s SMS_WSUS_SYNC_MANAGER 3/13/2013 3:47:31 PM 38	40				
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 38	40				
Wakeup by SCF change SMS_WSUS_SYNC_MANAGER 3/13/2013 3:47:58 PM 38	40				
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 38	40				
Wakeup by inbox drop SMS_WSUS_SYNC_MANAGER 3/13/2013 3:48:18 PM 38	40				
Found local super sources file SMC WICH & SVNC MANAGED 3/13/2013 3:48:23 DM 38	₄∩ ⊥				
Date/Time: 3/13/2013 3:47:30 PM Component: SMS_WSUS_SYNC_MANAGER					
Thread: 3840 (0xF00) Source:					
Sync failed: WSUS undate source not found on site CAS. Please refer to WCM.log for configuration error details Source: getSiteLindateSource	A				
	_				
	-				

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		_	Β×					
😂 🗏 🖨 🛤 📕 🔲								
Log Text	с.	Date/Time	1					
Read SUPs from SCF for NYCCFG.contoso.com	SMS	8/16/2013 1:43:45 PM	4; 🔺					
Found 1 SUPs SM: 8/16/2013 1:43:45 PM 4:								
Found active SUP NYCCFG.contoso.com from SCF File.	SM5	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	SM:	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.	SM:	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	SM5	8/16/2013 1:56:34 PM	7:					
Next scheduled sync is a retry sync at 8/16/2013 2:48:45 PM	SMS	8/16/2013 1:56:39 PM	7.					
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			A					
			~					
Elapsed time is 11287h 14m 46s 370ms (40634086.370 seconds)			11.					

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.

File View Help				
Connections	Sites			
Start Page NYCCFG (CONTOSO Administra	ilter:	- 64	Go 👻 🔂 Show	All 💡
Poincation Pools Pool Sites Operault Web Site WSUS Administration	fault Web Site SUS Administra	1D 1 1026867452	Status Unknown (Started (http)	Binding 808:* (net. :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:

- 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.

Folder To	os System Center 2012 Configuration Manager	(Connected to CAS - CAS Site Server)				
Home Folder						^ 🕜
Create Saved Searches Act	Access Access Access Access Access Access Access Access Aplication	Reinstate Copy Refresh te t Type Export Type Copy Copy	bloyment Move Move	Classify Relationships * Relationships	Properties Properties	
🗲 🤿 = 💽 \ • S	oftware Library + Overview + Application Manag	ement Applications				- 2
Software Library «	Applications 22 items					
4 @ Overview	Search			×	Search Add Crit	eria 🔻
A Deplication Manage	Icon Name	CI Unique ID				Dei
Applications	Internet Explorer 7	ScopeId_3FB7B59F-76DB-42AB-A87C-7	7A71E0CDE169/Applic	ation_0d3d524c-5c16-4b7e-b	od7b-751b5ebf9129/1	3
Packages	Internet Explorer 8	ScopeId_3FB7B59F-76DB-42AB-A87C-7	7A71E0CDE169/Applic	ation_4f87596a-ec2a-422c-8	753-6297bea2346c/1	3
📝 Approval Request	Internet Explorer 9	ScopeId_3FB7B59F-76DB-42AB-A87C-7	7A71E0CDE169/Applic	ation_8a348269-852f-47a7-8	8720-ef459e32384e/1	4
🖫 Global Conditions	Lync 2010	ScopeId_3FB7B59F-76DB-42AB-A87C-7	7A71E0CDE169/Applic	ation_26592622-a3d0-4ec5-b	042c-18b9b39de43c/1	2
📕 App-V Virtual Env	Microsoft Application Virtualization Client 4	ScopeId_3FB7B59F-76DB-42AB-A87C-7	7A71E0CDE169/Applic	ation_6580ba30-8a18-4aef-8	d70-294620b0f4c6/1	2
💦 Windows RT Sidel	Microsoft Application Virtualization Client 5	ScopeId_3FB7B59F-76DB-42AB-A87C-7	7A71E0CDE169/Applic	ation_8516bdff-d428-43d5-a	764-68ee1ee8a5e6/3	1
🕨 🛄 Software Updates	Microsoft RichCopy 4.0	ScopeId_3FB7B59F-76DB-42AB-A87C-7	7A71E0CDE169/Applic	ation_12d0da84-31fd-4c21-b	598-fc83cd2a8663/1	1
🕨 🛄 Operating Systems	Microsoft Update for KB2533623	ScopeId_3FB7B59F-76DB-42AB-A87C-7	7A71E0CDE169/Applic	ation_95b2e007-ed41-418d-l	beab-e23c2efa32b9/3	2
	Office Communicator 2007 R2	ScopeId_3FB7B59F-76DB-42AB-A87C-7	7A71E0CDE169/Applic	ation_4c54bb56-abbf-4fcd-b	509-a145572dc0ff/1	1
	Silverlight	ScopeId_3FB7B59F-76DB-42AB-A87C-3	7A71E0CDE169/Applic	ation_73ebb5d3-5791-46d0-	9e37-62b06bf27ab0/1	1 2
	Visio Viewer	ScopeId_3FB7B59F-76DB-42AB-A87C-7	7A71E0CDE169/Applic	ation_83b00c0d-e5cc-4352-a	8d4-c3a415c5f174/4	1
	Windows Management Framework 3.0	ScopeId_3FB7B59F-76DB-42AB-A87C-7	7A71E0CDE169/Applic	ation_3d631006-4c77-4c59-b	of3c-5ab551981307/5	2
	e in the		intercond (r. h.	······································	and noted at cate	*
Assets and Compl	Microsoft RichCopy 4.0					~
Software Library	Application Properties	Application Statistics		Related Objects		1
Monitoring	Software Version: Manufacturer	Devices with Application:	0	🔂 Content Sta	tus	
Administration	Superseded: No	Failure:	0			
	Comments:	Users with Application:	0			-
	Summary Deployment Types Deployments					

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:

Ś	QLQuery1.sqlis	trator (80))*		→ ×
[Select * fr	com dbo.v_CIAssignment where A	ssignmentName like ' <mark>%Ric</mark> ł	ıCopy%'
▲				▶ _
	Results 📑 Mes	sages		
	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.

	ar fa b r	where the second	c 1 00000000000000000000000000000000000			10 4
	Microsoft Applicatio	on virtualization Client 5	Scoperg_3FB/B29E-76	DB-42AB-A8/C-/A/1	EUCDE169/Application_8516bdff-d428-43d5-a764-68ee1ee8a5e6	/3 1
	Microsoft RichCopy	4.0	ScopeId_3FB7B59F-76	DB-42AB-A87C-7A71	E0CDE169/Application_12d0da84-31fd-4c21-b598-fc83cd2a8663,	1 1
	Microsoft Update fo	or KB2533623	ScopeId_3FB7B59F-76	DB-42AB-A87C-7A71	E0CDE169/Application_95b2e007-ed41-418d-beab-e23c2efa32b9	/3 2
	Office Communicat	tor 2007 R2	ScopeId_3FB7B59F-76	DB-42AB-A87C-7A71	E0CDE169/Application_4c54bb56-abbf-4fcd-b509-a145572dc0ff/	1 1
	Silverlight		ScopeId_3FB7B59F-76	DB-42AB-A87C-7A71	E0CDE169/Application_73ebb5d3-5791-46d0-9e37-62b06bf27ab)/1 2
	Visio Viewer		SconeId 3EB7B59E-76	DR-42AR-A87C-7A71	E0CDE169/Annlication_83b00c0d-e5cc-4352-a8d4-c3a415c5f174	/4 1 *
<						,
Micro	osoft RichCopy	4.0				~
Icon	Collection	Deployment Start Time	e Purpose	Compliance %	Deployment ID	
•	Win7	8/20/2013 3:07 PM	Required	100.0	{52DCC617-8588-4026-8BA9-01BBC566C6A3}	
Summa	ary Deployment Ty	ypes Deployments				

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:	<pre></pre>

FIGURE 2-14 Determining the PolicyID using PolicySpy.

 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	File Tools Window Help								
😂 🛢 👙 陆 🗛 11 🗐									
Log Text	Component								
Condition has changed or result has changed.									
Compiling policy 'ScopeId_3FB7B59F-76DB-42AB-A87C-7A71E0CDE169/Application_12d0da84-31fd-4c21-b598-fc83cd2a8663/CA.									
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 DataT									
DTSJob (A137055C-1AE1-41F2-BD06-EABA86E6C71A) created to download from 'http://NYCCFG.contoso.com:80/SMS_MP' to 'C: DataTransfe									
JTSJob {A137055C-1AE1-41F2-BD06-EABA86E6C71A} in state 'PendingDownload'. DataTransfe									
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 Status									
Successfully raised 1 event(s)	StatusAgent								
Raising event (#1 of 1):instance of CCM_PolicyAgent_PolicyDownloadStarted{ClientID = "GUID:37C7D492-07E0-4417-AC6D-A198	. StatusAgent								
juccessfully raised 1 event(s) StatusAgent									
Raising event (#1 of 1):instance of CCM_PolicyAgent_PolicyDownloadStarted{ClientID = "GUID:37C7D492-07E0-4417-AC6D-A198									
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_PolicyS.PolicyID="{52DCC617-8588-4026-88A9-01BBC566C6A3}",PolicySource="SMS:NYC",Policy "http://NYCCFG.contoso.com/SMS_MP/.sms_pbl?{52DCC617-8588-4026-88A9-01BBC566C6A3}.SHA256:BC57017EC1E304F4D4442D221750	/ersion = "1.00" fron 3289393292D39A55								

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="{52DCC617-8588-4026-88A9-01B8C566C6A3}",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).



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 {52DCC617-8588-4026-8BA9-01BBC56\$C6A3}				

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_3FB7859F-76D8-42A8-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_ApplicationClAssignment and CCM_ClVersionInfo using the appropriate AssignmentID and Scopeld. 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 ClStore, ClStateStore, ClDownloader, ClTaskMgr, 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.



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.



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 fcc76f7a64eb	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 dependent	No dependencies for DeploymentType ScopeId_3FB7B59F-76DB-42AB-487C-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	SconeId 3EB7B59E-76DB-42AB-A87C-7A71E0CDE169/Application_83b00c0d-e5cc-4352-a8d4-c3a415c5f174/4
Micro	soft RichCopy 4.0	
Icon	Priority Name Dep	endencies Technology Superseded Content ID
	1 Microsoft RichCopy No	MSI No Content_e900e6c0-b55c-496d-b210-0d53de88c3e3

FIGURE 2-24	A displa	, 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 CTN	i job {CAF66E46-23E1-41BC	-A772-7E13B3FA	F3E6 }.	
Created CTN	Created CTM job {CAF66E46-23E1-41BC-A772-7E13B3FAF3E6} for user S-1-5-18			
Attempting t	o persist location request f	or PackageID='C	ontent_e900e6c0-b55c-496d-b210-0d53de88c3e3' and PackageVersion='1'	
Attempting t	o create Location Request	for PackageID='0	Content_e900e6c0-b55c-496d-b210-0d53de88c3e3' and Version='1'	
Successfully	created Location Request			
Persisted loca	ation request			
System is not	t in quarantine state.			
Attempting t	o send Location Request fo	or PackageID='Co	ontent_e900e6c0-b55c-496d-b210-0d53de88c3e3'	
Created and	Sent Location Request '{96	C372E6-2239-43E	03-A998-656450A19CD6}' for package Content_e900e6c0-b55c-496d-b210	
CTM job {CA	CTM job {CAF66E46-23E1-41BC-A772-7E13B3FAF3E6} entered phase CCM_DOWNLOADSTATUS_DOWNLOADING_DATA			
Queued loca	Queued location request '{96C372E6-2239-43D3-A998-656450A19CD6}' for CTM job '{CAF66E46-23E1-41BC-A772-7E13B3FAF3E6}'.			
Persisted loca	ations for CTM job {CAF66	E46-23E1-41BC-A	772-7E13B3FAF3E6}:(LOCAL) http://NYCCFG.contoso.com/SMS_DP_SMS	
CTM job {CA	CTM job {CAF66E46-23E1-41BC-A772-7E13B3FAF3E6} (corresponding DTS job {BD0FCF2C-EF96-46D2-B072-603D4FC93AEA}) start			
CTM job {CA	CTM job {CAF66E46-23E1-41BC-A772-7E13B3FAF3E6} entered phase CCM_DOWNLOADSTATUS_DOWNLOADING_DATA			
CTM job {CA	CTM job {CAF66E46-23E1-41BC-A772-7E13B3FAF3E6} entered phase CCM_DOWNLOADSTATUS_DOWNLOADING_DATA			
CTM job {CA	F66E46-23E1-41BC-A772-7	E13B3FAF3E6} en	tered phase CCM_DOWNLOADSTATUS_DOWNLOADING_DATA	
CTM job {CA	F66E46-23E1-41BC-A772-7	E13B3FAF3E6} en	tered phase CCM_DOWNLOADSTATUS_DOWNLOADING_DATA	
CCTMJob::Pr	ocessProgress - Download	ed chunksize is 7	82 of 6325	
CTM job {CA	F66E46-23E1-41BC-A772-7	E13B3FAF3E6} su	ccessfully 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-A	772-7E13B3FAF38	56}.	

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: EC2B5CDC8AEFB1F43D9DB7F89676803E1CBE326C1A9C189A8CC1E03C5DDBAA9A				
Hash verification succeeded for content Content e000e6c0-b55c-496d-b210-0d53de88c3e3.1 downloaded under context System				
Saved Content ID Manning Content #000/6/C0-b55/c-496d-b210-0d53de88c-3e31_C:\Windows\crmcache\5				
Download succeeded for download request (81B3BD15-2E9E-4152-BBE5-A5C878C594DA)				
Date (Times, 8/20/2012 9:10:24 MM Company ContentAccore				
Date/Time: 6/20/2013 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.



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. 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 (0×1)	Source:		
Attempting to ShowBalloonT	display the notification ballo ip)	on with title 'Downl	oading and installing software' and tooltip 'Click to view progress.'.	(Microsoft.SoftwareCer

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 - Scop			Copy 4.0 - Windows Installer (*.msi file)" ApplicationDeliveryType - ScopeId_3FB78
7A71E0CDE169/DeploymentType_Se8Sd6bf-78b9-4c46-b920-fcc76f7a64eb, Revision - 1, ContentPath - C:\Wndows\ccmcache\5, E)-fcc76f7a64eb, Revision - 1, ContentPath - C:\W ndows\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.



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