Chris Amaris
Rand Morimoto
Pete Handley
David E. Ross

Technical Edit by Guy Yardeni

Microsoft® System Center 2012

UNLEASHED

SAMS

FREE SAMPLE CHAPTER

SHARE WITH OTHERS

Chris Amaris, MCITP, CISSP
Rand Morimoto, Ph.D., MCITP
Pete Handley, MCITP
David E. Ross, MCITP
Technical Edit by Guy Yardeni

Microsoft® System Center 2012

UNLEASHED

SAMS | 800 East 96th Street, Indianapolis, Indiana 46240 USA

Microsoft® System Center 2012 Unleashed

ISBN-13: 978-0672-33612-6
ISBN-10: 0-672-33612-X

Library of Congress Cataloging-in-Publication Data is on file.

Printed in the United States of America

First Printing June 2012

Trademarks

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Sams Publishing cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

Warning and Disclaimer

Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied. The information provided is on an “as is” basis. The authors and the publisher shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or from the use of the programs accompanying it.

Bulk Sales

Sams Publishing offers excellent discounts on this book when ordered in quantity for bulk purchases or special sales. For more information, please contact

U.S. Corporate and Government Sales
1-800-382-3419
corpsales@pearsontechgroup.com

For sales outside of the U.S., please contact

International Sales
international@pearson.com

Editor-in-Chief
Greg Wiegand

Executive Editor
Neil Rowe

Development Editor
Mark Renfrow

Managing Editor
Kristy Hart

Project Editor
Andy Beaster

Copy Editor
Karen Annett

Indexer
Erika Millen

Proofreader
Jess DeGabriele

Technical Editor
Guy Yardeni

Publishing Coordinator
Cindy Teeters

Book Designer
Gary Adair

Compositor
Gloria Schurick

Contributing Writers
Alec Minty
John Rodriguez
Tyson Kopczynski

Contributing Editors
Ed Crowley
Aman Ayaz

Contents at a Glance

Table of Contents

About the Authors

Chris Amaris, MCITP, MCTS, CISSP/ISSAP, CHS III, is the chief technology officer and cofounder of Convergent Computing. He has more than 20 years experience consulting for Fortune 500 companies, leading companies in the technology selection, design, planning, and implementation of complex information technology projects. Chris has worked with Microsoft System Center products, such as Operations Manager and Configuration Manager, since their original releases in 2000 and 1994. He specializes in messaging, security, performance tuning, systems management, and migration. Receiving his first Microsoft technologies certification in 1993, Chris is a current Microsoft Certified IT Professional (MCITP) with multiple Microsoft Certified Technology Specialist designations (MCTS) in System Center technologies, a Certified Information Systems Security Professional (CISSP) with an Information System Security Architecture Professional (ISSAP) concentration, Certified Homeland Security (CHS III), a Novell CNE, a Banyan CBE, and a Certified Project Manager. Chris is also an author, writer, and technical editor for a number of IT books, including *Network Security for Government and Corporate Executives*, *Exchange 2010 Unleashed*, and *Microsoft Windows Server 2008 R2 Unleashed*.

Rand Morimoto, Ph.D., MVP, MCITP, CISSP, has been in the computer industry for over 30 years and has authored, coauthored, or been a contributing writer for dozens of books on Windows, Security, Exchange, BizTalk, and Remote and Mobile Computing. Rand is the president of Convergent Computing, an IT-consulting firm in the San Francisco Bay area that has been one of the key early adopter program partners with Microsoft, implementing the latest Microsoft technologies, including Microsoft Windows Server 2008 R2, System Center 2012, Windows 7, Exchange Server 2010, Windows Server 2012, and SharePoint 2010 in production environments over 18 months before the initial product releases.

Pete Handley, MCITP, CISSP, has more than 15 years of experience in IT, including extensive knowledge of Active Directory, Microsoft Exchange, Windows Server 2008, and the System Center suite of products. He has been a contributing author for the Sams books *Microsoft Exchange 2003 Unleashed* and *Windows PowerShell Unleashed*. Pete specializes in Visual Basic and PowerShell scripting and is a subject matter expert on the integration and migration of Novell technologies to Microsoft technologies. Pete holds the Microsoft Certified Systems Engineer 2003 (MCSE) certification, the Microsoft Certified Information Technology Professional (MCITP) certification, the Novell Certified Directory Engineer (CDE) certification, and the Certified Information Systems Security Professional (CISSP) certification.

David E. Ross, MCITP, VCP, CCEA, CCSP, has over 13 years of experience in IT consulting, the majority of which have been spent playing the lead architect role on network design and implementation projects throughout the San Francisco Bay area. David is currently acting as a principal engineer for Convergent Computing, and is frequently involved in creating hybrid solutions involving multiple vendor technologies for organizations of all sizes. Specialties for David include Active Directory, Exchange, System Center, Lync, Citrix XenApp and XenDesktop design, virtualization solutions using VMware vSphere and Microsoft Hyper-V, and Cisco routing, switching, and security technologies.

Dedication

I dedicate this book to my wife Sophia, light of my life. And to my children, Michelle, Megan, Zoe, Zachary, and Ian, who give meaning to my life and work.

—Chris Amaris, MCITP, MCTS, CISSP/ISSAP, CHS III

I dedicate this book to Ana, looking forward to continuing a wonderful life together!

—Rand Morimoto, Ph.D., MVP, MCITP, CISSP

I dedicate this book to my parents Hal and Denise, who encouraged my early love of reading and gave me my first computer. You have each made it possible for me to learn and grow in so many ways, but the greatest lessons that I have learned have been by your examples. And to my wonderful and irrepressible wife Melissa, you are the joy at the center of my life and never far from my thoughts.

—Pete Handley, MCITP, CISSP

I dedicate this book to my wife Lisette, who serves as an inspiration to everyone around her, and encourages everyone to reach their full potential. Thanks for your loving support during this project, and for the sacrifices you made to help me reach my potential. Also to my fun-loving boys Caden and Cole, who keep me on my toes and provide the best distraction from long hours of book writing. Thanks for being a great family worth working hard for!

—David E. Ross, MCITP

I dedicate this book to everyone at Convergent Computing. Credit for the book should be spread throughout the entire organization for an effort that would be largely impossible without the contribution of the whole team.

—Guy Yardeni, MCSE, MCITP, CISSP

Acknowledgments

Chris Amaris, MCSE, MVP, CISSP
I want to thank Rand for providing the leadership and direction as we have transitioned from a server centric focus, to enterprise data center centric focus, to now a cloud centric focus. Your vision on the IT industry needs, trends, and technologies has allowed you to keep a steady hand on the tiller, ensuring that we are always ahead of the latest technology wave. The breadth and depth of knowledge of the Convergent Computing organization in the System Center technologies that allow us to support our clients and provide the basis for this book are all thanks to your vision and leadership.

And many, many thanks to my family! Sophia, thank you for keeping everything together while I disappeared at the drop of a hat into my office to finish another lab or chapter. Michelle, Megan, Zoe, Zachary, and Ian, thank you for keeping focused on your academics and seeing that through hard work anything is possible.

Rand Morimoto, Ph.D., MVP, MCITP, CISSP
Congratulations Chris for getting this System Center 2012 title out the door! And a big thanks to Pete and Dave who jumped in to the middle of this book, GREAT job in rounding out the authoring team on this one! And a huge thanks to Guy for doing the edits and making sure this book was prime time!

I want to thank the team at Sams Publishing for continuing to support our writing efforts and turning this book around and out to print in record time! Thank you Neil, Mark, Andy, and all the folks behind the scenes in making this happen! And my thanks to Karen Annett, who continues to be my favorite copy editor!!!

I also wanted to thank the consultants at Convergent Computing and our early adopter clients who fiddle with these new technologies really early on and then take the leap of faith in putting the products into production to experience (and at times feel the pain) as we work through best practices. The early adopter experiences give us the knowledge and experience we need to share with all who use this book as their guide in their production environments based on the lessons learned.

To Kelly, Noble, and Chip, yeah, one down, three more books to go before the year is up. You know where to find me in the wee hours of the night, downstairs at the kitchen table writing. Remember to work hard at everything you do, as you've found so far, you can accomplish a lot when you put your mind to things!

Pete Handley, MCITP, CISSP
I want to thank Rand for the opportunity to contribute to this book, and to Chris for your thorough and patient approach to learning. Thanks to Guy for your meticulous tech editing, and to Karen and the SAMS team for always sweating the details!

David E. Ross, MCITP

Thanks to my family for the sacrifices they made without complaint while I was getting oriented with the whole book-authoring process. Big thanks also to Rand not only for providing me the opportunity to work on this project, but for providing excellent guidance on the whole process. You made it very easy to come up to speed and learn the ropes very quickly; I appreciate it!

We Want to Hear from You!

As the reader of this book, *you* are our most important critic and commentator. We value your opinion and want to know what we're doing right, what we could do better, what areas you'd like to see us publish in, and any other words of wisdom you're willing to pass our way.

You can email or write me directly to let me know what you did or didn't like about this book—as well as what we can do to make our books stronger.

Please note that I cannot help you with technical problems related to the topic of this book, and that due to the high volume of mail I receive, I might not be able to reply to every message.

When you write, please be sure to include this book's title and author as well as your name and phone or email address. I will carefully review your comments and share them with the author and editors who worked on the book.

E-mail: feedback@samspublishing.com

Mail: Neil Rowe
Executive Editor
Sams Publishing
800 East 96th Street
Indianapolis, IN 46240 USA

Reader Services

Visit our website and register this book at informit.com/register for convenient access to any updates, downloads, or errata that might be available for this book.

This page intentionally left blank

Introduction

The release of System Center 2012 is a major shift in the System Center family of products of going from a product line that was previously sold and viewed as a series of individual products, to System Center 2012 being sold as a single product with tight integration between the various components. In addition, this shift is not just from the perspective of a sales or marketing focus of a single product, but also from the engineering integration of System Center 2012 where the components work better and tighter together.

Additionally, with System Center 2012, Microsoft has expanded beyond the traditional "only Microsoft" solution support to one that broadly embraces other platforms, such as the support for VMware, Citrix, storage area network products from various vendors, non-Microsoft mobile devices and operating systems, and the like. From a data center perspective where the data center has more than just Windows servers and Microsoft applications, this multivendor support is critical in Microsoft's ability to be a true data center management solution provider.

And as the industry evolves to support traditional on-premise servers and applications and now cloud-based products and technologies, System Center's ability to support applications and services in the cloud is a critical inclusion in the System Center 2012 product.

This book covers real-world experiences with System Center 2012, not like a "product guide" simply with step-by-step installation and feature configurations, but with real-world notes, tips, tricks, best practices, and lessons learned in the design, planning, implementation, migration, administration, management, and support of the System Center technologies based on years of early adopter and enterprise production deployments.

The 17 chapters of this book are written to highlight the most important aspects of the technologies that make up the System Center family of components. To combine the components into groups of technologies, this book covers the following:

- **Introduction**—The first chapter of this book provides an introduction to the System Center 2012 family of components, what they are, what they do, and what business and IT challenges they solve. The introduction paints the picture of what the rest of the book covers and how you as the reader can jump to those sections of the book most important to you in your day-to-day IT management tasks.
- **System Center 2012 Configuration Manager**—The first component covered in this book is the System Center 2012 Configuration Manager (SCCM) component, which is a toolset that has come a long way in the past decade. The earlier releases of Configuration Manager went by the name SMS, or Systems Management Server,

which was known to take full-time personnel to manage the management system. However, now easily four or five generations later, SCCM 2012 has really helped organizations with the patching, updating, imaging, reporting, and compliance management of their systems, both Microsoft and non-Microsoft endpoint clients and servers. The four chapters in this book that cover SCCM address the planning and design process of implementing SCCM in an enterprise, the implementation of the component, and, more important, how administrators use SCCM to image, update, manage, and support the servers and client systems in their environments.

- **System Center 2012 Operations Manager**—The second component covered in this book is the System Center 2012 Operations Manager (SCOM) component, which provides monitoring and alerting on servers and client systems as well as internetworking devices (routers/switches/firewalls) and cloud-based services. Rather than waiting for users to alert the help desk that a server is down, SCOM proactively monitors systems and networks and provides alerts before failures impact operations, plus it logs error events and system issues to help organizations address system problems—usually before they occur. The chapters dedicated to SCOM cover the planning and design of SCOM, the rollout and implementation of servers and monitoring agents, and the best practices on how to understand errors and alerts that allow IT administrators to be more proactive in managing their servers and the systems in their environments.
- **System Center 2012 Data Protection Manager**—System Center 2012 Data Protection Manager (DPM) is a relatively new addition to the Microsoft management family of components. As traditional tape backups have been replaced by digital snapshots and digital data backups of information, DPM provides organizations the ability to have backup copies of their data. DPM incrementally backs up information from servers so that instead of backing up information once a night, DPM makes backups all day long for faster backup times and more granular recovery windows. This book covers the planning, design, implementation, and general recovery process of file systems, Microsoft Exchange, SharePoint Server, SQL, Hyper-V hosts and guests, and Windows client systems using DPM 2012.
- **System Center 2012 Virtual Machine Manager**—In the past three to four years, virtualization has gone from something that was only done in test labs to data centers that are now fully virtualized—enabling organizations to have more than one server session running on a physical server system, and sometimes upward of 10 or 20 server sessions running on a single system. With the huge growth in virtualization in the data center, Microsoft released four major updates to the System Center Virtual Machine Manager (VMM) component in three years to address the needs of the enterprise. The two chapters dedicated to VMM go beyond the installation and setup of VMM 2012, and get into core components of the component that help organizations manage virtual guest sessions running on Microsoft Hyper-V, VMware, and Citrix XenServer, and also how to convert physical servers to virtual servers (P2V), delegate the ability to administer and manage guest sessions, manage the “fabric” of a network (storage and internetworking), and the ability to share virtual host resources with users and administrators in the enterprise.

- **System Center 2012 Service Manager**—After an initial five years in development and over two years in production deployments, Microsoft now has a help desk/incident management/asset life-cycle management/change management component called System Center 2012 Service Manager (SCSM) that organizations are finding extremely valuable in their enterprises. Being involved with the development of SCSM from its inception, the authors of this book have shared years of experience, tips, best practices, and lessons learned in the deployment, information tracking, reporting, and support of the SCSM component. SCSM brings together the information gathering, reporting, alerting, and knowledge-base information in the other System Center components into a single component that will help organizations better manage their IT infrastructures.
- **System Center 2012 Orchestrator**—System Center Orchestrator is a newcomer to the System Center family and has been instrumental in real-world implementations of System Center in helping to make process and runbook automated tasks that simplify IT processes. For tasks that IT professionals have manually done day in and day out in the past that takes hours or days to complete, Orchestrator scripts run through the processes methodically in minutes and seconds. The consistency with Orchestrator scripts helps organizations maintain standards and consistency in processes and achieve end goals more efficiently and effectively than in the past.

It is our hope that the real-world experience we have had in working with the entire System Center family of components and our commitment to relaying to you information that will be valuable in your planning, implementation, operation, and administration of System Center in your enterprise will help you more quickly gain and receive benefits from these management tools from Microsoft!

This page intentionally left blank

CHAPTER 3

Configuration Manager 2012 Implementation and Administration

IN THIS CHAPTER

System Center Configuration Manager (ConfigMgr) 2012 helps reduce the cost of managing the Windows infrastructure by providing scalable, secure, end-to-end administration and reporting functionality for the enterprise. It is important to fully understand the architectural design before Configuration Manager 2012 infrastructure servers and roles are deployed.

This chapter walks through the steps necessary to deploy, configure, and administer key Configuration Manager 2012 functionality. This functionality includes deploying and administering the roles and features needed to enable operating system deployment, systems configuration management, patch management, software provisioning, asset management, and reporting.

Sample Organization

To illustrate the implementation and administration of Configuration Manager 2012, a multilocation sample organization named Company XYZ will be used. This will provide a backdrop of reality against which the Configuration Manager 2012 design can be developed.

Existing Environment

Company XYZ is headquartered in San Francisco with offices in Paris, London, Tokyo, and New York City. The company has over 3,000 employees distributed primarily between San Francisco and Paris. London and Tokyo are medium-sized branch offices. Finally, the New York office is a very small office with only a handful of employees.

There is a network connection between the San Francisco and Paris offices. London and Tokyo connect to the Paris office. New York is connected to the separate San Francisco office. Figure 3.1 shows the corporate wide area network (WAN) topology.

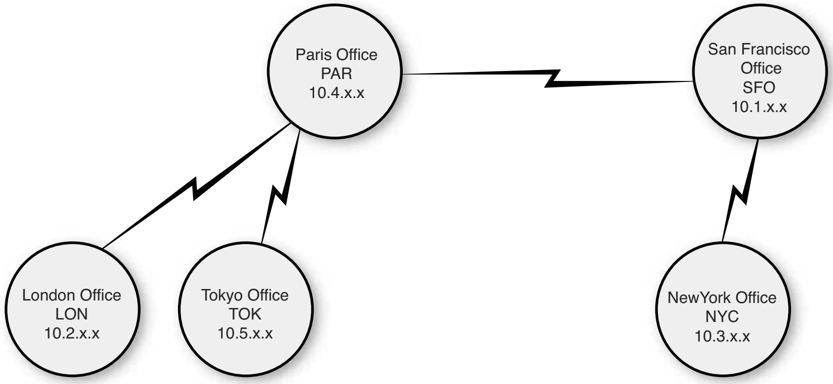


FIGURE 3.1 Company XYZ WAN topology.

The company has a single Active Directory forest and domain. The domain name is companyxyz.com and has a domain controller DC1. Each office has its own Active Directory site in the Active Directory site topology. Table 3.1 summaries the location information.

TABLE 3.1 Company XYZ Location Information

Location	AD Site	Network	Users
San Francisco	SFO	10.1.x.x	2,000
Paris	PAR	10.4.x.x	1,000
London	LON	10.2.x.x	100
Tokyo	TOK	10.5.x.x	100
New York	NYC	10.3.x.x	5

The San Francisco office has the central IT organization that covers the entire Company XYZ organization, but the Paris office also has a smaller IT organization that covers the Paris, London, and Tokyo locations. The Paris office has significant autonomy and needs administrative control over its infrastructure due to regulatory concerns.

This information will be used to inform the Configuration Manager 2012 design.

Developing a Configuration Manager 2012 Design

Based on the Company XYZ existing environment, the recommendation would be to have a Primary Site Server in San Francisco and a Primary Site Server in Paris based on the local IT presence and the requirement for local administrative control. The recommendation would be to place Secondary Site Servers in London and Tokyo based on the size of the offices. Given the small size of the New York office with only five users, no servers will be placed there.

Table 3.2 summarizes the locations, server roles, and server names needed for the infrastructure.

TABLE 3.2 Company XYZ Configuration Manager 2012 Design

Location	SCCM Site	Site Code	Server Name
San Francisco	Central Administration Site	XYZ	CM1
	Primary Site	SFO	CM2
Paris	Primary Site	PAR	CM3
London	Secondary Site	LON	CM4
Tokyo	Secondary Site	TOK	CM5
New York		NYC	

Figure 3.2 shows a diagram of the recommended Configuration Manager 2012 infrastructure.

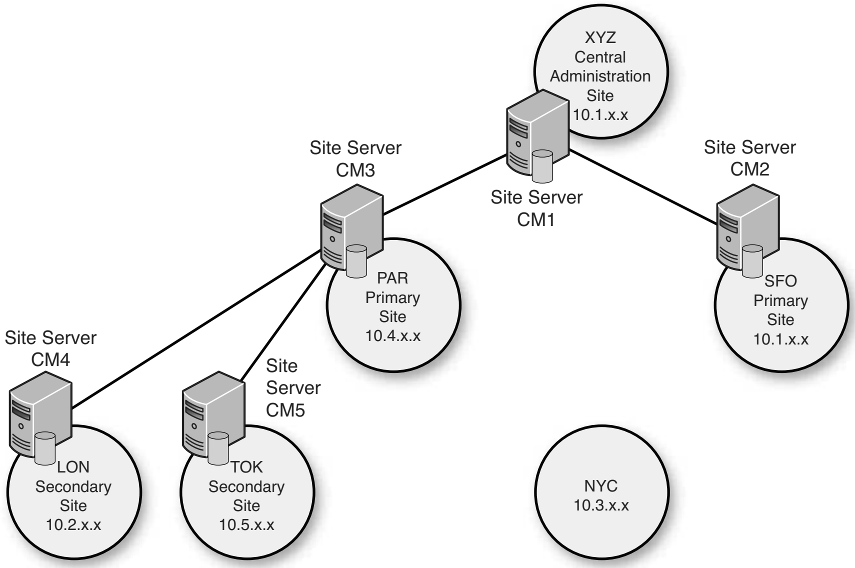


FIGURE 3.2 The Company XYZ ConfigMgr 2012 design.

The balance of this chapter implements and configures the Configuration Manager 2012 design for Company XYZ.

Configuring Installation Prerequisites

Before implementing SCCM 2012, several prerequisite steps need to be taken to prepare Active Directory and the Site Servers. These steps ensure that the SCCM implementation goes smoothly.

The required SCCM prerequisites are as follows:

- Extending the Active Directory schema
- Configuring the System Management container in Active Directory
- Adding Windows roles and features on Site Servers

These prerequisites prepare the environment for Configuration Manager 2012.

These installation prerequisites are in addition to the hardware and software requirements covered in Chapter 2, "Configuration Manager 2012 Design and Planning." The software requirements include the following:

- Windows Server 2008 64-bit SP2 or Windows Server 2008 R2 operating system
- Windows Active Directory domain
- .NET Framework 3.51 SP1
- .NET Framework 4.0
- SQL Server 2008 SP2 with Cumulative Update 7 or SQL Server 2008 R2 SP1 with Cumulative Update 4 (can be on a separate server)
- Opened TCP port 1433 and 4022 for SQL replication

The hardware and software requirements for all prospective Site Servers must be met before the installation prerequisites can be configured.

NOTE

If you install IIS after installing .NET Framework 4.0, then open a command prompt, browse to the location `%windir%\Microsoft.NET\Framework64\v4.0.30319`, and execute `aspnet_regiis.exe —i —enable`.

Extending the Active Directory Schema

The Active Directory schema should be extended to support dynamic client assignment during Configuration Manager agent deployment and to assist clients with the location of Configuration Manager server infrastructure. When the Active Directory schema is extended, clients can use the values provided through Active Directory to locate regional Site Servers and Distribution Points for package and content delivery.

NOTE

The Active Directory schema extensions for SCCM 2012 are identical to the Active Directory schema extensions for SCCM 2007. If the schema was already extended for SCCM 2007, the schema does not need to be extended again for SCCM 2012.

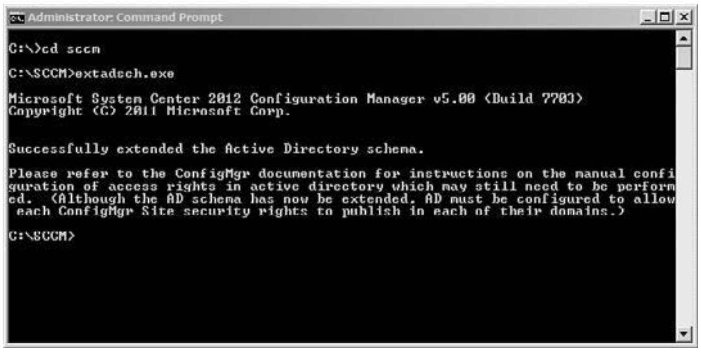
CAUTION

Take the appropriate safety measures when extending the Active Directory schema. Changes to the schema cannot be easily reversed; plan to test the schema extensions in a development environment before implementing them in your production environment.

To extend the Active Directory schema, execute the following steps:

1. Log on to a domain controller with an administrative account that is a member of the Schema Admins group.
2. Copy the `EXTADSCH.exe` from `\SMSSETUP\BIN\x64\` on the Configuration Manager installation media to a local folder on the Active Directory domain controller with the schema master FSMO role.
3. Open a command window as an administrator and execute the `EXTADSCH.exe` command with a Schema Admin account.

The command should report, "Successfully extended the Active Directory schema" when complete (as shown in Figure 3.3).



```
C:\>cd sccm

C:\SCCM>extadsch.exe

Microsoft System Center 2012 Configuration Manager v5.00 (Build 7703)
Copyright (C) 2011 Microsoft Corp.

Successfully extended the Active Directory schema.

Please refer to the ConfigMgr documentation for instructions on the manual confi
guration of access rights in active directory which may still need to be perform
ed.  (Although the AD schema has now be extended, AD must be configured to allow
 each ConfigMgr Site security rights to publish in each of their domains.)

C:\SCCM>
```

FIGURE 3.3 Successful Active Directory schema extension.

Review the `ExtADSch.log` file for any errors. This log file is located in the root of drive C on the server used to execute the schema extensions. The log file should show 14 attributes and four classes have been defined.

TIP

Sometimes, the attribute extensions will succeed, but the class extensions will fail. This is typically due to replication latency, especially in large distributed environments. The `EXTADSCH.exe` command can be run multiple times with no ill effect. Wait for replication to complete and then run the schema extension command again.

After replication is completed, the class extensions should be successful.

Configuring the System Management Container

When the Active Directory schema has been extended, Configuration Manager Site Servers store information about the hierarchy in special Active Directory objects. These objects are kept in a specific folder in the System container of the domain partition. The location for these objects doesn't exist by default, and must be manually created and configured.

In a distributed Configuration Manager hierarchy, it is considered best practice to place the Configuration Manager Site Servers in a custom security group, and delegate this security group's permissions to the System Management container in Active Directory. The following tasks assume the Configuration Manager Site Servers (CM1, CM2, CM3, CM4, and CM5) are members of the "SCCM Site Servers" universal security group. If this group doesn't exist, create it before continuing.

CAUTION

When a computer object is added to a group, it can take a long time for the setting to take effect. This is because the Kerberos ticket takes seven days to renew. The renewal time is governed by the *Maximum Lifetime for User Ticket Renewal* setting located in the Default Domain Policy GPO. It is not recommended to change this setting. Instead, restart the computer to refresh the Kerberos ticket.

The System Management container holds the Configuration Manager objects in Active Directory. This container can be created with the ADSI Edit console on the DC1 domain controller.

To create the System Management container with ADSI Edit, complete the following steps:

1. Run ADSI Edit from DC1.
2. Right-click the ADSI Edit node and select Connect To.
3. Type **`Domain`** in the Name field.
4. Select Default Naming Context from the list of well-known naming contexts.
5. Click OK.
6. Expand Default Naming Context.

7. Expand DC=companyxyz,DC=com.
8. Select the CN=System container.
9. Right-click CN=System, click New, and then click Object.
10. Select Container from the list and click Next.
11. Enter **`System Management`** for the CN attribute value, and then click Next.
12. Click Finish to complete the change.

The permissions for the System Management container need to be configured before the first Site Server is implemented.

To set the System Management container permission with ADSI Edit, complete the following steps:

1. Right-click the System Management container and select Properties.
2. Select the Security tab.
3. Click Advanced.
4. Click Add.
5. Type **`SCCM Site Servers`** and click OK.
6. Continue with the default selection of This Object and All Descendant Objects from Apply To.
7. Choose Allow in front of Full Control in the Permissions field and then click OK.
8. Click OK two times to commit all the changes and then close ADSI Edit.

As Configuration Manager Site Servers are added to the hierarchy, be sure to add them to the custom Site Servers security group (SCCM Servers). This ensures they can create the required Active Directory objects.

Adding Windows Roles and Features on Site Servers

The majority of client communications is over HTTP or HTTPS, which is serviced by the Windows IIS web server. IIS is a key component of many Configuration Manager Site Systems roles. This includes the Site Server itself in the following optional roles:

- Application Catalog Web Service Point
- Application Catalog Website Point
- Distribution Point
- Enrollment Point
- Enrollment Proxy Point

- Fallback Status Point
- Management Point
- Software Update Point

NOTE

Some Configuration Manager 2012 Site System roles will require additional installation of Windows roles or features, such as for the software update point, which requires the Windows Server Update Services (WSUS) role, or Distribution Point, which requires IIS request filtering to be configured. These additional configurations will be done as part of configuring those Site System roles.

It is important to make sure that IIS is installed correctly on each of the Site Systems; otherwise, SCCM will not operate correctly.

To implement IIS on the Site Server and Component Servers on a Windows Server 2008 R2–based system, complete the following steps:

1. Open Server Manager on the Site/Component Server.
2. Select the Features node.
3. Click the Add Features action.
4. Enable Background Intelligent Transfer Service (BITS).
5. When prompted, click Add Required Role Services.

NOTE

Clicking the Add Required Role Services button automatically enables IIS and common related features required to host the Configuration Manager service. This includes Web Server components, Management Tools, and Remote Server Administration Tools.

6. Enable the Remote Differential Compression feature and click Next.
7. On the Web Server Overview page, click Next.
8. Enable the ASP.NET role service, and click Add Required Role Services.
9. Enable the ASP role service.
10. Enable the Windows Authentication role service.
11. Enable the IIS 6 WMI Compatibility role service and the IIS 6 Metabase Compatibility if they are not already, and then click Next.

12. Review the components selected and click Install.
13. Close the wizard when the installation completes.

During this process, a number of roles, role services, and features get enabled automatically. If the preparation is being done on a system with some of these enabled or disabled, it can be confusing to know which ones need to be added.

To install using the command line, open Windows PowerShell as an administrator and enter the following commands:

```
Import-Module ServerManager
Add-WindowsFeature Net-Framework,BITS,RDC,Web-ASP-Net,Web-ASP,Web-Windows-Auth,
Web-WMI,Web-Metabase
```

When the preparation process is completed, at minimum the Web Server (IIS) role should be installed with the following list of role services:

- Static Content
- Default Document
- Directory Browsing
- HTTP Errors
- HTTP Redirection
- ASP.NET
- .NET Extensibility
- ISAPI Extensions
- ISAPI Filters
- HTTP Logging
- Logging Tools
- Request Monitor
- Tracing
- Windows Authentication
- Request Filtering
- Static Content Compression
- Dynamic Content Compression
- IIS Management Console
- IIS 6 Metabase Compatibility
- IIS 6 WMI compatibility

In addition, the following Windows features should be installed:

- Background Intelligent Transfer Service (BITS)
- Remote Differential Compression
- Web Server (IIS) Tools
- BITS Server Extensions Tools

In preinstalled systems, ensure that the preceding role services and features are installed.

Implementing the Central Administration Site

The Configuration Manager Central Administration Site is the primary site located at the very top of the Configuration Manager hierarchy. This site is needed if there will be more than one primary site in the hierarchy.

There is a very important implementation difference between the Configuration Manager 2012 Central Administration Site and the central site in previous versions. In previous versions, Primary Site Servers can be installed and later connected to the central site. This is no longer possible in Configuration Manager 2012 and Primary Site Servers must be connected to their Central Administration Site during installation. This means that the Central Administration Site must be installed before any primary sites in the hierarchy.

The net result of these changes is that the Central Administration Site is required and must be the first site implemented if there will be more than one Primary Site Server in the hierarchy, as is the case in the sample Company XYZ architecture.

Verify that all of the hardware and software requirements have been met and that the installation configuration prerequisites have been completed.

Installing the Central Administration Site Server

Before running the Configuration Manager setup, run the prerequisite checker to verify the required components have been successfully installed. The prerequisite checker can be launched from a link on the `splash.hta` page. The `splash.hta` page can be found in the root of the Configuration Manager media.

TIP

Make sure the Configuration Manager Site Server Computer Account is in the local administrators group on all component servers and other Site Servers—this includes the Site Database server. The computer account of the Site Server is used to access and manage the remote server by default. One way to accomplish this is by creating a group named SCCM Site Servers with the computer accounts of all SCCM Site Servers as members and then adding that group to the Local Administrator group on all Site Servers.

Before starting the installation process, create a folder on the C: drive called "SCCMUpdates" and share this folder. This folder will store the latest prerequisite components downloaded during the installation process. This folder can be reused during subsequent Site Server installations.

To install the XYZ Central Administration Site Server on the CM1 server and establish the Company XYZ hierarchy, complete the following steps:

1. Launch `splash.hta` from the Configuration Manager 2012 media.
2. To run the Prerequisite Checker tool, click on the Assess Server Readiness link in the Tools and Standalone Components section.

NOTE

The Prerequisite Checker tool has been much enhanced in SCCM 2012. It runs a wider range of checks and is a standalone executable (`prereqchk.exe`) that can be run unattended via a command line or script. This allows the prerequisite checking process to be automated for large organizations.

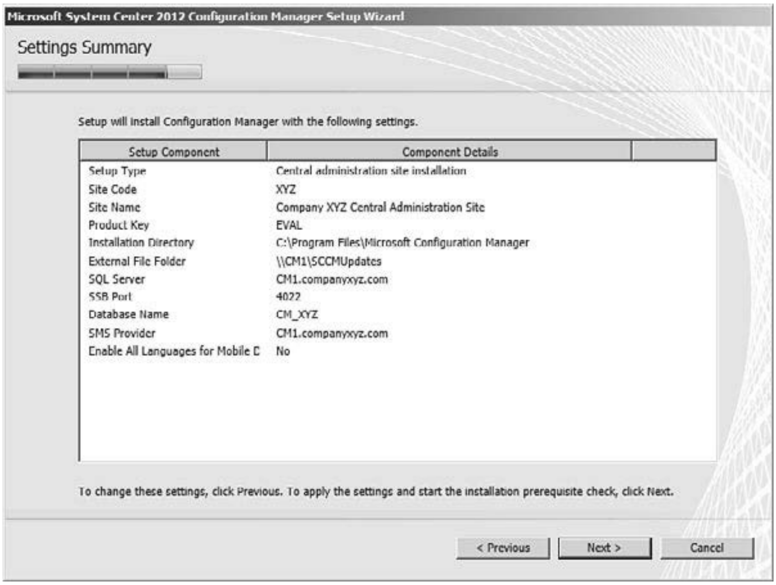
3. Remediate any issues the Prerequisite Checker tool finds and click OK to close the window.
4. After ensuring all the prerequisites have been met, click the Install link in the splash screen.
5. At the Before You Begin screen, click Next.
6. Select the Install Configuration Manager Central Administration Site option and click Next.
7. Enter a 25-character product key and click Next.
8. Accept the license terms and click Next.
9. Accept the license terms for the software that will be downloaded and installed automatically on Site Systems pushed through the hierarchy and click Next.

NOTE

This automates the prerequisite installations of Microsoft SQL Server 2008 R2 and Microsoft Silverlight for secondary site servers in SCCM 2012. This reduces the amount of preparation needed on a secondary site server and eases the administrative burden of deploying additional servers in the hierarchy.

10. Enter the location to download prerequisites and updates, in this example the previously created share **`\\CM1\SCCMUpdates`**, and click Next.
11. In the Server Language Selection, leave the default English and click Next.
12. In the Client Language Selection, leave the default English and click Next.

13. In the Site and Installation Settings, enter a site code and site name. In this example, the site code is **`XYZ`** and the site name is **`Company XYZ Central Administration Site`**.
14. Leave the default installation folder and click Next.
15. In the Database Information, specify the database server name and instance. Click Next.
16. In the SMS Provider Settings, leave the default of CM1 and click Next.
17. In the Customer Experience Improvement Program Configuration, choose the appropriate option and click Next.
18. In the Settings Summary (shown in Figure 3.4), review the settings and click Next.



Microsoft System Center 2012 Configuration Manager Setup Wizard
Settings Summary

Setup will install Configuration Manager with the following settings.

Setup Component	Component Details	
Setup Type	Central administration site installation	
Site Code	XYZ	
Site Name	Company XYZ Central Administration Site	
Product Key	EVAL	
Installation Directory	C:\Program Files\Microsoft Configuration Manager	
External File Folder	\\CM1\SCCMUpdates	
SQL Server	CM1.companyxyz.com	
SSB Port	4022	
Database Name	CM_XYZ	
SMS Provider	CM1.companyxyz.com	
Enable All Languages for Mobile C	No	

To change these settings, click Previous. To apply the settings and start the installation prerequisite check, click Next.

FIGURE 3.4 The central site installation Settings Summary.

19. The Prerequisite Checker executes a last-minute check. Verify that all prerequisites have been met or remediate any errors, and then click Begin Install.
20. The installation completes and should have green status symbols next to each component installation.
21. Click Close to exit the setup wizard.

Installation is now complete for the Central Administration Site and the console can be launched.

Validating the Installation of the Central Administration Site

To validate the installation, check the contents of the System Management container in Active Directory. The System Management container can be seen by launching Active Directory Users and Computers, selecting the View menu, choosing Advanced Features, and expanding the System folders or with ADSI Edit. The Site Server object should exist in this container for the Central Administration Site. In this example, the XYZ Central Administration Site should create an object in the System Management container named `SMS-Site-XYZ` of type `mSSMSSite`. As additional Site Servers in Site System roles are deployed, additional objects are created automatically.

It is important to validate the installation after each role is deployed; this ensures everything is functioning correctly before moving to the next step. It is also important to monitor site status on a continuous basis to ensure the health of the environment. For additional information on automatically monitoring the Configuration Manager hierarchy with Operations Manager, review Chapter 8, “Using Operations Manager 2012 for Monitoring and Alerting.”

In addition, open the Configuration Manager console and review the Site Status component in the System Status container. This console is called Configuration Manager console and is located under the Microsoft System Center 2012\Configuration Manager folder in the Start menu on the Site Server.

To view the Component Status in the ConfigMgr console, do the following:

1. Launch the Configuration Manager console.
2. Choose the Monitoring space.
3. Expand the System Status node.
4. Select the Site Status node and confirm that all statuses show as OK with green icons.
5. Select Component Status and confirm that all statuses show as OK with green icons.

The Site Status page shows a high-level summary of the Site System roles and the status. This is useful for seeing an overview of the Site Systems and ensuring that they are healthy. If a role is marked with a red error or a yellow warning icon, the component has received status messages indicating a problem with the component. Right-click the component, select Show Messages - All from the menu and select a viewing period for the messages.

The Component Status page shows all of the components that make up the Configuration Manager infrastructure for this site. The component status is based on status messages that are received from the component. Because the component has to send the Site Server status, and the Site Server has to process the status message, the condition of components can be delayed. This is especially true when looking at the status of child sites within the Central Site console because status messages are sent to parent sites based on the Site Sender configuration.

If a component is marked with a red error or a yellow warning icon, the component has received status messages indicating a problem with the component. Right-click the component, select Show Messages - All from the menu and select a viewing period for the messages.

TIP

The status summarizer for the different components is not automatically changed from red or yellow to green if the component that experienced the problem is fixed. The component summarizer simply counts the number of warning and error status messages that have been received.

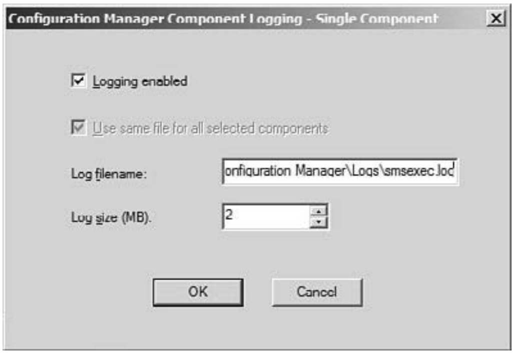
To reset the status of a component, right-click the component and select Reset Counts - All from the menu. The count of status messages is reset and the icon will change back to green in a few minutes.

The delay in status messages is often a source of frustration for administrators starting out with Configuration Manager. For a better, real-time view into site components, check the log files with `cmtrace.exe`, a Configuration Manager 2012 utility. You can identify the log file for a specific component by right-clicking the component and selecting Start, ConfigMgr Service Manager from the menu. Navigate to the component within the Service Manager, right-click the component from the Actions pane, and then select Logging.

NOTE

The `cmtrace.exe` log viewing utility replaces the previous `trace32.exe` utility from the Configuration Manager toolkit. The `cmtrace.exe` is included with the SCCM 2012 server and installs with the default setup.

The site component Logging option is shown in Figure 3.5. The SMS Executive logging option has been chosen and shows the name and location of the log file, which is `c:\Program Files\Microsoft Configuration Manager\Logs\smsexec.log`. The size of the log file, 2 MB, is also shown and can even be adjusted here.



Configuration Manager Component Logging - Single Component

☑ Logging enabled

☑ Use same file for all selected components

Log filename: onfiguration Manager\Logs\smsexec.loc

Log size (MB): 2

FIGURE 3.5 The component log location.

Now that the top-level Central Administration Site has been deployed successfully, the primary sites and other sites can be deployed in the Configuration Manager 2012 hierarchy.

Deploying the Primary Sites

Deploying primary sites follows a similar process as deploying the Central Administration Site Server. In the case of the Company XYZ Configuration Manager 2012 hierarchy, there are two primary sites. These are San Francisco (SFO) with the CM2 server and Paris (PAR) with the CM3 server.

Verify that all the hardware and software requirements have been met and the installation configuration prerequisites have been completed.

Installing a Primary Site Server

Before running the Configuration Manager setup, run the prerequisite checker to verify the required components have been successfully installed. The prerequisite checker can be launched from a link on the `splash.hta` page. The `splash.hta` page can be found in the root of the Configuration Manager media.

TIP

Make sure the Configuration Manager Site Server Computer Account is in the local administrators group on all component servers and other Site Servers; this includes the Site Database server. The computer account of the Site Server is used to access and manage the remote server by default. One way to accomplish this is by creating a group named **`SCCM Site Servers`** with the computer accounts of all SCCM Site Servers, then adding the local administrator groups on all Site Servers.

To install the SFO Primary Site Server on the CM2 server in the Company XYZ hierarchy, complete the following steps:

1. Launch `splash.hta` from the Configuration Manager 2012 media.
2. To run the Prerequisite Checker, click on the Assess Server Readiness link in the Tools and Standalone Components section.
3. Remediate any issues the prerequisite checker tool finds and click OK to close the window.

NOTE

It is normal to get a `WSUS SDK on site server` issue during the prerequisite check on a new Primary Site Server. If this server is intended to host the Site Server Software Update role, then the Windows WSUS role will be installed at that time.

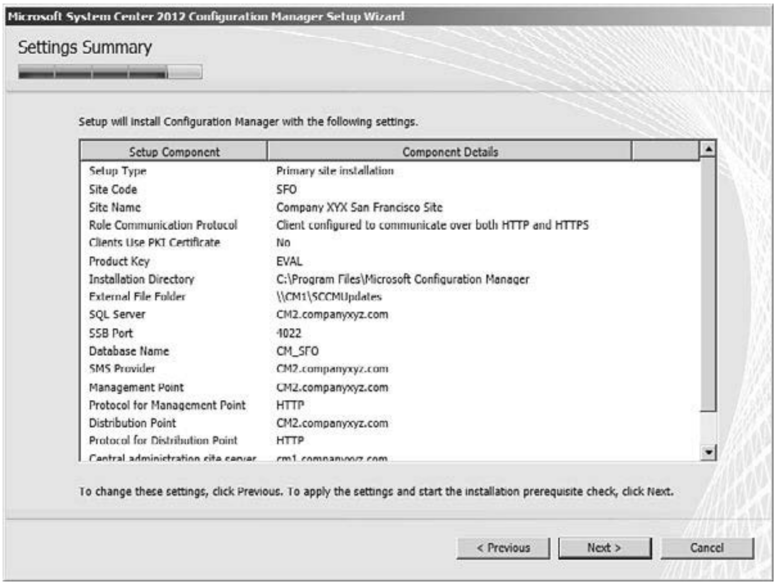
4. After ensuring all the prerequisites have been met, click the Install link in the splash screen.
5. At the Before You Begin screen, click Next.
6. Select the Install Configuration Manager Primary Site option and click Next.
7. Enter a 25-character product key and click Next.
8. Accept the license terms and click Next.
9. Accept the license terms for the software that will be downloaded and installed automatically on Site Systems pushed through the hierarchy and click Next.

NOTE

This automates the prerequisites installations of Microsoft SQL Server 2008 R2 and Microsoft Silverlight for secondary site servers in SCCM 2012. This reduces the amount of preparation needed on a secondary site server and eases the administrative burden of deploying additional servers in the hierarchy.

10. Because the prerequisites were downloaded previously, choose the Use Previously Downloaded Files option and enter the location of the downloaded prerequisites and updates, in this example the previously created share **`\\CM1\SCCMUpdates`**, and click Next.
11. In the Server Language Selection, leave the default English and click Next.
12. In the Client Language Selection, leave the default English and click Next.
13. In the Site and Installation Settings, enter a site code and site name. In this example, the site code is **`SFO`** and the site name is **`Company XYZ San Francisco Site`**.
14. Leave the default installation folder and click Next.
15. Enter the name of the Central Administration Site Server to join the existing hierarchy, in this case **`cm1.companyxyz.com`** and click Next.
16. In the Database Information, specify the database server name and instance. Click Next.
17. In the SMS Provider Settings, leave the default of CM2 and click Next.
18. In the Client Computer Communication Settings, choose the Configure the Communication Method on Each Site System Role option and click Next.
19. In the Site Systems Roles, leave the options to install a Management Point and a Distribution Point checked and click Next.
20. In the Customer Experience Improvement Program Configuration, choose the appropriate option and click Next.

21. In the Settings Summary (shown in Figure 3.6), review the settings and click Next to begin the installation.



Microsoft System Center 2012 Configuration Manager Setup Wizard
Settings Summary

Setup will install Configuration Manager with the following settings.

Setup Component	Component Details
Setup Type	Primary site installation
Site Code	SFO
Site Name	Company XYX San Francisco Site
Role Communication Protocol	Client configured to communicate over both HTTP and HTTPS
Clients Use PKI Certificate	No
Product Key	EVAL
Installation Directory	C:\Program Files\Microsoft Configuration Manager
External File Folder	\\CM1\SCCMUpdates
SQL Server	CM2.companyxyz.com
SSB Port	4022
Database Name	CM_SFO
SMS Provider	CM2.companyxyz.com
Management Point	CM2.companyxyz.com
Protocol for Management Point	HTTP
Distribution Point	CM2.companyxyz.com
Protocol for Distribution Point	HTTP
Central administration site server	cm1.companyxyz.com

To change these settings, click Previous. To apply the settings and start the installation prerequisite check, click Next.

FIGURE 3.6 The primary Site installation Settings Summary.

22. The Prerequisite Checker executes to do a last-minute check. Verify that all prerequisites have been met or remediate any errors, and then click Begin Install.

23. Installation completes and should have green status symbols next to each component installation.

24. Click Close to exit the setup wizard.

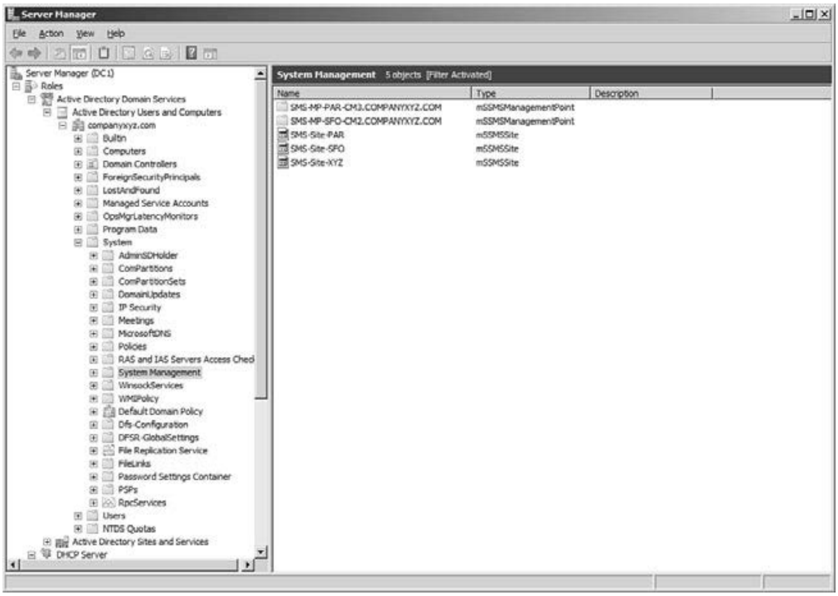
Installation is now complete for the Primary Site and the console can be launched.

Repeat the preceding steps for Company XYZ Paris Site, the PAR Primary Site Server on the CM3 server.

Validating the Installation of the Primary Site

To validate the installation, check the contents of the System Management container in Active Directory. The System Management container can be seen with the Advanced view of Active Directory Users and Computers, or with ADSI Edit. In this example, the Site Server object should exist in this container for the Central Administration Site of type `mSSMSSite`. The SFO primary site should create a record in the System Management container named `SMS-Site-SFO` of type `mSSMSSite`. There should also be an object for the Management Point, named `SMS-MP-SFO-CM2.COMPANYXYZ.COM` of type `mSSMSManagementPoint`. Similarly, the PAR primary site should create an object in the

System Management container named SMS-Site-PAR of type mSSMSSite. There should also be an object for the Management Point, named SMS-MP-PAR-CM3.COMPANYXYZ.COM of type mSSMSManagementPoint. Figure 3.7 shows the Active Directory records for the sites created.



System Management 5 objects [Filter Activated]

Name	Type	Description
SMS-MP-PAR-CM3.COMPANYXYZ.COM	mSSMSManagementPoint	
SMS-MP-SFO-CM2.COMPANYXYZ.COM	mSSMSManagementPoint	
SMS-Site-PAR	mSSMSSite	
SMS-Site-SFO	mSSMSSite	
SMS-Site-XYZ	mSSMSSite	

FIGURE 3.7 The Active Directory SCCM records for Primary Sites.

It is important to validate the installation after each role is deployed; this ensures everything is functioning correctly before moving to the next step. It is also important to monitor site status on a continuous basis to ensure the health of the environment. For additional information on automatically monitoring the Configuration Manager hierarchy with Operations Manager, review Chapter 8.

In addition, open the Configuration Manager console located under the Microsoft System Center 2012\Configuration Manager folder in the Start menu on the Site Server, expand the Monitoring option, and review the Site Status component in the System Status container.

To view the component status in the Configuration Manager console, do the following:

1. Launch the Configuration Manager console.
2. Choose the Monitoring space.
3. Expand the System Status node.
4. Select the Site Status node and confirm that all statuses show as OK with green icons.
5. Select Component Status and confirm that all statuses show as OK with green icons.

The Site Status page shows a high-level summary of the Site System roles and the status. This is useful for seeing an overview of the Site Systems and ensuring that they are healthy. If a role is marked with a red error or a yellow warning icon, the component has received status messages indicating a problem with the component. Right-click the component, select Show Messages - All from the menu and select a viewing period for the messages.

The Component Status page shows all of the components that make up the Configuration Manager infrastructure for this site. The component status is based on status messages that are received from the component. Because the component has to send the Site Server status, and the Site Server has to process the status message, the condition of components can be delayed. This is especially true when looking at the status of child sites within the Central Site console because status messages are sent to parent sites based on the Site Sender configuration.

If a component is marked with a red error or a yellow warning icon, the component has received status messages indicating a problem with the component. Right-click the component, select Show Messages - All from the menu, and select a viewing period for the messages.

TIP

The status summarizer for the different components is not automatically changed from red or yellow to green if the component that experienced the problem is fixed. The component summarizer simply counts the number of warning and error status messages that have been received.

To reset the status of a component, right-click the component and select Reset Counts - All from the menu. The count of status messages is reset and the icon will change back to green in a few minutes.

The delay in status messages is often a source of frustration for administrators starting out with Configuration Manager. For a better, real-time view into site components, check the log files with `cmtrace.exe`, a Configuration Manager 2012 utility. You can identify the log file for a specific component by right-clicking the component and selecting Start, ConfigMgr Service Manager from the menu. Navigate to the component within the Service Manager, right-click the component from the Actions pane, and then select Logging.

NOTE

The `cmtrace.exe` log viewing utility replaces the previous `trace32.exe` utility from the Configuration Manager toolkit. The `cmtrace.exe` is included with the SCCM 2012 server and installs with the default setup.

Now that the primary sites have been deployed successfully, the secondary sites can be deployed in the Configuration Manager 2012 hierarchy.

Deploying the Secondary Sites

Configuration Manager 2012 secondary sites are deployed through the console, via a push from a Primary Site Server. All the prerequisites, such as SQL Server 2008 and .NET Framework 4.0, are pushed out with the role remotely. However, this requires two features to be installed to work correctly. Those features are as follows:

- Remote Differential Compression
- .NET Framework 3.5

To install these prerequisites using the command line, run PowerShell as an administrator and enter the following commands:

```
Import-Module ServerManager
Add-WindowsFeature Net-Framework,RDC
```

In addition, the Primary Site Server Active Directory account (for example, CM3$) is the account performing the remote installation, so it must have local administrator rights to the target secondary site server.

If the Windows Firewall is in use, open ports 1433 and 4022 for SQL Server access.

TIP

The computer account of the Site Server is used to access and manage the remote secondary site server by default. One way to accomplish this is by creating a group named SCCM Site Servers with the computer accounts of all SCCM Site Servers, then adding the local administrator groups on all Site Servers.

To deploy a secondary site from a primary site, execute the following steps:

1. Launch the Configuration Manager console.

NOTE

The Configuration Manager console can be launched from the Central Administration Site Server or the Primary Site Server. Even if the installation is initiated with the Configuration Manager console on the Central Administration Site, the actual installation is performed from the Primary Site Server. This is a great example of the improved centralized administration capabilities of Configuration Manager 2012.

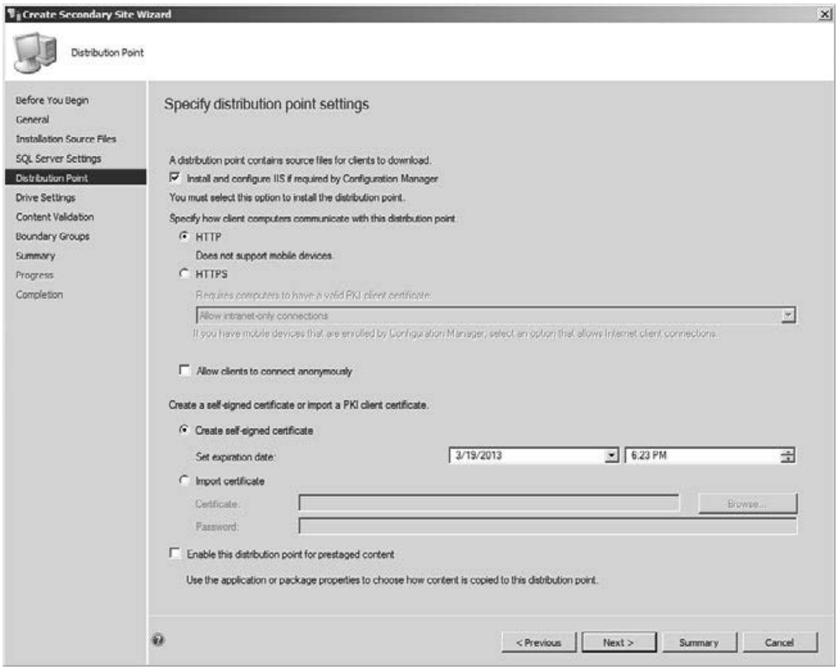
2. Choose the Administration space, expand Site Configuration, and select Sites.
3. Select the primary site from which to deploy the secondary site, in this example the PAR site.
4. Right-click on the Primary Site Server (the CM3 server in this example) and select Create Secondary Site.

5. At the Before You Begin screen, click Next.
6. In the Site and Installation Settings, enter a site code, Site Server, and site name. In this example, the site code is **`LON`**, the server is **`CM4.companyxyz.com`**, and the site name is **`Company XYZ London Site`**.

NOTE

The case of the server name is critical, as the install will fail if the name in the fully qualified domain name (FQDN) does not match the NetBIOS name exactly. If this happens, simply right-click on the failed installation and select Retry Secondary Site and change the case of the server name.

7. Leave the default installation folder and click Next.
8. Leave the default to copy the installation source files from the parent Site Server (in this case cm3.companyxyz.com) and click Next.
9. Leave the default to install SQL Server Express on the secondary site server and click Next.
10. Make sure to check the Install and Configure IIS option, as shown in Figure 3.8, and 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.

○ HTTPS

Requires computers to have a valid PKI client certificate:

Allow intranet-only connections

If you 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: 3/19/2013 6:23 PM

○ Import certificate

Certificate:

Password:

Browse...

☐ Enable this distribution point for prestaged content

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

FIGURE 3.8 Specify Distribution Point Settings.

NOTE

Later in the chapter, when configuring Internet-based client management (IBCM), the protocol setting will be changed from HTTP to HTTPS.

11. Leave the default drive settings and click Next.
12. Leave the default Content Validation settings and click Next.
13. Leave the Boundary Groups settings empty and click Next. These will be configured later.
14. Review the summary and click Next.
15. Click Close to exit the wizard.

The setup begins from the Primary Site Server. A new Site Server appears in the list of sites with a status of Pending. To see the summary status, right-click on the secondary server and select Show Install Status. This shows the summary status message for the secondary site server install.

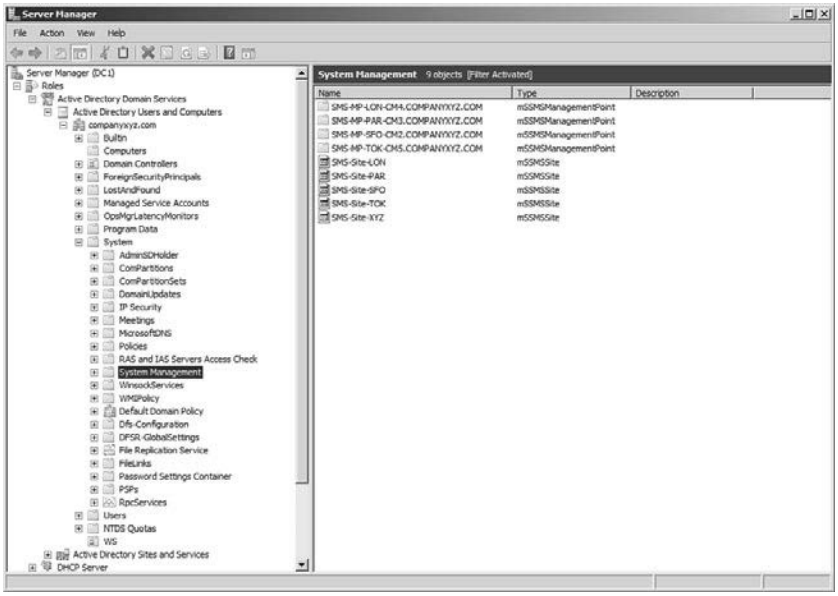
Because installation is being done remotely, it can be difficult to ascertain what could've gone wrong with the installation. However, the Show Install Status messages are very informative and specific. They show the prerequisite checks being done, the download progress, and the installation progress step-by-step. In the event of a failure of the secondary site installation, these messages can be reviewed for the specific reason for the failure. Once remediated, the secondary site server installation can be retried simply by right-clicking the failed secondary site server and selecting Retry Secondary Site.

TIP

The status of the secondary site server install can also be monitored in detail from the source Primary Site Server and the target secondary site server. In the root of the system drive of the Primary Site Server doing the push installation, the log file `ConfigMgrSetup.log` will show the status of the install in detail. Once the installation commences, there will be a corresponding `ConfigMgrSetup.log` in the root of the system drive of the secondary site server, which shows where the installation picks up locally. Review the log on the source Primary Site Server to troubleshoot remote access and file transfer issues. Review the log on the target secondary site server to troubleshoot issues with the installation of prerequisites and the secondary site role.

Validating the Installation of the Secondary Site

To validate the installation, check the contents of the System Management container in Active Directory. The System Management container can be seen with the Advanced view of Active Directory Users and Computers, or with ADSI Edit. The Site Server object should exist in this container for the Secondary Sites. In this example, the LON secondary site should create an object in the System Management container named `SMS-Site-LON` of type mSSMSSite. There should also be an object for the Management Point, named SMS-MP-LON-CM4.COMPANYXYZ.COM of type mSSMSManagementPoint. Similarly, the TOK secondary site should create an object in the System Management container named SMS-Site-TOK of type mSSMSSite. There should also be an object for the Management Point, named SMS-MP-TOK-CM5.COMPANYXYZ.COM of type mSSMSManagementPoint. Figure 3.9 shows the Active Directory objects for the sites created.



System Management 9 objects [Filter Activated]

Name	Type	Description
SMS-MP-LON-CM4.COMPANYXYZ.COM	mSSMSManagementPoint	
SMS-MP-PAR-CM3.COMPANYXYZ.COM	mSSMSManagementPoint	
SMS-MP-SFO-CM2.COMPANYXYZ.COM	mSSMSManagementPoint	
SMS-MP-TOK-CM5.COMPANYXYZ.COM	mSSMSManagementPoint	
SMS-Site-LON	mSSMSSite	
SMS-Site-PAR	mSSMSSite	
SMS-Site-SFO	mSSMSSite	
SMS-Site-TOK	mSSMSSite	
SMS-Site-XYZ	mSSMSSite	

FIGURE 3.9 The Active Directory SCCM records for Secondary Sites.

To view the component status for the secondary site servers in the Configuration Manager console, do the following:

1. Launch the Configuration Manager console.
2. Choose the Monitoring space.
3. Expand the System Status node.
4. Select the Site Status node and confirm that all statuses show as OK with green icons.
5. Select Component Status and confirm that all statuses show as OK with green icons.

If a component is marked with a red error or a yellow warning icon, the component has received status messages indicating a problem with the component. Right-click the component, select Show Messages - All from the menu and select a viewing period for the messages.

TIP

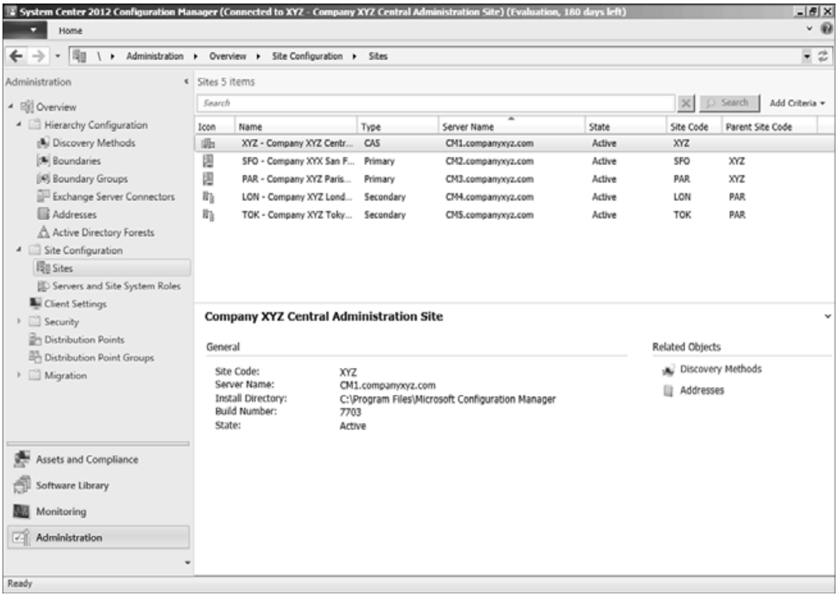
Sometime, the secondary site server installation process will not correctly install the prerequisite Background Intelligent Transfer Service (BITS) Windows feature. If this is the case, there'll be Message ID 4957 error messages in the `SMS_MP_CONTROL_MANAGER` component for the secondary site server. Add the BITS feature manually on the secondary site server if this occurs. The errors should resolve themselves in the next hourly cycle.

Configuring the Hierarchy

With the SCCM 2012 servers deployed, the next task is to configure the hierarchy. Configuration Manager 2012 deploys a more complete set of roles by default than the previous versions, but there still remain roles to be configured. The Configuration Manager 2012 console is divided into four spaces: Assets and Compliance, Software Library, Monitoring, and Administration. The hierarchy configuration takes place within the Administration space.

The Site Settings container within the Site Management node can be used to configure the different components and functionality provided by Configuration Manager. Prior to managing clients, the appropriate functionality should be implemented and configured to ensure clients are managed properly following the agent deployment.

The Configuration Manager console with the Administration space expanded is shown in Figure 3.10. This view also has the sites selected and shows the five servers that have been deployed (CM1, CM2, CM3, CM4, and CM5) in the Company XYZ infrastructure.



Icon	Name	Type	Server Name	State	Site Code	Parent Site Code
	XYZ - Company XYZ Centr...	CAS	CM1.companyxyz.com	Active	XYZ	
	SFO - Company XYX San F...	Primary	CM2.companyxyz.com	Active	SFO	XYZ
	PAR - Company XYZ Paris...	Primary	CM3.companyxyz.com	Active	PAR	XYZ
	LON - Company XYZ Lond...	Secondary	CM4.companyxyz.com	Active	LON	PAR
	TOK - Company XYZ Toky...	Secondary	CM5.companyxyz.com	Active	TOK	PAR

Company XYZ Central Administration Site

General

Site Code: XYZ
Server Name: CM1.companyxyz.com
Install Directory: C:\Program Files\Microsoft Configuration Manager
Build Number: 7703
State: Active

Related Objects

Discovery Methods
Addresses

FIGURE 3.10 The Configuration Manager console Administration space.

Establishing Boundaries and Boundary Groups

Establishing site boundaries and boundary groups is one of the most important aspects of Configuration Manager. Boundaries let managed systems receive content and communicate status to the closest server in the Configuration Manager hierarchy.

The boundaries, in effect, map physical locations, based on IP address, to systems such as workstations. Boundary groups allow administrators to logically group boundaries together and then assign resources such as Distribution Points for them to use.

Boundaries can be created based on IP subnet, IPv6 prefix, IP address range, and Active Directory sites. Typically in an Active Directory environment, the Configuration Manager is based on Active Directory site boundaries. Because the Active Directory site infrastructure should already map directly to the network topology, many of the same principles that apply to an Active Directory site topology also apply to the Configuration Manager topology. For example, instead of taking all the subnets in a specific network location and adding them as a site boundary, it is much easier to add the already configured Active Directory site boundary.

That said, there are still many different scenarios and environments where using an Active Directory site boundary simply isn't possible or practical for technical or even political justification. Configuration Manager allows a mixture of all the different boundaries. It is possible to configure different combinations of site boundaries in the console to address these scenarios.

CAUTION

Never configure overlapping boundaries. This can cause managed systems to use the wrong Site Server or Distribution Management Point. This often happens when using a combination of IP and Active Directory boundaries.

New to Configuration Manager 2012 is the ability to have the Active Directory sites be discovered automatically in the forest. This saves a tremendous amount of time. The Active Directory forest discovery operates very similarly to the Active Directory system discovery or group discovery.

To configure Active Directory forest discovery, do the following:

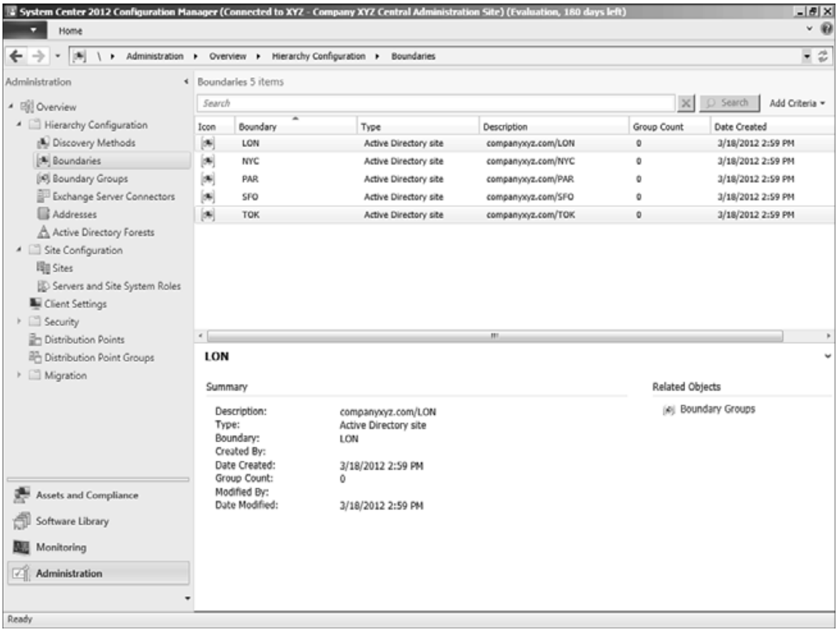
NOTE

Launching the console on the Central Administration Site provides complete administrative access to the entire Configuration Manager 2012 hierarchy.

1. Launch the Configuration Manager console on the Central Administration Server.
2. Choose the Administration space.
3. Expand the Hierarchy Configuration and select Discovery Methods.

4. Right-click on Active Directory Forest Discovery and select Properties.
5. Check Enable Active Directory Forest Discovery and the check box to automatically create site boundaries.
6. Change the Schedule option to run every day.
7. Click OK to save changes and Yes to run the full discoveries as possible.

Once the Active Directory forest discovery is completed, the Active Directory site boundaries will be created. Figure 3.11 shows the Active Directory site boundaries created for the Company XYZ organization.



Boundaries 5 items

Icon	Boundary	Type	Description	Group Count	Date Created
	LON	Active Directory site	companyxyz.com/LON	0	3/18/2012 2:59 PM
	NYC	Active Directory site	companyxyz.com/NYC	0	3/18/2012 2:59 PM
	PAR	Active Directory site	companyxyz.com/PAR	0	3/18/2012 2:59 PM
	SFO	Active Directory site	companyxyz.com/SFO	0	3/18/2012 2:59 PM
	TOK	Active Directory site	companyxyz.com/TOK	0	3/18/2012 2:59 PM

LON

Summary

Description:	companyxyz.com/LON
Type:	Active Directory site
Boundary:	LON
Created By:	
Date Created:	3/18/2012 2:59 PM
Group Count:	0
Modified By:	
Date Modified:	3/18/2012 2:59 PM

Related Objects

Boundary Groups

FIGURE 3.11 Discovered Active Directory boundaries.

Boundary groups are not discovered automatically, but rather are configured by the administrator. Boundary groups logically group the agents (through the boundaries) with resources such as Management Points and Distribution Points. This allows administrators to control where agents download their content from, thus controlling bandwidth utilization. For example, the Company XYZ organization has five locations: San Francisco, Paris, London, Tokyo, and New York. New York is the only office without a Configuration Manager 2012 Site Server. Boundary groups will be created for each location with the Site Server, so that local clients will download content from the local Site Servers. However, the New York boundary will be added to the SFO boundary group to ensure that the New York agents download content from the San Francisco Site Server. These boundary groups are shown in Figure 3.12.

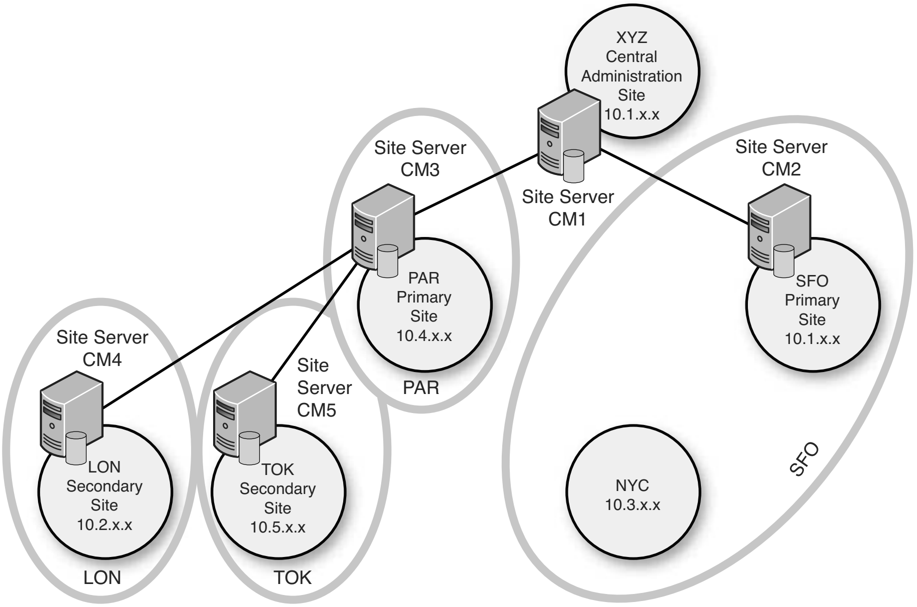


FIGURE 3.12 Company XYZ boundary groups.

To create a boundary group (in this example the Company XYZ SFO boundary group), execute the following steps:

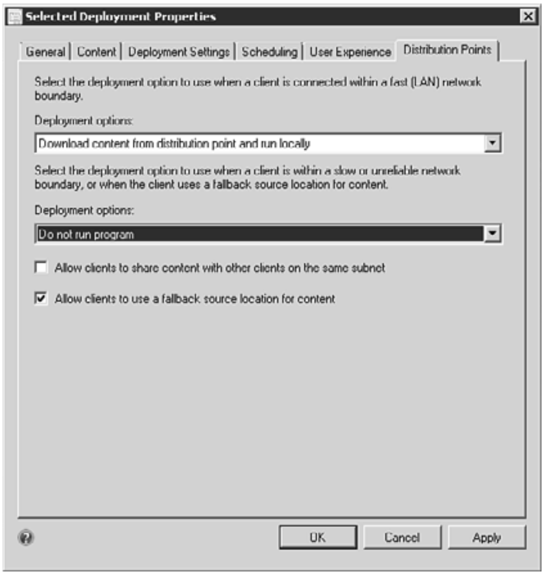
1. Make sure that your Active Directory sites and subnets are configured correctly and include all subnets and physical sites in the environment.
2. Launch the Configuration Manager console on the Central Administration Site Server.
3. Choose the Administration space.
4. Expand the Hierarchy Configuration and select the Boundary Groups node.
5. Right-click on the boundary group node and select Create Boundary Group.
6. In the general tab, enter the name of the boundary group (in this case, **`SFO`**).
7. Click the Add button to add boundaries to the boundary group.
8. Check the SFO boundary, and then click OK.
9. Choose the Reference tab.
10. In the Site Assignment section, check the Use This Boundary Group for Site Assignment check box and select the SFO site in the drop-down.
11. In the Content Location section, click the Add button.
12. Select the SFO Site Server and click OK.

NOTE

The connection defaults to “Fast.” This can be changed to “Slow” by clicking on the Change Connection button. This can be used to control how content is downloaded or if content is downloaded. This is useful for having backup content locations.

13. Click OK to create the boundary group.

When a server is configured within a boundary group, the server connection type defaults to Fast. The connection types are limited to Fast or Slow and are somewhat misleading. The true purpose of the connection types is during the creation of a deployment. When you want to deploy software, such as an application or patches, to a system, a deployment is needed. When configuring the deployment, several different distribution options are available. The deployment distribution options are shown in Figure 3.13.



Select the deployment option to use when a client is connected within a fast (LAN) network boundary.

Deployment options: Download content from distribution point and run locally

Select the deployment option to use when a client is within a slow or unreliable network boundary, or when the client uses a fallback source location for content.

Deployment options: Do not run program

☐ Allow clients to share content with other clients on the same subnet

☑ Allow clients to use a fallback source location for content

FIGURE 3.13 Distribution options.

The deployment allows the administrator to specify distribution characteristics depending on the configuration of the boundary groups. For example, if you configure a server connection in the boundary group as Slow and then configure the deployment to not run when the client is connected to a slow or unreliable network boundary, the software will not run on any system that identifies itself as being within this boundary.

NOTE

The topic of deployments is covered in Chapter 4 “Using Configuration Manager 2012 to Distribute Applications, Updates, and Operating Systems.”

The remaining boundary groups for Paris, London, and Tokyo can be created following the previous procedure. Now clients in the boundaries will automatically assign themselves to the appropriate site and download content from the appropriate location.

Configuring Discovery Methods

The Active Directory System Discovery option is the most common method used to find potential systems to manage. The main advantage to the AD System Discovery option is its efficiency in a well-maintained domain. Ensure that computer accounts that are no longer used have been disabled or removed from the Active Directory domain.

NOTE

Discovery of systems, groups, and users can be configured on each primary site in the SCCM 2012 hierarchy. However, discovery information is shared with all sites in the hierarchy. Rather than have duplicate discoveries, the best practice is to designate a single primary site in the hierarchy to do the discovery.

To enable the Active Directory System Discovery method, do the following:

1. From the ConfigMgr console, select the Administration space and expand the Hierarchy Configuration folder.
2. Select the Discovery Methods node.
3. Right-click and open the properties of the Active Directory System Discovery method for the SFO site. The SFO site will be the Company XYZ designated discovery site.
4. Enable Active Directory System Discovery.
5. Click the “*” button to add an AD container.
6. Click the Browse button and then click OK to select the entire companyxyz.com domain.
7. Accept the default options and click OK.
8. Select the Polling Schedule tab and click the Schedule button.
9. Change the recurrence to 1 hour and click OK.
10. Click OK to save the changes.
11. Click Yes at the pop-up to run the full discovery as soon as possible.

The status of the AD system discovery can be viewed in the `adsysdis.log` file.

To review the results of the discovery, do the following:

1. From the ConfigMgr console, expand Asset and Compliance.
2. Expand Overview, expand Devices, and right-click on the All Systems collection.

3. Click Update Membership.
4. Click Yes when prompted.
5. Click the Refresh action.

The collection should show all of the clients in the domain.

To enable the Active Directory Group Discovery method, do the following:

1. From the ConfigMgr console, select the Administration space and expand the Hierarchy Configuration folder.
2. Select the Discovery Methods node.
3. Open the properties of the Active Directory Group Discovery method for the SFO site. The SFO site will be the Company XYZ designated discovery site.
4. Enable Active Directory Group Discovery.
5. Click the Add button and select a location. Enter **`Company XYZ Domain`** for the Name.

NOTE

Active Directory Group Discovery supports the discovery of single groups for all groups with the location, such as a domain.

6. Click the Browse button and then click OK to select the entire companyxyz.com domain.
7. Accept the default options and click OK.
8. Select the Polling Schedule tab and click the Schedule button.
9. Change the recurrence to 1 hour and click OK.
10. Click OK to save the changes.
11. Click Yes at the pop-up to run the full discovery as soon as possible.

The previous steps should be repeated for the Active Directory User Discovery for SFO.

The Active Directory discoveries can be triggered manually by right-clicking on the discovery method and selecting Run Full Discovery Now. The detailed results of the discovery can be seen in the log files on the discovery server. The log files for each of the discoveries are as follows:

- Active Directory System Discovery (`adsysdis.log`)
- Active Directory Group Discovery (`adsgdis.log`)
- Active Directory User Discovery (`adusrdis.log`)

Any discovery errors or access errors will be shown in these detailed logs.

Configuring Hierarchy and Geographic Views

Configuration Manager infrastructures can be complex and hard to monitor. A very common request for administrators is to be able to view the hierarchy in a dynamic way. Another very common request is for administrators to be able to see their hierarchy map out geographically, with components in the correct place on a map. Configuration Manager 2012 delivers on both these requests.

The Configuration Manager 2012 hierarchy diagram shows the hierarchy in a graphical, dynamic, and active view. Each site is displayed in the diagram, with links and status. As sites are added and states change, the hierarchy diagram will update automatically.

Figure 3.14 shows the hierarchy diagram for Company XYZ. The diagram shows each of the five Configuration Manager 2012 Site Servers with a different icon for each site type. The overall alert status for each site is indicated as well, as can be seen in the warning state for the PAR site. Right-clicking on any component gives you detailed status, as is shown for the SFO site. The detailed status also allows you to link to key information such as site status messages and site properties.

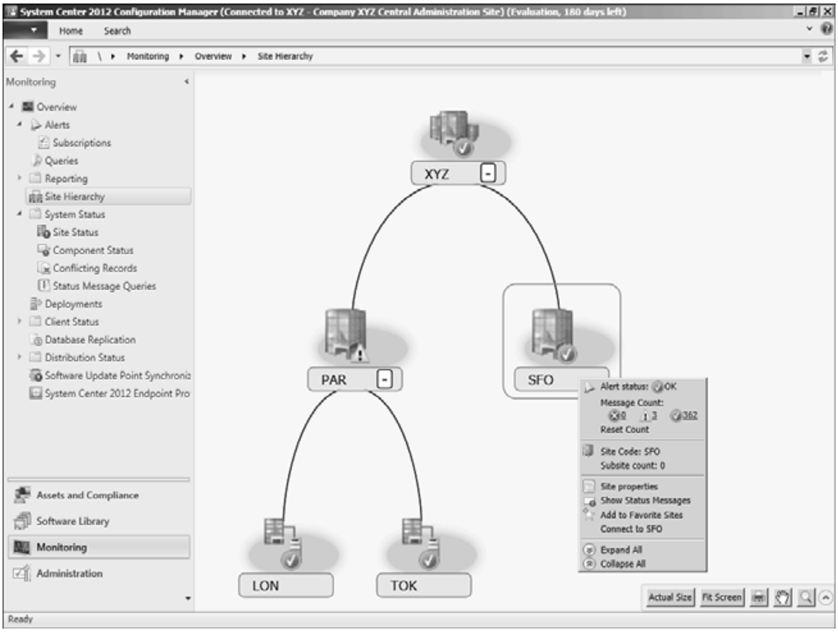


FIGURE 3.14 Company XYZ hierarchy diagram.

To access the hierarchy diagram, do the following:

1. Launch the Configuration Manager console.
2. Select the Administration space.
3. Select the Site Hierarchy folder.

In addition to the hierarchy diagram, there is also a geographical view. This view shows all the Site Servers on a Bing map. However, physical location information needs to be specified to enable the display of Site Servers on the map.

To specify the location information and display the geographical view, execute the following steps:

1. Launch the Configuration Manager console.
2. Select the Monitoring space.
3. Select the Site Hierarchy folder.
4. Right-click the Site Hierarchy folder and select Configure View Settings.
5. Select the Site Location tab.
6. For each site, enter a location. The location can be general, such as the city, or specific, such as the address.
7. Click OK to save the changes.
8. Right-click the Site Hierarchy folder and select Geographical View.

The view now shows a world map with the Site Servers correctly placed in their locations, as shown in Figure 3.15.

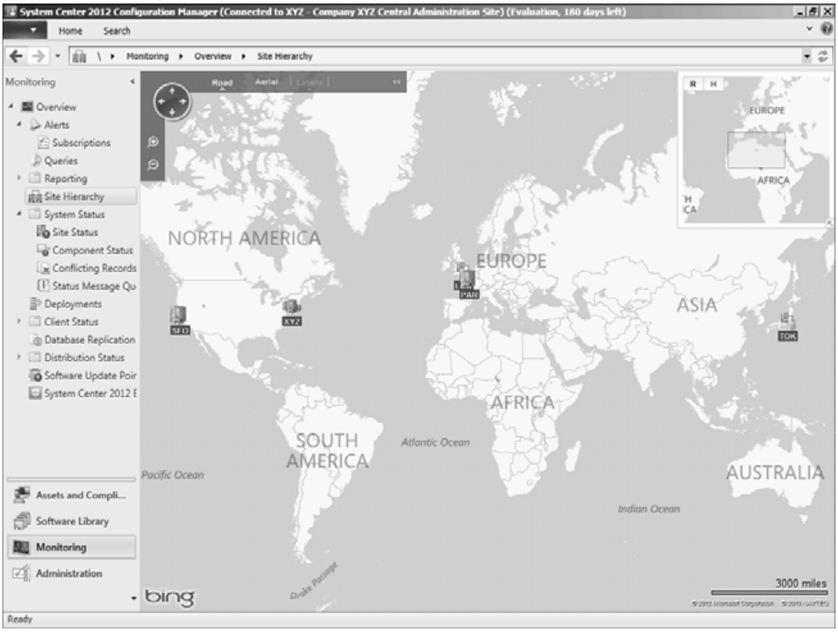
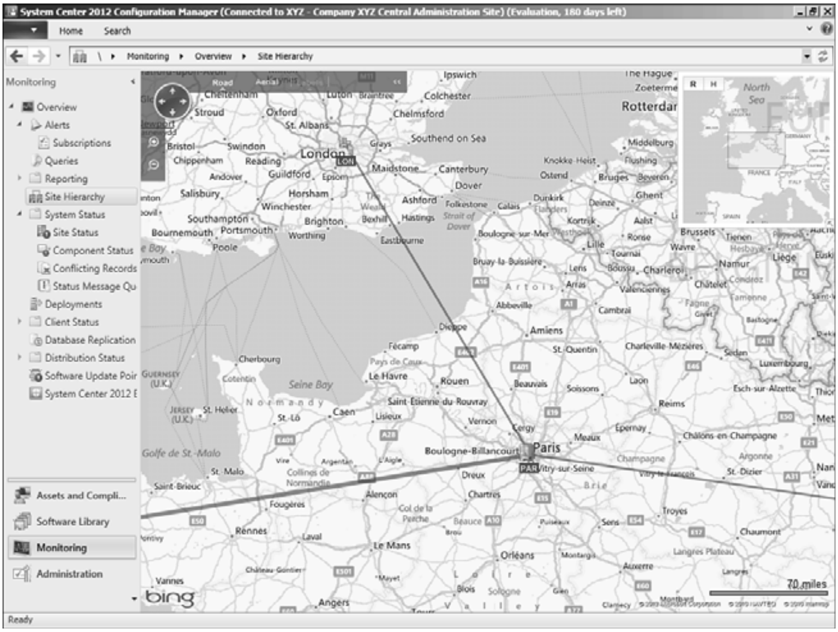


FIGURE 3.15 Company XYZ geographical view.

Like the hierarchy view, when the geographical view is active, hovering over a site with a mouse gives a high-level alert status and subsite count. The basis for the underlying map is the Bing Map engine. The map can be viewed either as a road map or an aerial satellite view. The map can also be zoomed into, to get detailed street information. In addition, selecting a site shows site links to neighboring sites. Figure 3.16 shows a zoom into the Company XYZ European region, with expanded map detail. The Paris site has been selected, which then shows the site links, including the site link to London.

NOTE

If it displays some instructions instead of the Bing Map, it may be because of the server's Internet Explorer settings; follow the instructions to solve the issue.



System Center 2012 Configuration Manager (Connected to XYZ - Company XYZ Central Administration Site) (Evaluation, 180 days left)

FIGURE 3.16 Company XYZ detailed geographical view.

Either view can be printed to capture the key information.

The hierarchy diagram and the geographical view provide exciting new and dynamic ways to view the Configuration Manager 2012 infrastructure.

Configuring Exchange Connectors

The Configuration Manager 2012 Exchange connector allows administrators to manage mobile devices that do not or cannot have agents installed on them, such as Apple iPhone, Apple iPad, or Google Android devices. Essentially any device that supports ActiveSync and is connected to Exchange Server can be managed through the connector.

To configure the Exchange connector, do the following steps:

1. Launch the Configuration Manager console.
2. Choose the Administration space.
3. Expand the Hierarchy Configuration folder.
4. Right-click on the Exchange Server Connectors node and select Add Exchange Server.
5. In the Server Address (URL) field, enter the address of the Exchange Client Access Server. The format of the URL is http://excas.companyxyz.com/powershell.
6. Select the Configuration Manager site to run the Exchange Server connector.
7. Click Next.
8. In the Account section, enter the account with which to connect to the Exchange server and click Next.

NOTE

The Account page very helpfully lists the Exchange Server cmdlets that the connector will need to be able to run the function correctly. The specified account should have the appropriate rights to run those cmdlets.

9. In the Discovery page, leave the defaults and click Next.
10. Adjust the policy settings as needed, and then click Next.
11. Review the summary and click Next to create the connector.

The connector will automatically synchronize with the targeted Exchange server. The synchronization can be forced by right-clicking on the connector and selecting Synchronize Now. Mobile devices will appear shortly in the list of devices.

Configuring Sites

Configuration Manager 2012 deploys certain Site System roles such as Management Points and Distribution Points, but does not deploy other roles nor completely configure those that it does deploy by default. Site configuration entails completing the configuration of the deployed roles and deploying of the required roles.

When deploying Site System roles to either the Site Server or a remote server, it is important to note the component installation wizard doesn't actually do the installation—it simply queues the installation for the Site Component Manager service. Even through the wizard always completes with a successful message, it is important to review the corresponding log files and the System Status container to ensure the component was actually installed correctly.

The log files for component installation are typically located on the server the component is being installed on, in a folder called `\Program Files\Microsoft Configuration Manager\Logs`. Additional status messages can be viewed in the `sitecomp.log` file on the Primary Site Server.

Deploying the Fallback Status Point Role

The Fallback Status Point (FSP) is very important. It provides a safety net for clients. The Configuration Manager agent should always be able to communicate status messages to the FSP, even if other communication has failed or is being blocked due to certificate or other issues.

To install FSP, complete the following steps:

1. From within the Administration space, expand Site Configuration and select Servers and Site Systems Roles.
2. Right-click CM2 and select Add Site System Roles.
3. On the General page, click Next.
4. Enable the Fallback Status Point role and click Next.
5. Accept the default configuration and click Next.

TIP

When a client is deployed, it sends several status messages to the FSP, even when the deployment is successful. If a large client rollout is planned, increase the number of messages allowed to prevent a backlog.

6. Review the summary and click Next.
7. Wait for the installation to complete, and then close the wizard.

Review the `fspMSI.log` and the `SMSFSPSetup.log` files for installation status. During normal operation, problems can be identified with the `fspmgr.log` file and using reports such as the Client Deployment Status Details or the Client Deployment Failure report.

Deploying the Reporting Service Point Role

The Reporting Service Point (RSP) provides reporting of Configuration Manager data through SQL Reporting Services (SRS). SRS is a significantly more powerful platform for developing and delivering reports.

The Reporting Service Point component is installed in three steps. Initially, the role is added to the correct server from the Site Management\Site Systems node. Then the Reporting Point needs to be configured with a data source; this is necessary to establish communication with the database holding the Configuration Manager data. Finally, reports need to be migrated from the legacy Reporting Point to the Reporting Service Point.

To install RSP on the Central Administration Site (CM1), complete the following steps:

1. From within the Administration space, select Servers and the Site System Roles folder.
2. Right-click CM1 and select Add Site System Roles.
3. On the General page, click Next.
4. Enable the Reporting Services Point role and click Next.
5. The Site Database Connection Settings will be discovered automatically. Click the Verify button to verify the settings.
6. In the Reporting Services Point Account, click the Set button and choose New Account.
7. Enter the appropriate credentials, and then click OK.
8. Click Next.
9. Review the summary and click Next.
10. Wait for the installation to complete, and then close the wizard.

This process should be completed not only for the Central Administration Site, but also for each primary site as well. This allows each of the sites to generate reports covering their specific information. For example, reports generated from the Central Administration Site in San Francisco will include information from the entire Company XYZ hierarchy. Reports generated from either the SFO or PAR primary sites will only include information from their portion of the hierarchy.

Review the `SRSRPSetup.log` and the `srsrp.log` files. These log files are located on the server hosting the Reporting Service Point in the Configuration Manager log folder (often `c:\Program Files\Microsoft Configuration Manager\Logs`). To check the status of the Reporting Services Point, go to the Monitoring space in the console, expand the Reporting folder, and select the Reports node. Reports will be listed there once the role is completed deploying.

Deploying Software Updates Point Role

For Site Servers that will be supporting the Software Updates role, there are two parts to the role setup. The first is to set up Windows Server Update Services (WSUS) and the second is to set up the Software Update Point role. In a Configuration Manager 2012 hierarchy that includes a Central Administration Site, the Software Update Point role will be installed on the Central Administration Site Server.

The Windows Server Update Services (WSUS) 3.0 SP2 components are required by Configuration Manager to support synchronization of patch data from Microsoft Update. WSUS is not used to deliver patches to managed systems; instead, the Configuration Manager hierarchy is used to effectively create an enterprise patch delivery and installation system.

To install WSUS 3.0 SP2, do the following on the Central Site Server (CM1 in the Company XYZ hierarchy):

1. Launch Windows Server Manager.
2. Right-click on the Roles folder and select Add Roles.
3. Click Next to skip the Welcome page.
4. Check the Windows Server Update Services role.
5. Click the Add Required Role Services if it pops up.
6. Click Next.
7. Click Next and Next past the Web Server (IIS) options.
8. At the WSUS welcome screen, click Next.
9. At the Confirmation screen, click Install.

NOTE

The WSUS installer downloads the latest version from the Internet and launches, continuing the installation.

10. Once the Windows Server Update Services 3.0 SP2 Setup Wizard launches, at the Welcome screen click Next.
11. Accept the terms of the license agreement and click Next.
12. Store the updates on `c:\WSUS` and click Next.
13. Select Using an Existing Database Server on This Computer.
14. Click Next.
15. If the connection is successful, click Next.
16. Leave the default website preference and then click Next.
17. Review the installation configuration and click Next.
18. Close the wizard when the installation is complete.
19. In the Before You Begin page of the Windows Server Update Services Configuration Wizard, click Cancel.

NOTE

There is no need to bother with the WSUS Configuration Wizard. All configuration of WSUS will be administered and managed using the Configuration Manager console.

Once the Windows WSUS role has been installed, the next step is to deploy the Software Update Point role. To do this, complete the following steps:

1. On the Central Administration Site Server (CM1 in the Company XYZ hierarchy), launch the Configuration Manager console.
2. In the Administration space, expand the Site Configuration folder and select the Servers and Site System Roles node.
3. Right-click the Central Administration Site Server, in this case CM1, and choose Add Site System Roles.
4. Click Next.
5. Check the Software Update Point role and click Next.
6. At the Software Update Point screen, leave the defaults and click Next.
7. At the Active Settings screen, check the Use This Server as the Active Software Update Point check box and click Next.
8. At the Synchronization Source screen, leave the defaults and click Next.
9. At the Synchronization Schedule screen, check the Enable Synchronization on a Schedule check box.
10. Change the schedule to run every 1 Days and click Next.
11. At the Supersedence Rules screen, leave the default and click Next.
12. At the Classifications screen, check All Classifications and click Next.
13. At the Products screen, check the required products and click Next.
14. At the Languages screen, check the appropriate languages and click Next.
15. Review the summary screen and then click Next.
16. Close the wizard when completed.

The Central Administration Site will now perform update synchronization for the entire Configuration Manager 2012 hierarchy.

Deploying Endpoint Protection Point Role

In Configuration Manager 2012, the System Center 2012 Endpoint Protection is integrated into the product rather than a separate install. There is now a Site Server role called Endpoint Protection Point, which provides endpoint protection services.

In a Configuration Manager 2012 hierarchy that includes a Central Administration Site, the Endpoint Protection Point role will be installed on the Central Administration Site Server.

To deploy the Endpoint Protection Point role, complete the following steps:

1. On the Central Administration Site Server (CM1 in the Company XYZ hierarchy), launch the Configuration Manager console.
2. In the Administration space, expand the Site Configuration folder and select the Servers and Site System Roles node.
3. Right-click the Central Administration Site Server, in this case CM1, and choose Add Site System Roles.
4. Click Next.
5. Check the Endpoint Protection Point role.
6. There will be a pop-up warning that software updates require special configuration or endpoint protection needs to use a different source. Click OK.
7. Click Next.
8. At the Endpoint Protection screen, accept the license terms and click Next.
9. Choose the appropriate Microsoft Active Protections Service (MAPS) membership type and click Next.
10. Review the summary screen and then click Next.
11. Close the wizard when completed.

The Central Administration Site will now perform endpoint protection for the entire Configuration Manager 2012 hierarchy.

Deploying Asset Intelligence Synchronization Point Role

An additional component called the Asset Intelligence Synchronization Point is also available. This component provides integration between Configuration Manager and Microsoft System Center Online services provided by Microsoft.

In a Configuration Manager 2012 hierarchy that includes a Central Administration Site, the Asset Intelligence Synchronization Point role will be installed on the Central Administration Site Server.

To deploy the Asset Intelligence Synchronization Point role, follow these steps:

1. On the Central Administration Site Server (CM1 in the Company XYZ hierarchy), launch the Configuration Manager console.
2. In the Administration space, expand the Site Configuration folder and select the Servers and Site System Roles node.
3. Right-click the Central Administration Site Server, in this case CM1, and choose Add Site System Roles.
4. Click Next.

5. Check the Asset Intelligence Synchronization Point role and click Next.
6. At the Asset Intelligence Synchronization Point Settings screen, leave the defaults and click Next.

NOTE

A certificate is not required. This was a legacy requirement back when Microsoft controlled what organizations could do asset intelligence synchronization, limiting it to organizations with Software Assurance contracts. After a time, Microsoft relaxed the requirement and now allows all organizations to perform asset intelligence synchronization without the certificate requirement.

7. At the Proxy Server Settings screen, leave the defaults and click Next.
8. At the Synchronization Schedule screen, leave the Enable Synchronization on a Schedule check box checked.
9. Change the schedule to run every one days and click Next.
10. Review the summary screen and then click Next.
11. Close the wizard when completed.

The Central Administration Site will now perform asset intelligence synchronization for the entire Configuration Manager 2012 hierarchy.

Preparing for OS Deployment

To support OS deployment user state migration and using network boot, the State Migration Point and PXE-enabled Distribution Point are required. To also support a complete operating system refresh with the ability to capture the users' existing settings, store them securely on the network, then reapply them to the new operating system; the State Migration Point is required.

The PXE functionality requires the WDS transport feature. This is available by default on Windows Server 2008, and can be installed automatically during the PXE configuration.

To enable CM2 to support PXE for OS deployment, complete the following steps:

1. Launch the Configuration Manager console.
2. In the Administration space, expand the Site Configuration folder and select the Servers and Site System Roles node.
3. Select the Primary Site Server, in this case CM2, and choose the Distribution Point role from the details window below.
4. Right-click the Distribution Point role and select Properties.

5. Select the PXE tab.
6. Enable PXE support for clients.
7. Click Yes after reviewing the ports information pop-up.
8. Check the Allow This Distribution Point to Respond to Incoming PXE Requests check box.
9. Check the Enable Unknown Computer Support check box and click OK to the warning pop-up.
10. Uncheck the Require a Password when Computers Use PXE check box.
11. Click OK to save changes to the Distribution Point.

The next step is to install the State Migration Point. This allows systems that are undergoing operating system deployment to upload the captured user state and then download the captured user state once the operating system is upgraded.

To deploy the State Migration Point role, follow these steps:

1. Launch the Configuration Manager console.
2. In the Administration space, expand the Site Configuration folder and select the Servers and Site System Roles node.
3. Right-click the Primary Site Server, in this case CM2, and choose Add Site System Roles.
4. Click Next.
5. Select the State Migration Point and click Next.
6. Click the orange "*" to specify a new folder to store state.
7. Enter a folder to use, such as **`c:\StateMigration`** and click OK.
8. Click Next.
9. Leave the default boundary groups and click Next.
10. Review the summary screen and then click Next.
11. Close the wizard when completed.

The preceding steps to configure PXE functionality and state migration functionality need to be completed on each Distribution Point and Site Server where Operating System Deployment (OSD) functionality is needed. Typically, this is all Primary Site Servers and all secondary site servers in the Configuration Manager 2012 hierarchy, as well as locations with just Distribution Points.

Configuring Client Settings

Client settings control 18 different areas of client configuration, ranging from BITS configuration through User and Device Affinity. In the past, these settings were monolithic and applied to the entire site. There was no granularity within the site nor any way to transfer settings across the hierarchy. In Configuration Manager 2012, the client settings are configured at a hierarchy level, meaning that the settings apply to the site and all child sites. In addition, custom settings can be created and deployed to collections. These custom settings and flexible targeting mechanism allow settings to be adjusted in a very fine-grained manner.

In the next sections, each of the settings are covered along with recommended settings. To review and edit any of the settings, select the Administration space.

Background Intelligent Transfer

The Background Intelligent Transfer settings allow administrators to control the download behavior of clients via the BITS protocol. By default, these settings are disabled, but if enabled, these settings allow the client to be throttled within a specified window with maximum transfer rates.

For most organizations, it is recommended that this be left disabled.

Client Policy

The client policy settings control how often the client checks in for policy updates, by default every 60 minutes. This essentially establishes a heartbeat for the policy refresh. If new policies are deployed, this polling interval limits how quickly that policy can be deployed.

This was a classic example where different settings were needed for different types of devices. Many organizations were comfortable with a one-hour polling interval for workstations, but wanted a much shorter polling interval for servers along the lines of 15 minutes. This was difficult to do in previous versions of SCCM, but in SCCM 2012 is easy to do with the custom client settings targeted at servers.

In addition, user policy polling can be disabled or enabled. This controls whether users will see user policy. Machine policies are always applied.

Is recommended that the default polling interval of 60 minutes be left in place unless there are specific reasons to adjust it.

Compliance Settings

The Compliance Settings section controls whether compliance is enabled or disabled. This setting is enabled by default. The schedule for compliance evaluation is also set in this section, with the default of every seven days.

It is recommended that compliance evaluation be left enabled and that schedule be adjusted to run every one day.

Computer Agent

The Computer Agent section contains a smorgasbord of settings related to notifications, the Application Catalog, and installation permissions. A few these have very useful applications.

The Install Permissions setting allows administrators to control which users can initiate installation of software and software updates in task sequences. The options are as follows:

- All Users
- Only Administrators
- Only Administrators and Primary Users
- No Users

This setting, in combination with custom settings targeted at collections, allows administrators to control who is allowed to manually install software advertised by SCCM.

The PowerShell Execution Policy allows administrators to control whether unsigned PowerShell scripts are allowed or not. The default Restricted setting prevents unsigned scripts from executing, whereas the Bypass setting allows unsigned scripts to execute.

The Deployment Deadline options control how often users will see pop-ups of impending deployment deadlines over 24 hours out, less than 24 hours out, and less than an hour away. This set of options combined with custom settings targeted at collections allows administrators flexibility in notifying users.

Computer Restart

The Computer Restart section controls the notifications that users receive before pending restart. The temporary notification, by default 90 minutes, is the advance warning the user gets before restart. The countdown notification, by default 15 minutes, is the countdown window that the user gets before restart.

Endpoint Protection

The Endpoint Protection section covers the settings related to the Microsoft anti-malware features of Configuration Manager 2012. It is disabled by default, but is highly recommended that it be enabled.

Most of the settings in this section control agent installation behavior, such as to install the agent (default is True), remove previously installed agents (default is True), and suppress restarts after installation (default is True).

Interestingly, the default remove previously installed agents will remove both Microsoft and non-Microsoft antivirus agents. The list of antivirus agents that will be removed includes the following:

- All current Microsoft anti-malware products except for Windows InTune and Microsoft Security Essentials
- Symantec AntiVirus Corporate Edition version 10
- Symantec Endpoint Protection version 11
- Symantec Endpoint Protection Small Business Edition version 12
- Mcafee VirusScan Enterprise version 8
- Trend Micro OfficeScan

Given the ease with which SCCM 2012 endpoint protection deploys, it may come as a surprise when it uninstalls other antivirus agents. To prevent this, it is recommended to use custom client settings with this option disabled.

The one setting that needs to be changed, after enabling the agent, is the Disable Alternate Sources option. This is enabled by default, which prevents the Endpoint Protection agent from using other sources such as Microsoft Windows Update to get definition updates. This option should be set to False, to allow the agent to get definition updates from Windows Update.

Hardware Inventory

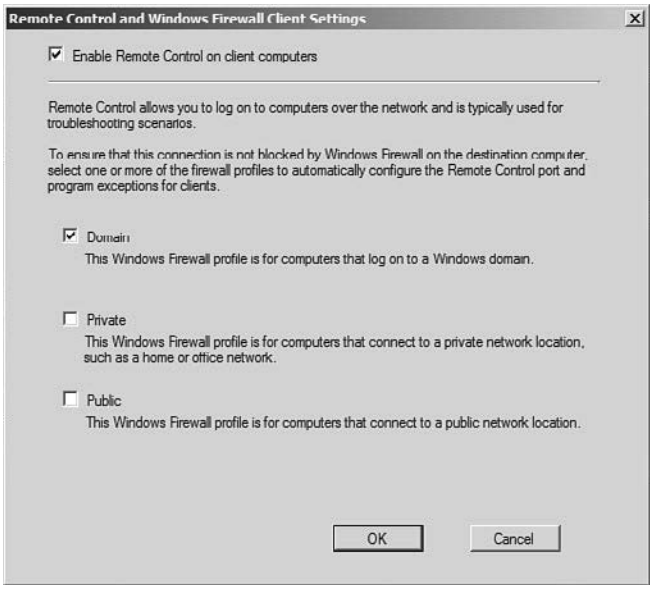
The Hardware Inventory section, enabled by default, primarily controls the interval on which hardware inventory is collected. The default of seven days is usually too long and it is recommended to change the schedule to once per day.

In addition, in this section additional hardware inventory classes can be configured to be collected. This includes Registry values for other important information, which previously required modifying text files directly. Embedding a `graphical user interface` (GUI) to do this in Configuration Manager 2012 is a very welcome enhancement.

Remote Tools

The Remote Tools section controls the remote tools if enabled on agents and the behavior of the remote tools if it is enabled. Remote tools are by default disabled.

A new feature of the remote tools settings is the ability to set the Windows Firewall as part of enabling the tool. As shown in Figure 3.17, the remote control feature is enabled in the check box to configure the remote control port and program exception for just the domain firewall. This ensures that while computers are connected to the domain, remote control will be allowed through the firewall. When not connected to the domain, those ports will be closed and not present a security risk.



Remote Control and Windows Firewall Client Settings

☑ Enable Remote Control on client computers

Remote Control allows you to log on to computers over the network and is typically used for troubleshooting scenarios.

To ensure that this connection is not blocked by Windows Firewall on the destination computer, select one or more of the firewall profiles to automatically configure the Remote Control port and program exceptions for clients.

☑ Domain
This Windows Firewall profile is for computers that log on to a Windows domain.

□ Private
This Windows Firewall profile is for computers that connect to a private network location, such as a home or office network.

□ Public
This Windows Firewall profile is for computers that connect to a public network location.

FIGURE 3.17 Enabling remote control with domain firewall exception.

Another welcome enhancement to Configuration Manager 2012 is the Allow Remote Control of an Unattended Computer option. This feature was completely absent from the previous version of SCCM, meaning that the user always had to be present when using remote tools. With SCCM 2012, administrators can now press Ctrl+Alt+Delete on a remote agent. However, this is explicitly allowed (the default) or disallowed in the remote tools client settings.

Software Deployment

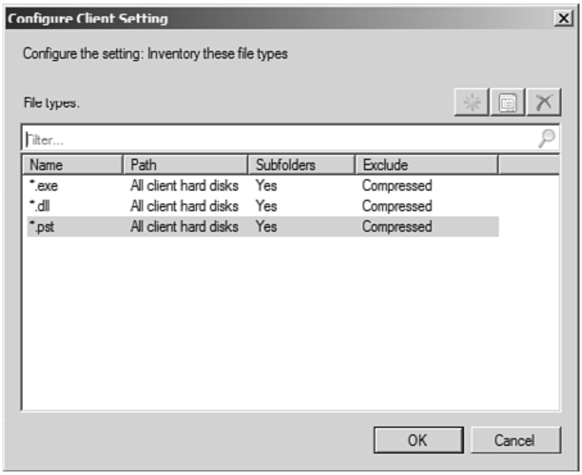
In the Software Deployment section, the only setting is for the deployment reevaluation schedule. This defaults to seven days and can be left at the default.

Software Inventory

The Software Inventory section of client settings controls how software inventory is collected. It is enabled by default with the schedule of every seven days.

It is recommended that the schedule be changed to every one days, to ensure that software reporting is as current as possible.

Unfortunately, in SCCM 2012 the inventory file types is blank. This means that no files will be inventoried by default. In previous versions of SCCM, all EXE files were inventoried out of the box. It is recommended that organizations inventory at a minimum all EXE (*.exe), all DLL (*.dll), and all PST (*.pst) files. Figure 3.18 shows the recommended file inventory types.



Configure Client Setting

Configure the setting: Inventory these file types

File types:

Name	Path	Subfolders	Exclude
*.exe	All client hard disks	Yes	Compressed
*.dll	All client hard disks	Yes	Compressed
*.pst	All client hard disks	Yes	Compressed

FIGURE 3.18 The recommended file inventory types.

Software Metering

In the Software Metering section, the only settings are to enable software metering and for the deployment reevaluation schedule. This defaults to seven days and should be adjusted to every one day, if the feature is enabled.

Software Updates

The Software Update section of client settings controls updates behavior. It is enabled by default, but there are several schedule options within the section that should be adjusted.

The software update scan schedule defaults to every seven days, but should be adjusted to every one days. This allows much more timely information to be collected, such as what updates have been applied. This is reflected in reports, which will be current as of the previous day.

The scheduled deployment reevaluation schedule defaults to every seven days and should be left as is. The schedule determines how often the agent checks to see if it is still in compliance with previous deployments, which might result in updates being deployed.

The next setting controls what the agent does when a particular software update deployment deadline is reached, should the agent also opportunistically install any other pending software update deployments. And it allows how far in advance to look for pending software update deployments. Because update deployments frequently result in reboots, it makes sense to deploy future updates at the same time.

The setting defaults to False, so it is recommended to change that to True and the next setting to seven days. This ensures that any updates with mandatory deadlines scheduled up to a week in advance will be deployed at the same time.

State Messaging

The State Messaging section of client settings controls a little-known, but key aspect of the Configuration Manager agent. As the agent is executing policy, deployments, and tasks, it generates status messages and delivers them to the server to be stored in the database.

The State Messaging section controls the frequency with which those messages get uploaded. The default is every 15 minutes, but can be adjusted depending on conditions.

User and Device Affinity

The User and Device Affinity section of client settings controls a much requested feature that Configuration Manager 2012 delivers. Device affinity allows devices such as desktops and laptops to be associated with their users. In SCCM 2012, this can be done automatically.

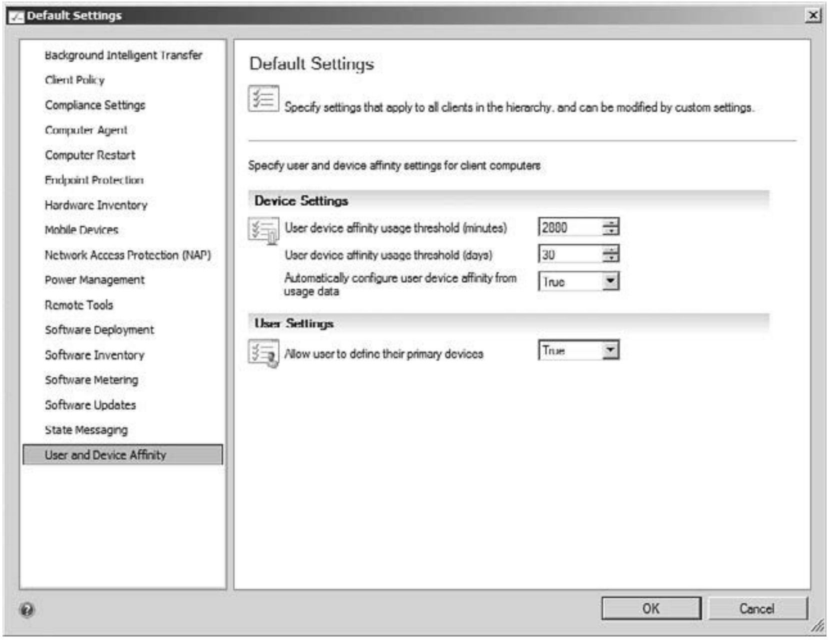
In the User and Device Affinity section, administrators can specify how much time a user needs to spend with the device for it to be automatically associated with the user account.

There are two threshold settings that create the automatic association. The first is the User Device Affinity Usage Threshold (min) setting, which sets how much time a user needs to spend using the machine for it to be considered associated with that user. The second is the User Device Affinity Usage Threshold (days) setting, which sets the span of time over which usage is measured.

To enable User und Device Affinity, the Automatically Configure User Device Affinity from Usage Data setting needs to be set to True.

In addition, the Allow Users to Define Their Primary Devices setting allows users to actually specify their primary device (that is, set the affinity). It is recommended that this be set to True to give users control.

Figure 3.19 shows the recommended User and Device Affinity settings.



Default Settings

Specify settings that apply to all clients in the hierarchy, and can be modified by custom settings.

Specify user and device affinity settings for client computers

Device Settings

User device affinity usage threshold (minutes) 2880

User device affinity usage threshold (days) 30

Automatically configure user device affinity from usage data True

User Settings

Allow user to define their primary devices True

FIGURE 3.19 The User and Device Affinity settings.

Configuring the Client Installation Settings

In Configuration Manager 2012, the client push installation settings are associated with each primary or secondary site in the hierarchy. The Client Installation Settings menu for each site holds the two installation options: Client Push Installation and Software Update-Based Client Installation. The Client Push Installation option is typically used to perform client deployments. The settings within the Client Push Installation configure the command-line options used when the client is pushed, the account used to access the remote computer, and if one of the Configuration Manager discovery methods triggers an installation of the client on remote systems.

A client can be pushed manually from the Configuration Manager console or executed automatically when a Discovery Method is executed. It is important to disable the Automatic Push Installation option until the client is tested and the correct options are set.

To configure the Client Installation account, complete the following steps:

1. Open the console, browse to Administration, expand Site Configuration, expand Sites, and select SFO Site.
2. Right-click on SFO Site and select Client Installation Settings, Client Push Installation.
3. Check the Enable Automatic Site Wide Client Push Installation check box.

4. Select the Accounts tab, click “*”, and then click New Account.
5. Add an account with local administrative rights to the systems.
6. Select the Installation Properties tab. The current installation property is `SMSSITECODE=SFO`.
7. Add **`FSP=CM2`** to the Installation properties. This specifies the fallback status point for clients. Separate the properties with a space.
8. Apply the changes.

This account will be used to push the Configuration Manager agent to client systems. The `SMSSITECODE=SFO` command is configured by default to set the agent’s assigned site. If the agent is being pushed from a primary site, but will be managed by a different primary site or secondary site, this value should be changed to `SMSSITECODE=AUTO`, allowing the client to choose the correct site code based off of the configured boundaries.

Repeat the previous steps for each primary site and secondary site that will be pushing out agents.

Implementing Internet-Based Client Management

Internet-based client management in Configuration Manager 2012 is really just configuring key roles to support the secure HTTPS protocol rather than the insecure HTTP protocol. That said, considerable preparation work needs to be done to implement the Public Key Infrastructure and certificates to support this change efficiently and effectively.

Creating a Public Key Infrastructure

A Public Key Infrastructure (PKI) is an important aspect of the Configuration Manager 2012 implementation. When a certificate is issued, its usage is governed by an Object Identifier (OID). A certificate can have more than one OID, essentially allowing the certificate to be used for more than one purpose.

A certificate with the Client Authentication OID is required on all managed clients, including mobile devices, to communicate with a Configuration Manager site via HTTPS.

A certificate with the Server Authentication OID (1.3.6.1.5.5.7.3.1) and Client Authentication OID (1.3.6.1.5.5.7.3.2) is required on all Configuration Manager 2012 Site Systems, including Site Servers, Management Points, Distribution Points, Software Update Points, and State Migration Points. The Server Authentication certificate is used on each Site Server to encrypt communication between the managed systems and the Configuration Manager component.

Deploying an Active Directory Enterprise Root CA

This example details the steps required to deploy an Enterprise Root CA in the Company ABC domain. When an Enterprise Root CA is configured, all clients in the domain automatically trust certificates issued from this CA.

All Configuration Manager Site Servers and managed clients must trust the Certificate Authority. Any Configuration Manager Site Servers or managed clients that don't trust this Certificate Authority will not communicate with the infrastructure and might become orphaned. This typically happens when non–domain member servers, such as bastion hosts in the demilitarized zone (DMZ), are not part of the domain but have a Configuration Manager agent installed. To correct this problem, install the CA certificate into the local computer's Trusted Root Certificate Authorities certificates store.

NOTE

Status messages will still be sent to the Fallback Status Point, even if the client system has become orphaned due to certificate configuration issues. It is important to deploy the Fallback Status Point before deploying clients.

To deploy an Enterprise Root CA, complete the following steps:

1. Open the Server Manager console on CERT, the intended CA server.
2. Select the Roles node.
3. Click the Add Roles action.
4. Click Next to skip the Roles Overview page.
5. Enable the Active Directory Certificate Services role, and then click Next.
6. Click Next to skip the AD CS overview page.
7. Enable the Certification Authority role service.
8. Enable the Certification Authority Web Enrollment role service.
9. Click Add Required Role Services when prompted, and then click Next.
10. Select Enterprise and click Next.
11. Select Root CA and click Next.
12. Select Create a New Private Key and click Next.
13. Accept the default Cryptography settings and click Next.
14. Accept the default CA Name settings and click Next.
15. Accept the default Validity Period settings and click Next.
16. Accept the default Certificate Database Location settings and click Next.
17. Click Next to skip the IIS Overview page.
18. Accept the default IIS Role Services and click Next.
19. Confirm the installation selections and click Install.
20. Wait for the installation to complete and click Close.

After implementing the CA, the CRL Distribution Point (CDP) settings need to be configured to allow HTTP access to the CRL files. For security reasons, this typically wouldn't be done on the issuing CA; the CRL would be published on a system designated for that role. However, for demonstration purposes, the CRL will be published on the server CERT, allowing Internet-based clients to check the CRL.

To publish the CRL, complete the following steps:

1. Open the Server Manager console on CERT.
2. Expand the Roles node.
3. Expand the Active Directory Certificate Services node.
4. Right-click companyxyz-CERT-CA and click Properties.
5. Select the Extensions tab.
6. Select http://<ServerDNSName>/CertEnroll/<CaName>... from the list of CDPs.
7. Enable Include in CRLs. Clients use this to find Delta CRL locations.
8. Enable Include in the CDP Extension of Issued Certificates.
9. Apply the changes, click Yes when you are prompted to restart the Active Directory Certificate Services, and then click OK to close the window.

Validating the Enterprise Root CA

The newly installed Enterprise Root CA should be validated before certificates are issued to clients. To validate the CA, check the local application event log on the server CERT. This can be accessed through the Diagnostics node of Server Manager.

If the application event log is clean and doesn't contain any error or warning messages about Certificate Services or related components, the server should be ready to issue certificates to clients. It is always a good practice to restart the certificate server to ensure the Certificate Services can start and stop without logging any issues. It is also important to resolve all problems before moving to the next section and deploying certificates to managed clients and Site Servers.

Deploying Certificates

An enterprise Certificate Authority simplifies management of certificates by providing a secure, scalable certificate provisioning process through Active Directory. This task assumes all of the Configuration Manager servers and the Enterprise Root CA server have been moved to an organizational unit (OU) called Servers, and all of the workstations have been moved to an OU called Workstations.

The Servers and Workstations OUs are child objects of an OU called Managed. The Managed OU is located in the root of the domain.

CAUTION

Do not move domain controllers from the default OU. Moving domain controllers out of the default Domain Controllers OU is not supported.

When an Enterprise Root CA is deployed, all domain controllers automatically receive a "Domain Controller" certificate. This certificate can be used for both client and server authentication.

Configuring the Auto-Enrollment Group Policy Object

A Group Policy Object (GPO) called Certificate Auto-Enrollment will be created and linked to the Servers OU and the Workstations OU. This group policy will be used to enable the certificate auto-enrollment function for all managed systems.

To create the Certificate Auto-Enrollment GPO, complete the following steps:

1. Open the Group Policy Management Console on DC1.
2. Expand Forest: companyabc.com.
3. Expand Domains.
4. Expand companyabc.com.
5. Select the Group Policy Objects container.
6. Right-click the Group Policy Objects container and select New.
7. Enter **`Certificate Auto-Enrollment`** in the Name field and click OK.

Once the GPO has been created, the setting that allows Certificate Auto-Enrollment can be enabled.

To enable the Certificate Auto-Enrollment setting in the GPO, complete the following steps:

1. Right-click the Certificate Auto-Enrollment GPO and select Edit.
2. The Group Policy Management Editor opens.
3. Expand Computer Configuration.
4. Expand Policies.
5. Expand Windows Settings.
6. Expand Security Settings.
7. Select the Public Key Policies container.
8. Double-click Certificate Services Client - Auto-Enrollment.

   The Certificate Services Client - Auto-Enrollment location is shown in Figure 3.20.

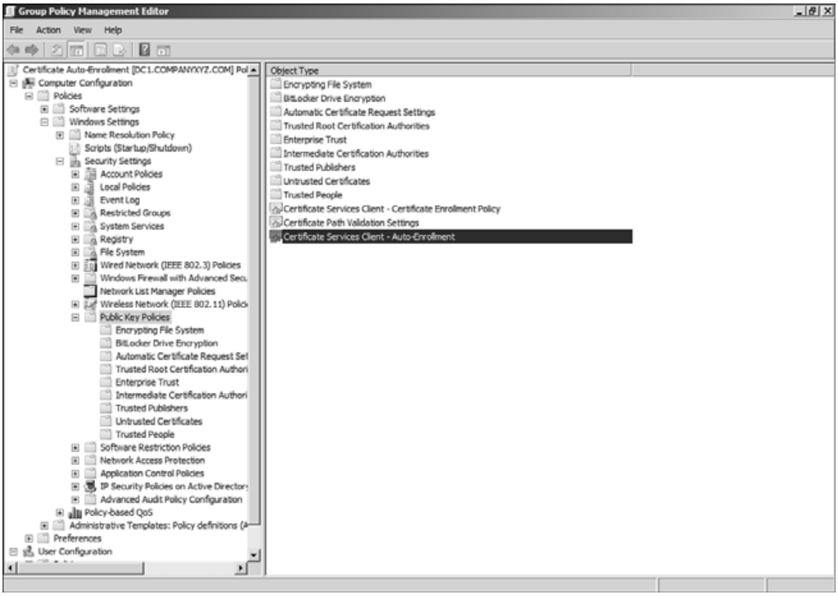

Group Policy Management Editor
File Action View Help
Certificate Auto-Enrollment [DC1.COMPANYXYZ.COM] Pol
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Security Settings
Account Policies
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policies
Windows Firewall with Advanced Secu
Network List Manager Policies
Wireless Network (IEEE 802.11) Polici
Public Key Policies
Encrypting File System
BitLocker Drive Encryption
Automatic Certificate Request Set
Trusted Root Certification Authori
Enterprise Trust
Intermediate Certification Authori
Trusted Publishers
Untrusted Certificates
Trusted People
Software Restriction Policies
Network Access Protection
Application Control Policies
IP Security Policies on Active Director
Advanced Audit Policy Configuration
Policy-based QoS
Administrative Templates: Policy definitions (A
Preferences
User Configuration
Object Type
Encrypting File System
BitLocker Drive Encryption
Automatic Certificate Request Settings
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authorities
Trusted Publishers
Untrusted Certificates
Trusted People
Certificate Services Client - Certificate Enrollment Policy
Certificate Path Validation Settings
Certificate Services Client - Auto-Enrollment

FIGURE 3.20 Certificate Services Client - Auto-Enrollment.

9. Select Enabled as the Configuration Model.
10. Enable the option to Renew Expired Certificates.
11. Enable the option to Update Certificates That Use Certificate Templates.
12. **Click OK to** save changes and close the Group Policy Management Editor.

Once the Auto-Enrollment setting within the GPO has been configured to allow automatic certificate enrollment, the GPO can be linked to the correct OUs.

To link the Certificate Auto-Enrollment GPO to the correct OUs, complete the following steps:

1. Open the Group Policy Management Console.
2. Expand the Managed OU and select the Servers OU.
3. Right-click the Servers OU and select Link an Existing GPO.
4. Select Certificate Auto-Enrollment from the list of GPOs and click OK.
5. Right-click the Workstations OU and select Link an Existing GPO.
6. Select Certificate Auto-Enrollment from the list of GPOs and click OK.

When this is complete, any domain member server or workstation placed in the corresponding OUs will be configured for automatic certificate enrollment. To complete the process, a certificate template with the correct settings and permissions needs to be created and then published.

Configuring Certificate Templates

The next step is to create certificate templates with the appropriate settings and permissions. The permissions on the certificate template govern the clients' ability to request the certificate. This is important because only the required certificates should be deployed to the system.

CAUTION

Provisioning certificates with unnecessary OIDs is not recommended. Only provision the minimum requirements needed by the client to communicate with Configuration Manager.

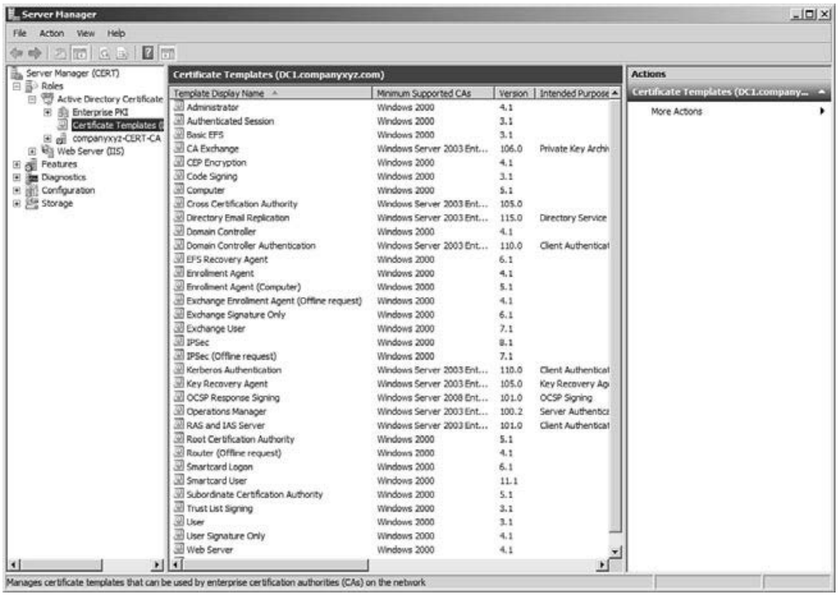
Creating the Client Authentication Certificate Template

Security permissions on the certificate template for Client Authentication will be configured to allow the domain computers security group to automatically request and receive this certificate through Active Directory. All systems in the Workstations and Servers OUs will receive this certificate.

To create Client Authentication templates for auto-enrollment, complete the following steps:

1. Open the Server Manager console on CERT.
2. Expand the Roles node.
3. Expand the Active Directory Certificate Services node.
4. Select the Certificate Templates container.

   The Certificate Templates container is shown in Figure 3.21.



Certificate Templates (DC1.companyxyz.com)

Template Display Name	Minimum Supported CAs	Version	Intended Purpose
Administrator	Windows 2000	4.1	
Authenticated Session	Windows 2000	3.1	
Basic EFS	Windows 2000	3.1	
CA Exchange	Windows Server 2003 Ent...	106.0	Private Key Archi
CEP Encryption	Windows 2000	4.1	
Code Signing	Windows 2000	3.1	
Computer	Windows 2000	5.1	
Cross Certification Authority	Windows Server 2003 Ent...	105.0	
Directory Email Replication	Windows Server 2003 Ent...	115.0	Directory Service
Domain Controller	Windows 2000	4.1	
Domain Controller Authentication	Windows Server 2003 Ent...	110.0	Client Authenticat
EFS Recovery Agent	Windows 2000	6.1	
Enrollment Agent	Windows 2000	4.1	
Enrollment Agent (Computer)	Windows 2000	5.1	
Exchange Enrollment Agent (Offline request)	Windows 2000	4.1	
Exchange Signature Only	Windows 2000	6.1	
Exchange User	Windows 2000	7.1	
IPSec	Windows 2000	8.1	
IPSec (Offline request)	Windows 2000	7.1	
Kerberos Authentication	Windows Server 2003 Ent...	110.0	Client Authenticat
Key Recovery Agent	Windows Server 2003 Ent...	105.0	Key Recovery Ag
OCSP Response Signing	Windows Server 2008 Ent...	101.0	OCSP Signing
Operations Manager	Windows Server 2003 Ent...	100.2	Server Authentic
RAS and IAS Server	Windows Server 2003 Ent...	101.0	Client Authenticat
Root Certification Authority	Windows 2000	5.1	
Router (Offline request)	Windows 2000	4.1	
Smartcard Logon	Windows 2000	6.1	
Smartcard User	Windows 2000	11.1	
Subordinate Certification Authority	Windows 2000	5.1	
Trust List Signing	Windows 2000	3.1	
User	Windows 2000	3.1	
User Signature Only	Windows 2000	4.1	
Web Server	Windows 2000	4.1	

Manages certificate templates that can be used by enterprise certification authorities (CAs) on the network

FIGURE 3.21 The Certificate Templates container.

5. Right-click the Workstation Authentication template.
6. Select Duplicate Template.
7. Choose Windows Server 2003 Enterprise and click OK.

CAUTION

The Windows Server 2008 Enterprise certificate option is not compatible with System Center Configuration Manager 2012. Choosing Windows Server 2008 Enterprise will result in a version 3 template. To create a version 2 template, select Windows Server 2003 Enterprise.

8. Type **`Client Certificate Auto-Enrollment`** in the Template Display Name field.
9. Select the Security tab.
10. Enable the Autoenroll permission for domain computers.
11. Select the Extensions tab.
12. Select the Application Policies item.
13. Verify the description states Client Authentication.
14. Click Apply and then click OK to close the window.

Creating the OS Deployment Template

Security permissions on the certificate template for OS Deployment will be configured to only allow manual certificate requests. Before PXE Service Points are implemented, the Client Authentication OS Deployment certificate will be requested through the web enrollment page.

To create the OS Deployment template, complete the following steps:

1. Open the Server Manager console on CERT.
2. Expand the Roles node.
3. Expand the Active Directory Certificate Services node.
4. Select the Certificate Templates container.
5. Right-click the Workstation Authentication template.
6. Select Duplicate Template.
7. Choose Windows Server 2003 Enterprise and click OK.
8. Type **`Configuration Manager OS Deployment`** in the Display Name field.
9. Select the Issuance Requirements tab.
10. Enable CA Certificate Manager Approval.
11. Select the Request Handling tab.
12. Enable the Allow Private Key to Be Exported option.
13. Select the Subject Name tab.
14. Enable the Supply in the Request option.
15. Select the Security tab and remove Domain Computers from the list.
16. Click Apply and then click OK to close the window.

Creating the Server Authentication Certificate Template

Security permissions on the certificate template for Server Authentication will be configured to only allow a custom security group to automatically request this certificate through Active Directory. Ultimately, all systems that will host web services will receive this certificate.

Before executing the next task, create a universal security group called SCCM Site Servers in the domain. Add the Configuration Manager servers and the Certificate Authority server to this group.

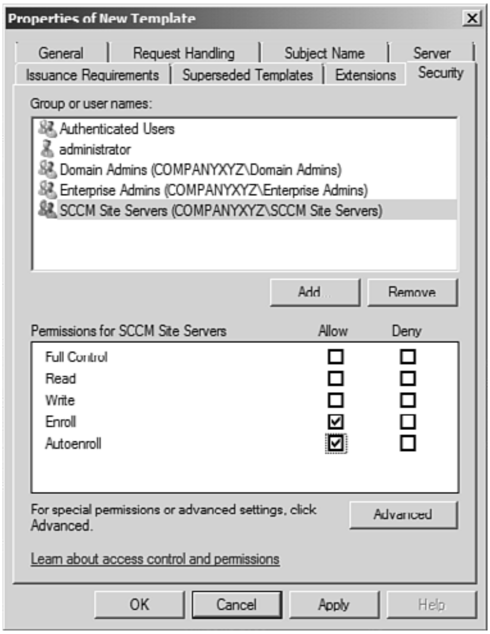
CAUTION

When a computer object is added to a group, it can take a long time for the setting to take effect. This is because the Kerberos ticket takes seven days to renew. The renewal time is governed by the *Maximum Lifetime for User Ticket Renewal* setting located in the Default Domain Policy GPO. It is not recommended to change this setting. Instead, restart the computer to refresh the Kerberos ticket.

To create Server Authentication template for auto-enrollment of the SCCM Site Servers, complete the following steps:

1. Open Server Manager and expand Roles, expand Active Directory Certificate Services, and select the Certificate Templates container.
2. Right-click the Workstation Authentication template.
3. Select Duplicate Template.
4. Choose Windows Server 2003 Enterprise and click OK.
5. Type **`Server Certificate Auto-Enrollment`** in the Display Name field.
6. Select the Security tab.
7. Remove the Domain Computers security group.
8. Click Add, type the group **`SCCM Site Servers`**, and then click OK.
9. Highlight SCCM Site Server.
10. Uncheck the Read permission.
11. Check the Enroll and Autoenroll permissions.

    The permission for this certificate is shown in Figure 3.22.



Group or user names:

- Authenticated Users
- administrator
- Domain Admins (COMPANYXYZ\Domain Admins)
- Enterprise Admins (COMPANYXYZ\Enterprise Admins)
- SCCM Site Servers (COMPANYXYZ\SCCM Site Servers)

Permissions for SCCM Site Servers	Allow	Deny
Full Control	□	□
Read	□	□
Write	□	□
Enroll	☑	□
Autoenroll	☑	□

For special permissions or advanced settings, click Advanced.

Learn about access control and permissions

FIGURE 3.22 Permissions for the Server Authentication template.

12. Select the Extensions tab.
13. Select the Application Policies extension item and click Edit.
14. Highlight the Client Authentication Policy and click Remove.
15. Click Add, choose Server Authentication from the list, and then click OK.
16. Click OK, click Apply to apply the settings, and close the window.

All servers that are added to the Servers OU and are members of the SCCM Site Servers security group will receive a certificate that can be used for server authentication.

Publishing the Certificate Templates

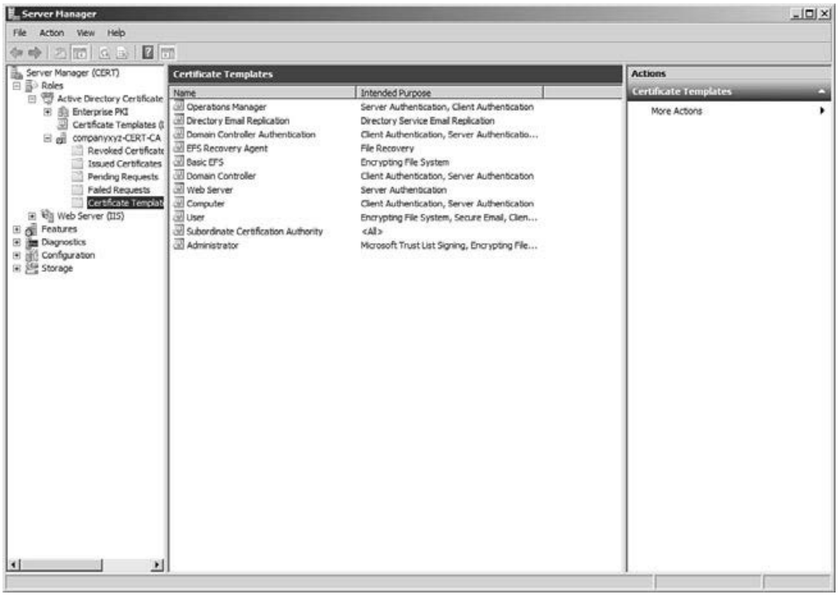
Now that the Client and Server Authentication certificates have been created, they can be published. This tells the Certificate Authority the template is available for client consumption.

To publish the authentication templates for auto-enrollment, complete the following steps:

1. Open Server Manager on CERT.
2. Expand Roles.

3. Expand Active Directory Certificate Services.
4. Expand companyxyz-CERT-CA.
5. Select the Certificate Templates container.

   The CA Certificate Templates container is shown in Figure 3.23.



Name	Intended Purpose
Operations Manager	Server Authentication, Client Authentication
Directory Email Replication	Directory Service Email Replication
Domain Controller Authentication	Client Authentication, Server Authenticatio...
EFS Recovery Agent	File Recovery
Basic EFS	Encrypting File System
Domain Controller	Client Authentication, Server Authentication
Web Server	Server Authentication
Computer	Client Authentication, Server Authentication
User	Encrypting File System, Secure Email, Clien...
Subordinate Certification Authority	<All>
Administrator	Microsoft Trust List Signing, Encrypting File...

FIGURE 3.23 The CA Certificate Templates container.

6. Right-click Certificate Templates.
7. Click New and then click Certificate Template to Issue.
8. Select the Client Certificate Auto-Enrollment template from the list.
9. Hold down the Ctrl key.
10. Select the Server Certificate Auto-Enrollment template from the list.
11. Select the Configuration Manager OS Deployment template from the list.
12. Click OK to complete the process.

The three certificates should be listed in the Certificates Template container for the CA. These certificates are ready for consumption by Configuration Manager Site Servers and managed clients.

Configuring the Certificate Services Website for SSL

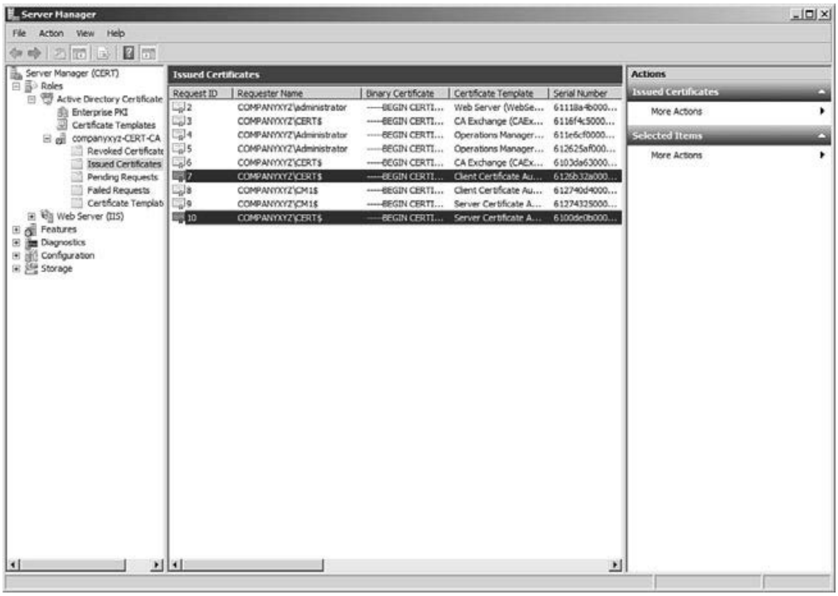
Certificates cannot be issued with the Certificate Services Enrollment web server unless it is configured to use SSL. This section describes the steps needed to secure the website with a server certificate. This also validates the ability for the certificate server to issue certificates.

To configure the Certificate Services website for SSL, complete the following tasks:

1. Open the command prompt on CERT.
2. Type **`gpupdate /force`** to refresh the group policies.
3. After the group policy is refreshed, open Server Manager.
4. Expand Roles.
5. Expand Active Directory Certificate Services.
6. Expand companyxyz-CERT-CA.
7. Select the Issued Certificates container.

The two new certificates should be listed in the container.

The CA Issued Certificates container is shown in Figure 3.24.



Issued Certificates

Request ID	Requester Name	Binary Certificate	Certificate Template	Serial Number
2	COMPANYXYZ\administrator	-----BEGIN CERTI...	Web Server (WebSe...	61118a4b000...
3	COMPANYXYZ\CERT$	-----BEGIN CERTI...	CA Exchange (CAEx...	6116f4c5000...
4	COMPANYXYZ\Administrator	-----BEGIN CERTI...	Operations Manager...	611e6cf0000...
5	COMPANYXYZ\Administrator	-----BEGIN CERTI...	Operations Manager...	612625af000...
6	COMPANYXYZ\CERT$	-----BEGIN CERTI...	CA Exchange (CAEx...	6103da63000...
7	COMPANYXYZ\CERT$	-----BEGIN CERTI...	Client Certificate Au...	6126b32a000...
8	COMPANYXYZ\CM1$	-----BEGIN CERTI...	Client Certificate Au...	612740d4000...
9	COMPANYXYZ\CM1$	-----BEGIN CERTI...	Server Certificate A...	61274325000...
10	COMPANYXYZ\CERT$	-----BEGIN CERTI...	Server Certificate A...	6100de0b000...

FIGURE 3.24 The CA Issued Certificates container.

The server CERT has received both the client and server signing certificate. The server signing certificate can be used to secure the Certificate Services website.

To secure the Certificate Services website, complete the following steps:

1. Open the Server Manager on CERT.
2. Expand Roles.
3. Expand Web Server (IIS).
4. Select Internet Information Services.
5. Expand the CERT web server.
6. Expand Sites.
7. Select Default Web Site.
8. Select Bindings from the Actions pane.
9. Click Add.
10. Select HTTPS for the binding type.
11. Select the correct certificate from the SSL certificate menu.
12. Click View to verify the correct certificate has been selected and then click OK.
13. Click OK and then click Close.

To test the newly installed certificate, open Internet Explorer and browse to the URL https://cert.companyxyz.com/certsrv. The Certificate Enrollment web page should open. Click the small lock icon beside the address bar, which shows the status of the certificate and that the Certificate Authority companyxyz-CERT-CA has identified this computer as cert.companyabc.com.

Configuring the WSUS Website for SSL

Because the WSUS component was installed on the CM1 server, the same certificate that was used to secure the Default Site can be used to secure the WSUS Administration site from within IIS.

CAUTION

Do *not* enable all virtual directories within the WSUS Administration site to use SSL. Only the APIRemoting30, ClientWebService, DSSAuthWebService, ServerSyncWebService, and SimpleAuthWebService should require SSL.

To configure WSUS for SSL communication, complete the following steps:

1. Open Internet Information Services Manager.
2. Expand Sites, and select the WSUS administration site, which is often the Default Web Site.
3. Click the Bindings action.

4. Click Add, select HTTPS, and click Edit.
5. Choose the certificate from the list.
6. Click View to verify the correct certificate was selected, click OK, and then click Close.
7. Select the APIRemoting30 virtual directory.
8. Double-click the SSL Settings option.
9. Enable the Require SSL option and click Apply.
10. Repeat for the ClientWebService, DSSAuthWebService, ServerSyncWebService, and SimpleAuthWebService virtual directories.

When the WSUS virtual directories are correctly configured, run the following command on the WSUS server to finalize the configuration needed to support SSL:

```
WSUSUtil.exe configuressl cm1.companyxyz.com
```

This utility is located in the Tools folder located within the WSUS installation folder. By default, this is folder is `c:\Program Files\Update Services\Tools`.

Requesting the OS Deployment Certificate

The OS Deployment client certificate is used by all systems during the OS deployment. This is essentially a shared certificate that is imported when the PXE Service Point is established.

The same procedure used to request the Document Signing certificate can be used to request the OS Deployment certificate. The main differences are instead of selecting the Configuration Manager Document Signing template from the template list, the Configuration Manager OS Deployment template must be selected. In the Name field, enter **`osd01.companyxyz.com`**.

NOTE

This certificate does *not* need to be added to the Local Computer certificate store. The Personal Information Exchange (PFX) file created will be imported during the deployment of the PXE Service Point detailed later.

Remember to approve the certificate osd1.companyxyz.com from within the Pending Requests container. When exporting the certificate, enter **`c:\Temp\OSD01.pfx`** as the file.

Enabling Internet-Based Client Management

In Configuration Manager 2012, the Site Servers roles have to be explicitly configured to enable Internet-based client management (IBCM). Each Management Point and Distribution Point that are to be enabled for IBCM will need to be configured to communicate over

HTTPS rather than HTTP. This is typically done on one or more systems dedicated to handling Internet traffic, but the actual configuration can depend on specific business and security requirements.

When a client communicates over the Internet, it needs to communicate with the following:

- Management Point
- Distribution Point
- Software Update Point
- Fallback Status Point
- Enrollment Proxy Point
- Application Catalog Website Point

All communication is done over HTTPS, with the exception of the Fallback Status Point, which communicates over HTTP. The first step in the process is to enable IBCM on the Site Server.

The FSP and SUP do not require additional configuration and are automatically enabled with the Site Server. Finally, to support IBCM, the following ports need to be open from the Internet:

- CRL Web Site: TCP 80
- Fallback Status Point: TCP 80
- Management Point: TCP 443
- Distribution Point: TCP 443
- Software Update Point: TCP 443

It is not recommended to connect any internal system directly to the Internet; for production deployments, consider using a reverse proxy, such as the Microsoft Threat Management Gateway (TMG).

Summary

System Center Configuration Manager 2012 provides a scalable, secure, end-to-end administration and reporting functionality. The deployment can be scaled out over many servers to support hundreds of thousands of managed clients, or installed on a single server for small enterprise deployments. In both cases, it is important to understand how each of the Configuration Manager roles work and the required dependencies for each role so the implementation is successful.

Best Practices

The following are best practices from this chapter:

- It is important to fully understand the architectural design before Configuration Manager 2012 server infrastructure servers and roles are deployed.
- If communication issues are a problem, make sure the settings on the local firewall have been configured correctly. For troubleshooting purposes, disable the local firewall temporarily.
- Status messages will still be sent to the Fallback Status Point, even if the client system has become orphaned due to certificate configuration issues. It is important to deploy the Fallback Status Point before deploying clients.
- Do not move domain controllers from the default OU. Moving domain controllers out of the default Domain Controllers OU is not supported. When an Enterprise Root CA is deployed, all domain controllers automatically receive a Domain Controller certificate. This certificate can be used for both client and server authentication.
- Provisioning certificates with unnecessary OIDs is not recommended. Only provision the minimum requirements needed by the client to communicate with Configuration Manager.
- The Windows Server 2008 Enterprise certificate option is not compatible with System Center Configuration Manager 2012. Choosing Windows Server 2008 Enterprise results in a version 3 template. To create a version 2 template, select Windows Server 2003 Enterprise.
- When a computer object is added to a group, it can take a long time for the setting to take effect. This is because the Kerberos ticket takes seven days to renew. The renewal time is governed by the Maximum Lifetime for User Ticket Renewal setting located in the Default Domain Policy GPO. It is not recommended to change this setting. Instead, restart the computer to refresh the Kerberos ticket.
- Make sure the subject name of the Site Servers' Document Signing certificate is set to: The site code of this Site Server is <SITE CODE>. The <SITE CODE> represents the site code that will be entered during the Configuration Manager implementation.
- Review the `ExtADSch.log` file for any errors after the AD schema has been extended. This log file is located in the root of drive C on the server used to execute the schema extensions. The log file should show 14 attributes and four classes have been defined.
- Do not bother with the WSUS Configuration Wizard. When the wizard opens after WSUS is successfully installed, click the Cancel button. The Configuration Manager console provides the interface to configure synchronization with Microsoft.

- Make sure the Configuration Manager Site Server Computer Account is in the local administrators group on all component servers and other Site Servers; this includes the Site Database server. The computer account of the Site Server is used to access and manage the remote server by default.
- The status summarizer for the different components is not automatically changed from red or yellow to green if the component that experienced the problem is fixed. The component summarizer simply counts the number of warning and error status messages that have been received. Manually reset the counts of status messages to clear the error or warning status.
- The `cmtrace.exe` log viewer provides a real-time view of the Configuration Manager status logs. This tool is invaluable when troubleshooting problems and understanding the environment.
- When deploying Site System roles to either the Site Server or a remote server, it is important to note the component installation wizard doesn't actually do the installation. Check the Site Status container from within the console along with the local installation logs for details on role installation.
- Increase the number of messages allowed per hour by the FSP to support large client deployments. This prevents a backlog of status messages from occurring.
- Never configure overlapping boundaries. This can cause managed systems to use the wrong Site Server or Distribution Point. This often happens when using a combination of IP and Active Directory boundaries.
- Define the Network Access Account on the Computer Client Agent when managing non–domain members. This account is provided as a way for non–domain members to authenticate to Configuration Manager. This account should be a Domain User without additional permissions.
- The default list of "Products" supported by the Software Update Point is refreshed and updated during the synchronization process. This adds things like Windows 7 and Windows Server 2008 R2 to the Windows section. Because the entire Windows product was selected, new operating systems will automatically be enabled as they are made available on the Windows Update site and through WSUS.
- Configuring Client Agents with a "simple" schedule allows the distribution of load placed on the system. Unless the server and environment have been sized to receive and process data from all clients simultaneously, care should be taken to distribute the load over a longer period.

This page intentionally left blank

Index

How can we make this index more useful? Email us at indexes@samspublishing.com

How can we make this index more useful? Email us at indexes@samspublishing.com

How can we make this index more useful? Email us at indexes@samspublishing.com

How can we make this index more useful? Email us at indexes@samspublishing.com

How can we make this index more useful? Email us at indexes@samspublishing.com

How can we make this index more useful? Email us at indexes@samspublishing.com