

OFFICIAL MICROSOFT LEARNING PRODUCT

6425B

Configuring and Troubleshooting Windows Server® 2008 Active Directory® Domain Services

Volume 2



Be sure to access the extended learning content on your
Course Companion CD enclosed on the back cover of the book.

Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, place or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The names of manufacturers, products, or URLs are provided for informational purposes only and Microsoft makes no representations and warranties, either expressed, implied, or statutory, regarding these manufacturers or the use of the products with any Microsoft technologies. The inclusion of a manufacturer or product does not imply endorsement of Microsoft of the manufacturer or product. Links may be provided to third party sites. Such sites are not under the control of Microsoft and Microsoft is not responsible for the contents of any linked site or any link contained in a linked site, or any changes or updates to such sites. Microsoft is not responsible for webcasting or any other form of transmission received from any linked site. Microsoft is providing these links to you only as a convenience, and the inclusion of any link does not imply endorsement of Microsoft of the site or the products contained therein.

© 2009 Microsoft Corporation. All rights reserved.

Microsoft, Access, Active Directory, ActiveX, Excel, Forefront, Hyper-V, Internet Explorer, MS, MSDN, Outlook, PowerPoint, Segoe, SharePoint, SQL Server, Visual Studio, Windows, Windows Live, Windows Mobile, Windows NT, Windows Server, and Windows Vista are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

All other trademarks are property of their respective owners.

Product Number: 6425B

Part Number: X16-23529

Released: 11/2009

MICROSOFT LICENSE TERMS

OFFICIAL MICROSOFT LEARNING PRODUCTS - TRAINER

EDITION – Pre-Release and Final Release Versions

These license terms are an agreement between Microsoft Corporation and you. Please read them. They apply to the Licensed Content named above, which includes the media on which you received it, if any. The terms also apply to any Microsoft

- updates,
- supplements,
- Internet-based services, and
- support services

for this Licensed Content, unless other terms accompany those items. If so, those terms apply.

By using the Licensed Content, you accept these terms. If you do not accept them, do not use the Licensed Content.

If you comply with these license terms, you have the rights below.

1. DEFINITIONS.

- "Academic Materials"** means the printed or electronic documentation such as manuals, workbooks, white papers, press releases, datasheets, and FAQs which may be included in the Licensed Content.
- "Authorized Learning Center(s)"** means a Microsoft Certified Partner for Learning Solutions location, an IT Academy location, or such other entity as Microsoft may designate from time to time.
- "Authorized Training Session(s)"** means those training sessions authorized by Microsoft and conducted at or through Authorized Learning Centers by a Trainer providing training to Students solely on Official Microsoft Learning Products (formerly known as Microsoft Official Curriculum or "MOC") and Microsoft Dynamics Learning Products (formerly known as Microsoft Business Solutions Courseware). Each Authorized Training Session will provide training on the subject matter of one (1) Course.
- "Course"** means one of the courses using Licensed Content offered by an Authorized Learning Center during an Authorized Training Session, each of which provides training on a particular Microsoft technology subject matter.
- "Device(s)"** means a single computer, device, workstation, terminal, or other digital electronic or analog device.
- "Licensed Content"** means the materials accompanying these license terms. The Licensed Content may include, but is not limited to, the following elements: (i) Trainer Content, (ii) Student Content, (iii) classroom setup guide, and (iv) Software. There are different and separate components of the Licensed Content for each Course.
- "Software"** means the Virtual Machines and Virtual Hard Disks, or other software applications that may be included with the Licensed Content.
- "Student(s)"** means a student duly enrolled for an Authorized Training Session at your location.

- i. **"Student Content"** means the learning materials accompanying these license terms that are for use by Students and Trainers during an Authorized Training Session. Student Content may include labs, simulations, and courseware files for a Course.
- j. **"Trainer(s)"** means a) a person who is duly certified by Microsoft as a Microsoft Certified Trainer and b) such other individual as authorized in writing by Microsoft and has been engaged by an Authorized Learning Center to teach or instruct an Authorized Training Session to Students on its behalf.
- k. **"Trainer Content"** means the materials accompanying these license terms that are for use by Trainers and Students, as applicable, solely during an Authorized Training Session. Trainer Content may include Virtual Machines, Virtual Hard Disks, Microsoft PowerPoint files, instructor notes, and demonstration guides and script files for a Course.
- l. **"Virtual Hard Disks"** means Microsoft Software that is comprised of virtualized hard disks (such as a base virtual hard disk or differencing disks) for a Virtual Machine that can be loaded onto a single computer or other device in order to allow end-users to run multiple operating systems concurrently. For the purposes of these license terms, Virtual Hard Disks will be considered "Trainer Content".
- m. **"Virtual Machine"** means a virtualized computing experience, created and accessed using Microsoft® Virtual PC or Microsoft® Virtual Server software that consists of a virtualized hardware environment, one or more Virtual Hard Disks, and a configuration file setting the parameters of the virtualized hardware environment (e.g., RAM). For the purposes of these license terms, Virtual Hard Disks will be considered "Trainer Content".
- n. **"you"** means the Authorized Learning Center or Trainer, as applicable, that has agreed to these license terms.

2. OVERVIEW.

Licensed Content. The Licensed Content includes Software, Academic Materials (online and electronic), Trainer Content, Student Content, classroom setup guide, and associated media.

License Model. The Licensed Content is licensed on a per copy per Authorized Learning Center location or per Trainer basis.

3. INSTALLATION AND USE RIGHTS.

- a. **Authorized Learning Centers and Trainers: For each Authorized Training Session, you may:**
 - i. either install individual copies of the relevant Licensed Content on classroom Devices only for use by Students enrolled in and the Trainer delivering the Authorized Training Session, provided that the number of copies in use does not exceed the number of Students enrolled in and the Trainer delivering the Authorized Training Session, **OR**
 - ii. install one copy of the relevant Licensed Content on a network server only for access by classroom Devices and only for use by Students enrolled in and the Trainer delivering the Authorized Training Session, provided that the number of Devices accessing the Licensed Content on such server does not exceed the number of Students enrolled in and the Trainer delivering the Authorized Training Session.
 - iii. and allow the Students enrolled in and the Trainer delivering the Authorized Training Session to use the Licensed Content that you install in accordance with (i) or (ii) above during such Authorized Training Session in accordance with these license terms.

- i. **Separation of Components.** The components of the Licensed Content are licensed as a single unit. You may not separate the components and install them on different Devices.
- ii. **Third Party Programs.** The Licensed Content may contain third party programs. These license terms will apply to the use of those third party programs, unless other terms accompany those programs.

b. Trainers:

- i. Trainers may Use the Licensed Content that you install or that is installed by an Authorized Learning Center on a classroom Device to deliver an Authorized Training Session.
- ii. Trainers may also Use a copy of the Licensed Content as follows:
 - A. **Licensed Device.** The licensed Device is the Device on which you Use the Licensed Content. You may install and Use one copy of the Licensed Content on the licensed Device solely for your own personal training Use and for preparation of an Authorized Training Session.
 - B. **Portable Device.** You may install another copy on a portable device solely for your own personal training Use and for preparation of an Authorized Training Session.

4. PRE-RELEASE VERSIONS. If this is a pre-release ("beta") version, in addition to the other provisions in this agreement, these terms also apply:

- a. **Pre-Release Licensed Content.** This Licensed Content is a pre-release version. It may not contain the same information and/or work the way a final version of the Licensed Content will. We may change it for the final, commercial version. We also may not release a commercial version. You will clearly and conspicuously inform any Students who participate in each Authorized Training Session of the foregoing; and, that you or Microsoft are under no obligation to provide them with any further content, including but not limited to the final released version of the Licensed Content for the Course.
- b. **Feedback.** If you agree to give feedback about the Licensed Content to Microsoft, you give to Microsoft, without charge, the right to use, share and commercialize your feedback in any way and for any purpose. You also give to third parties, without charge, any patent rights needed for their products, technologies and services to use or interface with any specific parts of a Microsoft software, Licensed Content, or service that includes the feedback. You will not give feedback that is subject to a license that requires Microsoft to license its software or documentation to third parties because we include your feedback in them. These rights survive this agreement.
- c. **Confidential Information.** The Licensed Content, including any viewer, user interface, features and documentation that may be included with the Licensed Content, is confidential and proprietary to Microsoft and its suppliers.
 - i. **Use.** For five years after installation of the Licensed Content or its commercial release, whichever is first, you may not disclose confidential information to third parties. You may disclose confidential information only to your employees and consultants who need to know the information. You must have written agreements with them that protect the confidential information at least as much as this agreement.
 - ii. **Survival.** Your duty to protect confidential information survives this agreement.
 - iii. **Exclusions.** You may disclose confidential information in response to a judicial or governmental order. You must first give written notice to Microsoft to allow it to seek a

protective order or otherwise protect the information. Confidential information does not include information that

- becomes publicly known through no wrongful act;
 - you received from a third party who did not breach confidentiality obligations to Microsoft or its suppliers; or
 - you developed independently.
- d. **Term.** The term of this agreement for pre-release versions is (i) the date which Microsoft informs you is the end date for using the beta version, or (ii) the commercial release of the final release version of the Licensed Content, whichever is first ("beta term").
- e. **Use.** You will cease using all copies of the beta version upon expiration or termination of the beta term, and will destroy all copies of same in the possession or under your control and/or in the possession or under the control of any Trainers who have received copies of the pre-released version.
- f. **Copies.** Microsoft will inform Authorized Learning Centers if they may make copies of the beta version (in either print and/or CD version) and distribute such copies to Students and/or Trainers. If Microsoft allows such distribution, you will follow any additional terms that Microsoft provides to you for such copies and distribution.

5. ADDITIONAL LICENSING REQUIREMENTS AND/OR USE RIGHTS.

a. Authorized Learning Centers and Trainers:

i. Software.

ii. **Virtual Hard Disks.** The Licensed Content may contain versions of Microsoft XP, Microsoft Windows Vista, Windows Server 2003, Windows Server 2008, and Windows 2000 Advanced Server and/or other Microsoft products which are provided in Virtual Hard Disks.

A. If the Virtual Hard Disks and the labs are launched through the Microsoft Learning Lab Launcher, then these terms apply:

Time-Sensitive Software. If the Software is not reset, it will stop running based upon the time indicated on the install of the Virtual Machines (between 30 and 500 days after you install it). You will not receive notice before it stops running. You may not be able to access data used or information saved with the Virtual Machines when it stops running and may be forced to reset these Virtual Machines to their original state. You must remove the Software from the Devices at the end of each Authorized Training Session and reinstall and launch it prior to the beginning of the next Authorized Training Session.

B. If the Virtual Hard Disks require a product key to launch, then these terms apply:

Microsoft will deactivate the operating system associated with each Virtual Hard Disk. Before installing any Virtual Hard Disks on classroom Devices for use during an Authorized Training Session, you will obtain from Microsoft a product key for the operating system software for the Virtual Hard Disks and will activate such Software with Microsoft using such product key.

C. These terms apply to all Virtual Machines and Virtual Hard Disks:

You may only use the Virtual Machines and Virtual Hard Disks if you comply with the terms and conditions of this agreement and the following security requirements:

- You may not install Virtual Machines and Virtual Hard Disks on portable Devices or Devices that are accessible to other networks.
 - You must remove Virtual Machines and Virtual Hard Disks from all classroom Devices at the end of each Authorized Training Session, except those held at Microsoft Certified Partners for Learning Solutions locations.
 - You must remove the differencing drive portions of the Virtual Hard Disks from all classroom Devices at the end of each Authorized Training Session at Microsoft Certified Partners for Learning Solutions locations.
 - You will ensure that the Virtual Machines and Virtual Hard Disks are not copied or downloaded from Devices on which you installed them.
 - You will strictly comply with all Microsoft instructions relating to installation, use, activation and deactivation, and security of Virtual Machines and Virtual Hard Disks.
 - You may not modify the Virtual Machines and Virtual Hard Disks or any contents thereof.
 - You may not reproduce or redistribute the Virtual Machines or Virtual Hard Disks.
- ii. Classroom Setup Guide.** You will assure any Licensed Content installed for use during an Authorized Training Session will be done in accordance with the classroom set-up guide for the Course.
- iii. Media Elements and Templates.** You may allow Trainers and Students to use images, clip art, animations, sounds, music, shapes, video clips and templates provided with the Licensed Content solely in an Authorized Training Session. If Trainers have their own copy of the Licensed Content, they may use Media Elements for their personal training use.
- iv. iv Evaluation Software.** Any Software that is included in the Student Content designated as "Evaluation Software" may be used by Students solely for their personal training outside of the Authorized Training Session.

b. Trainers Only:

- i. Use of PowerPoint Slide Deck Templates.** The Trainer Content may include Microsoft PowerPoint slide decks. Trainers may use, copy and modify the PowerPoint slide decks only for providing an Authorized Training Session. If you elect to exercise the foregoing, you will agree or ensure Trainer agrees: (a) that modification of the slide decks will not constitute creation of obscene or scandalous works, as defined by federal law at the time the work is created; and (b) to comply with all other terms and conditions of this agreement.
- ii. Use of Instructional Components in Trainer Content.** For each Authorized Training Session, Trainers may customize and reproduce, in accordance with the MCT Agreement, those portions of the Licensed Content that are logically associated with instruction of the Authorized Training Session. If you elect to exercise the foregoing rights, you agree or ensure the Trainer agrees: (a) that any of these customizations or reproductions will only be used for providing an Authorized Training Session and (b) to comply with all other terms and conditions of this agreement.

iii. Academic Materials. If the Licensed Content contains Academic Materials, you may copy and use the Academic Materials. You may not make any modifications to the Academic Materials and you may not print any book (either electronic or print version) in its entirety. If you reproduce any Academic Materials, you agree that:

- The use of the Academic Materials will be only for your personal reference or training use
- You will not republish or post the Academic Materials on any network computer or broadcast in any media;
- You will include the Academic Material's original copyright notice, or a copyright notice to Microsoft's benefit in the format provided below:

Form of Notice:

© 2009 Reprinted for personal reference use only with permission by Microsoft Corporation. All rights reserved.

Microsoft, Windows, and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the US and/or other countries. Other product and company names mentioned herein may be the trademarks of their respective owners.

6. INTERNET-BASED SERVICES. Microsoft may provide Internet-based services with the Licensed Content. It may change or cancel them at any time. You may not use these services in any way that could harm them or impair anyone else's use of them. You may not use the services to try to gain unauthorized access to any service, data, account or network by any means.

7. SCOPE OF LICENSE. The Licensed Content is licensed, not sold. This agreement only gives you some rights to use the Licensed Content. Microsoft reserves all other rights. Unless applicable law gives you more rights despite this limitation, you may use the Licensed Content only as expressly permitted in this agreement. In doing so, you must comply with any technical limitations in the Licensed Content that only allow you to use it in certain ways. You may not

- install more copies of the Licensed Content on classroom Devices than the number of Students and the Trainer in the Authorized Training Session;
- allow more classroom Devices to access the server than the number of Students enrolled in and the Trainer delivering the Authorized Training Session if the Licensed Content is installed on a network server;
- copy or reproduce the Licensed Content to any server or location for further reproduction or distribution;
- disclose the results of any benchmark tests of the Licensed Content to any third party without Microsoft's prior written approval;
- work around any technical limitations in the Licensed Content;
- reverse engineer, decompile or disassemble the Licensed Content, except and only to the extent that applicable law expressly permits, despite this limitation;
- make more copies of the Licensed Content than specified in this agreement or allowed by applicable law, despite this limitation;
- publish the Licensed Content for others to copy;

- transfer the Licensed Content, in whole or in part, to a third party;
 - access or use any Licensed Content for which you (i) are not providing a Course and/or (ii) have not been authorized by Microsoft to access and use;
 - rent, lease or lend the Licensed Content; or
 - use the Licensed Content for commercial hosting services or general business purposes.
 - Rights to access the server software that may be included with the Licensed Content, including the Virtual Hard Disks does not give you any right to implement Microsoft patents or other Microsoft intellectual property in software or devices that may access the server.
- 8. EXPORT RESTRICTIONS.** The Licensed Content is subject to United States export laws and regulations. You must comply with all domestic and international export laws and regulations that apply to the Licensed Content. These laws include restrictions on destinations, end users and end use. For additional information, see www.microsoft.com/exporting.
- 9. NOT FOR RESALE SOFTWARE/LICENSED CONTENT.** You may not sell software or Licensed Content marked as "NFR" or "Not for Resale."
- 10. ACADEMIC EDITION.** You must be a "Qualified Educational User" to use Licensed Content marked as "Academic Edition" or "AE." If you do not know whether you are a Qualified Educational User, visit www.microsoft.com/education or contact the Microsoft affiliate serving your country.
- 11. TERMINATION.** Without prejudice to any other rights, Microsoft may terminate this agreement if you fail to comply with the terms and conditions of these license terms. In the event your status as an Authorized Learning Center or Trainer a) expires, b) is voluntarily terminated by you, and/or c) is terminated by Microsoft, this agreement shall automatically terminate. Upon any termination of this agreement, you must destroy all copies of the Licensed Content and all of its component parts.
- 12. ENTIRE AGREEMENT.** This agreement, and the terms for supplements, updates, Internet-based services and support services that you use, are the entire agreement for the Licensed Content and support services.
- 13. APPLICABLE LAW.**
- a. **United States.** If you acquired the Licensed Content in the United States, Washington state law governs the interpretation of this agreement and applies to claims for breach of it, regardless of conflict of laws principles. The laws of the state where you live govern all other claims, including claims under state consumer protection laws, unfair competition laws, and in tort.
 - b. **Outside the United States.** If you acquired the Licensed Content in any other country, the laws of that country apply.
- 14. LEGAL EFFECT.** This agreement describes certain legal rights. You may have other rights under the laws of your country. You may also have rights with respect to the party from whom you acquired the Licensed Content. This agreement does not change your rights under the laws of your country if the laws of your country do not permit it to do so.
- 15. DISCLAIMER OF WARRANTY.** The Licensed Content is licensed "as-is." You bear the risk of using it. Microsoft gives no express warranties, guarantees or conditions. You may have additional consumer rights under your local laws which this agreement cannot change. To the extent permitted under your local laws, Microsoft excludes the implied warranties of merchantability, fitness for a particular purpose and non-infringement.

16. LIMITATION ON AND EXCLUSION OF REMEDIES AND DAMAGES. YOU CAN RECOVER FROM MICROSOFT AND ITS SUPPLIERS ONLY DIRECT DAMAGES UP TO U.S. \$5.00. YOU CANNOT RECOVER ANY OTHER DAMAGES, INCLUDING CONSEQUENTIAL, LOST PROFITS, SPECIAL, INDIRECT OR INCIDENTAL DAMAGES.

This limitation applies to

- anything related to the Licensed Content, software, services, content (including code) on third party Internet sites, or third party programs; and
- claims for breach of contract, breach of warranty, guarantee or condition, strict liability, negligence, or other tort to the extent permitted by applicable law.

It also applies even if Microsoft knew or should have known about the possibility of the damages. The above limitation or exclusion may not apply to you because your country may not allow the exclusion or limitation of incidental, consequential or other damages.

Please note: As this Licensed Content is distributed in Quebec, Canada, some of the clauses in this agreement are provided below in French.

Remarque : Ce le contenu sous licence étant distribué au Québec, Canada, certaines des clauses dans ce contrat sont fournies ci-dessous en français.

EXONÉRATION DE GARANTIE. Le contenu sous licence visé par une licence est offert « tel quel ». Toute utilisation de ce contenu sous licence est à votre seule risque et péril. Microsoft n'accorde aucune autre garantie expresse. Vous pouvez bénéficier de droits additionnels en vertu du droit local sur la protection des consommateurs, que ce contrat ne peut modifier. La ou elles sont permises par le droit local, les garanties implicites de qualité marchande, d'adéquation à un usage particulier et d'absence de contrefaçon sont exclues.

LIMITATION DES DOMMAGES-INTÉRÊTS ET EXCLUSION DE RESPONSABILITÉ POUR LES DOMMAGES. Vous pouvez obtenir de Microsoft et de ses fournisseurs une indemnisation en cas de dommages directs uniquement à hauteur de 5,00 \$ US. Vous ne pouvez prétendre à aucune indemnisation pour les autres dommages, y compris les dommages spéciaux, indirects ou accessoires et pertes de bénéfices.

Cette limitation concerne:

- tout ce qui est relié au le contenu sous licence , aux services ou au contenu (y compris le code) figurant sur des sites Internet tiers ou dans des programmes tiers ; et
- les réclamations au titre de violation de contrat ou de garantie, ou au titre de responsabilité stricte, de négligence ou d'une autre faute dans la limite autorisée par la loi en vigueur.

Elle s'applique également, même si Microsoft connaissait ou devrait connaître l'éventualité d'un tel dommage. Si votre pays n'autorise pas l'exclusion ou la limitation de responsabilité pour les dommages indirects, accessoires ou de quelque nature que ce soit, il se peut que la limitation ou l'exclusion ci-dessus ne s'appliquera pas à votre égard.

EFFET JURIDIQUE. Le présent contrat décrit certains droits juridiques. Vous pourriez avoir d'autres droits prévus par les lois de votre pays. Le présent contrat ne modifie pas les droits que vous confèrent les lois de votre pays si celles-ci ne le permettent pas.

Welcome!

Thank you for taking our training! We've worked together with our Microsoft Certified Partners for Learning Solutions and our Microsoft IT Academies to bring you a world-class learning experience—whether you're a professional looking to advance your skills or a student preparing for a career in IT.

- **Microsoft Certified Trainers and Instructors**—Your instructor is a technical and instructional expert who meets ongoing certification requirements. And, if instructors are delivering training at one of our Certified Partners for Learning Solutions, they are also evaluated throughout the year by students and by Microsoft.
- **Certification Exam Benefits**—After training, consider taking a Microsoft Certification exam. Microsoft Certifications validate your skills on Microsoft technologies and can help differentiate you when finding a job or boosting your career. In fact, independent research by IDC concluded that 75% of managers believe certifications are important to team performance¹. Ask your instructor about Microsoft Certification exam promotions and discounts that may be available to you.
- **Customer Satisfaction Guarantee**—Our Certified Partners for Learning Solutions offer a satisfaction guarantee and we hold them accountable for it. At the end of class, please complete an evaluation of today's experience. We value your feedback!

We wish you a great learning experience and ongoing success in your career!

Sincerely,

Microsoft Learning
www.microsoft.com/learning

Microsoft | Learning

¹ IDC, Value of Certification: Team Certification and Organizational Performance, November 2006

Acknowledgement

Microsoft® Learning would like to acknowledge and thank the following for their contribution towards developing this title. Their effort at various stages in the development has ensured that you have a good classroom experience.

Dan Holme – Subject Matter Expert

A graduate of Yale University and Thunderbird, Dan has spent 15 years as a consultant and trainer, delivering solutions to tens of thousands of IT professionals from the most prestigious organizations and corporations around the world. Dan's company, Intelliem, is a boutique consulting and training firm with a *Fortune*-caliber clientele and deep expertise and experience in Windows®, Active Directory®, and Microsoft Office SharePoint®. From his base in beautiful Maui, Dan travels around the globe supporting customers and delivering Microsoft technologies training. Dan is also a contributing editor for *Windows IT Pro* magazine, a Microsoft MVP (Windows Server® Directory Services, 2007, and Office SharePoint Server, 2008-2009), and the community lead of SharePointProConnections.com. Last year, Dan published two books with Microsoft Press: the *Windows Administration Resource Kit* and the training kit for the 70-640 MCTS exam, both of which are at the top of the bestseller list for Windows books. He is currently building SharePoint solutions to support the broadcast of the 2010 Winter Olympics in Vancouver as the Microsoft Technologies Consultant for NBC Olympics, a role he played last year in Beijing and previously in Torino.

Claudia Woods – Technical Reviewer

Claudia has been a LAN Administrator, Systems Engineer and Technology Instructor for more than 10 years. As such, she has designed, implemented, and documented technology solutions for a variety of customers. Claudia has also written, edited, and presented customized technology courses for several organizations in the United States. She is a regular attendee at IT events such as TechEd, MCT Summit, and FOSE.

Originally hailing from the southeastern region of the United States, Claudia currently resides in the United Kingdom. She is a staff instructor with an international technology training firm. Her Microsoft specialties include Windows Server, Active Directory, and Exchange Messaging.

Ryan Boswell – Technical Reviewer

Ryan has worked as a Systems Engineer, IT Consultant, and Technology Instructor for more than 10 years. He holds several Microsoft certifications, including multiple levels of MCSE, MCTS, MCITP, and MCT. His specialties include Windows Server technologies, Active Directory, System Center Configuration Manager, System Center Operations Manager, and Microsoft Hyper-V™. Ryan currently resides in Denver, Colorado.

Contents

Module 10: Configure Domain Name System (DNS)

Lesson 1: Review of DNS Concepts, Components and Processes	10-4
Lesson 2: Install and Configure DNS Server in an AD DS Domain	10-25
Lab A: Install the DNS Service	10-38
Lesson 3: AD DS, DNS, and Windows	10-43
Lesson 4: Advanced DNS Configuration and Administration	10-68
Lab B: Advanced Configuration of DNS	10-81

Module 11: Administer Active Directory® Domain Services (AD DS) Domain Controllers (DCs)

Lesson 1: Domain Controller Installation Options	11-4
Lab A: Install Domain Controllers	11-31
Lesson 2: Install a Server Core DC	11-39
Lab B: Install a Server Core DC	11-47
Lesson 3: Manage Operations Masters	11-52
Lab C: Transfer Operations Master Roles	11-71
Lesson 4: Configure DFS-R Replication of SYSVOL	11-76
Lab D: Configure DFS-R Replication of SYSVOL	11-84

Module 12: Manage Sites and Active Directory Replication

Lesson 1: Configure Sites and Subnets	12-4
Lab A: Configure Sites and Subnets	12-22
Lesson 2: Configure the Global Catalog and Application Partitions	12-26
Lab B: Configure the Global Catalog and Application Partitions	12-41
Lesson 3: Configure Replication	12-46
Lab C: Configure Replication	12-73

Module 13: Directory Service Continuity

Lesson 1: Monitor Active Directory	13-4
Lab A: Monitor Active Directory Events and Performance	13-29
Lesson 2: Manage the Active Directory Database	13-45
Lab B: Manage the Active Directory Database	13-64
Lesson 3: Back Up and Restore AD DS and Domain Controllers	13-72
Lab C: Back Up and Restore Active Directory	13-86

Module 14: Manage Multiple Domains and Forests

Lesson 1: Configure Domain and Forest Functional Levels	14-4
Lab A: Raise Domain and Forest Functional Levels	14-16
Lesson 2: Manage Multiple Domains and Trust Relationships	14-23
Lab B: Administer a Trust Relationship	14-68

Lab Answer Keys

Module 1 Lab: Install an AD DS DC to Create a Single Domain Forest	L1-1
Module 2 Lab A: Create and Run a Custom Administrative Console	L2-11
Module 2 Lab B: Find Objects in Active Directory	L2-22
Module 2 Lab C: Use DS Commands to Administer Active Directory	L2-30
Module 3 Lab A: Create and Administer User Accounts	L3-35
Module 3 Lab B: Configure User Object Attributes	L3-42
Module 3 Lab C: Automate User Account Creation	L3-52
Module 4 Lab A: Administer Groups	L4-57
Module 4 Lab B: Best Practices for Group Management	L4-66
Module 5 Lab A: Create Computers and Joining the Domain	L5-71
Module 5 Lab B: Administer Computer Objects and Accounts	L5-84
Module 6 Lab A: Implement Group Policy	L6-91
Module 6 Lab B: Manage Settings and GPOs	L6-96
Module 6 Lab C: Manage Group Policy Scope	L6-106
Module 6 Lab D: Troubleshoot Policy Application	L6-116

Module 7 Lab A: Delegate the Support of Computers	L7-125
Module 7 Lab B: Manage Security Settings	L7-131
Module 7 Lab C: Manage Software with GPSI	L7-146
Module 7 Lab D: Audit File System Access	L7-158
Module 8 Lab A: Delegate Administration	L8-165
Module 8 Lab B: Audit Active Directory Changes	L8-178
Module 9 Lab A: Configure Password and Account Lockout Policies	L9-185
Module 9 Lab B: Audit Authentication	L9-193
Module 9 Lab C: Configure Read-Only Domain Controllers	L9-200
Module 10 Lab A: Install the DNS Service	L10-211
Module 10 Lab B: Advanced Configuration of DNS	L10-219
Module 11 Lab A: Install Domain Controllers	L11-229
Module 11 Lab B: Install a Server Core DC	L11-241
Module 11 Lab C: Transfer Operations Master Roles	L11-245
Module 11 Lab D: Configure DFS-R Replication of SYSVOL	L11-252
Module 12 Lab A: Configure Sites and Subnets	L12-263
Module 12 Lab B: Configure the Global Catalog and Application Partitions	L12-271
Module 12 Lab C: Configure Replication	L12-277
Module 13 Lab A: Monitor Active Directory Events and Performance	L13-287
Module 13 Lab B: Manage the Active Directory Database	L13-312
Module 13 Lab C: Backup and Restore Active Directory	L13-322
Module 14 Lab A: Raise Domain and Forest Functional Levels	L14-331
Module 14 Lab B: Administer a Trust Relationship	L14-340

Module 10

Configure Domain Name System (DNS)

Contents:

Lesson 1: Review of DNS Concepts, Components and Processes	10-4
Lesson 2: Install and Configure DNS Server in an AD DS Domain	10-25
Lab A: Install the DNS Service	10-38
Lesson 3: AD DS, DNS, and Windows	10-43
Lesson 4: Advanced DNS Configuration and Administration	10-68
Lab B: Advanced Configuration of DNS	10-81

Module Overview

- Review of DNS Concepts, Components, and Processes
- Install and Configure DNS in an AD DS Domain
- AD DS, DNS, and Windows
- Advanced DNS Configuration and Administration

Windows® and Active Directory® services have a strong dependency on Domain Name System (DNS). You are, no doubt, familiar with DNS as a user of DNS and as an IT professional supporting users, applications, services, and systems that rely on it. In this module, you will learn how to implement DNS to support name resolution both within your Active Directory Domain Services (AD DS) domain and outside your domain and your intranet.

Objectives

After completing this module, you will be able to:

- Understand the structure role, structure, and functionality of DNS.
- Describe client and server name resolution processes.
- Install DNS.
- Manage DNS records.
- Configure DNS server settings.

- Understand the integration between AD DS and DNS.
- Choose a DNS domain for an Active Directory domain.
- Create a zone delegation for a new Active Directory domain.
- Configure replication for Active Directory-integrated zones.
- Describe the purpose of Service Locator (SRV) records in the domain controller location process.
- Understand read-only DNS servers.
- Understand and configure single-label name resolution.
- Configure advanced DNS server settings.
- Audit, maintain, and troubleshoot the DNS server role.

Lesson 1

Review of DNS Concepts, Components, and Processes

- Why DNS?
- The DNS Hierarchy
- Zones
- Resource Records (RRs)
- Resource Record Management
- Zone Replication
- Subdomains
- Placing DNS Servers and Zones
- DNS Client (Resolver)
- Query to DNS Server
- DNS Server Resolution
- Recursion

DNS is an integral and critical component of a Windows enterprise. In this lesson, you will review the role, structure, and functionality of DNS. You will also explore in detail the processes used to resolve DNS queries. Although some or much of this information should be familiar to you, the lesson will serve to ensure that you are fully aware of the concepts and terminology related to DNS.

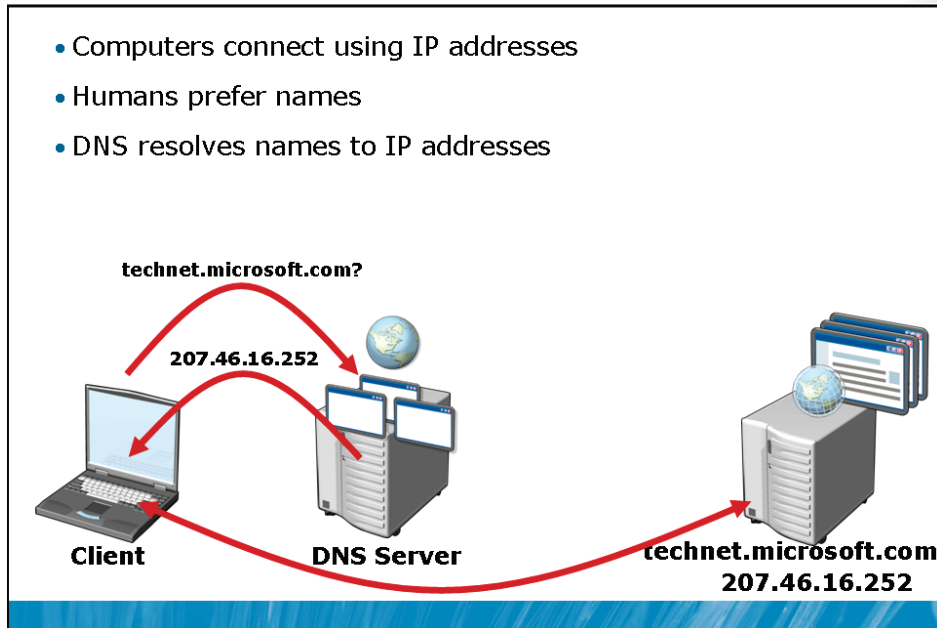
Objectives

After completing this lesson, you will be able to:

- Understand the structure role, structure, and functionality of DNS.
- Describe client and server name resolution processes.

Why DNS?

- Computers connect using IP addresses
- Humans prefer names
- DNS resolves names to IP addresses

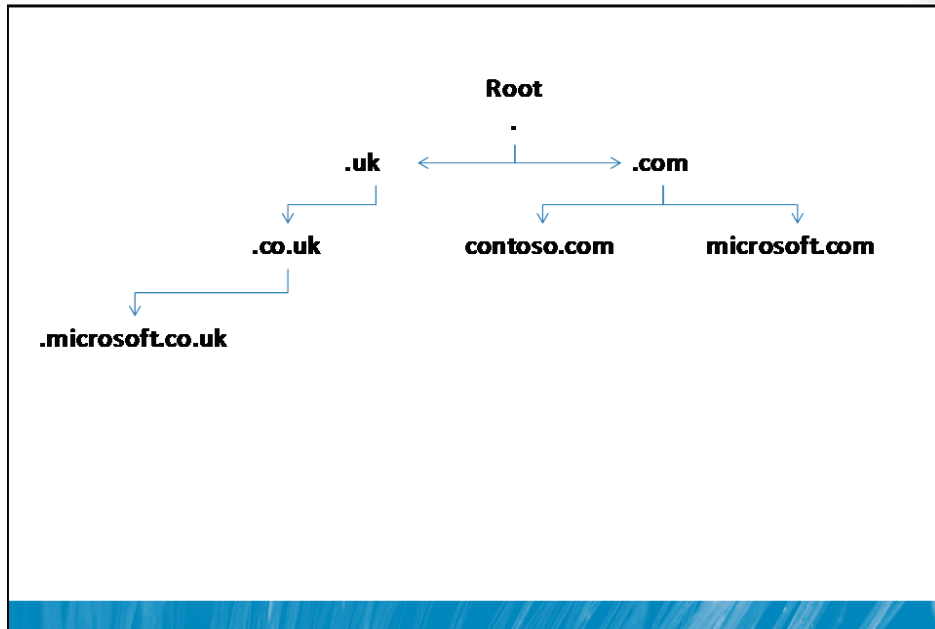


Key Points

DNS is used to resolve client queries for information about remote systems and services. Most commonly, DNS is used to resolve a client's query for the address of a specified DNS name.

Users and, therefore, applications tend to prefer to use names to refer to systems. Computers, however, locate each other with their IP addresses. DNS serves to resolve names to addresses. For example, if a user is browsing to <http://technet.microsoft.com>, the name `technet.microsoft.com` must be resolved to the IP address of the appropriate Web server. The client queries its DNS server and, through a series of processes that will be explained as this lesson progresses, the DNS server returns the IP address of the Web server: `207.46.16.252`.

The DNS Hierarchy



Key Points

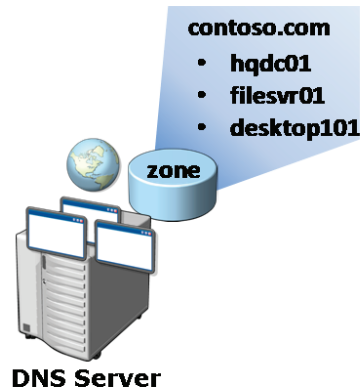
The names used in DNS create a hierarchy, from a root through a series of namespaces called *domains* to an individual record for a system (host) or service. A name such as *technet.microsoft.com* is read by humans from left to right, from the most specific part of the name—the individual host name, *technet*—to the most generic part of the name, *com*. The name can be resolved by starting at the root of the DNS namespace through the most generic, top-level domain (*com*), through the more specific domain (*microsoft*) to the most specific host name (*technet*).

Top-level domains (TLDs) such as *.com* are highly regulated by Internet authorities—there are a limited number of available TLDs, including *.com*, *.net*, *.org*, *.gov*, *.mil*, and *.edu*. Each country also has an ISO-based TLD, including *.us*, *.ca*, *.uk*, *.au*, and *.za*.

Above each of these TLDs is the root of the DNS namespace, which is actually represented by a dot ("."). The root dot is generally left out of DNS names, but it is interesting to note that *technet.microsoft.com* would be more accurately represented as *technet.microsoft.com.*, with the trailing dot.

Zones

- A database stored on a DNS server
- Supports resolution for a portion of the DNS namespace starting with a domain: contoso.com
- A server hosting a zone for a domain is authoritative for that domain



Key Points

For a DNS server to be able to resolve queries from clients—for example, to return a client's query for the IP address of another computer—the DNS server must have a database. This database is called a *zone*. A zone is a database that supports resolution for a distinct portion of the DNS namespace, starting with a specific domain such as contoso.com.

A server that hosts a zone for a domain is *authoritative* for that domain.

Resource Records (RRs)

- **Host or Address (A or AAAA) : name-to-IPv4/IPv6 address**
 - Name: hqdc01
 - Data: 10.0.0.11
- **Alias or Canonical Name (CNAME) : alias-to-name**
 - Name: ftp
 - Data: internetserver.contoso.com
- **Mail Exchange (MX): points to the e-mail server**
 - Data: exchange.contoso.com
- **Name service (NS): points to a name server**
 - Name: contoso.com
 - Data: nameserver01.contoso.com

Key Points

Within a zone—the DNS database—are records called *resource records (RRs)*.

There are several types of resource records, including:

- **Address (A or AAAA) (also known as "Host") records.** These records resolve a name to an IP address, and are used in the standard "DNS query" that you associate with DNS. A records resolve a name to an IPv4 address. AAAA records resolve a name to an IPv6 address.
- **Canonical Name (CNAME) (also known as "Alias") records.** These records map an alias to another fully qualified name. Alias records allow you to associate multiple names with a single server, and prevent you from having to manually update each record when the server's IP address changes. You can simply change the server's A record, and all CNAME records (which refer to the server by name, not by address) will continue to function.

- **Mail Exchange (MX) records.** The MX record contains the name of the e-mail server of a domain. You can think of MX as a type of alias, except that the alias is always called "MX." This is so that, no matter what language or naming standard is used by a domain, its mail server can always be located with a query for MX.domain.
- **Name Service (NS) records.** These records point to the authoritative DNS servers for a domain.

Resource Record Management

- Manual
- Dynamic
 - Client registers its own records
 - Secure dynamic updates: prevents spoofing

Key Points

The resource records in a zone can be created and maintained *manually* by an administrator.

Alternatively, *dynamic updates* can be enabled, through which systems are able to register their own DNS records.

If a zone is opened up for dynamic updates, there is a possibility for a rogue record to be created. For example, someone could create a record named `www` that points to a server other than the correct Web server for a domain. This is called *spoofing*.

In order to reduce the possibility of spoofing, Windows Server DNS supports *secure dynamic updates*. Clients must be authenticated to the domain in order to make an update to the DNS zone, and clients can only update their own DNS records.

Zone Replication

- **File-based zone**
 - Primary zone: writable copy of the zone hosted by one (and only one) DNS server
 - Secondary zone: read-only copy of the zone hosted by zero or more DNS servers
 - Zone transfer copies zone data from primary zone to secondary zones
 - Requires permission on source server for zone
 - Traditionally the entire zone (can be quite large) is copied
- **Active Directory integrated zone**
 - Zone is hosted on domain controllers
 - Multimaster replication: important in dynamic update environments
 - Data replicated using efficient Active Directory replication topology and processes
 - Incremental updates

Key Points

The DNS database—the zone—is an important component of a network infrastructure. As with any other critical service, an organization should try to have two DNS servers available for clients, in order to provide redundancy.

The DNS database can be stored and replicated to more than one DNS server in one of two ways:

- Like other traditional DNS implementations, Windows DNS servers can store a zone in a file. Only one DNS server can write to the zone: that DNS server hosts the *primary zone*. Other DNS servers copy the zone and create a read-only copy called a *secondary zone*. The process of copying the zone is called *zone transfer*. A DNS server hosting a secondary zone requires permissions on the server from which it copies the zone.

- When DNS zones are hosted on domain controllers, you have the option to store zone data in Active Directory itself, creating an *Active Directory integrated zone*. Zone data is replicated in the same multimaster fashion as other Active Directory data. This is particularly important if dynamic updates are enabled, because clients will be registering their records with their primary DNS server, which will be in their site. The zone is also replicated incrementally: only records that have changed are replicated. This is much more efficient than traditional whole-file zone transfer.

Subdomains

- A zone supports resolution for a portion of the DNS namespace, starting with a domain: contoso.com
- europe.contoso.com?
 - Subdomain
 - Records to support resolution for the subdomain
 - Delegation
 - NS records that point to name server(s) for subdomain
 - List of name server(s) is static and updated manually
 - Stub zone
 - NS records that point to name server(s) for subdomain
 - List of name servers is updated automatically
 - Requires TCP port 53 to be open between the host (parent) DNS server and *all* name servers in the stub domain

Key Points

As mentioned earlier, a zone supports resolution for a specific portion of the DNS namespace, starting with a domain such as contoso.com. You can create subdomains within a portion of the DNS namespace for which you have authority. For example, if you manage the contoso.com namespace, you can create a subdomain, europe.contoso.com.

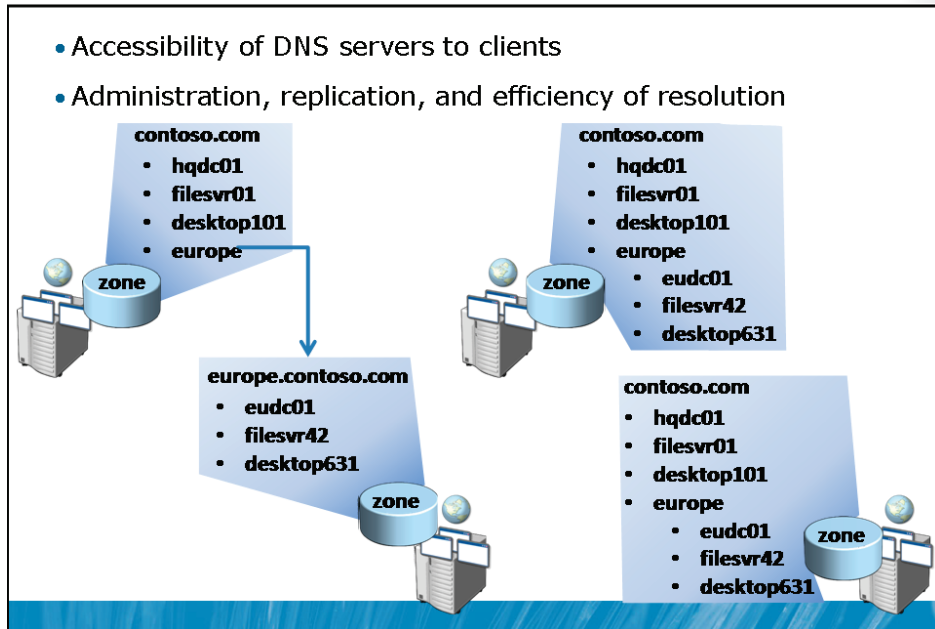
There are three options for creating a subdomain such as europe.contoso.com:

- **Subdomain.** A zone starts at a domain, and can contain one or more subdomains. If a zone contains a subdomain, the zone *includes all of the records necessary to support resolution for the subdomain*, and the DNS server is authoritative for the subdomain.

- **Delegation.** A delegation is a "link" to a subdomain, created by one or more NS records that point to one or more authoritative name server(s) for the subdomain. An NS record points to a name or IP address of a subdomain's name server. If the NS record points to a name, there must also be a host (A) record for the server in the parent domain. The NS records are created when you create the delegation, but if you need to change the IP addresses or names of the namespace servers, then you must *update the NS records manually*.
- **Stub zone.** A stub zone is very similar to a delegation, except that the NS records that point to the name server are updated automatically in the parent zone. This sounds like an ideal way to manage subdomains hosted on separate DNS servers, and stub zones are ideal in many environments. However, the automatic update of NS records requires that *TCP port 53 be open between the host (parent) name servers and all name servers in the child domain*. If it is not able to keep TCP port 53 open to support this requirement, then you should use a standard delegation instead.

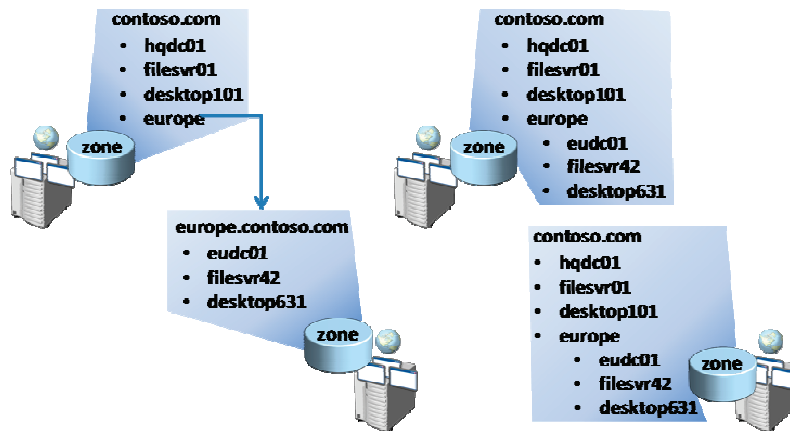
Placing DNS Servers and Zones

- Accessibility of DNS servers to clients
- Administration, replication, and efficiency of resolution



Key Points

In an environment that contains more than one domain, you can choose to place zones and DNS servers in a way that optimizes name resolution for clients, replication traffic, and administrative overhead.



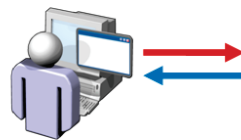
On the left of the illustration, the parent zone has a delegation or stub domain that points to the name servers of the child domain. Queries for records in the child domain are resolved by the DNS server that is authoritative for the child domain. The name servers might be located in Europe in order to support queries by clients for servers and services in Europe.

On the right side of the figure, DNS servers host a single zone that includes a subdomain for the child domain. This structure increases replication traffic between the two DNS servers, but clients in either location are able to resolve names from either domain from the authoritative DNS server in their location.

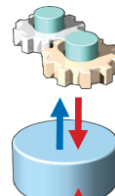
DNS Client (Resolver)

- Client application makes request
- DNS Client service examines DNS resolver cache
 - Pre-loaded with HOSTS file at service start or HOSTS file change
 - Caches query responses (including negative answers!)
 - ipconfig /flushdns

technet.microsoft.com?



DNS Client Service



DNS Resolver Cache



HOSTS File

- nslookup.exe
 - Queries the DNS server without checking the DNS resolver cache

Key Points

Now that you've learned about how the DNS namespace is hosted in zones on DNS servers, and how child domains are supported using delegations, subdomains, or stub zones, you are ready to explore in detail the way in which a name is resolved to an IP address.

When a client application, such as Microsoft® Internet Explorer®, needs to connect to a host such as technet.microsoft.com, the client application makes a call to the GetAddrInfo() API, which passes the host name to the DNS Client service.

The DNS Client service first checks the DNS resolver cache—a local, dynamically maintained database on the client—to determine whether the name has previously been resolved. The DNS resolver cache is preloaded with the contents of the HOSTS file (%systemroot%\system32\drivers\etc\hosts) when the cache is initialized during DNS Client startup, and when the HOSTS file is modified. When a name is successfully resolved, it is added to the DNS resolver cache. So, over time, the ability of the DNS client to resolve names locally increases.

Each resource record (RR) contains a time-to-live (TTL) value, which determines how long the record stays in the cache. When the TTL is reached, the record is removed from the cache.

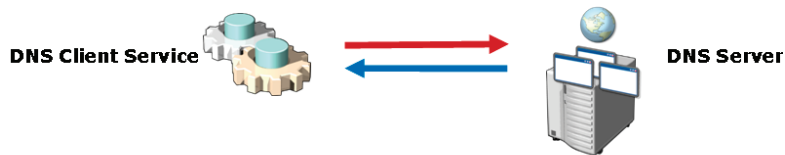
You can use the `ipconfig /displaydns` command to examine the contents of the local DNS resolver cache, and the `ipconfig /flushdns` command to flush the cache and reload it with the contents of the HOSTS file.

It's important to note that if a client queries a DNS server for a host record, and the DNS server returns a negative response, which indicates that the record cannot be found, that negative response is also cached. If you create a host record on the DNS server and retry the query, the client will fail because it continues to retrieve the negative response from its cache until that response is removed from the cache. In this case, the `ipconfig /flushdns` command can be used to force the client to re-query the DNS server.

You can use the `nslookup.exe` command to query a DNS server directly, bypassing the DNS resolver cache.

Query to DNS Server

- DNS Client queries primary DNS server
 - Requests recursive or iterative query
 - Recursive: DNS server continues performing query for client and returns a definitive answer
 - Iterative: DNS server returns only what it knows ("best guess") and client continues query
 - Queries secondary DNS server *only* if primary server doesn't respond
 - If primary server returns negative answer, secondary server *not* queried as "second opinion"
 - Ensure that each DNS server is able to resolve *all* client queries



Key Points

If the DNS Client service cannot resolve the query using the DNS resolver cache, it queries the primary DNS server. The query specifies the type of record that is being requested (for example, the address, host, or "A" record) and the name of the record being requested (for example, technet.microsoft.com).

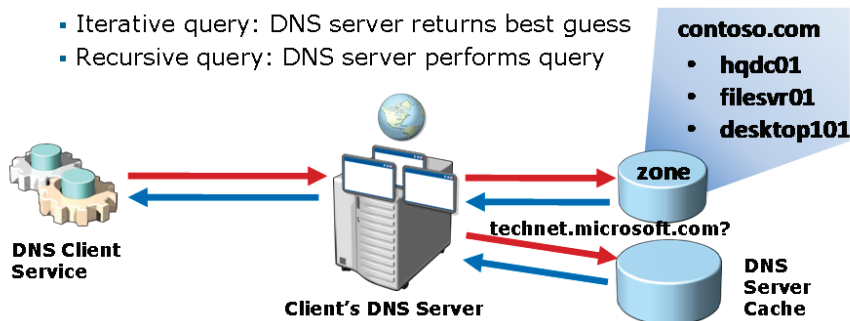
The query sent to the DNS server also specifies whether the client is requesting an *iterative or recursive query*. A recursive query is the most common type of query sent from a Windows client to its DNS server. The recursive query tells the DNS server to return a response that is definitive. When the DNS server receives a recursive query, it will go out and query other DNS servers, using a process that will be described in the next section, until the DNS server is able to resolve the client's query. If the DNS server is unable to resolve the client query, it returns a *negative response*, indicating that the domain name system does not have a record that matches the client's query.

If the primary DNS server returns a negative answer, indicating that the name cannot be resolved, the *DNS client does not query the secondary DNS server*. Additional DNS servers are queried only if the primary DNS server is not available. For this reason, it is important to ensure that *every DNS server is able to resolve all queries from all clients that direct queries to that server*.

Clients can optionally request an iterative query. The DNS server attempts to resolve the query locally, using processes that will be described in the next section, and will return a resolution (if available), or will return the most useful information that it can provide.

DNS Server Resolution

- DNS server checks its local zones
 - Resolution returned as an *authoritative response*
- DNS server checks its cache
 - Resolution returned as a *positive response*
- If no resolution found
 - Iterative query: DNS server returns best guess
 - Recursive query: DNS server performs query



Key Points

The DNS server, on receiving a client query, first checks the *locally-hosted zones*. If a resolution can be found, it is returned to the client as an *authoritative response*.

If no response is found, the server checks its *Cached Lookups*. Like the DNS client, the DNS server builds a cache of resolved resource records. The cache is initialized when the server starts and is populated with RRs as they are resolved from other DNS servers. A record is purged when its TTL is reached.

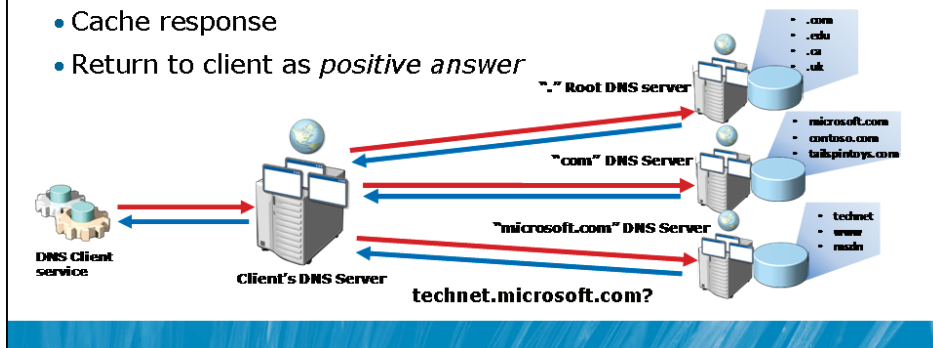
If a resolution is found in the cache, it is returned as a *positive response*.

If no resolution is found, and if the client requested an iterative query, the DNS server returns its best guess—the most useful information that it can provide. For example, the DNS server might not have a cached RR for the specific host that the client requests, but it might have a cached RR for the name server of the host's parent domain. In a worst-case scenario, the DNS server can refer the client to a list of root name servers: DNS servers that host the root (".") of the DNS namespace. The client takes whatever information is returned by the DNS server in an iterative query and uses that information to continue to try to resolve the name.

If the client requested a recursive query, the DNS server continues with processes described in the next section.

Recursion

- Iterative query to root DNS servers
 - Root DNS servers configured in DNS server's "root hints"
 - Root DNS server returns referral to .com name servers
- Iterative query to .com server
 - .com returns referral to microsoft.com name servers
- Iterative query to microsoft.com server
- Cache response
- Return to client as *positive answer*



Key Points

If the client requested a recursive query, the DNS server continues to process the query in an attempt to resolve it. In effect, the DNS server "proxies" the query and performs it on the client's behalf. This process is called *recursion*.

In the most extreme example of recursion, the DNS server has just started and its cache is empty. It does not have any cached NS records for microsoft.com or even .com name servers.

In this case, the DNS server starts by querying the root DNS servers. The DNS server has a list of these root servers in its "root hints." It sends the root DNS server an iterative query for technet.microsoft.com.

The root DNS servers cannot resolve technet.microsoft.com but they have in their zone NS records for name servers in the .com domain. They return this information as a referral. This is a good example of an iterative query: the root DNS server returns its "best guess," and the client (in this case itself a DNS server) continues the process.

Next, the DNS server sends another iterative query to the .com name server. Again, the server cannot resolve technet.microsoft.com, but it can provide NS records for microsoft.com as a referral.

With this referral, the DNS server queries the name server for microsoft.com. That DNS server is authoritative (hosts a zone) or microsoft.com, and is able to return an exact match for the host record for technet.microsoft.com.

The DNS server caches this resolution and returns it to the client as a *positive response*.

Lesson 2

Install and Configure DNS in an AD DS Domain

- Install and Manage the DNS Server Role
- Create a Zone
- Create a Zone: Dynamic Update
- Create Resource Records
- Configure Redundant DNS Servers
- Configure Forwarders
- Client Configuration

Now that you have reviewed the concepts, terminology, and processes related to DNS and name resolution, you are ready to install and configure the DNS server role in an AD DS domain.

Objectives

After completing this lesson, you will be able to:

- Install DNS.
- Add DNS zones.
- Manage DNS records.
- Configure DNS server settings.
- Configure DNS client settings.

Install and Manage the DNS Server Role

- **Methods**
 - Server Manager → Roles → Add Role
 - Active Directory Domain Services Installation Wizard
- **DNS Manager snap-in**
 - Server Manager
 - DNS Manager console (dnsmgmt.msc)
- **dnscmd.exe**

Key Points

The DNS server role is not installed on Windows Server 2008 by default. Like other functionality, it is added in a role-based manner when a server is configured to perform the role.

You can install the DNS server role using the Add Role link in Server Manager.

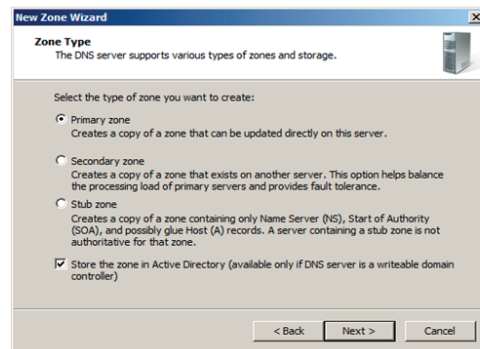
The DNS server role can also be added automatically by the Active Directory Domain Services Installation Wizard (dcpromo.exe). The domain controller options page of the wizard allows you to add the DNS server role.

When the DNS server role is installed, you will find the DNS Manager snap-in is available to add to your administrative consoles. The snap-in is also added automatically to the Server Manager console, and in the DNS Manager console (dnsmgmt.msc). To administer a remote DNS server, add the Remote Server Administrative tools to your administrative workstation running Windows Vista® SP1 or later operating systems.

A command-line administrative tool is also added: dnscmd.exe. DNSCmd can be used to script and automate DNS configuration. Type dnscmd.exe /? at the command prompt for help.

Create a Zone

- Right-click Forward Lookup Zones
- Select zone type
- Specify replication (Active Directory integrated zones only)
 - All DNS servers in forest
 - All DNS servers in domain
 - All domain controllers in domain (for compatibility with Windows® 2000 DCs)
- Enter zone name (DNS domain name)
- Manage updates



Key Points

After installing a DNS server, you can begin adding zones to the server.

To create a zone, right-click the *Forward Lookup Zones* node in the console tree and choose *New Zone*. The New Zone Wizard steps you through the process of creating a zone.

You will be able to select one of the three types of zones:

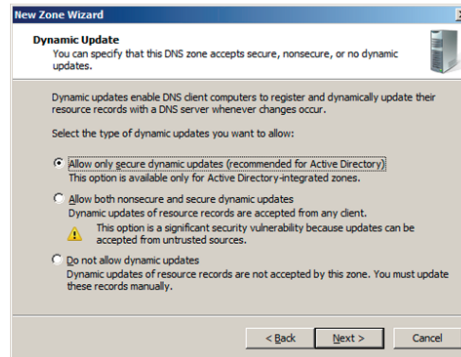
- **Primary zone.** The DNS server will be able to write to the zone.
- **Secondary zone.** The DNS server will maintain a copy of a zone hosted on another DNS server. The secondary zone is read-only.
- **Stub zone.** The DNS server will maintain a list of name servers for another domain. Stub zones will be discussed in detail later in this module.

You can also select to store the zone data in Active Directory if the DNS server is a domain controller. This creates an Active Directory integrated zone, which will be discussed later in this module. If you deselect this option, the zone data is stored in a file, rather than in Active Directory.

After choosing the zone type, you are prompted to enter the zone name—the fully qualified domain name for the zone.

If the zone is a primary zone, you can then choose how to manage updates, as described in the next section.

Create a Zone: Dynamic Update



Key Points

When you create a zone, you are also prompted to specify whether dynamic updates are supported. Dynamic updates reduce the management overhead of a zone, because clients can add, delete, and update their own resource records.

Dynamic updates leave open the possibility that an RR could be spoofed. For example, a computer could register a record named `www`, effectively redirecting traffic from your Web server to the incorrect address.

To eliminate the possibility of spoofing, Windows Server 2008 DNS Server service supports secure dynamic updates. A client must authenticate prior to updating its RRs, so the DNS server knows whether the client is the same computer that has the permission to modify the resource record.

Create Resource Records

- Right-click the zone
- Dialog box appears specific to the record type you choose

The image shows two side-by-side dialog boxes from a DNS management tool.

New Host Dialog:

- Title: New Host
- Name (uses parent domain name if blank):
- Fully qualified domain name (FQDN):
- IP address:
- ☐ Create associated pointer (PTR) record
- ☐ Allow any authenticated user to update DNS records with the same owner name
- Time to live (TTL): : : : (DDDDD:HH.MM.SS)
- Buttons: Add Host, Cancel

New Resource Record Dialog:

- Title: New Resource Record
- Alias (CNAME)
- Alias name (uses parent domain if left blank):
- Fully qualified domain name (FQDN):
- Fully qualified domain name (FQDN) for target host:
- ☐ Delete this record when it becomes stale
- Record time stamp:
- ☐ Allow any authenticated user to update all DNS records with the same name. This setting applies only to DNS records for a new name.
- Time to live (TTL): : : : (DDDDD:HH.MM.SS)
- Buttons: OK, Cancel

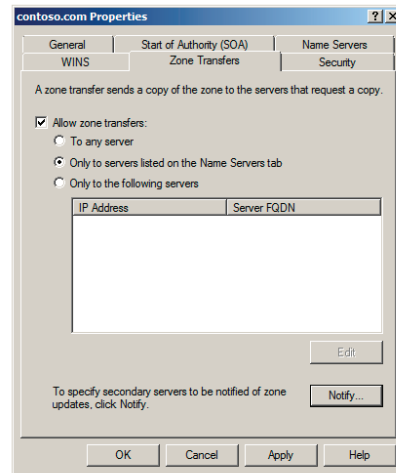
Key Points

In most environments, even those with dynamic updates enabled, there will be the need to add resource records to a zone.

To create a resource record, right-click the zone and choose the type of record you wish to create. A dialog box appears with input controls that are appropriate for the type of record you are adding.

Configure Redundant DNS Servers

- **Active Directory–integrated zone**
 - Add DNS server to another DC
- **Standard Primary Zone**
 - Add NS records for secondary servers
- **Master server**
 - The server from which the zone will be copied
 - Need not be the primary server
 - Allow Zone Transfers
- **Secondary server**
 - Create a new forward lookup zone
 - Choose a secondary zone
 - Configure the master server



Key Points

An enterprise should strive to ensure that a zone can be resolved authoritatively by at least two DNS servers.

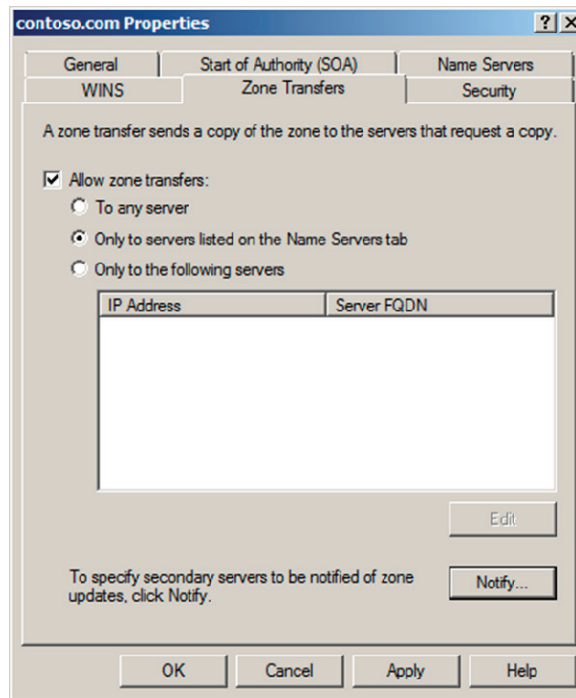
If the zone is Active Directory integrated, you can simply *add the DNS server role to another domain controller in the same domain* as the first DNS server. Active Directory integrated zones, and the replication of the DNS zone by AD DS, are described in the next lesson.

If the zone is not Active Directory integrated, you must add another DNS server and configure it to host a secondary zone. Remember that a secondary zone is a read-only copy of the primary zone.

The first step in this process is to configure the zone itself to refer to the secondary servers as name servers for the zone. Add NS records for the secondary servers to the parent zone.

A secondary server will copy the zone from another DNS server, called the master server. The master server need not be the primary server, but there are obvious advantages to using the primary zone as the master, to reduce the latency with which record updates are replicated to secondary servers.

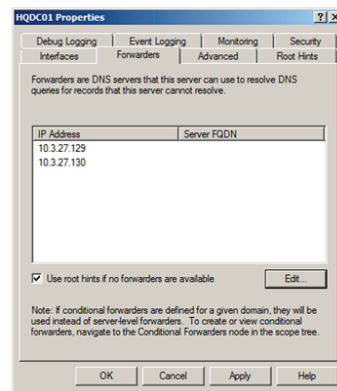
The master server must allow the secondary servers to connect and initiate a zone transfer. This is configured on the Zone Transfers tab of the zone properties on the master server, shown below:



You can then add the secondary zone to the forward lookup zones of the secondary server. The secondary server is configured to replicate the zone from the master server.

Configure Forwarders

- Right-click DNS server → Properties → Forwarders
- For all names not in your domain, resolve using your Internet service provider's (ISP's) DNS servers
- If forwarders are not available, use root servers based on root hints



Key Points

In Lesson 1, you learned that a DNS server will attempt to resolve a client's query using its local zones and cache. If it is unable to do so, and if the query is sent as a recursive query, the DNS server then performs the query on behalf of the client.

The first method with which to configure a DNS server to effectively perform a recursive query is to add *forwarders* to the DNS server. Forwarders are pointers to other DNS servers. Typically these servers are hosted by your Internet service provider (ISP) or are upstream DNS servers in your enterprise DNS infrastructure. For example, your Active Directory domain may use Windows DNS Server service to resolve names within the domain, then forward queries to your corporate DNS servers, which host zones for other enterprise domains.

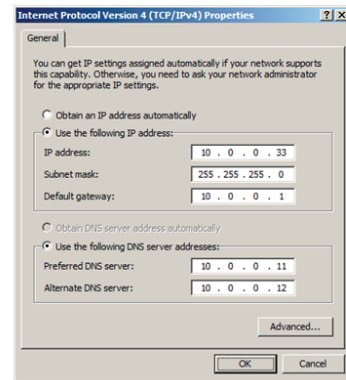
Forwarders are similar to the DNS servers that you configure in the IP properties of a network connection. That list of DNS servers is used by the DNS Client service. The list is not shared with the DNS server service. Forwarders serve the same purpose for the DNS server service.

If forwarders are not configured, the server will attempt to query a name server for the root of the DNS namespace ("."). These root servers are maintained as *root hints*. Although the root DNS name servers do not change frequently, they can change occasionally. Windows Update will include updates to the root hints.

There are several mechanisms with which a recursive query can be made more efficient, including conditional forwarders and stub zones. These options will be discussed in Lesson 4.

Client Configuration

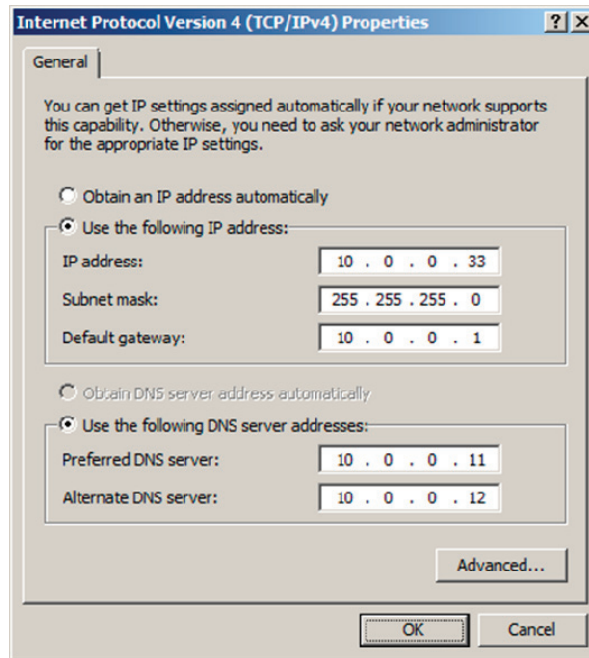
- IP configuration of client
 - `netsh interface ipv4 set dns "Local Area Connection" static 10.0.0.11 primary`
 - `netsh interface ipv4 add dns "Local Area Connection" 10.0.0.12`
- Dynamic Host Configuration Protocol (DHCP) scope option 6



Key Points

A DNS server is not much use unless clients are configured to query it. The DNS client is distinct from all Active Directory–related components of the Windows operating system, so a client does not assume that its domain controller is a DNS server; a client should have at least two DNS servers configured.

The configuration can be *fixed in the client's IP configuration*, as shown in the screen shot:



The netsh.exe command can also be used to configure the first and additional DNS servers for a network connection, as in the example below:

```
netsh interface ipv4 set dns "Local Area Connection"
    static 10.0.0.11 primary
netsh interface ipv4 add dns "Local Area Connection" 10.0.0.12
```

Alternatively, the DNS servers can be passed to clients by Dynamic Host Configuration Protocol (DHCP) using *DHCP scope option 6: DNS server*.

Remember that secondary and additional DNS servers are not queried if the primary DNS server returns a negative response. Additional DNS servers are queried only if the primary DNS server does not respond, and is offline.

Lab A: Install the DNS Service

- Exercise 1: Add the DNS Server Role
- Exercise 2: Configure Forward Lookup Zones and Resource Records

Logon information

Virtual machine	6425B-HQDC01-B	6425B-HQDC02-B
Logon user name	Do not log on	Pat.Coleman
Administrative user name		Pat.Coleman_Admin
Password		Pa\$\$w0rd

Estimated time: 30 minutes

Scenario

You are an administrator of Contoso, Ltd. You recently added a second domain controller to your enterprise, and you want to add redundancy to the DNS server hosting the domain's zone. Currently, the only DNS server for the contoso.com zone is HQDC01. You need to ensure that clients that resolve against the new DNS server, HQDC02, are able to access Internet Web sites. Additionally, you have been asked to configure a subdomain to support name resolution required for the testing of an application by the development team.

Exercise 1: Add the DNS Server Role

In this exercise, you will add the DNS server role to HQDC02, examine the domain zone that is automatically populated on the DNS server, and then configure HQDC02 to use itself as its primary DNS server.

The main tasks for this exercise are as follows:

1. Prepare for the lab.
2. Add the DNS server role.
3. Change the DNS server configuration of the DNS client.
4. Examine the domain forward lookup zone.
5. Configure forwarders for Internet name resolution.

► Task 1: Prepare for the lab

1. Start 6425B-HQDC01-B.
2. Wait for startup to complete.
3. Start 6425B-HQDC02-B.
4. Log on to HQDC02 as **Pat.Coleman** with the password **Pa\$\$w0rd**.

► Task 2: Add the DNS server role

1. On HQDC02, run Server Manager as an administrator, with the user name **Pat.Coleman_Admin** and the password **Pa\$\$w0rd**.
2. Add the DNS server role to HQDC02.
3. Close Server Manager.
4. Restart HQDC02. Then log on as **Pat.Coleman** with the password **Pa\$\$w0rd**.

This is not necessary in a production environment, but it speeds the process of restarting services and replicating the DNS records to HQDC02 for the purposes of this exercise.

- ▶ **Task 3: Change the DNS server configuration of the DNS client**
 1. Run the command prompt as an administrator, with the user name **Pat.Coleman_Admin** and the password **Pa\$\$w0rd**.
 2. Type **netsh interface ipv4 set dnsserver "Local Area Connection" static 10.0.0.12 primary** and then press ENTER.
 3. Type **netsh interface ipv4 add dnsserver "Local Area Connection" 10.0.0.11** and then press ENTER.

- ▶ **Task 4: Examine the domain forward lookup zone**
 1. Run DNS Manager as an administrator, with the user name **Pat.Coleman_Admin** and the password **Pa\$\$w0rd**.
 2. Examine the SOA, NS, and A records in the contoso.com forward lookup zone.

- ▶ **Task 5: Configure forwarders for Internet name resolution**
 - Configure two forwarders for HQDC02: 192.168.200.12 and 192.168.200.13. Because these DNS servers do not actually exist, the Server FQDN will display either <Attempting to resolve> or <Unable to resolve>. In a production environment, you would configure forwarders to upstream DNS servers on the Internet, usually those provided by your Internet service provider (ISP).

Results: After this exercise, you will have added the DNS server role to HQDC02 and simulated the configuration of forwarders to resolve internet DNS names.

Exercise 2: Configure Forward Lookup Zones and Resource Records

In this exercise, you will add a forward lookup zone for the development domain at Contoso. You will then add a host and CNAME record to the zone and confirm that name resolution for the new zone is functioning.

The main tasks for this exercise are as follows:

1. Create a forward lookup zone.
2. Create Host and CNAME records.
3. Test name resolution.

► Task 1: Create a forward lookup zone

- Create a new forward lookup zone named **development.contoso.com**. The zone should be a primary zone, stored in Active Directory and replicated to all domain controllers in the contoso.com domain. Configure the zone so that it does not allow dynamic updates.



Note: In a production environment you would most likely just replicate to all DNS servers. However for the purposes of our lab we will replicate to all domain controllers to ensure quick and guaranteed replication.

► Task 2: Create Host and CNAME records

1. In the development.contoso.com zone, create a host (A) record for APPDEV01 with the IP address **10.0.0.24**.
2. Create a CNAME record, **www.development.contoso.com** that resolves to **appdev01.development.contoso.com**.

► Task 3: Test name resolution

- At the command prompt, type **nslookup www.development.contoso.com** and then press ENTER.

Examine the output of the command. What does the output tell you?

Results: After this exercise, you will have created a new forward lookup zone, development.contoso.com, with host and CNAME records, and verified that names in the zone can be resolved.



Note: Do not shut down the virtual machines once you are finished with this lab as the settings you have configured here will be used in the next lab.

Lab Review Questions

Question: If you did not configure forwarders on HQDC02, what would be the result for clients that use HQDC02 as their primary DNS server?

Question: What would happen to clients' ability to resolve names in the development.contoso.com domain if you had chosen a stand-alone DNS zone, rather than an Active Directory-integrated zone? Why would this happen? What would you have to do to solve this problem?

Lesson 3

AD DS, DNS, and Windows

- AD DS, DNS, and Windows
- Integrate AD DS and the DNS Namespace
- Split-Brain DNS
- Create a Delegation for an Active Directory Domain
- Active Directory-Integrated Zones
- Application Partitions for DNS Zones
- DNS Application Partitions
- Dynamic Updates
- Background Zone Loading
- Service Locator (SRV) Records
- Demonstration: SRV Resource Records Registered by AD DS Domain Controllers
- Domain Controller Location
- Read-Only DNS Zones

You've learned how to configure DNS in a simple environment, using many of the default settings that support Active Directory domains out of the box. In this lesson, you will learn more about the components and processes that support Active Directory Domain Services (AD DS), and the interrelation between AD DS and DNS.

Objectives

After completing this lesson, you will be able to:

- Understand the integration between AD DS and DNS.
- Choose a DNS domain for an Active Directory domain.
- Create a zone delegation for a new Active Directory domain.

- Configure replication for Active Directory-integrated zones.
- Describe the purpose of SRV records in the domain controller location process.
- Understand read-only DNS servers.

AD DS, DNS, and Windows

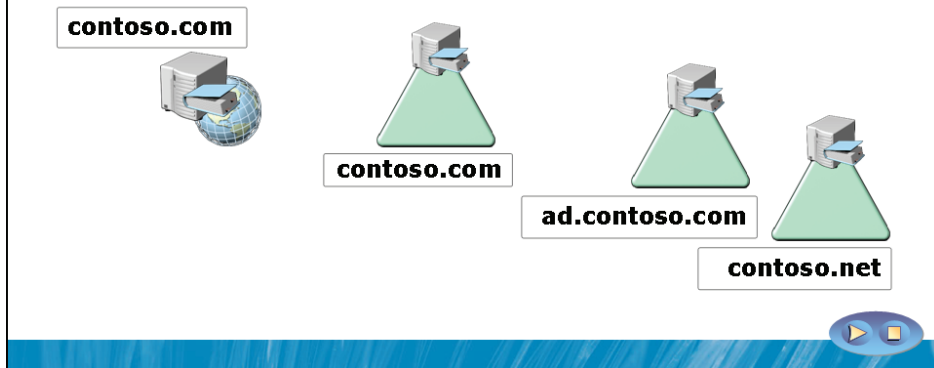
- An AD DS domain has a DNS domain name
- DNS zones can be stored in the Active Directory database
- Active Directory can replicate DNS zones to specific domain controllers
- Windows clients can update their own DNS records
- Active Directory can load large Active Directory-integrated zones in the background
- DCs register service locator records in DNS
- Clients use these records to locate DCs
- Read-Only Domain Controllers (RODCs) can support DNS even in a dynamic update zone

Key Points

Active Directory Domain Services, DNS, and the Windows operating system are integrated and interdependent in many ways. In this lesson, you will explore each in more detail.

Integrate AD DS and the DNS Namespace

- An Active Directory domain must have a DNS name
- Active Directory domain name vs. external DNS namespace
 - Active Directory uses same domain name
 - Active Directory uses subdomain of public domain
 - Active Directory uses separate domain name



Key Points

Active Directory requires DNS, and an AD DS domain must have a DNS domain name. Because DNS is also used as a globally available, standards-based namespace, you should give careful consideration to where in the namespace you set your AD DS domain.

Let's assume that you are an administrator of Contoso, Ltd., which maintains the registered domain name **contoso.com**, and which has a Web site at **www.contoso.com**. If you are planning the namespace for your AD DS domain, you could choose one of the following:

- **The same domain name as your external DNS domain name: **contoso.com**.**
If you use the same namespace, you have to implement "split-brain" DNS," which is described in the next section.

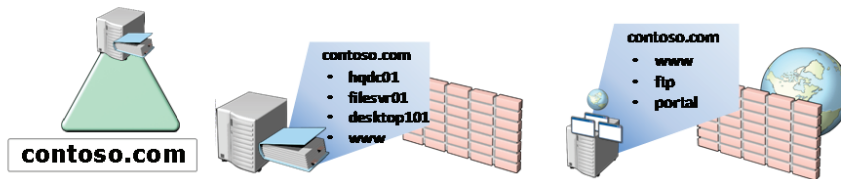
- **A subdomain of your external domain name: ad.contoso.com.** If you use a subdomain of a registered domain name, you can proceed easily because you are the owner of that portion of the DNS namespace. You should be careful, however, of going too deep in the DNS namespace. Users and admins alike will be typing fully qualified domain names far more frequently than you'd ever imagine, and a lengthy domain suffix will make each FQDN more painful to enter. In addition, URLs and UNC paths have length limits, which are easier to reach with lengthy DNS suffixes.
- **A separate domain name: contoso.net.** If you use a separate domain name for your Active Directory domain, it is recommended that you register the domain so that it is not usurped by another organization. You should ensure that you maintain ownership of that portion of the DNS namespace.

In today's increasingly connected world, the lines between network, intranet, extranet and the Internet are blurred, almost to obscurity. It is becoming less and less possible to maintain namespace separation, and less value is contributed by it. For this reason, many organizations are choosing to use the most familiar domain name, the domain name that is most closely associated with the organization, the domain name that's easiest to type: the public domain name. As mentioned briefly above and as discussed in the next topic, there are steps you must take to support this configuration, but the cost of the steps is typically far less than the benefits it provides. With *any* of these choices, you must manage name resolution, perimeter protection, and security, so there are equivalent levels of administrative effort to support any of these namespace choices. It therefore makes some sense to use a DNS name that makes it easiest for the users of your namespace.

In the early years of Active Directory, it was common to suggest or even recommend the use of a custom top-level domain, such as .msft or even the .local TLD. Due to changes in the networked world, including IP version 6 (IPv6) and increased interconnectivity, these options should be explored only after very careful consideration of their ability to support your business requirements, the benefits they might provide, and the cost in terms of administration and user support.

Split-Brain DNS

- The zone that supports AD DS
 - Secured from Internet exposure
 - Dynamic
 - Fully populated with AD DS client, server, and service records
- The zone that supports the external namespace
 - Secure
 - Static
 - Populated with the records related to external resources
- Some (manually maintained) duplication of records, such as `www`



Key Points

Whenever you use a domain name for an AD DS domain that is also used for connections to your network from the outside world, you need to ensure that there is a separation of DNS zones that provides different information to public and internal clients. This is called *split-brain DNS*.

The internal DNS zone must support the AD DS domain in full fidelity, with all of the resource records for servers, clients, and services in the domain. Ideally it will allow secure dynamic updates and will store its zone data in Active Directory itself.

The externally accessible DNS zone must provide to outside clients only the resource records that they require, for example `www` and `ftp`. This zone will typically be much smaller than the zone supporting the domain internally. The external zone will typically be updated manually, rather dynamically. The DNS Server hosting the external zone will often be placed behind the external firewall, with only port 53 opened to it.

There may well be some need for duplicate records in the two zones. If your internal users need access to the public web site, such as `www.contoso.com`, that resource record must exist in the internal zone against which clients query. Remember that, because the internal DNS server is considered authoritative for the zone (as is the external server), it will return either a resolution for a query or a negative response, indicating that the record simply doesn't exist. There is no "second query" or iterative query against the external zone. Therefore, you will create records that are required internally and externally, such as `www`, in both zones.

Create a Delegation for an Active Directory Domain

- Necessary if child domain zone hosted on different DNS servers
- Create the delegation in the *parent* DNS domain (zone)
 - Right-click zone → New Delegation
 - Refer to the server that is/will be the child domain DNS server
- Configure DNS client on child domain server
 - Primary DNS server should be the parent DNS server
- Install the DNS role and zone
 - Server Manager: Add role, then create primary zone
or
 - DCPromo can install DNS while promoting to a DC
- Optional but typical configuration
 - Reconfigure child DNS client to refer to itself as primary DNS server
 - Add parent DNS server as a forwarder on the child server
 - Configure new zone to be Active Directory integrated and secure dynamic update

Key Points

In Module 1, you created a new Windows Server 2008 AD DS domain and forest. When you promoted the domain controller, you received a message indicating that there was no delegation for the contoso.com domain. You ignored the message and the domain was established, with DNS on the domain controller. Clients configured with the IP address of the domain controller as their DNS server will query the DC and will be able to resolve names in the contoso.com domain. However, no external clients will be able to resolve contoso.com names because there is no delegation—no Name Service (NS) records in the .com domain that point to your authoritative DNS server.

This is not a problem for the course, because your domain is an "island"—it is separated from the rest of the Internet and there is no need for a delegation.

However, within a forest, it is important that there are delegations from a parent to a child domain *if the child domain's zone will be hosted on separate DNS servers*. If the child domain will be a subdomain of the existing zone, no delegation is necessary.

For example, if you wish to add a domain, europe.contoso.com, to the domain tree, clients in contoso.com must be able to resolve servers, services, and other records in europe.contoso.com in order to support replication and authentication in the forest.

Before you add a child domain to a tree, or a new tree to a forest, you must create a delegation in the parent domain or the forest root domain.

To create a delegation, right-click the zone for the parent domain and choose New Delegation. You will be prompted to enter name servers for the new domain. Refer to the server that is or will be the child domain's DNS server.

To create a delegation for a new domain tree, or for the forest root domain itself, create a new zone first in the existing root DNS zone. In the new zone, add an Address record that uses the *full DNS name* of the new domain's DNS server. Then add an NS record for the new domain that refers to the *full DNS name* of the domain controller.

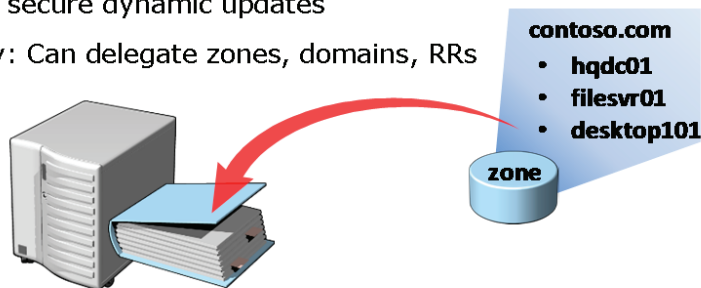
After you've created the delegation, you are ready to configure the server that will be the child domain's first domain controller. First, configure its DNS server to point to the DNS server on which you created the delegation.

Install the DNS role using Server Manager and then create the primary zone for the child domain. Alternatively, use the Active Directory Domain Services Installation Wizard (dcpromo.exe), which can install DNS as part of the installation of AD DS.

After the child domain has been created, reconfigure the child DNS server to refer to itself as its primary DNS server. Typically, you will add the parent DNS server as a forwarder, conditional forwarder, or stub zone to the child DNS server. You must ensure, one way or another, that systems in the child domain can resolve names in the parent domain. Finally, it is recommended in most scenarios that you use an Active Directory-integrated zone that supports secure dynamic updates for the child domain.

Active Directory Integrated Zones

- DNS zone data is stored in AD DS
- Allows multimaster writes to zone
- Replicates DNS zone information using AD DS replication
 - Leverages efficient replication topology
 - Uses efficient Active Directory replication processes: incremental updates
- Enables secure dynamic updates
- Security: Can delegate zones, domains, RRs



Key Points

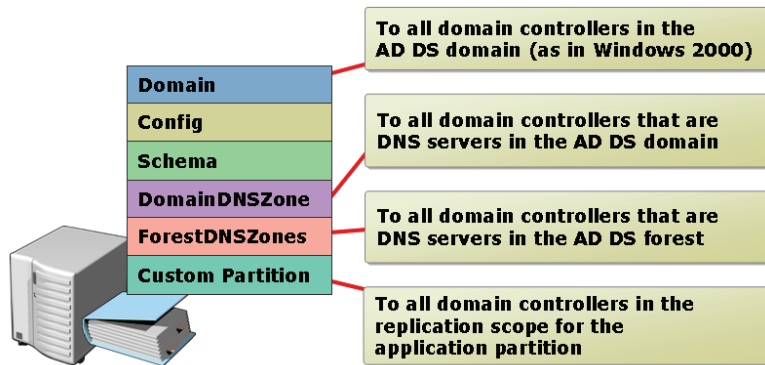
In Lesson 1, you learned that Windows DNS Server is able to store zone data in the AD DS database when the DNS server is an AD DS domain controller. This creates an *Active Directory-Integrated Zone*. The benefits of Active Directory-integrated zones are significant:

- **Multimaster updates.** Unlike standard primary zones, which can only be modified by a single primary server, Active Directory-integrated zones can be written to by any DC to which the zone is replicated. This *removes a single point of failure* in the DNS infrastructure. It is particularly important in *geographically distributed environments that use dynamic update zones*, because it allows clients to update their DNS records without having to connect to a potentially distant primary server.

- **Replication of DNS zone data using AD DS replication.** In Module 12, you will learn about the *efficient topology-generating and replication mechanisms* of AD DS replication. One of the characteristics of Active Directory replication is attribute-level replication, in which only changed attributes are replicated. An Active Directory-integrated zone can leverage these benefits of Active Directory replication, rather than replicating the entire zone file as in traditional DNS zone transfer models.
- **Secure dynamic updates.** An Active Directory-integrated zone can enforce secure dynamic updates.
- **Granular security.** As with other Active Directory objects, an Active Directory-integrated zone allows you to delegate administration of zones, domains, and resource records by modifying the access control list (ACL) on the object.

Application Partitions for DNS Zones

- Store DNS zones in one of the default application partitions
 - Replication scope is the difference
- Or create a custom partition and define its scope



Key Points

An Active Directory integrated zone stores its records in the AD DS database. The records can be stored in one of several partitions:

- **The DomainDNSZone partition.** This partition is replicated to all domain controllers that are DNS servers within the domain.
- **The ForestDNSZones partition.** This partition is replicated to all domain controllers that are DNS servers in the forest.

These default partitions are created when DNS is installed and configured during AD DS installation. You can use the DNS management tool or the `dnscmd.exe` command to create the partitions after AD DS is installed.

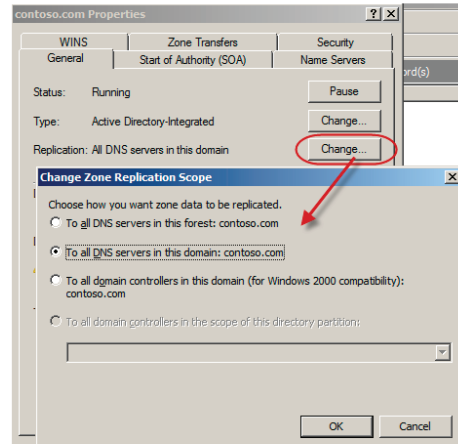
- **The Domain.** The Domain, which also contains records for objects, including users and computers, is replicated to all domain controllers, whether or not they are DNS servers. In Windows 2000, DNS zones were stored in the Domain NC. If you have Windows 2000 domain controllers that are DNS servers, you must use this replication option to support those systems.

Your choice of partition is primarily a matter of selecting the replication topology you want for your DNS zones. Of course, the zone must be replicated to a DNS server in order for that DNS server to be authoritative for the zone. If a DNS server does not have a replica of the zone, it must have a forwarder or stub zone to perform recursive queries for names in the zone.

- **A custom application partition.** If the default application partitions do not give you the replication model that you require to support your DNS infrastructure, you can create a custom application partition, for which you can specify which servers will replicate the partition.

DNS Application Partitions

- Create an application partition
 - `dnscmd ServerName /Createdirectorypartition FQDN`
- Change zone replication scope
 - Properties of zone → General → Change replication

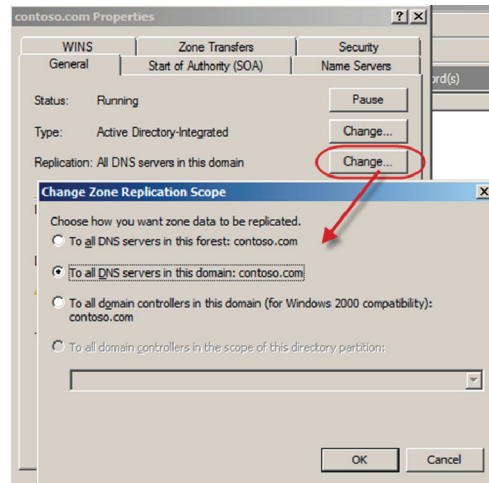


Key Points

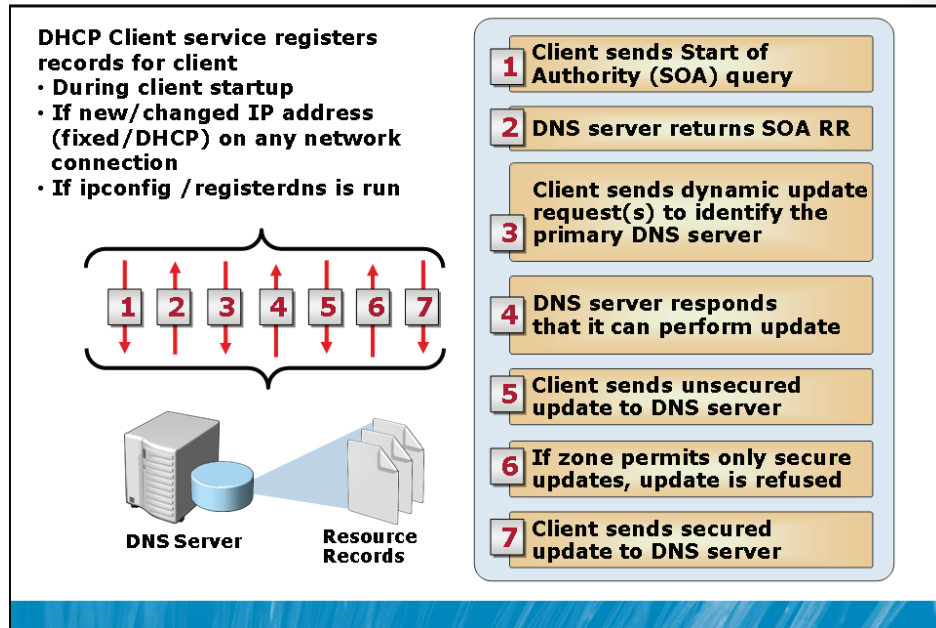
You can create an application partition using the `dnscmd.exe` command, as in the following example:

```
dnscmd hqdc01.contoso.com /createdirectorypartition MyZone.contoso.com
```

You can change the replication scope of a zone from its properties. Click the Change button next to Replication, as shown in the figure below:



Dynamic Updates



Key Points

By default, Windows systems attempt to register their records with their DNS server. This behavior can be modified in the IP configuration of the client or through Group Policy.

It is the DHCP Client service that performs the registration, whether the client's IP address is obtained from a DHCP server or is fixed. The registration occurs:

- When the client starts and the DHCP Client service is started.
- When an IP address is configured, added, or changed on any network connection.
- When an administrator runs `ipconfig /registerdns`.

The client attempts to identify the DNS server that is the primary DNS server for the zone. If the zone is not an Active Directory-integrated zone, this may require several iterations in which the client identifies a name server, sends an update, and is refused because the name server hosts only a secondary zone. Eventually, if the zone supports dynamic updates, the client reaches a DNS server that can write to the zone. This is the primary server for a standard, file-based zone or any DC that is a name server for an Active Directory-integrated zone.

If the zone is configured for *secure* dynamic updates, the DNS server refuses the change. The client then authenticates and re-sends the update.

In some configurations, you may not want clients to update their records even in a dynamic update zone. Alternatively, you can configure the DHCP server to register the records on the clients' behalf. By default, a client registers its A (host/address) record, and the DHCP server registers the PTR (pointer/reverse lookup) record. PTR records are discussed in Lesson 4.

Background Zone Loading

When a domain controller with Active Directory-integrated DNS zones starts, it:

- **Enumerates all zones to be loaded**
- **Loads root hints from files or AD DS servers**
- **Loads all zones that are stored in files rather than in AD DS**
- **Begins responding to queries and remote procedure calls (RPCs)**
- **Starts one or more threads to load the zones that are stored in AD DS**

Key Points

It is possible for a zone that supports an AD DS domain to be quite large, particularly if A records for clients are maintained in a large domain. In previous versions of Windows, it took a long time for DNS Server service to start when it had to load a large zone.

Windows Server 2008 loads zones in the background, allowing the DNS server to start responding to queries very quickly. If a query is sent for a zone that is not yet loaded, the server works to load that zone.

Service Locator (SRV) Records

SRV resource records allow DNS clients to locate TCP/IP-based services. SRV resource records are used when:

- **A domain controller needs to locate replication partners**
- **A client computer authenticates to AD DS**
- **A user changes his or her password**
- **A Microsoft Exchange server performs a directory lookup**
- **An admin opens Active Directory Users and Computers**

SRV record syntax:

```
protocol.service.name TTL class type priority weight port target
```

Example of an SRV record

```
_ldap._tcp.contoso.com 600 IN SRV 0 100 389 hqdc01.contoso.com
```

Key Points

A Service Locator (SRV) resource record resolves a query for a network service, allowing a client to locate a host that provides a specific service.

SRV records are used in these and many other scenarios:

- When a domain controller needs to replicate changes from its partners
- When a client computer needs to authenticate to AD DS
- When a user changes his or her password
- When an Microsoft Exchange server performs a directory lookup
- When an administrator opens Active Directory Users and Computers

An SRV record follows the syntax shown below:

```
protocol.service.name TTL class type priority weight port target
```

An example of an SRV record is shown below:

```
_ldap._tcp.contoso.com 600 IN SRV 0 100 389 hqdc01.contoso.com
```

The components of the record are:

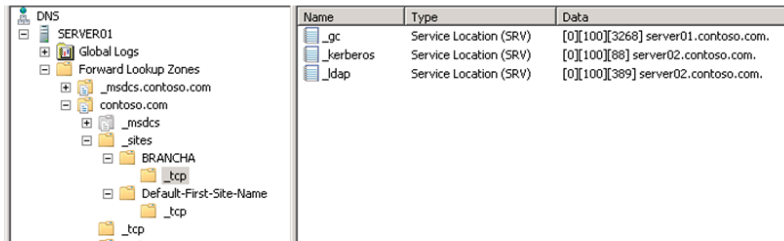
- The protocol service name, such as the LDAP service offered by a domain controller
- The time-to-live value, in seconds
- The class (all records in a Windows DNS server will be IN or INternet)
- The type: SRV
- The priority and weight, which help clients determine which host should be preferred.
- The port on which the service is offered by the server. Port 389 is the standard port for LDAP on a Windows DC.
- The target, or host of the service, which in this case is the domain controller named hqdc01.contoso.com

When a client process is looking for a domain controller, it can query DNS for an LDAP service. The query returns both the SRV record and the A record for the server(s) that provide the requested service.

Demonstration: SRV Resource Records Registered by AD DS Domain Controllers

In this demonstration, we will:

- Look at the service locator (SRV) records registered in
 - `_tcp.contoso.com`: all DCs in the domain
 - `_tcp.siteName._sites.contoso.com`: all DCs in site `siteName`
- Simulate a client's query to DNS for domain controllers
- Learn how to register SRV records dynamically or statically
- View `%systemroot%\system32\config\netlogon.dns`



Name	Type	Data
_gc	Service Location (SRV)	[0][100][3268] server01.contoso.com.
_kerberos	Service Location (SRV)	[0][100][88] server02.contoso.com.
_ldap	Service Location (SRV)	[0][100][389] server02.contoso.com.

Key Points

In this demonstration, your instructor will show you the SRV records registered by a domain controller in the `contoso.com` forest. You will:

- Use DNS Manager to see the service locator records registered in.
 - `_tcp.contoso.com`, which lists all domain controllers in the domain
 - `_tcp.siteName._sites.contoso.com`, which lists domain controllers that are covering a specific site
 - `_msdcs.contoso.com`, which tracks the domain controllers in a forest and is used by DCs to locate each other
- Simulate a client query for a domain controller.

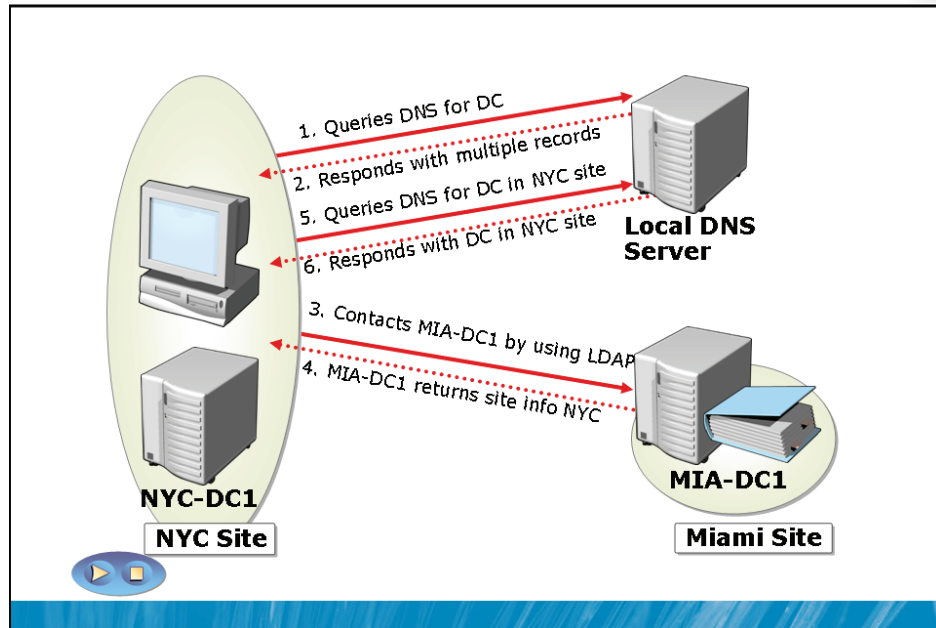
```
nslookup
set type=srv
_ldap._tcp.contoso.com
```

- Learn how domain controllers register their resource records in a dynamic update zone. Delete an SRV record, and then stop and restart the NetLogon service. The NetLogon service registers DC records at startup.
- View the %systemroot%\system32\config\netlogon.dns file, which contains the records that must be registered manually if the zone does not support dynamic updates.

Demonstration Steps

1. Run **DNS Management** with administrative credentials using the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd** then in the console tree, expand **HQDC01**, **Forward Lookup Zones**, and **contoso.com**, and then click the **_tcp** node. Examine the SRV records.
2. In the console tree, expand **HQDC01**, **Forward Lookup Zones**, **contoso.com**, **_sites**, **BRANCHA**, and then click the **_tcp** node. Examine the SRV records.
3. Run Command Prompt with the administrative credentials used earlier.
4. Type **nslookup** and then press ENTER.
5. Type **set type=srv**, and then press ENTER.
6. Type **_ldap._tcp.contoso.com**, and then press ENTER.
7. Switch to **DNS Manager**.
8. Expand **HQDC01**, **Forward Lookup Zones**, and **contoso.com**, and then click the **_tcp** node.
9. Right-click the SRV record for **hqdc01.contoso.com**, and then click **Delete**.
10. Switch to Command Prompt.
11. Type **net stop netlogon** and then press ENTER.
12. Type **net start netlogon** and then press ENTER.
13. Switch to **DNS Manager**.
14. In the console tree, right-click the **_tcp** node, and then click **Refresh**. Examine the SRV record for **hqdc01.contoso.com**.
15. Open **notepad.exe**.
16. Click **File**, click **Open**, type **%systemroot%\system32\config\netlogon.dns** in the **File Name** box, and then press ENTER.
17. Examine the default SRV records.

Domain Controller Location



Key Points


When a client authenticates, it attempts to locate a domain controller in its site. If a client has not authenticated before, it queries `_ldap._tcp.domainName`, and retrieves a list of all DCs in the domain. The client attempts an LDAP bind with each, and the first DC to respond is selected for the next step. Note that, at this point, it is possible that a DC in another site responds first.

The client then attempts to authenticate with the DC. The DC examines the client's IP address and compares it to the information about sites and subnets. If the DC is not in the client's site, it tells the client what site the client is in.

The client then queries DNS for `_ldap._tcp.siteName.domainName`, which returns a list of domain controllers that are covering that site. Again, the client attempts an LDAP bind with each, and the first one to respond is selected. The client then proceeds to authenticate with that DC.

The client stores its site membership in the registry, and it forms an affinity with the DC with which it authenticated. The next time the client needs to contact a DC, it starts with its affinity DC. If that DC is not available, the client retrieves its site information from the registry and queries for _ldap._tcp.siteName.domainName.

The process is summarized in the slide below:

- 
1. New client queries for all DCs in the domain
 - Retrieves SRVs from _tcp.domain
 2. Attempts LDAP bind to all
 3. First DC to respond
 - Examines client IP and subnet definitions
 - Refers client to a site
 4. Client stores site in registry
 5. Client queries for all DCs in the site
 - Retrieves SRVs from _tcp.site._sites.domain
 6. Attempts LDAP bind to all
 7. First DC to respond
 - Authenticates client
 - Client forms affinity
 8. Subsequently
 - Client binds to affinity DC
 - DC offline? Client queries for DCs in registry-stored site
 - Client moved to another site? DC refers client to another site

Domain controller location will be revisited in Module 12, where you will learn how SRV records and the domain controller location process serve to localize authentication to an efficient domain controller.

Read-Only DNS Zones

- DNS server on an RODC with Active Directory-integrated zones
- RODC can resolve client queries
- Changes not allowed on the read-only DNS zone
 - Records cannot be added manually
 - Dynamic updates cannot be made
- Dynamic updates are "referred" to writeable DC
 - Client attempts update
 - RODC returns an SOA of a writeable Windows Server 2008 domain controller
- RODC performs "replicate single object" (RSO)
 - Replicates the updated DNS record for the client it referred from the DC it referred the client to

Key Points

A DNS server on a Read-Only Domain Controller (RODC) can be authoritative for zones that are replicated to the RODC, and can resolve queries for clients that use the RODC as their DNS server.

Of course, a key characteristic of an RODC is that it cannot make changes to Active Directory, so resource records cannot be added manually to the zone on an RODC, and dynamic updates are not accepted from clients.

Dynamic updates are serviced by referring clients to a writeable DC when they attempt to send an update to an RODC. It is useful for the RODC to include the client's updated resource record in the zone as quickly as possible, so the RODC keeps track of the client that attempted the update, and the writable DC to which the client was referred. After a short wait, the RODC performs a "replicate single object" (RSO) operation, in which it retrieves the updated DNS record for the client from the writable DC, bypassing standard replication mechanisms.

Lesson 4

Advanced DNS Configuration and Administration

- Resolving Single-Label Names
- Resolve Names Outside Your Domain
- Reverse Lookup Zone
- DNS Server and Zone Maintenance
- Test and Troubleshoot DNS Server
- Test and Troubleshoot DNS Client

You've learned how to configure a simple DNS implementation and how DNS supports AD DS. In this module, you will explore selected topics of advanced DNS configuration and administration.

Objectives

After completing this lesson, you will be able to:

- Understand and configure single-label name resolution.
- Configure advanced DNS server settings.
- Audit, maintain, and troubleshoot the DNS server role.

Resolving Single-Label Names

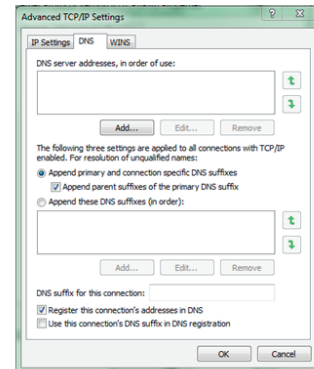
http://legalapp

- Client-side resolution process

1. Query DNS with fully qualified domain name (FQDN) created by adding
 - DNS suffix of client: ad.contoso.com
 - Domain name "devolution" ad.contoso.com then contoso.com
 - or
 - DNS suffix search order
 - Manage with Group Policy
2. WINS
 - 12 seconds = timeout!

- Server-side resolution

- GlobalNames Zone: Specialized zone with single-label CNAME RRs
- WINS forward lookup: If zone lookup fails, DNS queries WINS



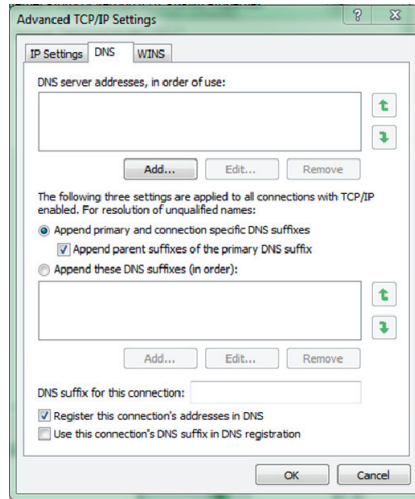
Key Points

In the normal course of operations, a user or application may want or need to refer to a host by a single-label name. For example, a user may open Internet Explorer and browse to `http://legalapp`.

It is important that you understand how the DNS Client service works to resolve a single-label name.

First, the client tries to resolve the name as a fully qualified name by appending a DNS domain suffix to the single-label name. The suffix is determined using one of the two following options, the first of which is configured in the Advanced TCP/IP Settings of a connection, and the second by using Group Policy.

- **The client's network connection DNS suffix.** The client appends the suffix of its DNS connection, such as ad.contoso.com. If using the connection-based suffix, you can optionally configure a client to use *domain name devolution*, which means that if the connection suffix fails, the client retries with the parent domain name, which would be contoso.com in this example. The devolution stops at that point—it does not query using a top-level domain name.



- **DNS suffix search order.** You can specify the DNS suffixes that a client should try. This is easiest to manage by using Group Policy. If DNS suffix search order is used, there is no devolution. You must specify *exactly* the domain names you want the client to try.

If the DNS suffix does not result in a resolution, the DNS client "gives up" and queries DNS with a single-label name. If this does not work, NetBIOS name resolution is attempted, which starts with a query to a Windows Internet Name Service (WINS) server and, if that fails, resorts to a NetBIOS broadcast on the local segment.

The DNS client does not have much time in which to resolve the name. In fact, after 12 seconds, the resolution fails, at which point it is up to the client application to determine what steps to take. This means that it's possible that the client will time out before all name combinations are queried.

Windows Server 2008 DNS Server provides a new option to support the resolution of single-label names: the GlobalNames zone. The GlobalNames zone is a specialized zone that you create on your DNS servers. Typically you would want it to be replicated in the ForestDNSZones partition so that it is available to all DNS servers in the forest. The zone contains CNAME records with a single-label names and their resolution to fully-qualified domain names.

When a client submits a single-label query, the DNS server can resolve the query by retrieving the CNAME record from the GlobalNames zone and then looking up the appropriate A record for the FQDN.

To use GlobalNames, you must create the GlobalNames zone, then enable its use in resolution using the dnscmd.exe command. Details are available in the article listed under "Additional Reading."

Additional Reading

- Providing Single-Label DNS Name Resolution
<http://go.microsoft.com/fwlink/?LinkId=168531>
- Deploying the GlobalNames Zone
<http://go.microsoft.com/fwlink/?LinkId=168532>

Resolve Names Outside Your Domain

- **Secondary zone**
 - Create a copy of a zone from another DNS server
 - Requires permissions from the master DNS server
- **Forwarders**
 - Send unresolved query as recursive query to other DNS server(s)
- **Root hints**
 - Begin iterative queries against root, ".", name servers
 - DNS server has list of root servers updated with Windows Update
- **Conditional forwarders**
 - Send unresolved query for specific domain to other server(s)
- **Stub zone**
 - Can be for *any* domain; dynamically updates NS records
 - Requires TCP Port 53 to be open to *all* name servers in the domain

Key Points

There are several ways to provide resolution for DNS records outside of your domain—records for which your DNS servers are not authoritative.

- **Secondary zone.** The first option is to make the servers authoritative by hosting a secondary zone of the external domain. This requires permission to perform a zone transfer from a name server in the zone, so it is typically not an option that is available for you to use for domains outside of your enterprise.
- **Forwarders.** Forwarders, detailed in Lesson 2, are pointers to upstream DNS servers, DNS servers provided by your ISP, or Internet DNS servers. Your DNS server can perform queries against servers listed as forwarders.

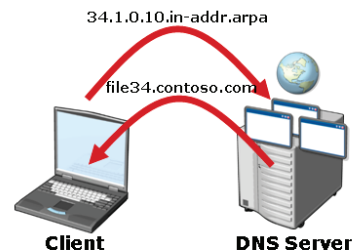
If you choose to point to a DNS server other than one which you or your ISP maintain, it is best to ask permission before performing recursive queries against a third-party DNS server.

- **Root hints.** Root hints point to name servers for the root of the DNS namespace ("."). DNS server has a list of root servers that is updated by Windows Update, although the list does not change often.

- **Conditional Forwarders.** Conditional Forwarders point to name servers against which to query for specific domain names. A conditional forwarder creates a "direct shortcut" to a server to query for a domain, and bypasses the need to recursively query a (non-conditional) forwarder, or to go to the root of the DNS namespace with a root hint.
- **Stub zone.** You learned about stub domains earlier in this module, as they can be used as a form of delegation for a child domain. Stub domains can also be very useful for resolving names outside your enterprise. Remember that the key benefit of a stub domain is that the DNS server dynamically maintains the list of name servers for the domain. You can think of a stub zone as a dynamic conditional forwarder. The "cost" is that TCP port 53 must be open to all name servers of the domain.

Reverse Lookup Zone

- Query for IP address, response with host name
- IP address is reversed (specific-to-generic) and appended with in-addr.arpa domain
 - IP address: 10.0.1.34
 - Query: 34.1.0.10.in-addr.arpa
- Special domain to support this: in-addr.arpa
 - Pointer (PTR) record with name (IP octet) and data (hostname)
 - Fixed IP client registers its PTR
 - DHCP server registers PTR for client
- Not required, but recommended
 - Services/applications use reverse lookup as a security check: Who is this request coming from?



Key Points

Whereas a typical DNS query requests an IP address for a host name, a reverse lookup requests a host name for a given IP address.

A fully qualified name is processed right-to-left, from most generic (such as .com) to most specific (such as technet). But an IP address is more generic on the left—the first octet is the most generic, and the last octet is the most specific. Therefore, to submit a DNS query with an IP address, the client *reverses the order of the octets* and appends a reserved domain name, in-addr.arpa.

So if a client wants to know the host name for the computer with the IP address 10.0.1.34, it queries for **34.1.0.10.in-addr.arpa**.

If you recall the domain name system hierarchy, you'll remember that the root is indicated by a ".", and below it are the most "generic" domains—the top-level domains. As you navigate down the hierarchy, you get more specific. The in-addr.arpa domain is the top-level domain for reverse lookups. Below it are domains for each octet of IP addresses. This suggests that DNS supports only standard subnet masks, where the subnet mask for an octet is either 0 or 255. Although this is true on the Internet as a whole, Windows Server 2008 DNS Server allows you to create subnetted reverse lookup zones if you require them.

Like forward lookup zones, reverse lookup zones have resource records. The most typical RR in a reverse lookup zone is the Pointer (PTR) record, with the name set to the value of the last octet of a host's IP address and the data of the record as the host's fully qualified domain name.

Also like forward lookup zones, reverse lookup zones support dynamic updates. By default, when Windows DHCP Server assigns an IP address to a client, the DHCP server registers the PTR record for the client.

Reverse lookup zones are not required, but they are recommended. Some applications and services use reverse lookups as a security check, to validate the identity of a request from a client. The application can use the IP address of the client to look up its PTR record, and then can validate that the A record for the host matches. Assuming secure updates are in place, that ensures that the request is from the correct client.

DNS Server and Zone Maintenance

- Scavenge stale resource records
 - Important in dynamic environments, particularly for SRV RRs
 - Server aging and scavenging properties
 - Defaults for Active Directory-integrated zones
 - Zone aging and scavenging properties
 - Active Directory-integrated zone inherits server property or per-zone
 - Primary zone ignores server property; must set per-zone.
 - Scavenging
 - Configure automatic scavenging: Server properties → Advanced
 - Manually launch scavenging: Right-click server
- Manage the cache
 - View the cache: View menu → Advanced Features
 - Clear server cache: Right-click server or Cached Lookups node

Key Points

The DNS Server role is fairly self-maintaining; however, one feature is important to configure in a zone that supports dynamic updates: scavenging. Scavenging is the process of deleting aged records. It is important not only for client and server A records, but more so for SRV records registered by domain controllers. In certain scenarios, it's possible to have SRV records that refer to incorrect, moved, or removed domain controllers. Scavenging ensures that they are eventually removed.

You can implement scavenging at the server or zone level for Active Directory-integrated zones. The server's Properties dialog box allows you to set server aging and scavenging properties, which act as the default for Active Directory-integrated zones, which inherit the server properties. You can override the server defaults on a zone-by-zone basis by using the zone's Properties dialog box.

For standard primary zones, you must set scavenging at the zone level.

After you've specified the time limits after which scavenging of records is allowed, you must actually perform the scavenging. This is most easily managed by configuring the server for automatic scavenging, which can be done on the Advanced tab of the server's Properties dialog box. You can also manually initiate scavenging by right-clicking the server in the DNS Manager snap-in.

Another server maintenance task which you may need to perform is viewing or flushing the cache. This is useful when you discover that clients are obtaining incorrect resolutions from a server for zones for which it is not authoritative. You can view the Cached Lookups of a server by clicking the View menu in the DNS Manager snap-in and selecting Advanced Features. You can then clear the server cache, if necessary, by right-clicking the server node or the Cached Lookups node in the console tree.

Test and Troubleshoot DNS Server

- Event logs
 - Visible in DNS Manager, Server Manager, and Event Viewer
- Debug logging
 - Server Properties dialog box
- Recursive and iterative query tests
 - Server Properties dialog box
- `dcdiag.exe /test:DNS`
 - Performs a wide variety of tests to ensure that AD DS and DNS are working well together
- Network Monitor (packet capture)

Key Points

DNS events are logged in the DNS log, which is exposed in DNS Manager, Server Manager, and Event Manager. As with other event logs in Windows Server 2008, you can centralize the collection of events using subscriptions, as detailed in Module 13. This is a recommended practice, as it allows you to keep an eye on a central location for signs of trouble in your DNS infrastructure.

Occasionally, it may be useful to perform debug logging, which logs details of DNS transactions. You can enable debug logging in the server's Properties dialog box.

Also in the server's Properties dialog box, you can perform test recursive and iterative queries, to ensure that stub zones, conditional forwarders, forwarders, and root hints are working as expected.

The integration between DNS and AD DS was detailed in Lesson 3. The `dcdiag.exe /test:DNS` command performs an exhaustive series of tests to ensure that this integration is working. You can perform a more granular test if you suspect a specific problem. Type `dcdiag.exe /?` for more details.

Test and Troubleshoot DNS Client

- `ipconfig /all`
- `NSLookup`
 - `set server=IP address` [Default: Primary DNS Server]
 - `set type=record type` [Default: A]
 - `record`
- `ipconfig /displaydns` : display client DNS resolver cache
- `ipconfig /flushdns` : purge client DNS resolver cache
- `ipconfig /registerdns` : register client DNS records

Key Points

In the end, DNS and the DNS Server role are about resolving client queries. Sometimes you need to troubleshoot the client-side experience and components of DNS.

You can use the following commands to troubleshoot the client side of DNS.

- **ipconfig /all.** This command will display the IP configuration of the client, including its DNS servers. Make sure that the client is using the correct servers, and that those servers are accessible.
- **NSLookup.** This performs DNS queries directly. A typical test with NSLookup includes:

```
set server=IP address
```

Which specifies the DNS server to query. The default is the primary DNS server of the client. When a response is received, NSLookup identifies the server that returned the response. If a reverse lookup zone is not available with a PTR record containing the IP address of the DNS server, the DNS server's name will display as Unknown, but its IP address will be identified. The next line is:

```
set type=record type
```

This line sets the type of record to query, such as SRV. The default is an address/host (A) record. The last line is:

```
record
```

This specifies the record to query, which is typically a fully qualified domain name when the resolution of an A record is being tested.

- **ipconfig /displaydns.** This command shows the contents of the DNS resolver cache on the client.
- **ipconfig /flushdns.** This purges the client's DNS resolver cache.
- **ipconfig /registerdns.** This command triggers a dynamic update in which the client registers its A records.

Lab B: Advanced Configuration of DNS

- Exercise 1: Enable Scavenging of DNS Zones
- Exercise 2: Create Reverse Lookup Zones
- Exercise 3: Explore Domain Controller Location
- Exercise 4: Configure Name Resolution for External Domains

Logon information

Virtual machine	6425B-HQDC01-B	6425B-HQDC02-B	6425B-TSTDC01-A	6425B-BRANCHDC01-B
Logon user name	Do not Logon	Pat.Coleman	Sara.Davis	Do not Logon
Administrative user name		Pat.Coleman_Admin	Sara.Davis_Admin	
Password		Pa\$\$w0rd	Pa\$\$w0rd	

Estimated time: 60 minutes

Scenario

You are the DNS administrator at Contoso, Ltd. You want to improve the health and efficiency of your DNS infrastructure by enabling scavenging and by creating a reverse lookup zone for the domain. You also want to examine the records that enable clients to locate domain controllers. Finally, you are asked to configure name resolution between contoso.com and the domain of a partner company, tailspintoys.com.

Exercise 1: Enable Scavenging of DNS Zones

In this exercise, you will enable scavenging of DNS zones, in order to remove stale resource records.

The main tasks for this exercise are as follows:

1. Prepare for the lab.
2. Enable scavenging of a DNS zone.
3. Configure default scavenging settings.

► Task 1: Prepare for the lab

Some of the virtual machines should already be started and available after completing Lab A. However, if they are not, you should step through Exercises 1 and 2 in Lab A before continuing as there are dependencies between Lab A and Lab B.

1. Start 6425B-HQDC01-B.
2. Log on to HQDC01 as **Pat.Coleman** with the password **Pa\$\$w0rd**.
3. Open **D:\Labfiles\Lab10b**.
4. Run **Lab10b_Setup.bat** with administrative credentials. Use the account **Administrator** with the password **Pa\$\$w0rd**.
5. The lab setup script runs. When it is complete, press any key to continue.
6. Close the Windows Explorer window, **Lab10b**.
7. Start 6425B-HQDC02-B.
8. Log on to HQDC02 as **Pat.Coleman** with the password **Pa\$\$w0rd**.
9. Start 6425B-TSTDC01-A.
10. Log on to TSTDC01 as **Sara.Davis** with the password **Pa\$\$w0rd**.
11. Start 6425B-BRANCHDC01-B.
12. Wait for BRANCHDC01 to complete startup before continuing.

► **Task 2: Enable scavenging of a DNS zone**

1. On HQDC02, run DNS Manager as an administrator, with the user name **Pat.Coleman_Admin** and the password **Pa\$\$wOrd**.
2. Enable scavenging for the contoso.com zone. Accept the defaults for scavenging-related intervals.

► **Task 3: Configure default scavenging settings**

- Configure HQDC02 so that, by default, scavenging is enabled for all zones. Accept the defaults for scavenging-related intervals.

Results: After this exercise, you will have configured scavenging of the contoso.com domain and enabled scavenging as the default for all zones.

Exercise 2: Create Reverse Lookup Zones

In this exercise, you will create a reverse lookup zone for the contoso.com domain.

The main tasks for this exercise are as follows:

1. Create a reverse lookup zone.
2. Explore and verify the functionality of a reverse lookup zone.

► Task 1: Create a reverse lookup zone

- Create a reverse lookup zone for IPv4 network 10. Allow only secure dynamic updates, and replicate the zone to all domain controllers in the contoso.com domain.



Note: In a production environment you would most likely just replicate to all DNS servers. However for the purposes of our lab we will replicate to all domain controllers to ensure quick and guaranteed replication

► Task 2: Explore and verify the functionality of a reverse lookup zone

1. Run the command prompt as an administrator, with the user name **Pat.Coleman_Admin** and the password **Pa\$\$w0rd**.
2. Type **nslookup www.development.contoso.com**, and then press ENTER.
Note that the first section of the command output, which identifies the DNS server that was queried, indicates the IP address of the server but, next to Server, reports that the server is Unknown. That is because the nslookup.exe command cannot resolve the IP address to a name.
3. Switch to DNS Manager.
4. In the console tree, click the **10.in-addr.arpa** zone under **Reverse Lookup Zones**.
5. Examine the records in the zone.
6. Switch to the command prompt.
7. Type **ipconfig /registerdns**, and then press ENTER.
8. Switch to DNS Manager.
9. Right-click the **10.in-addr.arpa** zone, and then click **Refresh**.

10. Examine the resource records that have appeared.
11. Switch to the command prompt.
12. Type **nslookup www.development.contoso.com**, and then press ENTER.

Note that the DNS server that was queried at 10.0.0.12 is now resolved to its name.

Results: After this exercise, you will have created and experienced the functionality of a reverse lookup zone.

Exercise 3: Explore Domain Controller Location

In this exercise, you will examine the resource records that allow clients to locate domain controllers.

The main tasks for this exercise are as follows:

1. Explore `_tcp`.
2. Explore `_tcp.brancha._sites.contoso.com`.

► **Task 1: Explore `_tcp`**

- Examine the records in `_tcp.contoso.com`. What do the records represent?

► **Task 2: Explore `_tcp.brancha._sites.contoso.com`**

- Examine the records in `_tcp.brancha._sites.contoso.com`. What do the records represent?

Results: After this exercise, you will have examined the Service Locator (SRV) records in the `contoso.com` domain.

Exercise 4: Configure Name Resolution for External Domains

In this exercise, you will configure name resolution between two completely separate domains.

The main tasks for this exercise are as follows:

1. Configure a stub zone.
2. Configure a conditional forwarder.
3. Validate name resolution for external domains.

► Task 1: Configure a stub zone

- On HQDC02, create a stub zone for `tailspintoys.com` that refers to the IPv4 address **10.0.0.31** as the master server.

► Task 2: Configure a conditional forwarder

1. On TSTDC01, run DNS Management as an administrator, with the user name **Sara.Davis_Admin** and the password **Pa\$\$w0rd**.
2. Create a conditional forwarder for `contoso.com` that forwards to the IPv4 address **10.0.0.11**.

► Task 3: Validate name resolution for external domains

1. On TSTDC01, open a command prompt and type **nslookup www.development.contoso.com**, and then press ENTER. The command should return the address **10.0.0.24**.
2. Switch to DNS Manager and create a host (A) record for `www.tailspintoys.com` that resolves to **10.0.0.143**.
3. On HQDC02, open a command prompt and type **nslookup www.tailspintoys.com**, and then press ENTER. The command should return the address **10.0.0.143**.

Results: After this exercise, you will have configured DNS name resolution between the `contoso.com` and `tailspintoys.com` domains.



Note: After completing this exercise, turn off all virtual machines and discard undo disks.

Lab Review Questions

Question: In this lab, you used a stub zone and a conditional forwarder to provide name resolution between two distinct domains. What other options might you have chosen to use?

Module 11

Administer Active Directory® Domain Services (AD DS) Domain Controllers (DCs)

Contents:

Lesson 1: Domain Controller Installation Options	11-4
Lab A: Install Domain Controllers	11-31
Lesson 2: Install a Server Core DC	11-39
Lab B: Install a Server Core DC	11-47
Lesson 3: Manage Operations Masters	11-52
Lab C: Transfer Operations Master Roles	11-71
Lesson 4: Configure DFS-R Replication of SYSVOL	11-76
Lab D: Configure DFS-R Replication of SYSVOL	11-84

Module Overview

- Domain Controller Installation Options
- Install a Server Core DC
- Manage Operations Masters
- Configure DFS-R Replication of SYSVOL

Domain controllers (DCs) host the directory service and perform the services that support identity and access management in a Windows® enterprise. To this point in the course, you have learned to support the logical and management components of an Active Directory® directory service infrastructure: users, groups, computers, and Group Policy. Each of these components is contained in the directory database and in SYSVOL on DCs. In this module, you will begin your exploration of the service-level components of Active Directory, starting with the DCs themselves. You will learn how to add Windows Server® 2008 DCs to a forest or domain, how to prepare a Windows Server 2003 forest or domain for its first Windows Server 2008 DC, how to manage the roles performed by DCs, and how to migrate the replication of SYSVOL from the File Replication Service (FRS) used in previous versions of Windows to the Distributed File System Replication (DFS-R) mechanism that provides more robust and manageable replication.

Objectives

After completing this module, you will be able to:

- Install a standard or read-only domain controller into new or existing domains or trees.
- Add and remove domain controllers using a variety of GUI or command-line methods.
- Configure a domain controller on Server Core.
- Understand and identify operations master roles.
- Manage the placement, transfer, and seizure of operations master roles.
- Migrate SYSVOL replication from FRS to DFS-R.

Lesson 1

Domain Controller Installation Options

- Install a DC with the Windows Interface
- Unattended Installation Options and Answer Files
- Install a New Windows Server 2008 Forest
- Prepare an Existing Domain for Windows Server 2008 DCs
- Install an Additional DC in a Domain
- Install a New Windows Server 2008 Child Domain
- Install a New Domain Tree in a Forest
- Stage the Installation of an RODC
- Attach a Serve to a Prestaged RODC Account
- Install AD DS from Media
- Remove a Domain Controller

In Module 1, "Introducing Active Directory Domain Services," you used the Add Roles Wizard in Server Manager to install Active Directory Domain Services (AD DS). Then you used the Active Directory Domain Services Installation Wizard to create the first DC in the contoso.com forest. Because DCs are critical to authentication, it is highly recommended to maintain at least two DCs in each domain in your forest to provide a level of fault tolerance in the event that one DC fails. You might also need to add DCs to remote sites or create new domains or trees in your Active Directory forest. In this lesson, you will learn user-interface, command-line, and unattended methods for installing DCs in a variety of scenarios.

Objectives

After completing this lesson, you will be able to:

- Install a DC using the Windows interface, dcpromo.exe command-line parameters, or an answer file for unattended installation.
- Add Windows Server 2008 DCs to a domain or forest with Windows Server 2003 and Windows 2000 Server DCs.
- Create new domains and trees.
- Perform a staged installation of a read-only DC.
- Install a DC from installation media to reduce network replication.
- Remove a DC.

Install a DC with the Windows Interface

- Two major steps
 - Add the AD DS role
 - Install and configure AD DS with the Active Directory Domain Services Installation Wizard
- DCPROMO.exe
 - Installs the AD DS role if it is not already installed

Key Points

If you want to use the Windows interface to install a DC, there are two major steps. First, you must install the AD DS role, which, as you learned in Module 1, "Introducing Active Directory Domain Services", can be accomplished using the Add Roles Wizard in Server Manager. After the AD DS role installation has copied the binaries required for the role to the server, you must install and configure AD DS by launching the Active Directory Domain Services Installation Wizard, using one of these methods:

- Click **Start** and, in the **Start Search** box, type **dcpromo**. Then click **OK**. When you complete the Add Roles Wizard, click the link to launch the Active Directory Domain Services Installation Wizard.
- After adding the AD DS role, links will appear in Server Manager that remind you to run the Active Directory Domain Services Installation Wizard. Click any of those links.



Note: All-in-one wizard. Microsoft documentation for Windows Server 2008 emphasizes the role-based model, so it recommends that you add the AD DS role and then run Dcpromo.exe (the Active Directory Domain Services Installation Wizard). However, you can simply run Dcpromo.exe and, as a first step, the wizard detects that the AD DS binaries are not installed and adds the AD DS role automatically.

Unattended Installation Options and Answer Files

- Options can be specified at the command line
 - */option:value* – for example,
/newdnsdomainname:contoso.com
 - **dcpromo.exe /?[:operation]** for help
- Options can be specified in an answer file

```
[DCINSTALL]
NewDomainDNSName=contoso.com
```

 - And called using
dcpromo.exe /unattend:"*path to answer file*"
- Options on command line will override answer file
- Options not specified will be prompted by wizard
 - Except in Server Core
- Recommendation: use dcpromo.exe on full installation and export answer file for command line or Server Core

Key Points

You can also add or remove a DC at the command line, using unattended installation supported by the Windows Server 2008 version of dcpromo.exe. Unattended installation options provide values to the Active Directory Domain Services Installation Wizard. For example, the NewDomainDNSName option specifies a fully qualified domain name (FQDN) for a new domain.

These options can be provided at the command line by typing dcpromo */unattendOption:value*, for example, dcpromo /newdomaindnsname:contoso.com. Alternatively, you can provide the options in an unattended installation answer file. The answer file is a text file that contains a section heading, [DCINSTALL], followed by options and their values in the *option=value* form. For example, the following file provides the NewDomainDNSName option:

```
[DCINSTALL]
NewDomainDNSName=contoso.com
```

The answer file is called by adding its path to the unattend parameter, for example:

dcpromo /unattend:"path to answer file"

The options in the answer file can be overridden by parameters on the command line. For example, if the NewDomainDNSName option is specified in the answer file and the /NewDomainDNSName parameter is used on the command line, the value on the command line takes precedence. If any required values are neither in the answer file nor on the command line, the Active Directory Domain Services Installation Wizard will prompt for the answers, so you can use the answer file to partially automate an installation, providing a subset of configuration values to be used during an interactive installation.

The wizard is not available when running dcpromo.exe from the command line in Server Core. In that case, the dcpromo.exe command will return with an error code.

For a complete list of parameters that you can specify as part of an unattended installation of AD DS, open an elevated command prompt and type the following command:

dcpromo /?[:operation]

where *operation* is one of the following:

- **Promotion** returns all parameters you can use when creating a domain controller.
- **CreateDCAccount** returns all parameters you can use when creating a prestaged account for a read-only domain controller (RODC).
- **UseExistingAccount** returns all parameters you can use to attach a new DC to a prestaged RODC account.
- **Demotion** returns all parameters you can use when removing a domain controller.

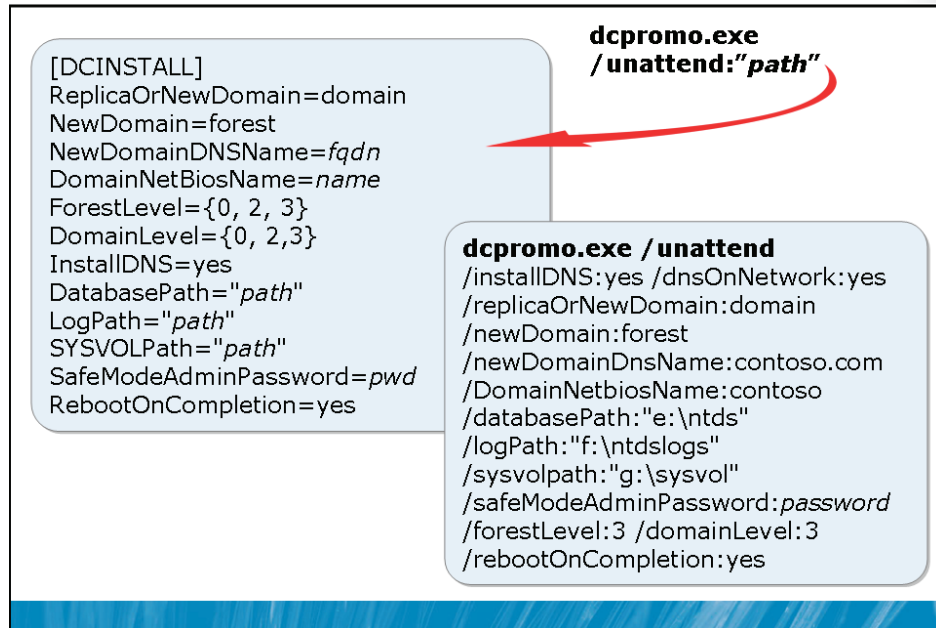


Note: Generate an answer file. When you use the Windows interface to create a domain controller, the Active Directory Domain Services Installation Wizard gives you the option, on the Summary page, to export your settings to an answer file. If you need to create an answer file for use from the command line—for example, on a Server Core installation—you can use this shortcut to create an answer file with the correct options and values.

Additional Reading

- For a complete reference of dcpromo parameters and unattended installation options, see:
<http://go.microsoft.com/fwlink/?LinkId=168475>

Install a New Windows Server 2008 Forest



Key Points

Module 1, "Introducing Active Directory Domain Services," discussed the installation of the first Windows Server 2008 DC in a new forest, using the Windows interface. In that module, you learned the detailed steps to add the AD DS role to a server by using Server Manager and then running Dcpromo.exe to promote the server to a domain controller. When creating a new forest root domain, you must specify the forest root domain name system (DNS) name, its NetBIOS name, and the forest and domain functional levels. The first domain controller cannot be a read-only domain controller and must be a global catalog (GC) server. If the Active Directory Domain Services Installation Wizard detects that it is necessary to install or configure DNS, it does it automatically.

You can also use an answer file by typing **dcpromo /unattend:"path to answer file"** where the answer file contains unattended installation options and values. The following example contains the minimum parameters for an unattended installation of a new Windows Server 2008 domain controller in a new forest:

```
[DCINSTALL]
ReplicaOrNewDomain=domain
NewDomain=forest
NewDomainDNSName=fully qualified DNS name
DomainNetBiosName=domain NetBIOS name
ForestLevel={0=Windows 2000 Server Native;
              2=Windows Server 2003 Native;
              3=Windows Server 2008}
DomainLevel={0=Windows Server 2000 Native;
              2=Windows Server 2003 Native;
              3=Windows Server 2008}
InstallDNS=yes
DatabasePath="path to folder on a local volume"
LogPath="path to folder on a local volume"
SYSVOLPath="path to folder on a local volume"
SafeModeAdminPassword=password
RebootOnCompletion=yes
```

You can also specify one or more unattended installation parameters and values at the command line. For example, if you don't want the Directory Services Restore Mode password in the answer file, leave the entry blank and specify the **/SafeModeAdminPassword:***password* parameter when you run dcpromo.exe.

You can also include all options on the command line itself. The following example creates the first DC in a new forest in which you don't expect to install any Windows Server 2003 domain controllers:

```
dcpromo /unattend /installDNS:yes /dnsOnNetwork:yes
        /replicaOrNewDomain:domain /newDomain:forest
        /newDomainDnsName:contoso.com /DomainNetbiosName:contoso
        /databasePath:"e:\ntds" /logPath:"f:\ntdslogs"
        /sysvolpath:"g:\sysvol"
        /safeModeAdminPassword:password /forestLevel:3 /domainLevel:3
        /rebootOnCompletion:yes
```

Prepare an Existing Domain for Windows Server 2008 DCs

- ADPrep (adprep.exe) prepares AD DS for the first DC running a version of Windows *newer* than current DCs
 - DVD:\sources folder
- adprep /forestprep
 - Log on to the Schema master (see Lesson 3) as a member of Enterprise Admins, Schema Admins, *and* Domain Admins
 - Run once per forest. Wait for change to replicate.
- adprep /domainprep /gpprep
 - Log on to Infrastructure master (see Lesson 3) as a member of Domain Admins
 - Run once per domain. Wait for change to replicate.
- adprep /rodcprep
 - Log on to any computer as a member of Enterprise Admins
 - Run once per forest. Wait for change to replicate

Key Points

If you have an existing forest with DCs running Windows Server 2003 or Windows 2000 Server, you must prepare them prior to creating your first Windows Server 2008 DC.

The ADPrep command is used to prepare Active Directory for a DC that is running a version of Windows Server that is newer than the existing DCs in the forest or domain. Adprep.exe is a command-line tool that is included on the installation disk of each version of Windows Server. Adprep.exe performs operations that must be completed in an existing Active Directory environment before you can add a DC that runs that version of Windows Server.

Adprep.exe has parameters that perform a variety of operations that help prepare an existing Active Directory environment for a DC that runs a later version of Windows Server. Not all versions of Adprep.exe perform the same operations, but generally the different types of operations that Adprep.exe can perform include the following:

- Updating the Active Directory schema
- Updating security descriptors
- Modifying access control lists (ACLs) on Active Directory objects and on files in the SYSVOL shared folder
- Creating new objects, as needed
- Creating new containers, as needed

To prepare the forest for the first DC running Windows Server 2008, follow these steps:

1. Log on to the schema master as a member of the **Enterprise Admins**, **Schema Admins**, and **Domain Admins** groups.

Lesson 3 discusses operations masters and provides steps for identifying which DC is the schema master.

2. Copy the contents of the **\sources\adprep** folder from the Windows Server 2008 DVD to a folder on the schema master.
3. Open an elevated command prompt, and change directories to the **adprep** folder.
4. Type **adprep /forestprep**, and then press ENTER.

You must allow time for the operation to complete. After the changes have replicated throughout the forest, you can continue to prepare the domains for Windows Server 2008.

To prepare a domain for the first DC running Windows Server 2008, perform these steps:

1. Log on to the domain infrastructure operations master as a member of **Domain Admins**.
Lesson 3 provides steps for identifying which DC is the infrastructure operations master.
2. Copy the contents of the **\sources\adprep** folder from the Windows Server 2008 DVD to a folder on the infrastructure master.
3. Open a command prompt and change directories to the **adprep** folder.
4. Type **adprep /domainprep /gpprep**, and then press ENTER.

On Windows Server 2003, you might receive an error message stating that updates were unnecessary. You can ignore this message.

Allow the change to replicate throughout the forest before you install a DC that runs Windows Server 2008.

To prepare AD DS for the first RODC, follow these steps:

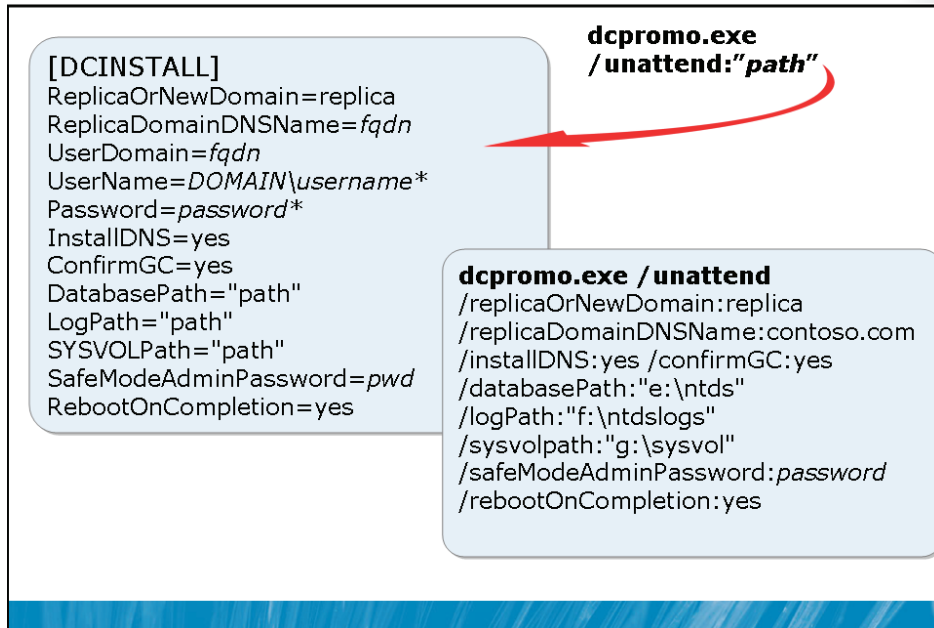
1. Log on to any computer as a member of the **Enterprise Admins**.
2. Copy the contents of the **\sources\adprep** folder from the Windows Server 2008 DVD to a folder on the computer.
3. Open an elevated command prompt, and change directories to the **adprep** folder.
4. Type **adprep /rodcprep**, and then press ENTER.

RODCPREP, anytime. You can also run **adprep /rodcprep** at any time in a Windows 2000 Server or Windows Server 2003 forest. It does not have to be run in conjunction with **/forestprep**; however, you must run it and allow its changes to replicate throughout the forest prior to installing the first RODC.

Additional Reading

- Running Adprep.exe:
<http://go.microsoft.com/fwlink/?LinkId=168477>
- ADPrep:
<http://go.microsoft.com/fwlink/?LinkId=168478>
- Windows Server 2008: Appendix of Changes to Adprep.exe to Support AD DS:
<http://go.microsoft.com/fwlink/?LinkId=168479>

Install an Additional DC in a Domain



Key Points

Additional DCs can be added by installing AD DS and launching the Active Directory Domain Services Installation Wizard. You are prompted to choose the deployment configuration; to enter network credentials; to select a domain and site for the new DC; and to configure the DC with additional options such as DNS Server, Global Catalog (GC), or Read-Only Domain Controller. The remaining steps are the same as for the first DC: configuring file locations and the Directory Services Restore Mode Administrator password.

If you have one DC in a domain, and if you select the Use Advanced Mode Installation check box on the Welcome To The Active Directory Domain Services Installation Wizard page, you are able to configure advanced options, which are:

- **Install From Media.** By default, a new domain controller replicates all data for all directory partitions it will host from other domain controllers during the Active Directory Domain Services Installation Wizard. To improve the performance of installation, particularly over slow links, you can use installation media created by existing domain controllers. Installation media is a form of backup. The new DC is able to read data from the installation media directly and then replicate only updates from other domain controllers. Install From Media (IFM) is discussed in the “Installing AD DS from Media” section.
- **Source Domain Controller.** If you want to specify the domain controller from which the new DC replicates its data, you can click Use This Specific Domain Controller.



Note: Dcpromo /adv is still supported. In Windows Server 2003, dcpromo /adv was used to specify advanced installation options. The adv parameter is still supported; it simply pre-selects the Use Advanced Mode Installation check box on the Welcome page.

To use Dcpromo.exe with command-line parameters to specify unattended installation options, you can use the minimal parameters shown in the following example:

```
dcpromo /unattend /replicaOrNewDomain:replica  
/replicaDomainDNSName:contoso.com /installDNS:yes /confirmGC:yes  
/databasePath:"e:\ntds" /logPath:"f:\ntdslogs"  
/sysvolpath:"g:\sysvol"  
/safeModeAdminPassword:password /rebootOnCompletion:yes
```

If you are not logged on to the server with domain credentials, specify the *userdomain* and *username* parameters as well. A minimal answer file for an additional domain controller in an existing domain is as follows:

```
[DCINSTALL]
ReplicaOrNewDomain=replica
ReplicaDomainDNSName=FQDN of domain to join
UserDomain=FQDN of domain of user account
UserName=DOMAIN\username (in Administrators group of the domain)
Password=password for user specified by UserName (* to prompt)
InstallDNS=yes
ConfirmGC=yes
DatabasePath="path to folder on a local volume"
LogPath="path to folder on a local volume"
SYSVOLPath="path to folder on a local volume"
SafeModeAdminPassword=password
RebootOnCompletion=yes
```


Install a New Windows Server 2008 Child Domain

[DCINSTALL]

```

ReplicaOrNewDomain=domain
NewDomain=child
ParentDomainDNSName=fqdn
UserDomain=fqdn
UserName= DOMAIN\username*
Password=password*
ChildName=name*
DomainNetBiosName=name
DomainLevel={0,2,3}*
InstallDNS=yes
CreateDNSDelegation=yes
DNSDelegationUserName=DOMAIN\
rname
DNSDelegationPassword=password
DatabasePath="path"
LogPath="path"
SYSVOLPath="path"
SafeModeAdminPassword=pwd
RebootOnCompletion=yes
          
```

dcpromo.exe /unattend:"path"

dcpromo.exe /unattend

```

/installDNS:yes
/replicaOrNewDomain:domain
/newDomain:child
/ParentDomainDNSName:contoso.com
/newDomainDnsName:na.contoso.com
/childName:subsidiary
/DomainNetbiosName:subsidiary
/databasePath:"e:\ntds"
/logPath:"f:\ntdslogs"
/sysvolpath:"g:\sysvol"
/safeModeAdminPassword:password
/forestLevel:3 /domainLevel:3
/rebootOnCompletion:yes
          
```

Key Points

If you have an existing domain, you can create a new child domain by creating a Windows Server 2008 domain controller. Before you do, however, you must run adprep /forestprep as described in the earlier section, "Preparing an Existing Domain for Windows Server 2008 DCs."

Then install AD DS and launch the Active Directory Domain Services Installation Wizard and, on the Choose A Deployment Configuration page, click Existing Forest and Create A New Domain In An Existing Forest. You are prompted to select the domain functional level. Because it is the first DC in the domain, it cannot be an RODC, and it cannot be installed from media. If you select the Use Advanced Mode Installation check box on the Welcome page, the wizard presents you with a Source Domain Controller page on which you specify a domain controller from which to replicate the configuration and schema partitions.

Using `dcpromo.exe`, you can create a child domain with the minimal options shown in the following command:

```
dcpromo /unattend /installDNS=yes
/replicaOrNewDomain:domain /newDomain:child
/ParentDomainDNSName:contoso.com
/newDomainDnsName:subsidiary.contoso.com /childName:subsidiary
/DomainNetbiosName:subsidiary
/databasePath:"e:\ntds" /logPath:"f:\ntdslogs"
/sysvolpath:"g:\sysvol"
/safeModeAdminPassword:password /forestLevel:3 /domainLevel:3
/rebootOnCompletion=yes
```

The following answer file reflects the same minimal parameters:

```
[DCINSTALL]
ReplicaOrNewDomain=domain
NewDomain=child
ParentDomainDNSName=FQDN of parent domain
UserDomain=FQDN of user specified by UserName
UserName= DOMAIN\username (has permissions to add a child domain)
Password=password for user specified by UserName or * for prompt
ChildName=single-label prefix for domain
        (Child domain FQDN will be ChildName.ParentDomainDNSName)
DomainNetBiosName=Domain NetBIOS name
DomainLevel=domain functional level (not lower than current forest
level)
InstallDNS=yes
CreateDNSDelegation=yes
DNSDelegationUserName=DOMAIN\username with permissions to create
        DNS delegation, if different than UserName,
above
DNSDelegationPassword=password for DNSDelegationUserName or * for
prompt
DatabasePath="path to folder on a local volume"
LogPath="path to folder on a local volume"
SYSVOLPath="path to folder on a local volume"
SafeModeAdminPassword=password
RebootOnCompletion=yes
```

Install a New Domain Tree in a Forest

```
[DCINSTALL]
ReplicaOrNewDomain=domain
NewDomain=tree
NewDomainDNSName=fqdn
DomainNetBiosName=name
UserDomain=fqdn
UserName= DOMAIN\username*
Password=password*
DomainLevel={0,2,3}*
InstallDNS=yes
CreateDNSDelegation=yes
DNSDelegationUserName=DOMA
rname
DNSDelegationPassword=passwo
DatabasePath="path"
LogPath="path"
SYSVOLPath="path"
SafeModeAdminPassword=pwd
RebootOnCompletion=yes
```

dcpromo.exe /unattend:"path"

```
dcpromo.exe /unattend
/installDNS:yes
/replicaOrNewDomain:domain
/newDomain:tree
/newDomainDnsName:tailspintoys.com
/DomainNetbiosName:tailspintoys
/databasePath:"e:\ntds"
/logPath:"f:\ntdslogs"
/sysvolpath:"g:\sysvol"
/safeModeAdminPassword:password
/domainLevel:2
/rebootOnCompletion:yes
```

Key Points

You learned in Module 1, "Introducing Active Directory Domain Services," that in an Active Directory forest, a tree is composed of one or more domains that share contiguous DNS namespace. So, for example, the contoso.com and subsidiary.contoso.com domains would be in a single tree.

Additional trees are simply additional domains in the same forest that are not in the same namespace. For example, if Contoso, Ltd, bought Tailspin Toys, the tailspintoys.com domain would be in a separate tree in the domain. There is very little functional difference between a child domain and a domain in another tree, and the process for creating a new tree is, therefore, very similar to creating a child domain.

First, you must run adprep /forestprep as described in the earlier section, "Preparing an Existing Domain for Windows Server 2008 DCs." Then you can install AD DS and run the Active Directory Domain Services Installation Wizard.

You must select Use Advanced Mode Installation on the Welcome page of the wizard. On the Choose A Deployment Configuration page, click Existing Forest, select Create A New Domain In An Existing Forest, and select Create A New Domain Tree Root Instead Of A New Child Domain. The rest of the process is identical to creating a new child domain.

The following options provided as parameters to dcpromo.exe create a new tree for the tailspintoys.com domain within the contoso.com forest:

```
dcpromo /unattend /installDNS:yes
/replicaOrNewDomain:domain /newDomain:tree
/newDomainDnsName:tailspintoys.com /DomainNetbiosName:tailspintoys
/databasePath:"e:\ntds" /logPath:"f:\ntdslogs"
/sysvolpath:"g:\sysvol"
/safeModeAdminPassword:password /domainLevel:2
/rebootOnCompletion:yes
```

The domain functional level is configured at 2—Windows Server 2003 Native—so the domain could include Windows Server 2003 domain controllers.

An unattended installation answer file that creates the same new tree would look similar to the following:

```
[DCINSTALL]
ReplicaOrNewDomain=domain
NewDomain=tree
NewDomainDNSName=FQDN of new domain
DomainNetBiosName=NetBIOS name of new domain
UserDomain=FQDN of user specified by UserName
UserName= DOMAIN\username (with permissions to create a new domain)
Password=password for user specified by UserName or * for prompt
DomainLevel=domain functional level (not lower than current forest
level)
InstallDNS=yes
ConfirmGC=yes
CreateDNSDNSDelegation=yes
DNSDelegationUserName=account with permissions to create DNS
delegation
                        required only if different than UserName, above
DNSDelegationPassword=password for DNSDelegationUserName or * for
prompt
DatabasePath="path to folder on a local volume"
LogPath="path to folder on a local volume"
SYSVOLPath="path to folder on a local volume"
SafeModeAdminPassword=password
RebootOnCompletion=yes
```

Stage the Installation of an RODC

- Create the account for the RODC
 - Right-click the Domain Controllers OU → Pre-Create Read-only Domain Controller Account
 - Delegation of RODC Installation and Administration
 - Delegate to a group
 - Members of the group can join RODC to domain
 - Members of the group are local Administrators after join
- Attach the server to the RODC account
 - Server must be a member of a *workgroup*
 - **dcpromo /UseExistingAccount:attach**

Key Points

As you remember from Module 9, "Improve the Security of Authentication in an Active Directory Domain Services (AD DS) Domain," RODCs are designed to support branch office scenarios by providing authentication local to the site while mitigating the security and data integrity risks associated with placing a DC in a less well-controlled environment. Many times, there are few or no IT support personnel in a branch office. How, then, should a domain controller be created in a branch office?

To answer this question, Windows Server 2008 enables you to create a staged, or delegated, installation of an RODC. The process includes two stages:

- **Create the account for the RODC.** A member of Domain Admins creates an account for the RODC in Active Directory. The parameters related to the RODC are specified at this time: the name, the Active Directory site in which the RODC will be created, and, optionally, the user or group that can complete the next stage of the installation.

- **Attach the server to the RODC account.** After the account has been created, AD DS is installed, and the server—which must be a member of a *workgroup* and not the domain—is joined to the domain and as an RODC attached to the prestaged account. These steps can be the users or groups specified when the RODC account was prestaged; these users do not require any privileged group membership. A server can also be attached by a member of Domain Admins or Enterprise Admins, but the ability to delegate this stage to a nonprivileged user makes it much easier to deploy RODCs in branches without IT support. The domain controller will replicate its data from another writable DC in the domain, or you can use the IFM method discussed in the “Installing AD DS from Media” section.

Creating the Prestaged Account for the RODC

To create the account for the RODC, using the Active Directory Users And Computers snap-in, right-click the Domain Controllers OU and choose Pre-Create Read-Only Domain Controller Account. A wizard appears that is very similar to the Active Directory Domain Services Installation Wizard. You are asked to specify the RODC name and site. You are also able to configure the password replication policy, as detailed in Module 9, “Improve the Security of Authentication in an Active Directory Domain Services (AD DS) Domain.”

On the Delegation Of RODC Installation And Administration page, you can specify one security principal—user or group—that can attach the server to the RODC account you create. The user or group will also have local administrative rights on the RODC after the installation. It is recommended that you delegate to a group rather than to a user. If you do not specify a user or group, only members of the Domain Admins or Enterprise Admins groups can attach the server to the account.

You can create prestaged RODC accounts by using `dcpromo.exe` with numerous parameters or by creating an answer file for `dcpromo.exe`. The steps for doing so are detailed at: <http://go.microsoft.com/fwlink/?LinkId=168471>.

Attach a Server to a Prestaged RODC Account

[DCINSTALL]
 ReplicaDomainDNSName=*fqdn*
 UserDomain=*fqdn*
 UserName= *DOMAIN\username**
 Password=*password**
 InstallDNS=yes
 ConfirmGC=yes
 DatabasePath="*path*"
 LogPath="*path*"
 SYSVOLPath="*path*"
 SafeModeAdminPassword=*pwd*
 RebootOnCompletion=yes

- GUI Active Directory Domain Services Wizard:
dcpromo.exe
/useexistingaccount:attach

dcpromo.exe
/useexistingaccount:attach
/unattend:"*path*"

dcpromo.exe /unattend
/UseExistingAccount:Attach
 /ReplicaDomainDNSName:contoso.com
 /UserDomain:contoso.com
 /UserName:contoso\dan
 /password:*
 /databasePath:"e:\ntds"
 /logPath:"f:\ntdslogs"
 /sysvolpath:"g:\sysvol"
 /safeModeAdminPassword:*password*
 /rebootOnCompletion:yes

Key Points

After you have prestaged the account, the server can be attached to it.

To attach a server to a prestaged RODC account:

1. Ensure that the server is a member of a workgroup, not a member of the domain.

Promote from a workgroup. When you create an RODC by using the staged approach—when you attach an RODC to a prestaged account—the server must be a member of a workgroup, not of the domain, when you launch **dcpromo.exe** or the Active Directory Domain Services Installation Wizard. The wizard will look in the domain for the existing account with its name and will attach to that account.

2. Run **dcpromo.exe /UseExistingAccount:attach**.

The wizard prompts for network credentials and then finds the RODC account in the domain indicated by the credentials. Remaining steps are similar to other domain controller promotion operations.

To use an answer file, provide the following options and values:

```
[DCINSTALL]
ReplicaDomainDNSName=FQDN of domain to join
UserDomain=FQDN of user specified by UserName
UserName=DOMAIN\username (in Administrators group of the domain)
Password=password for user specified by UserName
InstallDNS=yes
ConfirmGC=yes
DatabasePath="path to folder on a local volume"
LogPath="path to folder on a local volume"
SYSVOLPath="path to folder on a local volume"
SafeModeAdminPassword=password
RebootOnCompletion=yes
```

Run `dcpromo` with the `/unattend:"answer file path"` and the `/UseExistingAccount:Attach` options, as in the following example:

```
dcpromo /useexistingaccount:attach /unattend:"c:\rodcanwer.txt"
```

All the options just shown in the answer file can also be specified or overridden directly on the command line. Just type a command similar to the following:

```
dcpromo /unattend /UseExistingAccount:Attach
/ReplicaDomainDNSName:contoso.com
/UserDomain:contoso.com /UserName:contoso\dan /password:*
/databasePath:"e:\ntds" /logPath:"f:\ntdslogs"
/sysvolpath:"g:\sysvol"
/safeModeAdminPassword:password /rebootOnCompletion:yes
```


Install AD DS from Media

- Install from media (IFM)
- Create installation media—a specialized backup of AD DS
- Use installation media for creation of DC
 - Significantly reduce over-the-network replication
- DC will need to replicate changes since backup was made
- `ntdsutil` – activate instance `ntds` – `ifm`
 - create `sysvol full path` : media with `sysvol` for writable DC
 - create `full path` : media without `sysvol` for writable DC
 - create `sysvol rodc path` : media with `sysvol` for read-only DC
 - create `rodc path` : media without `sysvol` for read-only DC
- Active Directory Domain Services Installation Wizard, select **Use Advanced Mode**
 - **ReplicationSourcePath** option/switch

Key Points

When you add domain controllers to a forest, data from existing directory partitions are replicated to the new DC. In an environment with a large directory or where bandwidth is constrained between a new DC and a writable DC from which to replicate, you can install AD DS more efficiently by using the install-from-media (IFM) option.

Installing from media involves creating installation media—a specialized backup of Active Directory that can be used by the Active Directory Domain Services Installation Wizard as a data source for populating the directory on a new DC. Then the new DC will replicate only updates from another writable DC. So if the installation media is recent, you can minimize the impact of replication to a new DC.

Remember that it is not only the directory that must be replicated to a new DC, but SYSVOL as well. When you create your installation media, you can specify whether to include SYSVOL on the installation media.

Using IFM also allows you to control the timing of impact to your network bandwidth. You can, for example, create installation media and transfer it to a remote site during off hours, and then create the domain controller during normal business hours. Because the installation media is from the local site, impact to the network is reduced, and only updates will be replicated over the link to the remote site.

To create installation media:

1. Open an elevated command prompt on a writable domain controller, running Windows Server 2008.

The installation media can be used to create both writable and read-only DCs.

2. Run **ntdsutil.exe**.
3. At the **ntdsutil** prompt, type **activate instance ntds**, and then press ENTER.
4. Type **ifm**, and then press ENTER.
5. At the **ifm:** prompt, type one of the following commands, based on the type of installation media you want to create:
 - **create sysvol full path**. Creates installation media with SYSVOL for a writable domain controller in the folder specified by *path*.
 - **create full path**. Creates installation media without SYSVOL for a writable domain controller or an Active Directory Lightweight Directory Services (AD LDS) instance in the folder specified by *path*.
 - **create sysvol rodc path**. Creates installation media with SYSVOL for a read-only domain controller in the folder specified by *path*.
 - **create rodc path**. Creates installation media without SYSVOL for a read-only domain controller in the folder specified by *path*.

When you run the Active Directory Domain Services Installation Wizard, select the Use Advanced Mode Installation check box, and you will be presented with the Install From Media page later in the wizard. Choose Replicate Data From Media At The Following Location. You can use the ReplicationSourcePath installation option in an answer file or on the dcpromo.exe command line.

Remove a Domain Controller

[DCINSTALL]

```

UserName= DOMAIN\username*
UserDomain=fqdn
Password=password*
AdministratorPassword=password*
RemoveApplicationPartitions=yes
RemoveDNSDelegation=yes
DNSDelegationUserName=DOMAIN\user
name
DNSDelegationPassword=password*

```

- GUI Active Directory Domain Services Wizard:
dcpromo.exe
- Command line:
dcpromo.exe /uninstallbinaries
- If DC cannot contact the domain
dcpromo /forceremoval
 - Then you must clean up metadata: KB 216498

dcpromo.exe
/uninstallbinaries
/unattend:"path"

dcpromo.exe /unattend
/uninstallbinaries
/UserName:contoso\dan
/password:*
/administratorpassword:Pa\$\$w0rd

Key Points

You can remove a domain controller by using Dcpromo.exe, either to launch the Active Directory Domain Services Installation Wizard or from a command prompt, specifying options at the command line or in an answer file. When a domain controller is removed while it has connectivity to the domain, it updates the forest metadata about the domain controller, so that the directory knows the DC has been removed.

To use an answer file, provide the following options and values:

```
[DCINSTALL]
UserName=DOMAIN\username (in Administrators group of the domain)
UserDomain=FQDN of user specified by UserName
Password=password for user specified by UserName
AdministratorPassword=password will be assigned to local Administrator
RemoveApplicationPartitions=yes
RemoveDNSDelegation=yes
DNSDelegationUserName=DOMAIN\username with permissions to remove
DNS delegation
DNSDelegationPassword=password for the account
```

Run dcpromo with the /unattend:"answer file path" and the /UninstallBinaries options, as in the following example:

```
dcpromo /uninstallbinaries /unattend:"c:\rodcanwer.txt"
```

All the options just shown in the answer file can also be specified or overridden directly on the command line. Just type a command similar to the following:

```
dcpromo /unattend /uninstallbinaries
/UserName:contoso\dan
/password:*
/administratorpassword:Pa$$w0rd
```

If a domain controller must be demoted while it cannot contact the domain, you must use the forceremoval option of dcpromo.exe. Type dcpromo /forceremoval, and the Active Directory Domain Services Installation Wizard steps you through the process. You are presented warnings related to any roles the domain controller hosts. Read each warning and, after you have mitigated or accepted the impact of the warning, click Yes. You can suppress warnings, using the demotefsno:yes option of dcpromo.exe. After the DC has been removed, you must manually clean up the forest metadata.

Additional Reading

- For detailed steps for removing a domain controller, see <http://go.microsoft.com/fwlink/?LinkId=168480>
- See article 216498 in the Microsoft Knowledge Base for information about performing metadata cleanup. The article is located at <http://go.microsoft.com/fwlink/?LinkId=80481>

Lab A: Install Domain Controllers

- Exercise 1: Create an Additional DC with the Active Directory Domain Services Installation Wizard
- Exercise 2: Add a Domain Controller from the Command Line
- Exercise 3: Remove a Domain Controller
- Exercise 4: Create a Domain Controller from Installation Media

Logon information

Virtual machine	6425B-HQDC01-A	6425B-HQDC02-A
Logon user name	Pat.Coleman	Administrator
Administrative user name	Pat.Coleman_Admin	Pat.Coleman_Admin
Password	Pa\$\$w0rd	Pa\$\$w0rd

Estimated time: 30 minutes

Scenario

You have been hired to replace the former administrator at Contoso, Ltd. The first thing you discover is that the domain has only one domain controller. You decide to add a second domain controller to provide fault tolerance for the directory service. You have already installed a new server named HQDC02.

Exercise 1: Create an Additional DC with the Active Directory Domain Services Installation Wizard

In this exercise, you will use the Active Directory Domain Services Installation Wizard (DCPromo.exe) to create an additional domain controller in the contoso.com domain. You will not complete the installation, however. Instead, you will save the settings as an answer file, which will be used in the next exercise.

The main tasks for this exercise are as follows:

1. Prepare for the lab.
2. Promote a domain controller using the Active Directory Domain Services Installation Wizard.

► Task 1: Prepare for the lab

- Start 6425B-HQDC01-A, and log on as **Pat.Coleman** with the password **Pa\$\$w0rd**.
- Start 6425B-HQDC02-A, a workgroup server, and log on as the local **Administrator** with the password **Pa\$\$w0rd**.

► Task 2: Promote a domain controller using the Active Directory Domain Services Installation Wizard

- On HQDC02, run **DCPromo.exe**. Accept all of the defaults provided by the Active Directory Administration Wizard except those listed below:
 - Additional domain controller in an existing forest
 - Domain: **contoso.com**
 - Alternate credentials: **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
 - Select domain: **contoso.com**.
 - When a warning appears informing you that HQDC01 has a dynamically assigned IP address, click **Yes, the computer will use a dynamically assigned IP address**.
 - When a warning appears informing you that a DNS delegation could not be found, click **Yes**.
 - Directory Services Restore Mode Administrator Password: **Pa\$\$w0rd**

- On the **Summary** page, review your selections. If any settings are incorrect, click **Back** to make modifications.
- Export the settings to a file on your desktop called **AdditionalDC**.
- Cancel the installation of the domain controller on the **Summary** page. Do not continue with the Active Directory Domain Services Installation Wizard.

Results: After this exercise, you should have simulated promoting HQDC02 to a domain controller.

Exercise 2: Add a Domain Controller from the Command Line

In this exercise, you will examine the answer file you created in Exercise 1. You will use the installation options in the answer file to create a dcpromo.exe command line to install the additional domain controller.

The main tasks for this exercise are as follows:

1. Create the DCPromo command.
2. Execute the DCPromo command.

► Task 1: Create the DCPromo command

- Open the **AdditionalDC.txt** file you created in Exercise 1. Examine the answers in the file. Can you identify what some of the options mean?

Tip: Lines beginning with a semicolon are comments or inactive lines that have been commented out.

- Open a second instance of Notepad, as a new text file. Turn on word wrap. Position the windows so you can see both the blank text file and the AdditionalDC.txt file as a reference.
- In Notepad, type the dcpromo.exe command line just as you would do in a command prompt. Determine the command line to install the domain controller with the same options as those listed in the answer file. Parameters on the command line take the form /option:value whereas, in the answer file, they take the form option=value. Configure both the **Password** and **SafeModeAdminPassword** values as **Pa\$\$w0rd**. Instruct DCPromo to reboot when complete.
- As you will learn in Lab B, you can set the Password value to an asterisk (*) and you will be prompted to enter the password when you run the command.
- When you have created the command, open the **Exercise2.txt** file, found in the \\HQDC01\d\$\Labfiles\Lab11a folder. Compare the correct command in **Exercise2.txt** to the command you created in the previous step. Make any necessary corrections to your command.

► **Task 2: Execute the DCPromo command**

- Open the Command Prompt window.
- Switch to the Notepad file with the dcpromo.exe command you built in Task 1. Turn off word wrap, copy the command line you created and paste it into the command prompt window, then press ENTER to execute the command.

HQDC02 is promoted to a domain controller. This takes a few minutes.

Results: After this exercise, you should have promoted HQDC02 as an additional domain controller in the contoso.com domain and forest.

Exercise 3: Remove a Domain Controller

In this exercise, you will remove a domain controller from the contoso.com domain.

The main tasks for this exercise are as follows:

- Remove a domain controller.

► Task 1: Remove a domain controller

- After HQDC02 has restarted, log on as **Pat.Coleman** with the password **Pa\$\$w0rd**.
- Run DCPromo as an administrator, with the user name **Pat.Coleman_Admin** and the password **Pa\$\$w0rd**. Accept all defaults presented by the wizard, and configure the new Administrator password to be **Pa\$\$w0rd**. Restart the server when the process has completed.

Results: After this exercise, you should have demoted HQDC02 to a member server.

Exercise 4: Create a Domain Controller from Installation Media

You can reduce the amount of replication required to create a domain controller by promoting the domain controller, using the IFM option. IFM requires that you provide installation media, which is, in effect, a backup of Active Directory. In this exercise, you will create the installation media on HQDC01, transfer it to HQDC02, and then simulate the promotion of HQDC02 to a domain controller using the installation media.

The main tasks for this exercise are as follows:

1. Create installation media.
2. Promote a domain controller using installation media.

► Task 1: Create installation media

1. On HQDC01, run the Command Prompt as an administrator, with the user name **Pat.Coleman_Admin** and the password **Pa\$\$w0rd**.
2. Use **ntdsutil.exe** to create installation media in a folder named **C:\IFM**.

► Task 2: Promote a domain controller using installation media

1. Switch to HQDC02, and log on as **Pat.Coleman** with the password **Pa\$\$w0rd**.
2. Copy the IFM folder from the HQDC01 drive C to drive C on HQDC02.
3. On HQDC02, run **DCPromo.exe**. Accept all of the defaults provided by the Active Directory Administration Domain Services Installation Wizard except those listed below:
 - Additional domain controller in an existing forest.
 - Domain: **contoso.com**.
 - User: **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
 - Select domain: **contoso.com**.
 - When a warning appears informing you that HQDC01 has a dynamically assigned IP address, click **Yes, the computer will use a dynamically assigned IP address**.

- When a warning appears informing you that a DNS delegation could not be found, click **Yes**.
- Install from Media: Replicate data from media stored at C:\IFM.
- After the Source Domain Controller page, cancel the wizard without completing the promotion.

Results: After this exercise, you should have created installation media on HQDC01 and simulated the promotion of HQDC02 to a domain controller using the installation media.



Note: Shut down HQDC02, but do not shut down HQDC01 as it will be used in Lab B.

Lab Review Questions

Question: Why would you choose to use an answer file, or a dcpromo.exe command line to install a domain controller rather than the Active Directory Domain Services Installation Wizard?

Question: In what situations does it make sense to create a domain controller using installation media?

Lesson 2

Install a Server Core DC

- Understand Server Core
- Install Server Core
- Server Core Configuration Commands

Many organizations want to implement the maximum available security for servers acting as domain controllers because of the sensitive nature of information stored in the directory—particularly user passwords. Although the role-based configuration of Windows Server 2008 reduces the security surface of a server by installing only the components and services required by its roles, it is possible to reduce its servers and security surface further by installing Server Core. A Server Core installation is a minimal installation of Windows that forgoes even the Windows Explorer GUI and the Microsoft .NET Framework. You can administer a Server Core installation remotely, using GUI tools; however, to configure and manage a server locally, you must use command-line tools. In this lesson, you will learn to create a domain controller from the command line within a Server Core installation. You will also learn how to remove domain controllers from a domain.

Objectives

After completing this lesson, you will be able to:

- Identify the benefits and functionality of installing Server Core.
- Install and configure Server Core.
- Add and remove AD DS using command line tools.

Understand Server Core

Minimal installation: 3 GB disk space, 256 MB RAM

No GUI: Command-line local UI. Can use GUI tools *remotely*.

- | • Roles | • Features |
|------------------------------------|--------------------------------------|
| ▪ Active Directory Domain Services | ▪ Microsoft Failover Cluster |
| ▪ Active Directory AD LDS | ▪ Network Load Balancing |
| ▪ DHCP Server | ▪ Subsystem for UNIX applications |
| ▪ DNS Server | ▪ Windows Backup |
| ▪ File Services | ▪ Multipath I/O |
| ▪ Print Server | ▪ Removable Storage Management |
| ▪ Streaming Media Services | ▪ Windows Bitlocker Drive Encryption |
| ▪ Web Server: HTML. R2 adds .NET | ▪ SNMP |
| ▪ Hyper-V | ▪ WINS |
| | ▪ Telnet client |
| | ▪ Quality of Service (QoS) |

Key Points

Windows Server 2008 (Server Core Installation), better known as Server Core, is a minimal installation of Windows that consumes about 3 gigabytes (GB) of disk space and less than 256 megabytes (MB) of memory. Server Core installation limits the server roles and features that can be added but can improve the security and manageability of the server by reducing its attack surface. The number of services and components running at any one time are limited, so there are fewer opportunities for an intruder to compromise the server. Server Core also reduces the management burden of the server, which requires fewer updates and less maintenance.

Server Core supports nine server roles:

- Active Directory Domain Services (AD DS)
- Active Directory Lightweight Directory Services (AD LDS)
- Dynamic Host Configuration Protocol (DHCP) Server
- DNS Server

- File Services
- Print Server
- Streaming Media Services
- Web Server (IIS) (as a static Web server—ASP.NET cannot be installed)
- Hyper-V™ (Windows Server Virtualization)

Server core also supports these 11 optional features:

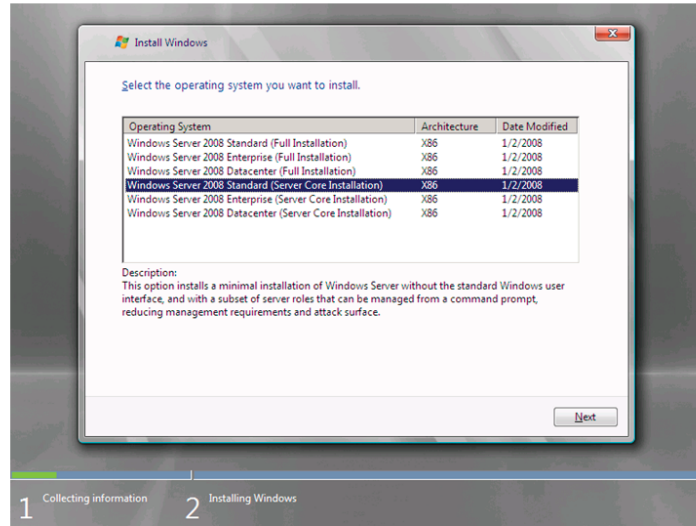
- Microsoft Failover Cluster
- Network Load Balancing
- Subsystem for UNIX-based applications
- Windows Backup
- Multipath I/O
- Removable Storage Management
- Windows Bitlocker® Drive Encryption
- Simple Network Management Protocol (SNMP)
- Windows Internet Naming Service (WINS)
- Telnet client
- Quality of Service (QoS)

Additional Reading

- Server Core Installation Option:
<http://go.microsoft.com/fwlink/?LinkId=168473>

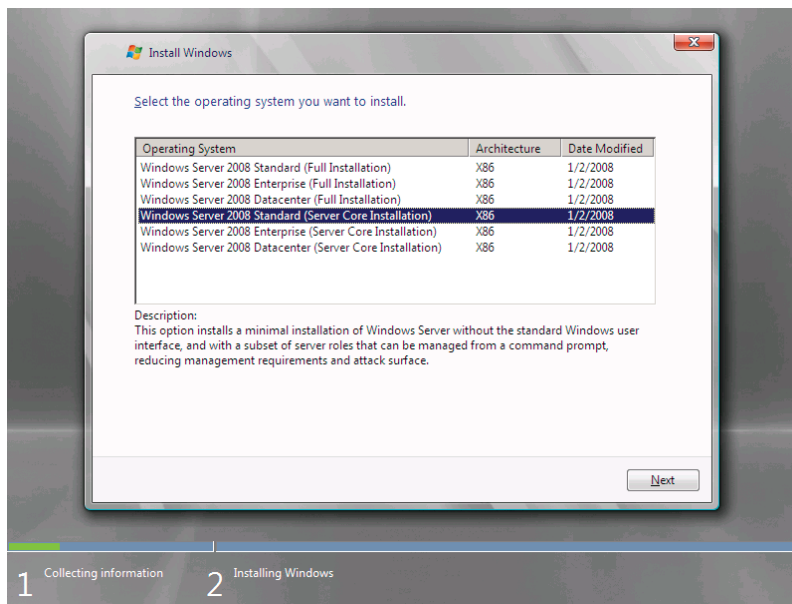
Install Server Core

- Select the Server Core Installation option in Windows setup



Key Points

You can install Server Core by using the same procedure as a full installation. The differences between a full installation and a Server Core installation are, first, that you select Server Core Installation in the Installing Windows Wizard shown on the following page, and that when the installation is complete and you log on, a command prompt appears rather than the Windows Explorer interface.



When you install Windows Server 2008 from the installation DVD, the initial password for the Administrator account is blank. When you log on to the server for the first time, use a blank password. You will be prompted to change the password on first logon.

Server Core Configuration Commands

Task	Command
Change the Administrator Password	When you log on with Ctrl+Alt+Delete, you will be prompted to change the password. You can also type the following command: Net user administrator*
Set a static IPv4 Configuration	Netsh interface ipv4
Activate Windows Server	Cscript c:\windows\system32\slmgr.vbs -ato
Join a domain	Netdom
Add Server Core roles, components, or features	Ocsetup.exe package or feature Note that the package or feature names are case sensitive
Display installed roles, components, and features	Oclist.exe
Enable Remote Desktop	Cscript C:\windows\system32\scregedit.wsf /AF 0
Promote a domain controller	Dcpromo.exe
Configure DNS	Dnscmd.exe
Configure DFS	Dfscmd.exe

Key Points

On a full installation of Windows Server 2008, the Initial Configuration Tasks window opens to guide you through post-installation configuration of the server. Server Core provides no GUI, so you must complete the tasks by using command-line tools. The following table lists common configuration tasks and the commands you can use. To learn more about any command, open a command prompt and type the name of the command followed by /?.

Server Core Configuration Commands

Task	Command
Change the Administrator password	When you log on with CTRL+ALT+DELETE, you will be prompted to change the password. You can also type the following command: net user administrator *
Set a static IPv4 configuration	netsh interface ipv4
Activate Windows Server	cscript c:\windows\system32\slmgr.vbs -ato
Join a domain	netdom
Add Server Core roles, components, or features	ocsetup.exe package or feature Note that the package or feature names are case sensitive.
Display installed roles, components, and features	oclist.exe
Enable Remote Desktop	cscript c:\windows\system32\scregedit.wsf /AR 0
Promote a domain controller	dcpromo.exe
Configure DNS	dnscmd.exe
Configure DFS	dfscmd.exe

The Ocsetup.exe command is used to add supported Server Core roles and features to the server. The exception to this rule is AD DS. Do not use Ocsetup.exe to add or remove AD DS. Use Dcpromo.exe instead.

Because there is no Active Directory Domain Services Installation Wizard in Server Core, you must use the command line to run Dcpromo.exe with parameters that configure AD DS. To learn about the parameters of dcpromo.exe, open a command line and type dcpromo.exe /?. Each configuration scenario has additional usage information. For example, type dcpromo.exe /?:Promotion for detailed usage instructions for promoting a domain controller.

Additional Reading

- Appendix of Unattended Installation Parameters:
<http://go.microsoft.com/fwlink/?LinkId=168474>

Lab B: Install a Server Core DC

- Exercise 1: Perform Post-Installation Configuration on Server Core
- Exercise 2: Create a Domain Controller with Server Core

Logon information

Virtual machine	6425B-HQDC01-A	6425B-HQDC03-A
Logon user name	Do not log on	Administrator
Administrative user name		Pat.Coleman_Admin
Password		Pa\$\$w0rd

Estimated time: 30 minutes

Scenario

You are a domain administrator for Contoso, Ltd., and you want to add a domain controller to the AD DS environment. In order to enhance the security of the new DC, you plan to use Server Core. You have already installed Server Core on a new computer, and you are ready to configure the server as a domain controller.

Exercise 1: Perform Post-Installation Configuration on Server Core

In this exercise, you will perform post-installation configuration of the server to prepare it with the name and TCP/IP settings required for the remaining exercises in this Lab.

The main tasks for this exercise are as follows:

1. Prepare for the lab.
2. Perform post-installation configuration of Server Core.

► Task 1: Prepare for the Lab

The 6425B-HQDC01-A virtual machine should already be available after completing Lab A.

- Start 6425B-HQDC01-A, but do not log on.
- Start 6425B-HQDC03-A, but do not log on.

► Task 2: Perform post-installation configuration of Server Core

- Log on to HQDC03 as **Administrator** with the password **Pa\$\$w0rd**.
- Configure the IPv4 address and DNS server by typing each of the following commands:

```
netsh interface ipv4 set address name="Local Area Connection"  
source=static address=10.0.0.13 mask=255.255.255.0  
gateway=10.0.0.1
```

```
netsh interface ipv4 set dns name="Local Area Connection"  
source=static address=10.0.0.11 primary
```

- Confirm the IP configuration you entered previously with the command **ipconfig /all**.
- Rename the server by typing **netdom renamecomputer %computername% /newname:HQDC03**. You will be prompted to press **Y** to confirm the operation.
- Restart by typing **shutdown -r -t 0**.

- Log on as **Administrator** with the password **Pa\$\$w0rd**.
- Join the domain using the following command:

```
netdom join %computename% /domain:contoso.com  
/UserD:CONTOSO\Pat.Coleman_Admin /PasswordD:Pa$$w0rd  
/OU:"ou=servers,dc=contoso,dc=com"
```

- Restart by typing **shutdown -r -t 0**.

Results: After this exercise, you should have configured the Server Core installation as a member of the contoso.com domain named HQDC03.

Exercise 2: Create a Domain Controller with Server Core

In this exercise, you will add the DNS and AD DS roles to the Server Core installation.

The main tasks for this exercise are as follows:

1. Add the DNS Server role to Server Core.
2. Create a domain controller on Server Core with the `dcpromo.exe` command.

► Task 1: Add the DNS Server role to Server Core

- Log on to HQDC03 as **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
- Display available server roles by typing **oclist**. What is the package identifier for the DNS server role? What is its status?
- Type **ocsetup**, and then press ENTER. Surprise! There is a minor amount of GUI in Server Core. Click **OK** to close the window.
- Type **ocsetup DNS-Server-Core-Role**. Note that package identifiers are case sensitive.
- Type **oclist** and confirm that the DNS server role is installed.

► Task 2: Create a domain controller on Server Core with the `dcpromo.exe` command

- Make sure you are still logged on to HQDC03 as **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
- Type **dcpromo.exe /?**, and then press ENTER. Review the usage information.
- Type **dcpromo.exe /?:Promotion**, and then press ENTER. Review the usage information.
- Type the following command to add and configure the AD DS role, and then press ENTER:

```
dcpromo /unattend /ReplicaOrNewDomain:replica  
/ReplicaDomainDNSName:contoso.com /ConfirmGC:Yes  
/UserName:CONTOSO\Pat.Coleman_Admin /Password:*  
/safeModeAdminPassword:Pa$$w0rd
```


- When prompted to enter network credentials, type **Pa\$\$w0rd**, and then click **OK**. The AD DS role will be installed and configured, and then the server will reboot.

Results: After this exercise, you should have promoted the Server Core server, HQDC03, to a domain controller in the contoso.com domain.



Note: You can shut down both virtual machines as different virtual machines are used in the next Lab.

Lab Review Questions

Question: Did you find the configuration of Server Core to be particularly difficult?

Question: What are the advantages of using Server Core for domain controllers?

Lesson 3

Manage Operations Masters

- Understand Single Master Operations
- Operation Master Roles
- Optimize the Placement of Operations Masters
- Identify Operations Masters
- Transfer Operations Master Roles
- Seize Operations Master Roles

In an Active Directory domain, all domain controllers are equivalent. They are all capable of writing to the database and replicating changes to other domain controllers. However, in any multimaster replication topology, certain operations must be performed by one and only one system. In an Active Directory domain, operations masters are domain controllers that play a specific role. Other domain controllers are capable of playing the role but do not. This lesson will introduce you to the five operations masters found in Active Directory forests and domains. You will learn their purposes, how to identify the operations masters in your enterprise, and the nuances of administering and transferring roles.

Objectives

After completing this lesson, you will be able to:

- Define the purpose of the five single master operations in Active Directory forests.
- Identify the domain controllers performing operations master roles.
- Plan the placement of operations master roles.
- Transfer and seize operations master roles.

Understand Single Master Operations

- In any multimaster replication topology, some operations must be “single master”
- Many terms used for single master operations in AD DS
 - Operations master (or operations master roles)
 - Single master roles
 - Operations tokens
 - Flexible single master operations (FSMOs)
- Roles

Forest <ul style="list-style-type: none"> • Domain naming • Schema 	Domain <ul style="list-style-type: none"> • Relative identifier (RID) • Infrastructure • PDC Emulator
---	---

Key Points

In any replicated database, some changes must be performed by one and only one replica because they are impractical to perform in a multimaster fashion. Active Directory is no exception. A limited number of operations are not permitted to occur at different places at the same time and must be the responsibility of only one domain controller in a domain or forest. These operations, and the domain controllers that perform them, are referred to by a variety of terms:

- Operations masters
- Operations master roles
- Single master roles
- Operations tokens
- Flexible single master operations (FSMOs)

Regardless of the term used, the idea is the same. One domain controller performs a function, and while it does, no other domain controller performs that function.

All Active Directory domain controllers are capable of performing single master operations. The domain controller that actually does perform an operation is the domain controller that currently holds the operation's token.

An operation token, and thus the role, can be transferred easily to another domain controller without a reboot.

To reduce the risk of single points of failure, the operations tokens can be distributed among multiple DCs.

AD DS contains five operations master roles. Two roles are performed for the entire forest:

- Domain naming
- Schema

Three roles are performed in each domain:

- Relative identifier (RID)
- Infrastructure
- PDC Emulator

Each of these roles is detailed in the following sections. In a forest with a single domain, there are, therefore, five operations masters. In a forest with two domains, there are eight operations masters because the three domain master roles are implemented separately in each of the two domains.

Operations Master Roles

- **Forest-wide**
 - Domain naming: adds/removes domains to/from the forest
 - Schema: makes changes to the schema
- **Domain-wide**
 - RID: provides “pools” of RIDs to DCs, which use them for SIDs
 - Infrastructure: tracks changes to objects in other domains that are members of groups in this domain
 - PDC: plays several very important roles
 - Emulates a Primary Domain Controller (PDC): compatibility
 - Special password update handling
 - Default target for Group Policy updates
 - Master time source for domain
 - Domain master browser

Key Points

Forest-Wide Operations Master Roles

The schema master and the domain naming master must be unique in the forest. Each role is performed by only one domain controller in the entire forest.

Domain Naming Master Role

The domain naming role is used when adding or removing domains in the forest. When you add or remove a domain, the domain naming master must be accessible, or the operation will fail.

Schema Master Role

The domain controller holding the schema master role is responsible for making any changes to the forest’s schema. All other DCs hold read-only replicas of the schema. If you want to modify the schema or install an application that modifies the schema, it is recommended you do so on the domain controller holding the schema master role. Otherwise, changes you request must be sent to the schema master to be written into the schema.

Domain-Wide Operations Master Roles

Each domain maintains three single master operations: RID, Infrastructure, and PDC Emulator. Each role is performed by only one domain controller in the domain.

RID Master Role

The RID master plays an integral part in the generation of security identifiers (SIDs) for security principals such as users, groups, and computers. The SID of a security principal must be unique. Because any domain controller can create accounts, and therefore, SIDs, a mechanism is necessary to ensure that the SIDs generated by a DC are unique. Active Directory domain controllers generate SIDs by assigning a unique RID to the domain SID. The RID master for the domain allocates pools of unique RIDs to each domain controller in the domain. Thus, each domain controller can be confident that the SIDs it generates are unique.



Note: The RID master role is like DHCP for SIDs. If you are familiar with the concept that you allocate a scope of IP addresses for the Dynamic Host Configuration Protocol (DHCP) server to assign to clients, you can draw a parallel to the RID master, which allocates pools of RIDs to domain controllers for the creation of SIDs.

Infrastructure Master Role

In a multidomain environment, it is common for an object to reference objects in other domains. For example, a group can include members from another domain. Its multivalued member attribute contains the distinguished names of each member. If the member in the other domain is moved or renamed, the infrastructure master of the group's domain updates the group's member attribute accordingly.



Note: The infrastructure master. You can think of the infrastructure master as a tracking device for group members from other domains. When those members are renamed or moved in the other domain, the infrastructure master identifies the change and makes appropriate changes to group memberships so that the memberships are kept up to date.

PDC Emulator Role

The PDC Emulator role performs multiple, crucial functions for a domain:

- **Emulates a Primary Domain Controller (PDC) for backward compatibility**

In the days of Windows NT® 4.0 domains, only the PDC could make changes to the directory. Previous tools, utilities, and clients written to support Windows NT 4.0 are unaware that all Active Directory domain controllers can write to the directory, so such tools request a connection to the PDC. The domain controller with the PDC emulator role registers itself as a PDC so that down-level applications can locate a writable domain controller. Such applications are less common now that Active Directory is nearly 10 years old, and if your enterprise includes such applications, work to upgrade them for full Active Directory compatibility.

- **Participates in special password update handling for the domain**

When a user's password is reset or changed, the domain controller that makes the change replicates the change immediately to the PDC emulator. This special replication ensures that the domain controllers know about the new password as quickly as possible. If a user attempts to log on immediately after changing passwords, the domain controller responding to the user's logon request might not know about the new password. Before it rejects the logon attempt, that domain controller forwards the authentication request to a PDC emulator, which verifies that the new password is correct and instructs the domain controller to accept the logon request. This function means that any time a user enters an incorrect password, the authentication is forwarded to the PDC emulator for a second opinion. The PDC emulator, therefore, should be highly accessible to all clients in the domain. It should be a well-connected, high-performance DC.

- **Manages Group Policy updates within a domain**

If a Group Policy object (GPO) is modified on two DCs at approximately the same time, there could be conflicts between the two versions that could not be reconciled as the GPO replicates. To avoid this situation, the PDC emulator acts as the focal point for all Group Policy changes. When you open a GPO in the Group Policy Management Editor (GPME), the GPME binds to the domain controller performing the PDC emulator role. Therefore, all changes to GPOs are made on the PDC emulator by default.

- **Provides a master time source for the domain**

Active Directory, Kerberos, File Replication Service (FRS), and DFS-R each rely on timestamps, so synchronizing the time across all systems in a domain is crucial. The PDC emulator in the forest root domain is the time master for the entire forest, by default. The PDC emulator in each domain synchronizes its time with the forest root PDC emulator. Other domain controllers in the domain synchronize their clocks against that domain's PDC emulator. All other domain members synchronize their time with their preferred domain controller. This hierarchical structure of time synchronization, all implemented through the Win32Time service, ensures consistency of time. Universal Coordinated Time (UTC) is synchronized, and the time displayed to users is adjusted based on the time zone setting of the computer.



Note: Change the time service only one way. It is highly recommended to allow Windows to maintain its native, default time synchronization mechanisms. The only change you should make is to configure the PDC emulator of the forest root domain to synchronize with an extra time source. If you do not specify a time source for the PDC emulator, the System event log will contain errors reminding you to do so. See <http://go.microsoft.com/fwlink/?LinkId=91969>, and the articles it refers to, for more information.

- **Acts as the domain master browser**

When you open Network in Windows, you see a list of workgroups and domains, and when you open a workgroup or domain, you see a list of computers. These two lists, called *browse lists*, are created by the Browser service. In each network segment, a master browser creates the browse list: the lists of workgroups, domains, and servers in that segment. The domain master browser serves to merge the lists of each master browser so that browse clients can retrieve a comprehensive browse list.

Optimize the Placement of Operations Masters

- Forest root DC (first DC in forest) has all roles by default
- Best practice guidance
 - Co-locate the schema master and domain naming master on a GC
 - Co-locate the RID master and PDC emulator roles
 - Place the infrastructure master on a DC that is not a GC*
 - Have a failover plan
- * Real-world enhancements to best-practice guidance
 - Consider configuring *all* DCs as GCs
 - In a single domain forest, it doesn't increase replication traffic
 - If all DCs are GCs, infrastructure master role is not "necessary"
 - Still exists, but does not start on a GC and isn't needed

Key Points

When you create the forest root domain with its first domain controller, all five operations master roles are performed by the domain controller. As you add domain controllers to the domain, you can transfer the operations master role assignments to other domain controllers to balance the load among domain controllers or to optimize placement of a single master operation. The best practices for the placement of operations master roles are as follows:

- **Co-locate the schema master and domain naming master**

The schema master and domain naming master roles should be placed on a single domain controller that is a GC server. These roles are rarely used, and the domain controller hosting them should be tightly secured. The domain naming master must be hosted on a GC server because when a new domain is added, the master must ensure that there is no object of any type with the same name as the new domain. The GC's partial replica contains the name of every object in the forest. The load of these operations master roles is very light unless schema modifications are being made.

- **Co-locate the RID master and PDC emulator roles**

Place the RID and PDC emulator roles on a single domain controller. If the load mandates that the roles be placed on two separate domain controllers, those two systems should be physically well connected and have explicit connection objects created in Active Directory so that they are direct replication partners. They should also be direct replication partners with domain controllers that you have selected as standby operations masters.

- **Place the infrastructure master on a DC that is not a GC**

The infrastructure master should be placed on a domain controller that is not a GC server but is physically well connected to a GC server. The infrastructure master should have explicit connection objects in Active Directory to that GC server so that they are direct replication partners. The infrastructure master can be placed on the same domain controller that acts as the RID master and PDC emulator.



Note: It doesn't matter if they're all GCs. If all DCs in a domain are GC servers—which indeed is a best practice recommendation that will be discussed in Module 12, "Manage Sites and Active Directory Replication"—you do not need to worry about which DC is the infrastructure master. When all DCs are GCs, all DCs have up-to-date information about every object in the forest, which eliminates the need for the infrastructure master role.

- **Have a failover plan**

In the following sections, you will learn to transfer single operations master roles between domain controllers, which is necessary if there is lengthy planned or unplanned downtime of an operations master. Determine, in advance, a plan for transferring operations roles to other DCs in the event that one operations master is offline.

Identify Operations Masters

- User interface tools
 - PDC Emulator: Active Directory Users And Computers
 - RID: Active Directory Users And Computers
 - Infrastructure: Active Directory Users And Computers
 - Schema: Active Directory Schema
 - Domain Naming: Active Directory Domains and Trusts
- Command line tools
 - NTDSUtil
 - DCDiag
 - **netdom query fsmo**

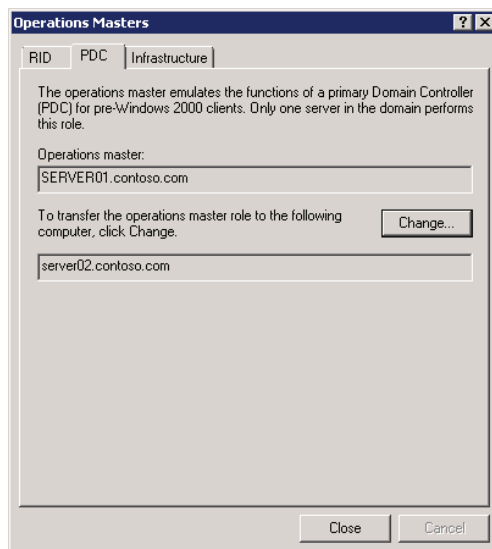
Key Points

To implement your role placement plan, you must know which DCs are currently performing single master operations roles. Each role is exposed in an Active Directory administrative tool as well as in other user interface and command-line tools.

To identify the current master for each role, use the following tools:

- **PDC Emulator: The Active Directory Users And Computers snap-in**

Right-click the domain and choose **Operations Masters**. Click the **PDC** tab. An example is shown on the following page, which indicates that SERVER01.contoso.com is currently the PDC operations master.



- **RID Master: The Active Directory Users And Computers snap-in**
Right-click the domain and choose **Operations Masters**. Click the **RID** tab.
- **Infrastructure Master: The Active Directory Users And Computers snap-in**
Right-click the domain and choose **Operations Masters**. Click the **Infrastructure** tab.
- **Domain Naming: The Active Directory Domains And Trusts snap-in**
Right-click the root node of the snap-in (**Active Directory Domains And Trusts**) and choose **Operations Master**.
- **Schema Master: The Active Directory Schema snap-in**
Right-click the root node of the snap-in (**Active Directory Schema**) and choose **Operations Master**.



Note: Registering the Active Directory Schema snap-in. You must register the Active Directory Schema snap-in before you can create a custom Microsoft Management Console (MMC) with the snap-in. At a command prompt, type **regsvr32 schmmgmt.dll**.

You can also use several other tools to identify operations masters, including the following commands:

- NTDSUtil

```
ntdsutil
roles
connections
connect to server DomainControllerFQDN:portnumber
quit
select operation target
list roles for connected server
quit
quit
quit
```

- dcdiag /test:knowsofroleholders /v
- netdom query fsmo

Transfer Operations Master Roles

- **Transfer roles in these scenarios**
 - To distribute roles away from the forest domain root DC
 - Prior to taking a role holding DC offline for maintenance
 - Prior to demoting a role holding DC
- **Procedure**
 - Ensure that the new role holder is up to date with replication from the current role holder
 - Open the appropriate administrative snap-in
 - Connect to the *target* domain controllers
 - Open the Operations Master dialog box and click Change
 - *Or* use NTDSUtil to change transfer the master

Key Points

You can transfer a single operations master role easily. You will transfer roles in the following scenarios:

- When you establish your forest, all five roles are performed by the first domain controller you install. When you add a domain to the forest, all three domain roles are performed by the first domain controller in that domain. As you add domain controllers, you can distribute the roles to reduce single-point-of-failure and improve performance.
- If you plan to take a domain controller offline that is currently holding an operations master role, transfer that role to another domain controller prior to taking it offline.
- If you are decommissioning a domain controller that currently holds an operations master role, transfer that role to another domain controller prior to decommissioning. The Active Directory Domain Services Installation Wizard will attempt to do so automatically, but you should prepare for demoting a domain controller by transferring its roles.

To transfer an operations master role, follow these steps:

1. It is recommended to make sure that the new role holder is up to date with replication from the former role holder before transferring the role. You can use skills introduced in Module 12 to force replication between the two systems.
2. Open the administrative tool that exposes the current master.
For example, open the Active Directory Users And Computers snap-in to transfer any of the three domain master roles.
3. Connect to the domain controller to which you are transferring the role.
This is accomplished by right-clicking the root node of the snap-in and choosing Change Domain Controller or Change Active Directory Domain Controller. (The command differs between snap-ins.)
4. Open the **Operations Master** dialog box, which will show you the domain controller currently holding the role token for the operation. Click the **Change** button to transfer the role to the domain controller to which you are connected.

When you transfer an operations master role, both the current master and the new master are online. The token is transferred, the new master immediately begins to perform the role, and the former master immediately ceases to perform the role. This is the preferred method of moving operations master roles.

Seize Operations Master Roles

- Recognize operations master failures
 - Typically you notice when you attempt to perform an action for which the master is responsible, and receive an error
- Respond to an operations master failure
 - Determine whether the DC can be brought online, and when
 - Evaluate whether the enterprise can continue to function temporarily without the DC
 - See Student Manual for specific guidance
- Seize the role using NTDSUtil
 - Refer to procedure in Student Manual
- Return a role to its original holder?
 - Only for PDC and Infrastructure tokens
 - If Schema, RID, or domain naming have been seized, you must decommission the failed DC *offline*, then re-promote it

Key Points

Recognize Operations Master Failures

Several operations master roles can be unavailable for quite some time before their absence becomes a problem. Other master roles play a crucial role in the day-to-day operation of your enterprise. You can identify problems with operations masters by examining the Directory Service event log.

However, you will often discover that an operations master has failed when you attempt to perform a function managed by the master, and the function fails. For example, if the RID master fails, eventually you will be prevented from creating new security principals.

Respond to an Operations Master Failure

If a domain controller performing a single master operation fails, and you cannot bring the system back to service, you have the option of seizing the operations token. When you seize a role, you designate a new master without gracefully removing the role from the failed master.

Seizing a role is a drastic action, so before seizing a role, think carefully about whether it is necessary. Determine the cause and expected duration of the offline operations master. If the operations master can be brought online in sufficient time, wait. What is sufficient time? It depends on the impact of the role that has failed.

PDC Emulator failure

The PDC Emulator is the operations master that will have the most immediate impact on normal operations and on users if it becomes unavailable. Fortunately, the PDC Emulator role can be seized to another domain controller and then transferred back to the original role holder when the system comes back online.

Infrastructure master failure

A failure of the infrastructure master will be noticeable to administrators but not to users. Because the master is responsible for updating the names of group members from other domains, it can appear as if group membership is incorrect although, as mentioned earlier in this lesson, membership is not actually affected. You can seize the infrastructure master role to another domain controller and then transfer it back to the previous role holder when that system comes online.

RID master failure

A failed RID master will eventually prevent domain controllers from creating new SIDs and, therefore, will prevent you from creating new accounts for users, groups, or computers. However, domain controllers receive a sizable pool of RIDs from the RID master, so unless you are generating numerous new accounts, you can often go for some time without the RID master online while it is being repaired. Seizing this role to another domain controller is a significant action. After the RID master role has been seized, the domain controller that had been performing the role cannot be brought back online.

Schema master failure

The schema master role is necessary only when schema modifications are being made, either directly by an administrator or by installing an Active Directory integrated application that changes the schema. At other times, the role is not necessary. It can remain offline indefinitely until schema changes are necessary. Seizing this role to another domain controller is a significant action. After the schema master role has been seized, the domain controller that had been performing the role cannot be brought back online.

Domain naming master failure

The domain naming master role is necessary only when you add a domain to the forest or remove a domain from a forest. Until such changes are required to your domain infrastructure, the domain naming master role can remain offline for an indefinite period of time. Seizing this role to another domain controller is a significant action. After the domain naming master role has been seized, the domain controller that had been performing the role cannot be brought back online.

Seize an Operations Master Role

Although you can transfer roles by using the administrative tools, you must use Ntdsutil.exe to seize a role. To seize an operations master role, perform the following steps:

1. From the command prompt, type **ntdsutil**, and then press ENTER.
2. At the ntdsutil prompt, type **roles**, and then press ENTER.

The next steps establish a connection to the domain controller you want to perform the single master operation role.
3. At the fsmo maintenance prompt, type **connections**, and then press ENTER.
4. At the server connections prompt, type **connect to server**
DomainControllerFQDN, and then press ENTER.

DomainControllerFQDN is the FQDN of the domain controller you want to perform the role.

Ntdsutil responds that it has connected to the server.
5. At the server connections prompt, type **quit**, and then press ENTER.
6. At the fsmo maintenance prompt, type **seize role**, and then press ENTER.

Role is one of the following:
 - schema master
 - domain naming master
 - RID master
 - PDC
 - infrastructure master
7. At the fsmo maintenance prompt, type **quit**, and then press ENTER.
8. At the ntdsutil prompt, type **quit**, and then press ENTER.

Returning a Role to Its Original Holder

To provide for planned downtime of a domain controller if a role has been transferred, not seized, the role can be transferred back to the original domain controller.

If, however, a role has been seized and the former master is able to be brought back online, you must be very careful. The PDC emulator and infrastructure master are the only operations master roles that can be transferred back to the original master after having been seized.



Note: Do not return a seized schema, domain naming, or RID master to service! After seizing the schema, domain naming, or RID roles, you must completely decommission the original domain controller.

If you have seized the schema, domain naming, or RID roles to another domain controller, you must not bring the original domain controller back online without first completely decommissioning the domain controller. That means you must keep the original role holder physically disconnected from the network, and you must remove AD DS by using the `dcpromo /forceremoval` command. You must also clean the metadata for that domain controller as described at <http://go.microsoft.com/fwlink/?LinkId=80481>.

After the domain controller has been completely removed from Active Directory, if you want the server to rejoin the domain, you can connect it to the network and join the domain. If you want it to be a domain controller, you can promote it. If you want it to resume performing the operations master role, you can transfer the role back to the DC.



Note: Better to rebuild. Because of the critical nature of domain controllers, it is recommended that you completely reinstall the former domain controller in this scenario.

Lab C: Transfer Operations Master Roles

- Exercise 1: Identify Operations Masters
- Exercise 2: Transfer Operations Master Roles

Logon information

Virtual machine	6425B-HQDC01-B	6425B-HQDC02-B
Logon user name	Pat.Coleman	Do not log on
Administrative user name	Pat.Coleman_Admin	
Password	Pa\$\$w0rd	

Estimated time: 30 minutes

Scenario

You are a domain administrator at Contoso, Ltd. One of the redundant power supplies has failed on HQDC01 and you must take the server offline for servicing. You want to ensure that AD DS operations are not interrupted while the server is offline.

Exercise 1: Identify Operations Masters

In this exercise, you will use both user interface and command-line tools to identify operations masters in the contoso.com domain.

The main tasks for this exercise are as follows:

1. Prepare for the lab.
2. Identify operations masters using the Active Directory administrative snap-ins.
3. Identify operations masters using NetDom.

► Task 1: Prepare for the lab

- Start 6425B-HQDC01-B and log on as **Pat.Coleman** with the password **Pa\$\$w0rd**.
- Open **D:\Labfiles\Lab11c**.
- Run **Lab11c_Setup.bat** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
- The lab setup script runs. When it is complete, press any key to continue.
- Close the Windows Explorer window, **Lab11c**.
- Start 6425B-HQDC02-B, but do not log on.

► Task 2: Identify operations masters using the Active Directory administrative snap-ins

- Run **Active Directory Users and Computers** as an administrator, with the user name **Pat.Coleman_Admin** and the password **Pa\$\$w0rd**.
- Use **Active Directory Users and Computers** to identify the operations master role token holders for RID, PDC and Infrastructure. Which DC holds those roles?
- Close Active Directory Users and Computers.
- Run **Active Directory Domains and Trusts** as an administrator, with the user name **Pat.Coleman_Admin** and the password **Pa\$\$w0rd**.
- Use **Active Directory Domains and Trusts** to identify the operations master role token holders for Domain Naming. Which DC holds this role?
- Close Active Directory Domains and Trusts.

- Run the Command Prompt as an administrator, with the user name **Pat.Coleman_Admin** and the password **Pa\$\$w0rd**.
 - Type **regsvr32 schmmgmt.dll**, and then press ENTER.
 - Run **mmc.exe** as an administrator, with the user name **Pat.Coleman_Admin** and the password **Pa\$\$w0rd**.
 - Add the **Active Directory Schema** snap-in to the console.
 - Use **Active Directory Schema** to identify the operations master role token holders for Schema. Which DC holds this role?
 - Close the console. You do not need to save any changes.
- **Task 3: Identify operations masters using NetDom**
- Run the Command Prompt as an administrator, with the user name **Pat.Coleman_Admin** and the password **Pa\$\$w0rd**.
 - Type the command **netdom query fsmo**, and press ENTER.

Results: After this exercise, you should have used both administrative snap-ins and NetDom to identify operations masters.

Exercise 2: Transfer Operations Master Roles

In this exercise, you will prepare to take the operations master offline by transferring its role to another domain controller. You will then simulate taking it offline, bringing it back online, and returning the operations master role.

The main tasks for this exercise are as follows:

1. Transfer the PDC role using the Active Directory Users And Computers snap-in.
2. Consider other roles before taking a domain controller offline.
3. Transfer the PDC role using NTDSUtil.

► Task 1: Transfer the PDC role using the Active Directory Users And Computers snap-in

- Run **Active Directory Users and Computers** as an administrator, with the user name **Pat.Coleman_Admin** and the password **Pa\$\$w0rd**.
- Connect to HQDC02.

Before transferring an operations master, you must connect to the domain controller to which the role will be transferred.

The root node of the snap-in indicates the domain controller to which you are connected: Active Directory Users And Computers [hqdc02.contoso.com].

- Transfer the PDC operations master role to HQDC02.

► Task 2: Consider other roles before taking a domain controller offline

You are preparing to take HQDC01 offline. You have just transferred the PDC operations role to HQDC02.

- List other operations master roles that must be transferred prior to taking HQDC01 offline?
- List other server roles that must be transferred prior to taking HQDC01 offline?

► Task 3: Transfer the PDC role using NTDSUtil

You have finished performing maintenance on HQDC01. You bring it back online.

Remember you cannot bring a domain controller back online if the RID, schema, or domain naming roles have been seized. But you can bring it back online if a role was transferred.

- Run the Command Prompt as an administrator, with the user name **Pat.Coleman_Admin** and the password **Pa\$\$w0rd**.
- Use **NTDSUtil** to connect to HQDC01 and transfer the PDC role back to it.

Results: After this exercise, you should have transferred the PDC role to HQDC02 using the Active Directory Users And Computers snap-in, and then transferred it back to HQDC01 using NTDSUtil.



Note: You can shut down these virtual machines when finished with them as they will need to be restarted for the next lab.

Lab Review Questions

Question: If you transfer all roles before taking a domain controller offline, is it OK to bring the domain controller back online?

Question: If a domain controller fails and you seize roles to another domain controller, is it OK to bring the failed domain controller back online?

Lesson 4

Configure DFS-R Replication of SYSVOL

- Raise the Domain Functional Level
- Understand Migration Stages
- Migrate to DFS-R Replication of Sysvol

SYSVOL, a folder located at %SystemRoot%\SYSVOL by default, contains logon scripts, group policy templates (GPTs), and other resources critical to the health and management of an Active Directory domain. Ideally, SYSVOL should be consistent on each domain controller. However, changes to Group Policy objects and to logon scripts are made from time to time, so you must ensure that those changes are replicated effectively and efficiently to all domain controllers. In previous versions of Windows, the FRS was used to replicate the contents of SYSVOL between domain controllers. FRS has limitations in both capacity and performance that causes it to break occasionally. Unfortunately, troubleshooting and configuring FRS is quite difficult. In Windows Server 2008 domains, you have the option to use DFS-R to replicate the contents of SYSVOL. In this lesson, you will learn how to migrate SYSVOL from FRS to DFS-R.

Objectives

After completing this lesson, you will be able to:

- Raise the domain functional level.
- Migrate SYSVOL replication from FRS to DFS-R.

Raise the Domain Functional Level

- All domain controllers in the domain must be Windows Server 2008 or greater
 - DCs in other domains and member server OSs don't matter
- Active Directory Domains And Trusts
 - Right-click domain → Raise Domain Functional Level

Key Points

In Module 1, "Introducing Active Directory Domain Services," you were introduced to the concept of domain and forest functional levels. In Module 14, "Manage Multiple Domains and Forests," you will learn about forest and domain functional levels in detail. A domain's functional level is a setting that both restricts the operating systems that are supported as domain controllers in a domain and enables additional functionality in Active Directory. A domain with a Windows Server 2008 domain controller can be at one of three functional levels: Windows 2000 Native, Windows Server 2003 Native, and Windows Server 2008. At Windows 2000 Native domain functional level, domain controllers can be running Windows 2000 Server or Windows Server 2003. At Windows Server 2003 Native domain functional level, domain controllers can be running Windows Server 2003. At Windows Server 2008 domain functional level, all domain controllers must be running Windows Server 2008.

As you raise functional levels, new capabilities of Active Directory are enabled. At Windows Server 2008 domain functional level, for example, you can use DFS-R to replicate SYSVOL. Simply upgrading all domain controllers to Windows Server 2008 is not enough: You must specifically raise the domain functional level. You do this by using Active Directory Domains And Trusts.

To raise the domain functional level:

1. Run the **Active Directory Domains and Trusts** snap-in.
2. Right-click the domain and choose **Raise Domain Functional Level**.
3. Select **Windows Server 2008** as the desired functional level, and then click **Raise**.

After you've set the domain functional level to Windows Server 2008, you cannot add domain controllers running Windows Server 2003 or Windows 2000 Server. The functional level is associated only with domain controller operating systems; member servers and workstations can be running Windows Server 2003, Windows 2000 Server, Windows Vista®, Windows XP, or Windows 2000 Workstation.

Understand Migration Stages

- **Four states (stages)**
 - 0 (start): Default state. FRS replicates SYSVOL
 - 1 (prepared)
 - Copy of SYSVOL called SYSVOL_DFSR, replicated by DFS-R
 - SYSVOL replicated by FRS and used by clients
 - 2 (redirected)
 - SYSVOL share redirected to SYSVOL_DFSR for client use.
 - SYSVOL replicated by FRS (for fallback)
 - 3 (eliminated): FRS replication of SYSVOL stopped. Folder remains.
- **DFSRMig (dfsrmig.exe)**
 - **setglobalstate** *state* where *state* is 0-3. Sets global (desired) state.
 - **getglobalstate** reports current global DFSR migration state
 - **getmigrationstate** reports migration state of each DC towards state

Key Points

Because SYSVOL is critical to the health and functionality of your domain, Windows does not provide a mechanism with which to convert from FRS to DFS-R replication of SYSVOL instantly. In fact, migration to DFS-R involves creating a parallel SYSVOL structure. When the parallel structure is successfully in place, clients are redirected to the new structure as the domain's system volume. When the operation has proven successful, you can eliminate FRS.

Migration to DFS-R thus consists of four stages or states:

- **0 (start).** The default state of a domain controller. Only FRS is used to replicate SYSVOL.
- **1 (prepared).** A copy of SYSVOL is created in a folder called SYSVOL_DFSR and is added to a replication set. DFS-R begins to replicate the contents of the SYSVOL_DFSR folders on all domain controllers. However, FRS continues to replicate the original SYSVOL folders and clients continue to use SYSVOL.

- **2 (redirected).** The SYSVOL share, which originally refers to SYSVOL\domain\sysvol, is changed to refer to SYSVOL_DFSR\domain\sysvol. Clients now use the SYSVOL_DFSR folder to obtain logon scripts and Group Policy templates.
- **3 (eliminated).** Replication of the old SYSVOL folder by FRS is stopped. The original SYSVOL folder is not deleted, however, so if you want to remove it entirely, you must do so manually.

You move your domain controllers through these stages, using the DFSMig command. You will use three options with dfsrmig.exe:

- **setglobalstate *state***
The setglobalstate option configures the current global DFSR migration state, which applies to all domain controllers. The state is specified by the *state* parameter, which is 0–3. Each domain controller will be notified of the new DFSR migration state and will migrate to that state automatically.
- **getglobalstate**
The getglobalstate option reports the current global DFSR migration state.
- **getmigrationstate**
The getmigrationstate option reports the current migration state of each domain controller. Because it might take time for domain controllers to be notified of the new global DFSR migration state, and because it might take even more time for a DC to make the changes required by that state, DCs will not be synchronized with the global state instantly. The getmigrationstate option enables you to monitor the progress of DCs toward the current global DFSR migration state.

If there is a problem moving from one state to the next higher state, you can revert to previous states by using the setglobalstate option. However, after you have used the setglobalstate option to specify state 3 (eliminated), you cannot revert to earlier states.

Migrate to DFS-R Replication of SYSVOL

1. Raise the domain functional level to WS2008
2. `dfsrmig /setglobalstate 1`
 - Wait for migration to Prepared state. Can take 15 minutes to an hour or longer
 - Use **dfsrmig /getmigrationstate** to monitor progress
3. `dfsrmig /setglobalstate 2`
 - Wait. **dfsrmig /getmigrationstate** to monitor progress
4. `dfsrmig /setglobalstate 3`
 - Wait. Can take 15 minutes to an hour or longer
 - Use **dfsrmig /getmigrationstate** to monitor progress
 - During migration to state 3 (eliminated), any changes to SYSVOL must be *manually* made to SYSVOL_DFSR as well

Key Points

To migrate SYSVOL replication from FRS to DFS-R, perform the following steps:

1. Open the **Active Directory Domains and Trusts** snap-in.
2. Right-click the domain and choose **Raise Domain Functional Level**.
3. If the **Current domain functional level** box does not indicate Windows Server 2008, choose **Windows Server 2008** from the **Select an available domain functional level** list.
4. Click **Raise**. Click **OK** twice in response to the dialog boxes that appear.
5. Log on to a domain controller and open a command prompt.
6. Type `dfsrmig /setglobalstate 1`.
7. Type `dfsrmig /getmigrationstate` to query the progress of DCs toward the Prepared global state. Repeat this step until the state has been attained by all DCs.

This can take 15 minutes to an hour or longer.

8. Type **dfsrmig /setglobalstate 2**.
9. Type **dfsrmig /getmigrationstate** to query the progress of DCs toward the Redirected global state. Repeat this step until the state has been attained by all DCs.

This can take 15 minutes to an hour or longer.
10. Type **dfsrmig /setglobalstate 3**.

After you begin migration from state 2 (prepared) to state 3 (replicated), any changes made to the SYSVOL folder will have to be replicated manually to the SYSVOL_DFSR folder.
11. Type **dfsrmig /getmigrationstate** to query the progress of DCs toward the Eliminated global state. Repeat this step until the state has been attained by all DCs.

This can take 15 minutes to an hour or longer.
12. For more information about the dfsrmig.exe command, type **dfsrmig.exe /?**.

Lab D: Configure DFS-R Replication of SYSVOL

- Exercise 1: Observe the Replication of SYSVOL
- Exercise 2: Prepare to Migrate to DFS-R
- Exercise 3: Migrate SYSVOL Replication to DFS-R
- Exercise 4: Verify DFS-R Replication of SYSVOL

Logon information

Virtual machine	6425B-HQDC01-B	6425B-HQDC02-B
Logon user name	Pat.Coleman	Pat.Coleman
Administrative user name	Pat.Coleman_Admin	Pat.Coleman_Admin
Password	Pa\$\$w0rd	Pa\$\$w0rd

Estimated time: 30 minutes

Scenario

You are an administrator at Contoso. You have recently upgraded the last remaining Windows Server 2003 domain controller to Windows Server 2008, and you want to take advantage of the improved replication of SYSVOL using DFS-R.

Exercise 1: Observe the Replication of SYSVOL

In this exercise, you will observe SYSVOL replication with File Replication Service (FRS) by adding a logon script to the NETLOGON share and observing its replication to another domain controller.

The main tasks for this exercise are as follows:

1. Prepare for the lab.
2. Observe SYSVOL replication.

► Task 1: Prepare for the lab

- Shut down all VMs.
- Start 6425B-HQDC01-B, and log on as **Pat.Coleman** with the password **Pa\$\$w0rd**.
- Open **D:\Labfiles\Lab11d**.
- Run **Lab11d_Setup.bat** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
- The lab setup script runs. When it is complete, press any key to continue.
- Close the Windows Explorer window, **Lab11d**.
- Start 6425B-HQDC02-B, and log on as **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.

► Task 2: Observe SYSVOL replication

- On HQDC01, open **%SystemRoot%\ Sysvol\sysvol\contoso.com\Scripts**.
- Run Notepad as an administrator, with the user name **Pat.Coleman_Admin** and the password **Pa\$\$w0rd**.
- Save a test file as **%SystemRoot%\ Sysvol\sysvol\contoso.com\Scripts \TestFRS.txt**.
- On HQDC02, open **%SystemRoot%\Sysvol\sysvol\contoso.com\Scripts \Scripts**.

- Confirm that **TestFRS.txt** has replicated to the HQDC02 Scripts folder.
If the file does not appear immediately, wait a few moments. It can take up to 15 minutes for replication to occur. You can, optionally, continue with Exercise 2. Before continuing even further with Exercise 3, check back to ensure that the file has replicated.
- After you have observed the replication, close the Windows Explorer window showing the Scripts folder on both HQDC01 and HQDC02.

Results: After this exercise, you should have observed the replication of a test file between the SYSVOL\Scripts folders of two domain controllers.

Exercise 2: Prepare to Migrate to DFS-R

Before you can migrate to DFS-R of SYSVOL, the domain must contain only Windows Server 2008 domain controllers, and the domain functional level must be raised to Windows Server 2008. In this exercise, you will confirm the fact that DFS-R migration is not supported in other domain functional levels. Then, you will raise the domain functional level to Windows Server 2008.

The main tasks for this exercise are as follows:

1. Confirm that the current domain functional level is lower than Windows Server 2008.
2. Confirm that DFS-R replication is not available at domain functional levels lower than Windows Server 2008.
3. Raise the domain functional level.
4. Confirm that DFS-R replication is available at Windows Server 2008 domain functional level.

► Task 1: Confirm that the current domain functional level is lower than Windows Server 2008

- On HQDC01, run **Active Directory Users and Computers** as an administrator, with the user name **Pat.Coleman_Admin** and the password **Pa\$\$w0rd**.
- Confirm that the current domain functional level is Windows Server 2003 but *do not raise the functional level*. Instead, cancel out of the dialog box.

► Task 2: Confirm that DFS-R replication is not available at domain functional levels lower than Windows Server 2008

- Run the Command Prompt as an administrator, with the user name **Pat.Coleman_Admin** and the password **Pa\$\$w0rd**.
- Type **dfsrmig /getglobalstate**, and then press ENTER. A message appears informing you that dfsrmig is supported only on domains at the Windows Server 2008 functional level.

► **Task 3: Raise the domain functional level**

- In **Active Directory Users and Computers**, raise the domain functional level to **Windows Server 2008**.
- Close **Active Directory Users and Computers**.

► **Task 4: Confirm that DFS-R replication is available at Windows Server 2008 domain functional level**

- Switch to the command prompt. Type **dfsrmig /getglobalstate**, and then press ENTER. A message appears informing you that DFS-R migration has not yet been initialized.

Results: After this exercise, you should have raised the domain functional level to Windows Server 2008, and confirmed that by doing so you have made it possible to migrate SYSVOL replication to DFS-R.

Exercise 3: Migrate SYSVOL Replication to DFS-R

In this exercise, you will migrate the replication mechanism from FRS to DFS-R.

The main task for this exercise is as follows:

1. Migrate SYSVOL replication to DFS-R

► Task 1: Migrate SYSVOL replication to DFS-R

1. Switch to the Command Prompt
2. Type **dfsrmig /setglobalstate 0**, and then press ENTER.

The following message appears:

```
Current DFSR global state: 'Start'  
New DFSR global state: 'Start'  
Invalid state change requested.
```

The default global state is already 0, 'Start,' so your command is not valid. However, this does serve to initialize DFSR migration.

3. Type **dfsrmig /getglobalstate**, and then press ENTER.

The following message appears:

```
Current DFSR global state: 'Start'  
Succeeded.
```

4. Type **dfsrmig /getmigrationstate**, and then press ENTER.

The following message appears:

```
All Domain Controllers have migrated successfully to Global state  
( 'Start' ).  
Migration has reached a consistent state on all Domain  
Controllers.  
Succeeded.
```

5. Type **dfsrmig /setglobalstate 1**, and then press ENTER.

The following message appears:

```
Current DFSR global state: 'Start'
New DFSR global state: 'Prepared'

Migration will proceed to 'Prepared' state. DFSR service will
copy the contents of SYSVOL to SYSVOL_DFSR
folder.

If any DC is unable to start migration then try manual polling.
OR Run with option /CreateGlobalObjects.
Migration can start anytime between 15 min to 1 hour.
Succeeded.
```

6. Type **dfsrmig /getmigrationstate**, and then press ENTER.
A message appears that reflects the migration state of each domain controller. Migration can take up to 15 minutes.
7. Repeat this step until you receive the following message that indicates migration has progressed to the 'Prepared' state and is successful:

```
All Domain Controllers have migrated successfully to Global state
('Prepared').
Migration has reached a consistent state on all Domain
Controllers.
Succeeded.
```

When you receive the message just shown, continue to the next step.

During migration to the 'Prepared' state, you might see one of these messages:

```
The following Domain Controllers are not in sync with Global state
('Prepared'):
```

```
Domain Controller (Local Migration State) - DC Type
=====
```

```
HQDC01 ('Start') - Primary DC
HQDC02 ('Start') - Writable DC
```

```
Migration has not yet reached a consistent state on all Domain
Controllers.
State information might be stale due to AD latency.
```


or

The following Domain Controllers are not in sync with Global state ('Prepared'):

Domain Controller (Local Migration State) - DC Type

=====

HQDC01 ('Start') - Primary DC

HQDC02 ('Waiting For Initial Sync') - Writable DC

Migration has not yet reached a consistent state on all Domain Controllers.

State information might be stale due to AD latency.

or

The following Domain Controllers are not in sync with Global state ('Prepared'):

Domain Controller (Local Migration State) - DC Type

=====

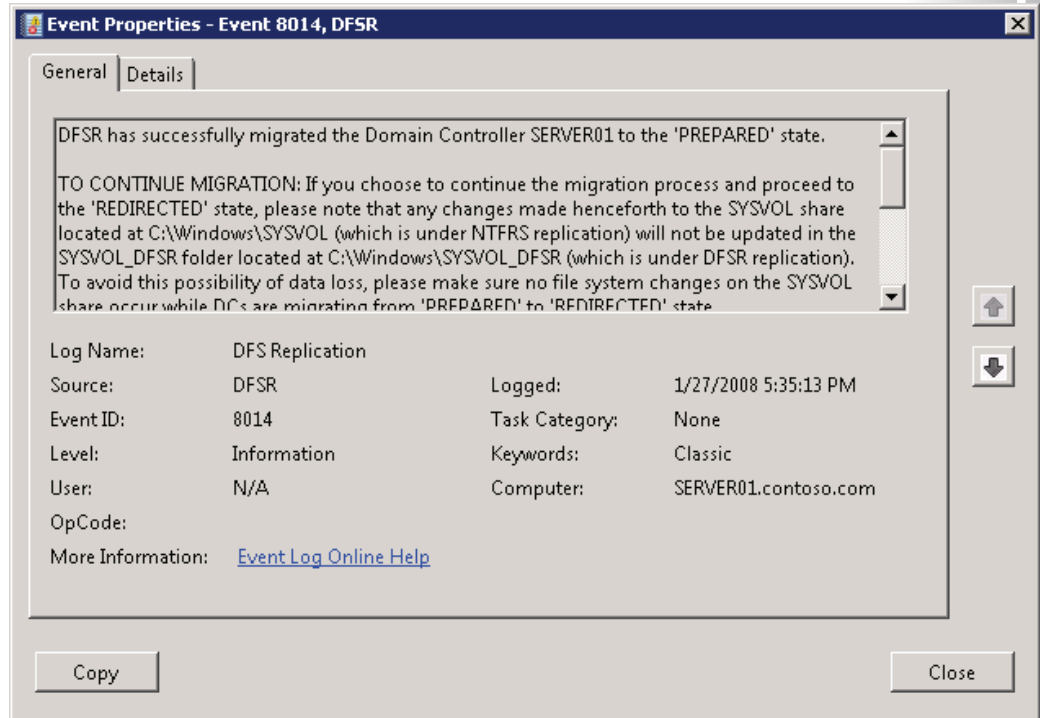
HQDC02 ('Waiting For Initial Sync') - Writable DC

Migration has not yet reached a consistent state on all Domain Controllers.

State information might be stale due to AD latency.

8. Click **Start**, point to **Administrative Tools**, right-click **Event Viewer**, and then choose **Run as administrator**.
9. Click **Use another account**.
10. In the **User name** box, type **Pat.Coleman_Admin**.
11. In the **Password** box, type **Pa\$\$w0rd**, and then press ENTER.
Event Viewer opens.
12. In the console tree, expand **Applications and Services Logs**, and select **DFS Replication**.

13. Locate the event with **Event ID 8014** and open its properties.
You should see the details shown in the following screen shot.



14. Close Event Viewer.
15. Switch to the Command Prompt.

16. Type **dfsrmig /setglobalstate 2**, and then press ENTER.

The following message appears:

```
Current DFSR global state: 'Prepared'
New DFSR global state: 'Redirected'

Migration will proceed to 'Redirected' state. The SYSVOL share
will be
changed to SYSVOL_DFSR folder.

If any changes have been made to the SYSVOL share during the state
transition from 'Prepared' to 'Redirected', please robocopy the
changes
from SYSVOL to SYSVOL_DFSR on any replicated RWDC.
Succeeded.
```

17. Type **dfsrmig /getmigrationstate**, and then press ENTER.

A message appears that reflects the migration state of each domain controller. Migration can take up to 15 minutes.

18. Repeat step 17 until you receive the following message that indicates migration has progressed to the 'Prepared' state and is successful:

```
All Domain Controllers have migrated successfully to Global state
('Redirected').
Migration has reached a consistent state on all Domain
Controllers.
Succeeded.
```

When you receive the message just shown, continue to the next task.

During migration, you might receive messages like the following:

```
The following Domain Controllers are not in sync with Global state
('Redirected'):

Domain Controller (Local Migration State) - DC Type
=====

HQDC02 ('Prepared') - Writable DC

Migration has not yet reached a consistent state on all Domain
Controllers.
State information might be stale due to AD latency.
```

Results: After this exercise, you should have migrated the replication of SYSVOL to DFS-R in the contoso.com domain.

Exercise 4: Verify DFS-R Replication of SYSVOL

In this exercise, you will verify that SYSVOL is being replicated by DFS-R.

The main tasks for this exercise are as follows:

1. Confirm the new location of SYSVOL.
2. Observe SYSVOL replication.

► Task 1: Confirm the new location of SYSVOL

- At the Command Prompt, type **net share**, and then press ENTER. Confirm that the NETLOGON share refers to the %SystemRoot%\SYSVOL_DFSR\Sysvol\contoso.com\Scripts folder, and that the SYSVOL share refers to the %SystemRoot%\SYSVOL_DFSR\Sysvol folder.

► Task 2: Observe SYSVOL replication

- On HQDC01, open %SystemRoot%\SYSVOL_DFSR\Sysvol\contoso.com\Scripts.

Note that the TestFRS.txt file created earlier is already in the Scripts folder. While the domain controllers were at the Prepared state, files were replicated between the legacy, FRS SYSVOL folder and the new, DFS-R SYSVOL folder.

- Run Notepad as an administrator, with the user name **Pat.Coleman_Admin** and the password **Pa\$\$w0rd**.
- Save a test file as %SystemRoot%\SYSVOL_DFSR\Sysvol\contoso.com\Scripts\TestDFSR.txt.
- On HQDC02, open %SystemRoot%\SYSVOL_DFSR\Sysvol\contoso.com\Scripts.
- Confirm that the TestDFSR.txt file has replicated to the HQDC02 Scripts folder.

If the file does not appear immediately, wait a few moments.

Results: After this exercise, you should have observed the replication of a test file between the SYSVOL_DFSR Scripts folders of two domain controllers.



Note: After completing this exercise, turn off all virtual machines and discard undo disks.

Lab Review Questions

Question: What would you expect to be different between two enterprises, one which created its domain initially with Windows 2008 domain controllers, and one that migrated to Windows Server 2008 from Windows Server 2003?

Question: What must you be aware of while migrating from the Prepared to the Redirected state?

Module 12

Manage Sites and Active Directory Replication

Contents:

Lesson 1: Configure Sites and Subnets	12-4
Lab A: Configure Sites and Subnets	12-22
Lesson 2: Configure the Global Catalog and Application Partitions	12-26
Lab B: Configure the Global Catalog and Application Partitions	12-41
Lesson 3: Configure Replication	12-46
Lab C: Configure Replication	12-73

Module Overview

- Configure Sites and Subnets
- Configure the Global Catalog and Application Partitions
- Configure Replication

You've learned in previous modules that domain controllers (DCs) in a Windows Server® 2008 domain are peers. Each maintains a copy of the directory, each performs similar services to support authentication of security principals, and changes made on any one domain controller will be replicated to all other domain controllers. As an administrator of a Windows® enterprise, one of your tasks is to ensure that authentication is provided as efficiently as possible, and that replication between domain controllers is optimized. Active Directory® sites are the core component of the directory service that supports the goals of service localization and replication. In this module, you will learn how to create a distributed directory service that supports domain controllers in portions of your network that are separated by expensive, slow, or unreliable links. You'll learn where domain controllers should be placed and how to manage replication and service utilization. You'll also learn how to control which data is replicated to each domain controller by configuring global catalogs (GCs) and application partitions.

Objectives

After completing this module, you will be able to:

- Configure sites and subnets.
- Understand domain controller location and manage domain controllers in sites.
- Configure replication of the partial attribute set to global catalog servers.
- Implement universal group membership caching.
- Understand the role of application directory partitions.
- Configure replication topology with connection objects, bridgehead servers, site links, and site link bridges.
- Report, analyze, and troubleshoot replication with repadmin.exe and dcdiag.exe.

Lesson 1

Configure Sites and Subnets

- Understand Sites
- Plan Sites
- Create Sites
- Manage Domain Controllers in Sites
- Domain Controller Location: SRV Records
- Domain Controller Location: Client

Active Directory represents human beings as user objects in the directory service. It represents machines by computer objects. It represents network topology with objects called *sites* and *subnets*. Active Directory site objects are used to manage replication and service localization and, fortunately, in many environments, the configuration of sites and subnets can be quite straightforward. In this lesson, you will learn the fundamental concepts and techniques required to configure and manage sites and subnets.

Objectives

After completing this lesson, you will be able to:

- Identify the role of sites and subnets.
- Describe the process with which a client locates a domain controller.
- Configure sites and subnets.
- Manage domain controller server objects in sites.

Understand Sites

- Loosely related to network “sites”
 - A highly connected portion of your enterprise
- Active Directory objects that support
 - Replication
 - Active Directory changes must be replicated to all DCs
 - Some DCs might be separated by slow, expensive links
 - Balance between replication “cost” & convergence
 - Service localization
 - DC (LDAP & Kerberos)
 - DFS
 - Active Directory-aware (site aware) apps
 - *Location* property searching, for example, printer location

Key Points

When administrators describe their network infrastructure, they often mention how many sites comprise their enterprise. To most administrators, a site is a physical location, an office or city, for example. Sites are connected by links—network links that might be as basic as dial-up connections or as sophisticated as fiber links. Together, the physical locations and links make up the network infrastructure.

Active Directory represents the network infrastructure with objects called *sites* and *site links*, and although the words are similar, these objects are not identical to the sites and links described by administrators. This lesson focuses on sites, and Lesson 3 discusses site links.

It's important to understand the properties and roles of sites in Active Directory to understand the subtle distinction between Active Directory sites and network sites. Active Directory sites are objects in the directory, specifically in the Configuration container (CN=Configuration,DC=*forest root domain*). These objects are used to achieve two service management tasks:

- To manage replication traffic
- To facilitate service localization

Replication Traffic

Replication is the transfer of changes between domain controllers. When you add a user or change a user's password, for example, the change you make is committed to the directory by one domain controller. That change must be communicated to all other domain controllers in the domain.

Active Directory assumes there are two types of networks within your enterprise: highly connected and less highly connected. Conceptually, a change made to Active Directory should replicate immediately to other domain controllers within the highly connected network in which the change was made. However, you might not want the change to replicate immediately over a slower, more expensive, or less reliable link to another site. Instead, you might want to manage replication over less highly connected segments of your enterprise to optimize performance, reduce costs, or manage bandwidth.

An Active Directory site represents a highly connected portion of your enterprise. When you define a site, the domain controllers within the site replicate changes almost instantly. Replication between sites can be scheduled and managed.

Service Localization

Active Directory is a distributed service. That is, assuming you have at least two domain controllers, there are multiple servers (domain controllers) providing the same services of authentication and directory access. If you have more than one network site, and if you place a domain controller in each, you want to encourage clients to authenticate against the domain controller in their site. This is an example of service localization.

Active Directory sites help you localize services, including those provided by domain controllers. During logon, Windows clients are automatically directed to a domain controller in their site. If a domain controller is not available in their site, they are directed to a DC in another site that will be able to authenticate the client efficiently.

Other services can be localized as well. Distributed File System Namespaces (DFS Namespaces), for example, is a localized service. DFS clients will obtain replicated resources from the most efficient server, based on their Active Directory site. In fact, because clients know what site they are in, any distributed service could be written to take advantage of the Active Directory site structure to provide intelligent localization of service usage.

Plan Sites

- **Active Directory sites may not map one-to-one with network sites**
 - Two locations, well connected, may be one Active Directory site
 - A large enterprise on a highly connected campus (one “site”) may be broken into multiple Active Directory sites for service localization
- **Criteria**
 - Connection speed: 512 kbps link is a guideline, but as low as 28 kbps is used
 - Service placement: If no DCs or Active Directory-aware services, not much point in a site
 - User population: If the number of users warrants a DC, consider a site
 - Directory query traffic by users or applications
 - Desire to control replication traffic between DCs

Key Points

Because sites are used to optimize replication and to enable service localization, you must spend time designing your Active Directory site structure. Active Directory sites might not map one to one with your network’s sites. Consider two scenarios:

- You have offices in two distinct locations. You place one domain controller in each location. The locations are highly connected, and to improve performance, you decide to configure a single Active Directory site that includes both locations.
- You have an enterprise on a large, highly connected campus. From a replication perspective, the enterprise could be considered a single site. However, you want to encourage clients to use distributed services in their location, so you configure multiple sites to support service localization.

Therefore, an Active Directory site can include more than one network site or be a subset of a single network site. The key is to remember that sites serve both replication management and service localization roles. Several characteristics of your enterprise can be used to help you determine which sites are necessary:

Connection Speed

An Active Directory site represents a unit of the network that is characterized by fast, reliable, inexpensive connectivity. Much documentation suggests that the slowest link speed within a site should be no less than 512 kilobits per second (kbps). However, this guidance is not immutable. Some organizations have links as slow as 56 or even 28 kbps within a site.

Service Placement

Because Active Directory sites manage Active Directory replication and service localization, it is not useful to create a site for a network location that does not host a domain controller or other Active Directory-aware service such as a replicated DFS resource.



Note: Sites where there are no domain controllers. Domain controllers are only one distributed service in a Windows enterprise. Other services, such as replicated DFS resources, are site-aware as well. You might configure sites to localize services other than authentication, in which case, you will have sites without domain controllers.

User Population

Concentrations of users can also influence your site design, although indirectly. If a network location has a sufficient number of users for whom the inability to authenticate would be problematic, place a domain controller in the location to support authentication within the location. After a domain controller or other distributed service is placed in the location to support those users, you might want to manage Active Directory replication to the location or localize service use by configuring an Active Directory site to represent the location.

Summarizing Site Planning Criteria

Every Active Directory forest includes at least one site. The default site created when you instantiate a forest with the first domain controller is creatively named Default-First-Site-Name. You should create additional sites when:

- A part of the network is separated by a slow link.
- A part of the network has enough users to warrant hosting domain controllers or other services in that location.
- Directory query traffic warrants a local domain controller.
- You want to control service localization.
- You want to control replication between domain controllers.

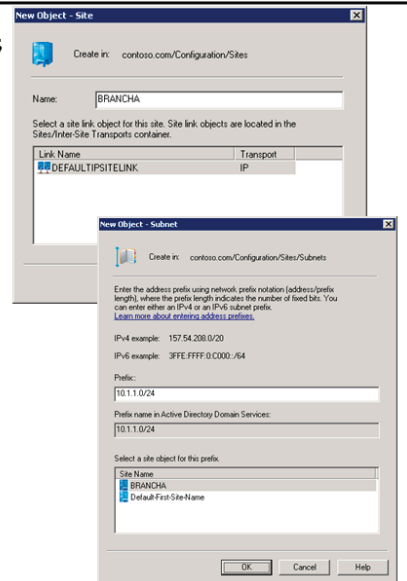
A Note on Server (DC) Placement

Network administrators often want to know when placing a domain controller in a remote site is recommended. The answer is, “It depends.” Specifically, it depends on the resources required by users in the site and the tolerance for downtime. If users in a remote site perform all work tasks by accessing resources in the data center, for example, then if the link to the remote site fails, the users cannot access the resources they require, and a local domain controller would not improve the situation. However, if users access resources in the remote site and the link fails, a local domain controller can continue to provide authentication for users, and they can continue to work with their local resources.

In most branch office scenarios, there are resources in the branch office that users require to perform their work tasks. Those resources, if not stored on the user’s own computer, require domain authentication of the user. Therefore, a domain controller is generally recommended. The introduction of read-only domain controllers (RODCs) in Windows Server 2008 reduces the risk and management burden of domain controllers in branch offices, so it will be easier for most organizations to deploy DCs in each network location.

Create Sites

- Active Directory Sites and Services
 - Default-First-Site-Name
 - Should be renamed
 - Create a site
 - Assign to site link
 - Create a subnet
 - Assign to site
 - A site can have >1 subnet
 - A subnet can be associated with only one site

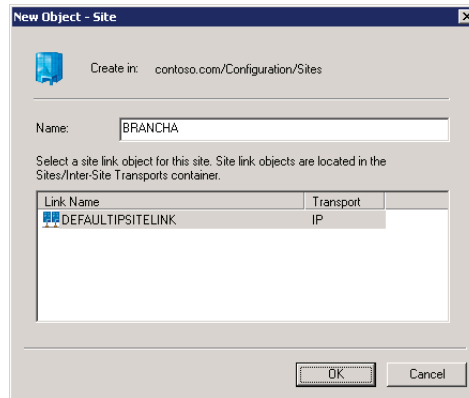


Key Points

Sites and replication are managed using the Active Directory Sites And Services snap-in. To define an Active Directory site, you will create an object of class site. The site object is a container that manages replication for domain controllers in the site. You will also create one or more subnet objects. A subnet object defines a range of IP addresses and is linked to one site. Service localization is attained when a client's IP address can be associated with a site through the relationship between the subnet object and the site object.

To create a site:

1. Right-click the **Sites** node in **Active Directory Sites And Services** and then click **New Site**.
2. In the **New Object – Site** dialog box that appears, enter a site name, and select a site link.



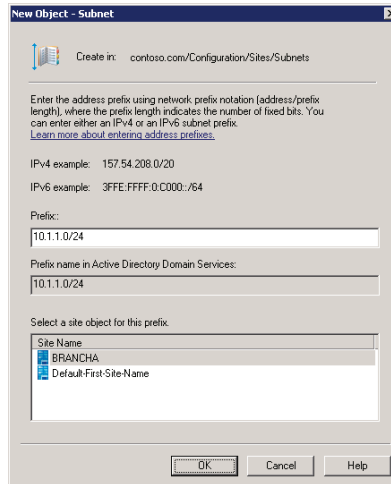
The default site link, DEFAULTIPSITELINK, will be the only site link available to you until you create additional site links, as discussed in Lesson 3.

After creating a site, you can right-click it and choose **Rename** to rename it. It is recommended that you rename the **Default-First-Site-Name** site to reflect a site name that is aligned with your business and network topology.

Sites are useful only when a client or server knows the site to which it belongs. This is typically achieved by associating the system's IP address with a site, and subnet objects achieve this association.

To create a subnet object:

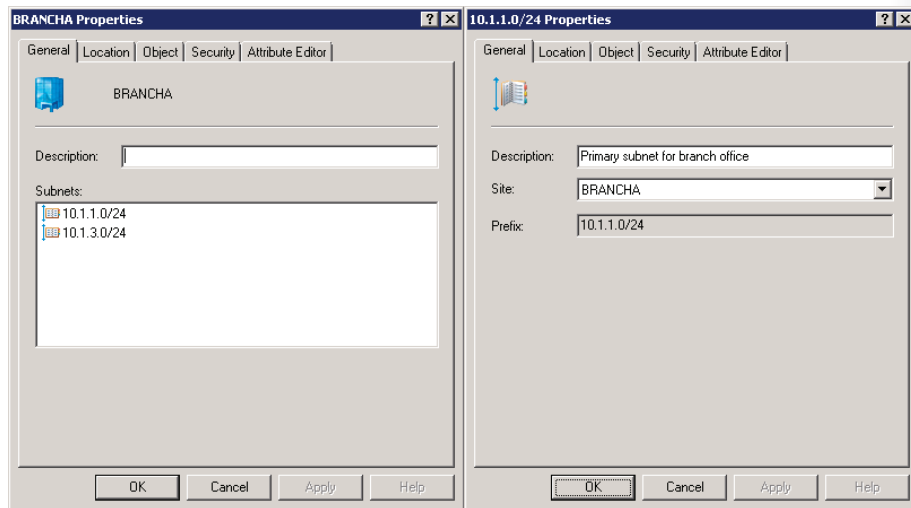
1. Right-click the **Subnets** node in the **Active Directory Sites and Services** snap-in and choose **New Subnet**. The **New Object – Subnet** dialog box appears.
2. Enter the network prefix and subnet mask length.



The subnet object is defined as a range of addresses using network prefix notation. For example, to enter a subnet representing the addresses 10.1.1.1 to 10.1.1.254 with a 24-bit subnet mask, the prefix would be 10.1.1.0/24. For more information about entering addresses, click the link [Learn More About Entering Address Prefixes](#) in the New Object – Subnet dialog box.

3. After entering the network prefix, select the site object with which the subnet is associated.

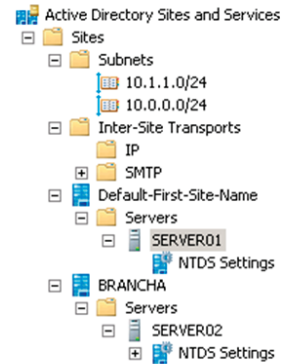
A subnet can be associated with only one site; however, a site can have more than one subnet linked to it. The Properties dialog box of a site, shown in the following screen shot, shows the subnets associated with the site. You cannot change the subnets in this dialog box, however; instead, you must open the properties of the subnet, shown in the following screen shot, to change the site to which the subnet is linked.



Note: Defining every IP subnet. In your production environment, be certain to define every IP subnet as an Active Directory subnet object. If a client's IP address is not included within a subnet range, the client is unable to determine which Active Directory site it belongs to, which can lead to performance and functionality problems. Don't forget backbone subnets and subnets used for remote access such as virtual private network (VPN) address ranges.

Manage Domain Controllers in Sites

- DCs should be in the correct site
 - The SERVERS container will show only DCs, not all server
- Add a DC to a site
 - First DC will be in Default-First-Site-Name
 - Additional DCs will be added to sites based on their subnet address
 - DCPromo prompts you for the site
 - You can right-click the Servers container of a site and pre-create the server object before promoting the DC
- Move DC to a new site: right-click DC and choose **Move**
- Delete a DC: right-click DC and choose **Delete**

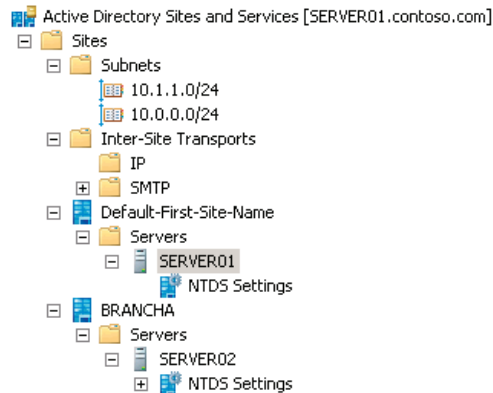


Key Points

There are times when you might need to manage domain controllers in Active Directory sites:

- You create a new site and move an existing domain controller to it.
- You demote a domain controller.
- You promote a new domain controller.

When you create your Active Directory forest, the first domain controller is automatically placed under the site object named Default-First-Site-Name. You can see the domain controller SERVER01.contoso.com in the following screen shot.



Additional domain controllers will be added to sites based on their IP addresses. For example, if a server with IP address 10.1.1.17 is promoted to a domain controller, the server will automatically be added to the BRANCHA site because the 10.1.1.0/24 subnet was associated with the BRANCHA site (see the previous slide). The previous screen shot shows SERVER02 in the BRANCHA site.

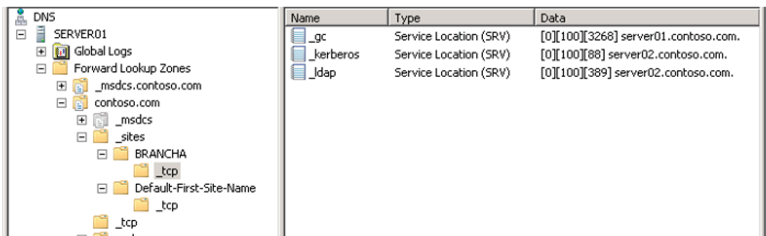
Each site contains a Servers container, which itself contains an object for each domain controller in the site. The Servers container in a site should show only domain controllers, not all servers. When you promote a new domain controller, the domain controller will, by default, be placed in the site associated with its IP address. However, the Active Directory Domain Services Installation Wizard will enable you to specify another site. You can also pre-create the server object for the domain controller in the correct site by right-clicking the Servers container in the appropriate site and choosing Server from the New menu.

Finally, you can move the domain controller to the correct site after installation by right-clicking the server and choosing Move. In the Move Server dialog box, select the new site and click OK. The domain controller is moved. It is a best practice to place a domain controller in the site object that is associated with the DC's IP address. If a DC is multihomed, it can belong to only one site. If a site has no domain controllers, users will still be able to log on to the domain; their logon requests will be handled by a domain controller in an adjacent site or another domain controller in the domain.

To remove a domain controller object, right-click it and choose Delete.

Domain Controller Location: SRV Records

- Domain controllers register service locator records (SRV) in DNS in the following locations
 - `_tcp.contoso.com`: all DCs in the domain
 - `_tcp.siteName._sites.contoso.com`: all DCs in site *siteName*



The screenshot shows the DNS console for SERVER01. The left pane displays the hierarchy: Global Logs, Forward Lookup Zones, contoso.com, _msdcs, _sites, BRANCHA, Default-First-Site-Name, and _tcp. The right pane shows a table of SRV records.

Name	Type	Data
_gc	Service Location (SRV)	[0][100][3268] server01.contoso.com.
_kerberos	Service Location (SRV)	[0][100][88] server02.contoso.com.
_ldap	Service Location (SRV)	[0][100][389] server02.contoso.com.

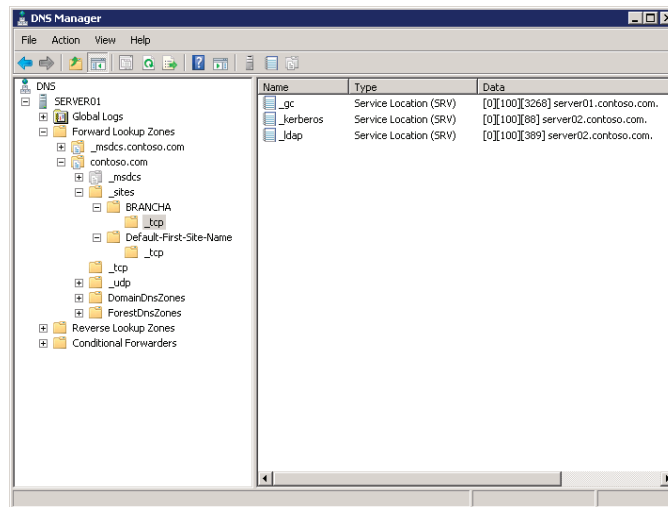
- Clients query DNS for domain controllers

Key Points

You started this lesson by examining Active Directory Domain Services (AD DS) as a distributed service, providing authentication and directory access on more than one domain controller. You learned to identify where, in your network topology, to define sites and place domain controllers. Now you are ready to examine how, exactly, service localization works—how Active Directory clients become site aware and locate the domain controller in their site. Although this level of detail is unlikely to appear on the certification examination, it can be extremely helpful when you need to troubleshoot authentication of a computer or of a user.

Service Locator Records

When a domain controller is added to the domain, it advertises its services by creating Service Locator (SRV) records, also called locator records, in DNS. Unlike host records (A records), which map host names to IP addresses, SRV records map services to host names. The domain controller advertises its ability to provide authentication and directory access by registering Kerberos and LDAP SRV records. These SRV records are added to several folders within the DNS zones for the forest. The first folder is within the domain zone. It is called `_tcp` and it contains the SRV records for all domain controllers in the domain. The second folder is specific to this site, in which the domain controller is located, with the path `_sites\sitename_tcp`, where *sitename* is the name of the site.



In the previous screen shot, you can see the Kerberos and LDAP SRV records for SERVER02.contoso.com in its site, `_sites\BRANCHA_tcp`. You can also see the `_tcp` folder at the first level beneath the zone.

The same records are registered in several places in the `_msdcs.domainName` zone, for example, `_msdcs.contoso.com` in the previous screen shot. This zone contains records for Microsoft Domain Controller Services. The underscore characters are a requirement of RFC 2052.

Locator records contain:

- **The service name and port.** This portion of the SRV record indicates a service with a fixed port. It does not have to be a well-known port. SRV records in Windows Server 2008 include LDAP (port 389), Kerberos (port 88), Kerberos Password protocol (KPASSWD, port 464), and GC services (port 3268).
- **Protocol.** TCP or UDP will be indicated as a transport protocol for the service. The same service can use both protocols, in separate SRV records. Kerberos records, for example, are registered for both TCP and UDP. Microsoft clients use only TCP, but UNIX clients can use TCP.
- **Host name.** The name corresponds to the A (Host) record for the server hosting the service. When a client queries for a service, the DNS server returns the SRV record and associated A records, so the client does not need to submit a separate query to resolve the IP address of a service.


The service name in the SRV record follows the standard DNS hierarchy, with components separated by dots. For example, the Kerberos service of a domain controller is registered as:

kerberos._tcp.siteName._sites.domainName

Reading this SRV record name right to left like other DNS records, it translates to:

- *domainName*: the domain or zone, for example contoso.com
- **_sites**: all sites registered with DNS
- *siteName*: the site of the domain controller registering the service
- **_tcp**: any TCP-based services in the site
- **kerberos**: a Kerberos Key Distribution Center (KDC) using TCP as its transport protocol

Domain Controller Location: Client

- | | |
|--|--|
| <ol style="list-style-type: none"> 1. New client queries for all DCs in the domain <ul style="list-style-type: none"> ▪ Retrieves SRVs from <code>_tcp.domain</code> 2. Attempts LDAP bind to all 3. First DC to respond <ul style="list-style-type: none"> ▪ Examines client IP and subnet definitions ▪ Refers client to a site 4. Client stores site in registry | <ol style="list-style-type: none"> 5. Client queries for all DCs in the site <ul style="list-style-type: none"> ▪ Retrieves SRVs from <code>_tcp.site._sites.domain</code> 6. Attempts LDAP bind to all 7. First DC to respond <ul style="list-style-type: none"> ▪ Authenticates client ▪ Client forms affinity 8. Subsequently <ul style="list-style-type: none"> ▪ Client binds to affinity DC ▪ DC offline? Client queries for DCs in registry-stored site ▪ Client moved to another site? DC refers client to another site |
|--|--|
- 

Key Points

Imagine a Windows client has just been joined to the domain. It restarts, receives an IP address from a DHCP server, and is ready to authenticate to the domain. How does the client know where to find a domain controller?

It does not. Therefore, the client queries the domain for a domain controller by querying the `_tcp` folder which, you'll remember, contains the SRV records for all domain controllers in the domain. DNS returns a list of all matching DCs, and the client attempts to contact all of them on this, its first startup. The first domain controller that responds to the client examines the client's IP address, cross-references that address with subnet objects, and informs the client of the site to which the client belongs. The client stores the site name in its registry, then queries for domain controllers in the site-specific `_tcp` folder. DNS returns a list of all DCs in the site. The client attempts to bind with all, and the DC that responds first authenticates the client.

The client forms an affinity for this DC and will attempt to authenticate with the same DC in the future. If the DC is unavailable, the client queries the site's _tcp folder again and attempts to bind with all DCs in the site. But what happens if the client is a mobile computer—a laptop? Imagine that the computer has been authenticating in the BRANCHA site and then the user brings the computer to the BRANCHB site. When the computer starts up, it actually attempts to authenticate with its preferred DC into BRANCHA site. That DC notices the client's IP address is associated with BRANCHB and informs the client of its new site. The client then queries DNS for domain controllers in BRANCHB.

You can see how, by storing subnet and site information in Active Directory and by registering services in DNS, a client is encouraged to use services in its site—the definition of service localization.

Additional Reading

- For more information about domain controller location, see <http://go.microsoft.com/fwlink/?LinkId=168550>

Site Coverage

What happens if a site has no domain controller? Sites can be used to direct users to local copies of replicated resources such as shared folders replicated within a DFS namespace, so you might have sites without a DC. In this case, a nearby domain controller will register its SRV records in the site in a process called site coverage. To be precise, a site without a DC will generally be covered by a domain controller in a site with the lowest cost to the site requiring coverage. You'll learn more about site link costs in Lesson 3. You can also manually configure site coverage and SRV record priority if you want to implement strict control over authentication in sites without DCs. The URL just listed contains details about the algorithm that determines which DC automatically covers a site without a DC.

Lab A: Configure Sites and Subnets

- Exercise 1: Configure the Default Site
- Exercise 2: Create Additional Sites

Logon information

Virtual machine	6425B-HQDC01-B	6425-HQDC02-B	6425B-HQDC03-B	6425B-BRANCHDC01-B
Logon user name	Pat.Coleman	Do not log on	Do not log on	Do not log on
Administrative user name	Pat.Coleman_Admin			
Password	Pa\$\$w0rd			

Estimated time: 30 minutes

Scenario

You are an administrator for Contoso, Ltd. You are preparing to improve the service localization and Active Directory replication of your enterprise. The previous administrator made no changes to the out-of-box configuration of sites and subnets. You want to begin the process of defining your physical topology in Active Directory.

Exercise 1: Configure the Default Site

In this exercise, you will rename the Default-First-Site-Name site and associate two subnets with the site.

The main tasks for this exercise are as follows:

1. Prepare for the lab.
2. Rename Default-First-Site-Name.
3. Create a subnet and associate it with a site.

► Task 1: Prepare for the lab

- Start 6425B-HQDC01-B, and log on as **Pat.Coleman** with the password **Pa\$\$w0rd**. This virtual machine may take several minutes to start.
- After logging on to HQDC01, start 6425B-HQDC02-B but do not log on.
- After HQDC02 has completed startup, start 6425B-HQDC03-B but do not log on.
- After HQDC03 has completed startup, start 6425B-BRANCHDC01-B, but do not log on.
- Wait for BRANCHDC01 to finish startup before continuing to the next task.

► Task 2: Rename Default-First-Site-Name

- Run **Active Directory Sites and Services** as an administrator, with the user name **Pat.Coleman_Admin** and the password **Pa\$\$w0rd**.
- Rename Default-First-Site-Name to **HEADQUARTERS**.

► Task 3: Create a subnet and associate it with a site

- Create two subnets: **10.0.0.0/24** and **10.0.1.0/24**, and associate each with the **HEADQUARTERS** site.

Results: After this exercise, you should have a site named HEADQUARTERS and two subnets (10.0.0.0/24 and 10.0.1.0/24) associated with the site.

Exercise 2: Create Additional Sites

In this exercise, you will create a second site and associate a subnet with it.

The main tasks for this exercise are as follows:

1. Create additional sites.
2. Create subnets and associate them with sites.

► Task 1: Create additional sites

- Create a site named **HQ-BUILDING-2**.
- Create a site named **BRANCHA**.

► Task 2: Create subnets and associate them with sites

- Create a subnet, **10.1.0.0/24**, and associate it with the **HQ-BUILDING-2** site.
- Create a subnet, **10.2.0.0/24**, and associate it with the **BRANCHA** site.

Results: After this exercise, you should have created 2 new sites, HQ-BUILDING-2 and BRANCHA, and associated them with the 10.1.0.0/24 and 10.2.0.0/24 subnets.

Exercise 3: Move Domain Controllers into Sites

► Task 1: Move domain controllers to new sites

- Move HQDC03 to the **HQ-BUILDING-2** site.
- Move BRANCHDC01 to the **BRANCHA** site.



Important: Do not shut down the virtual machines once you are finished with this lab as the settings you have configured here will be used in subsequent labs in this module.

Lab Review Questions

Question: You have a site with 50 subnets, each with a subnet address of 10.0.x.0/24, and you have no other 10.0.x.0 subnets, what could you do to make it easier to identify the 50 subnets and associate them with a site?

Question: Why is it important that all subnets are identified and associated with a site in a multisite enterprise?

Lesson 2

Configure the Global Catalog and Application Partitions

- Review Active Directory Partitions
- Understand the Global Catalog
- Place Global Catalog Servers
- Configure a Global Catalog Server
- Universal Group Membership Caching
- Understand Application Directory Partitions

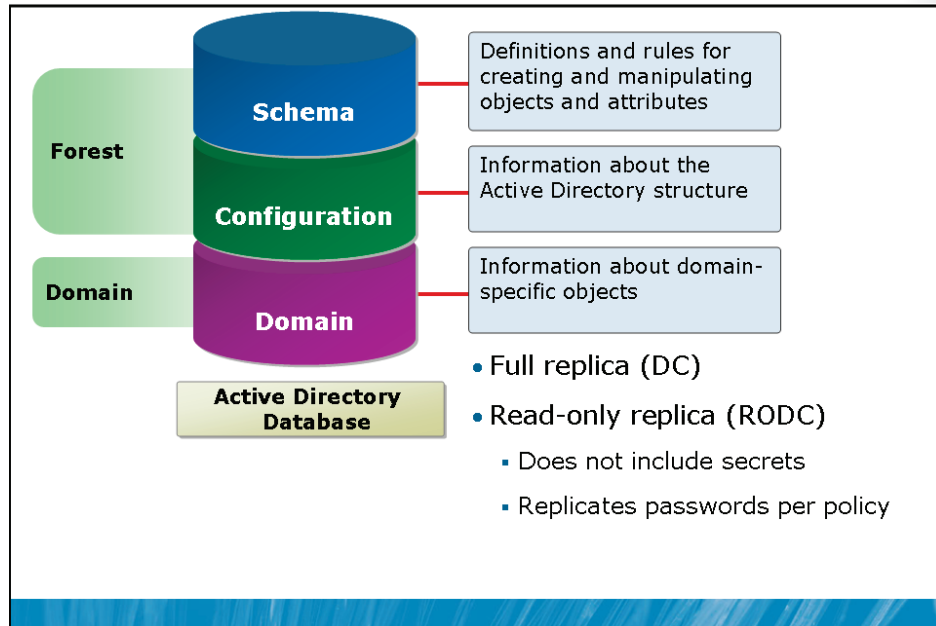
As soon as you have more than one domain controller in your domain, you must consider replication of the directory database between domain controllers. In this lesson, you will learn which directory partitions are replicated to each domain controller in a forest and how to manage the replication of the GC and of application partitions.

Objectives

After completing this lesson, you will be able to:

- Define the purpose of the GC.
- Configure domain controllers as GC servers.
- Implement universal group membership caching.
- Understand the role of application directory partitions.

Review Active Directory Partitions



Key Points

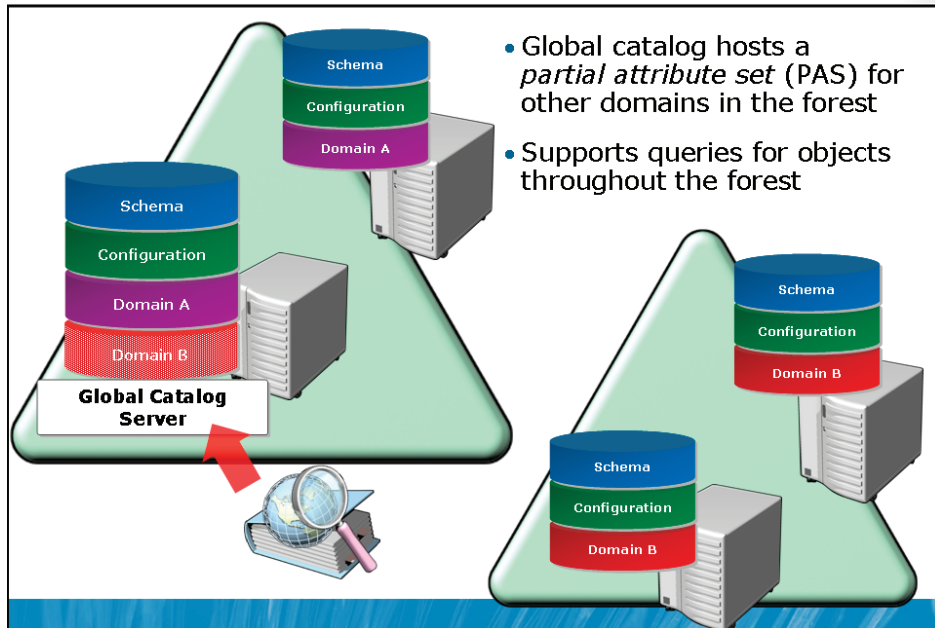
In Module 1, you learned that Active Directory Domain Services (AD DS) includes a data store for identity and management, specifically the directory database, Ntds.dit. Within that single file are directory partitions. Each directory partition, also called a *naming context*, contains objects of a particular scope and purpose. Three major naming contexts have been discussed in this course:

- **Domain.** The Domain naming context (NC) contains all the objects stored in a domain, including users, groups, computers, and Group Policy containers (GPCs).
- **Configuration.** The Configuration partition contains objects that represent the logical structure of the forest, including domains, as well as the physical topology, including sites, subnets, and services.
- **Schema.** The Schema defines the object classes and their attributes for the entire directory.

Each domain controller maintains a copy, or replica, of several naming contexts. The Configuration is replicated to every domain controller in the forest, as is the Schema. The Domain naming context for a domain is replicated to all domain controllers within a domain but not to domain controllers in other domains, so each domain controller has at least three replicas: the Domain NC for its domain, Configuration, and Schema.

Traditionally, replicas have been complete replicas, containing every object of an attribute, and replicas have been writable on all DCs. Beginning with Windows Server 2008, RODCs change the picture slightly. An RODC maintains a read-only replica of all objects in the Configuration, Schema, and Domain NCs of its domain. However, certain attributes are not replicated to an RODC—specifically, secrets such as user passwords—unless the password policy of the RODC allows such replication. There are also attributes that are domain and forest secrets that are never replicated to an RODC.

Understand the Global Catalog



Key Points

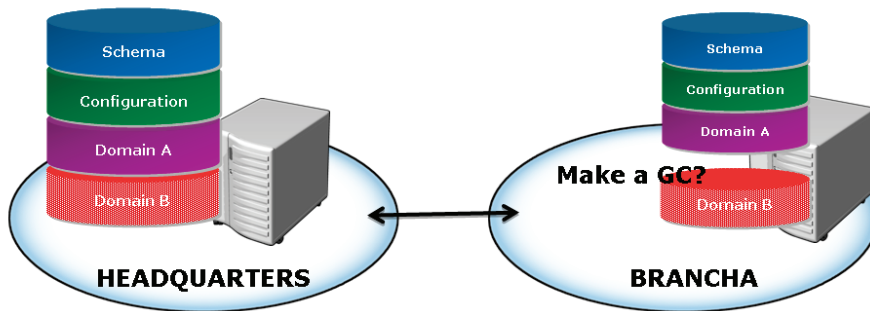
Imagine a forest with two domains. Each domain has two domain controllers. All four domain controllers will maintain a replica of the Schema and Configuration NCs for the forest. The domain controllers in Domain A have replicas of the Domain NC for Domain A, and the domain controllers in Domain B have replicas of the Domain NC for Domain B.

What happens if a user in Domain B is searching for a user, computer, or group in Domain A? The Domain B domain controllers do not maintain any information about objects in Domain A, so a domain controller in Domain B could not answer a query about objects in the Domain NC of Domain A.

That's where the global catalog comes in. The global catalog (GC) is a partition that stores information about every object in the forest. When a user in Domain B looks for an object in Domain A, the GC provides the results of the query. To optimize efficiency of the GC, it does not contain every attribute of every object in the forest. Instead, it contains a subset of attributes that are useful for searching across domains. That is why the GC is also called the partial attribute set (PAS). In terms of its role supporting search, you can think of the GC as a kind of index for the AD DS data store.

Place Global Catalog Servers

- Recommendation: Every DC a GC
- In particular
 - If an application in a site queries the GC (port 3268)
 - If a site contains an Exchange server
 - If a connection to a GC in another site is slow/unreliable



Key Points

The GC improves efficiency of the directory service tremendously and is required for applications such as Microsoft Exchange Server and Microsoft Office Outlook®. Therefore, you want a GC to be available to these and other applications. The GC can be served only by a domain controller and, in an ideal world, *every domain controller would be a GC server*. In fact, many organizations are now configuring all of their domain controllers as GC servers.

The potential downside to such a configuration relates to replication. The GC is another partition that must be replicated. In a single domain forest, very little overhead is actually added by configuring all domain controllers as GC servers because all domain controllers already maintain a full set of attributes for all domain and forest objects. In a large, multidomain forest, there will be overhead related to replication of changes to the partial attribute set of objects in other domains. However, many organizations are finding that Active Directory replication is efficient enough to replicate the GC without significant impact to their networks and that the benefits far outweigh such impact. If you choose to configure all DCs as GC servers, you no longer need to worry about the placement

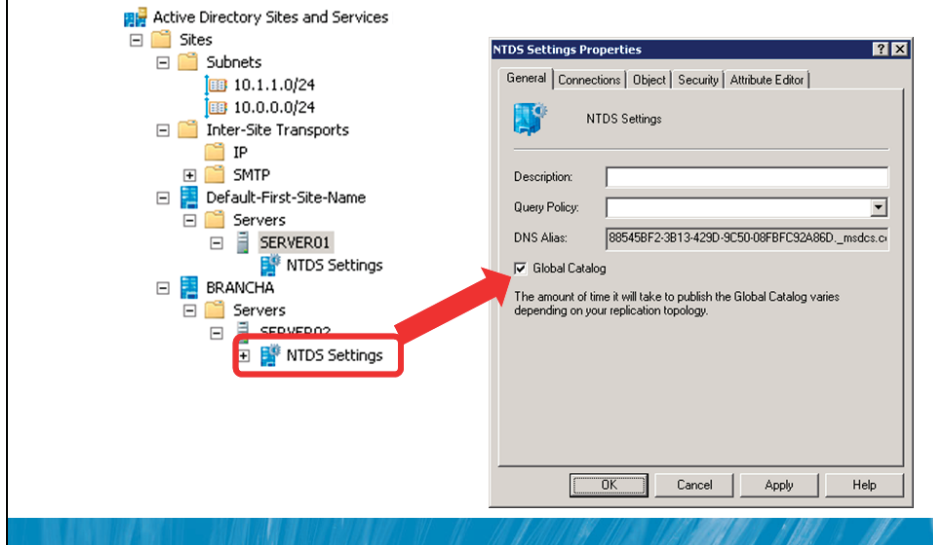
of the infrastructure operations master; its role is no longer necessary in a domain where all DCs are GC servers.

It is particularly recommended to configure a GC server on a domain controller in a site where one or more of the following is true:

- A commonly used application performs directory queries, using port 3268, the GC.
- The connection to a GC server is slow or unreliable.
- The site contains a computer running Exchange Server.

Configure a Global Catalog Server

- Right-click the NTDS Settings node underneath the DC



Key Points

When you create the first domain in the forest, the first domain controller is configured as a GC.

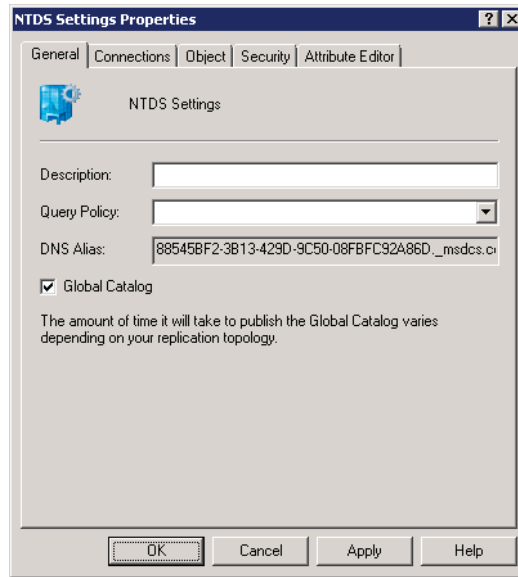
You must decide for each additional DC whether it should be a GC server. The Active Directory Domain Services Installation Wizard and the Dcpromo.exe command each enable you to configure a GC server when promoting a domain controller.

You can also add or remove the GC from a domain controller by using Active Directory Sites and Services.

To configure a DC as a GC:

1. Expand the site, the Servers container within the site, and the domain controller's server object.
2. Right-click the **NTDS Settings** node and choose **Properties**.

3. On the **General** tab, shown in the following screen shot, select the **Global Catalog** check box.



To remove the GC from a domain controller, perform the same steps, clearing the Global Catalog check box.

Universal Group Membership Caching

- Universal group membership replicated in the GC
 - Normal logon: user's token built with UGs from GC
 - GC not available at logon: DC *denies authentication*
- If every DC is a GC, this is never a problem
- If connectivity to a GC is not reliable
 - DCs can *cache* UG membership for a user when user logs on
 - GC later not available: user authenticated with cached UGs
- In sites with unreliable connectivity to GC: enable UGMC
- Right-click NTDS Settings for site → Properties
 - Enables UGMC for all DCs in the site

Key Points

In Module 4, you learned that Active Directory supports groups of universal scope. Universal groups are designed to include users and groups from multiple domains in a forest. The membership of universal groups is replicated in the GC. When a user logs on, the user's universal group membership is obtained from a GC server. If a GC is not available, universal group membership is not available. It's possible that a universal group is used to deny the user access to resources, so Windows prevents a security incident by denying domain authentication to the user. If the user has logged on to his or her computer before, he or she can log on using cached credentials, but as soon as the user attempts to access network resources, access will be denied.

To summarize: if a GC server is not available, users will effectively be unable to log on and access network resources.

If every domain controller is a GC server, this problem will not arise.

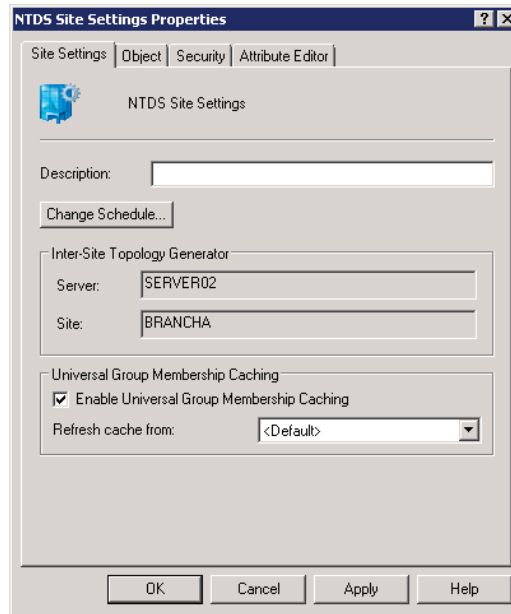
However, if replication is a concern, and if you have, therefore, chosen not to configure a domain controller as a GC server, you can facilitate successful logon by enabling universal group membership caching (UGMC). When you configure universal group membership caching on a domain controller in a branch office, for example, that domain controller will obtain universal group membership information from a GC for a user when the user first logs on in the site, and the domain controller will cache that information indefinitely, updating universal group membership information every eight hours. That way, if the user later logs on and a GC server is not accessible, the domain controller can use its cached membership information to permit logon by the user.

It is recommended, therefore, that *in sites with unreliable connectivity to a GC server, you should configure UGMC on the site's domain controllers.*

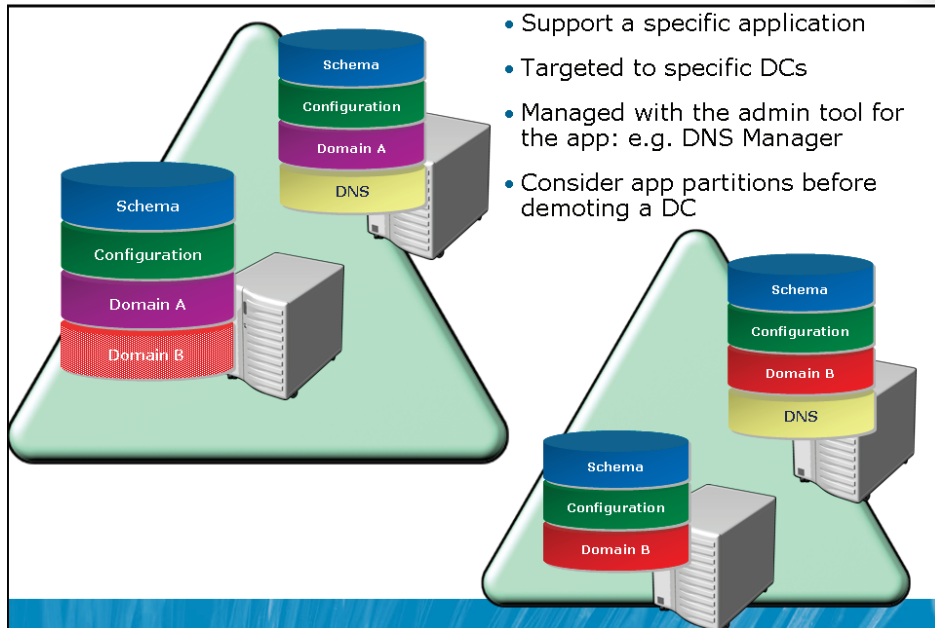
To configure UGMC:

1. Open the **Active Directory Sites and Services** snap-in and select the site in the console tree.
2. In the details pane, right-click **NTDS Site Settings** and choose **Properties**.

3. The **NTDS Site Settings Properties** dialog box, shown in the following screen shot, exposes the Enable Universal Group Membership Caching option. You can select the check box and specify the GC from which to refresh the membership cache.



Understand Application Directory Partitions



Key Points

Whereas the Domain, Configuration, and Schema partitions of the directory are replicated to all DCs in a domain; and the Configuration and Schema partitions are further replicated to all DCs in the forest; and the partial attribute set is replicated by global catalog servers; Active Directory also supports application directory partitions. An application directory partition is a portion of the data store that contains objects required by an application or service that is outside of the core AD DS service. Unlike other partitions, application partitions can be targeted to replicate to specific domain controllers; they are not, by default, replicated to all DCs.

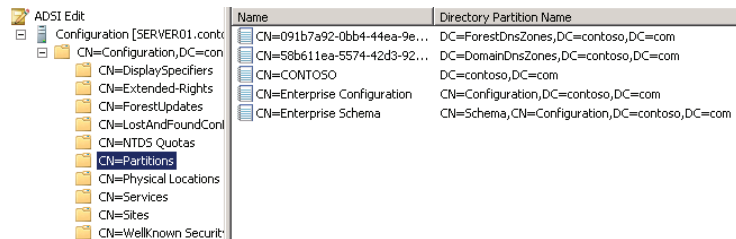
Application directory partitions are designed to support directory-enabled applications and services. They can contain any type of object except security principals such as users, computers, or security groups. Because these partitions are replicated only as needed, application directory partitions provide the benefits of fault tolerance, availability, and performance while optimizing replication traffic.

The easiest way to understand application directory partitions is to examine the application directory partitions maintained by Microsoft DNS Server. When you create an Active Directory-integrated zone, DNS records are replicated between DNS servers by using an application directory partition. The partition and its DNS record objects are not replicated to every domain controller, only to those acting as DNS servers.

To explore the application directory partitions in your forest:

1. Open **ADSI Edit**.
2. Right-click the root of the snap-in, **ADSI Edit**, and choose **Connect To**.
3. In the **Select a well known naming context** drop-down list, choose **Configuration**, and then click **OK**.
4. Expand **Configuration** and the folder representing the **Configuration** partition, and then select the Partitions folder, **CN=Partitions**, in the console tree.

In the details pane, you will see the partitions in your AD DS data store, as shown in the following screen shot.



Note the two application partitions in the figure, *ForestDnsZones* and *DomainDnsZones*. Most application partitions are created by applications that require them. DNS is one example, and Telephony Application Programming Interface (TAPI) is another. Members of the Enterprise Admins group can also create application directory partitions manually by using Ntdsutil.exe.

An application partition can appear anywhere in the forest namespace that a domain partition can appear. The DNS partitions distinguished names—DC=DomainDnsZones,DC=contoso,DC=com, for example—place the partitions as children of the DC=contoso,DC=com domain partition. An application partition can also be a child of another application partition or a new tree in the forest.

Generally speaking, you will use tools specific to the application to manage the application directory partition, its data, and its replication. For example, simply adding an Active Directory–integrated zone to a DNS server will automatically configure the domain controller to receive a replica of the DomainDns partition. With tools such as Ntdsutil.exe and Ldp.exe, you can manage application directory partitions directly.

It is important that you consider application partitions prior to demoting a domain controller. If a domain controller is hosting an application directory partition, you must evaluate the purpose of the partition, whether it is required by any applications, and whether the domain controller holds the last remaining replica of the partition, in which case, demoting the domain controller will result in permanently losing all information in the partition. Although the Active Directory Domain Services Installation Wizard will prompt you to remove application directory partitions, it is recommended that you manually remove application directory partitions prior to demoting a domain controller.

Additional Reading

- For more information about application directory partitions, visit <http://go.microsoft.com/fwlink/?LinkId=168551>
- To learn how to manage application directory partitions, see <http://go.microsoft.com/fwlink/?LinkId=168553>
- For more information about application directory partitions and domain controller demotion, see <http://go.microsoft.com/fwlink/?LinkId=168554>

Lab B: Configure the Global Catalog and Application Partitions

- Exercise 1: Configure a Global Catalog
- Exercise 2: Configure Universal Group Membership Caching
- Exercise 3: Examine DNS and Application Directory Partitions

Logon information

Virtual machine	6425B-HQDC01-B	6425-HQDC02-B	6425B-HQDC03-B	6425B-BRANCHDC01-B
Logon user name	Pat.Coleman	Do not log on	Do not log on	Do not log on
Administrative user name	Pat.Coleman_Admin			
Password	Pa\$\$w0rd			

Estimated time: 30 minutes

Scenario

You are the administrator of Contoso, Ltd. In your continued effort to improve the availability and resiliency of the directory service, you decide to configure additional global catalog servers and universal group membership caching. You are also curious about the relationship between Active Directory-integrated DNS zones and the DNS application partitions.

Exercise 1: Configure a Global Catalog

The first domain controller in a forest acts as a GC server. You might want to place GC servers in additional locations to support directory queries, logon, and applications such as Exchange Server. In this exercise, you will configure BRANCHDC01 to host a replica of the partial attribute set—the global catalog.

The main tasks for this exercise are as follows:

1. Prepare for the lab.
2. Configure a global catalog server.

► Task 1: Start and log on to the virtual machines

The virtual Machines should already be started and available after completing Lab A. However, if they are not, you should complete the below steps then step through Exercises 1 to 3 in Lab A before continuing.

1. Start 6425B-HQDC01-B, and log on as **Pat.Coleman** with the password **Pa\$\$w0rd**. This virtual machine may take several minutes to start.
2. After logging on to HQDC01, start 6425B-HQDC02-B but do not log on.
3. After HQDC02 has completed startup, start 6425B-HQDC03-B but do not log on.
4. After HQDC03 has completed startup, start 6425B-BRANCHDC01-B but do not log on.
5. Wait for BRANCHDC01 to finish startup before continuing to the next task.

► Task 2: Configure a global catalog server

1. Run **Active Directory Sites and Services** as an administrator, with the user name **Pat.Coleman_Admin** and the password **Pa\$\$w0rd**.
2. Configure HQDC02 to be a global catalog server.
3. Confirm that BRANCHDC01 is a global catalog server.

Results: After this exercise, you should have configured HQDC02 to be a global catalog server and confirmed that BRANCHDC01 is already a global catalog server.

Exercise 2: Configure Universal Group Membership Caching

In sites without GC servers, user logon might be prevented if the site's domain controller is unable to contact a GC server in another site. To reduce the likelihood of this scenario, you can configure a site to cache the membership of universal groups. In this exercise, you will create a site to reflect a branch office and configure the site to cache universal group membership.

The main tasks for this exercise are as follows:

- Configure universal group membership caching.
- **Task 1: Configure universal group membership caching**
- Configure the NTDS Site Settings of BRANCHA so that domain controllers cache universal group membership.

Results: After this exercise, you should have configured domain controllers in BRANCHA to cache universal group membership.

Exercise 3: Examine DNS and Application Directory Partitions

In this exercise, you will explore the DNS records related to replication and the DomainDnsZone application directory partition, using ADSI Edit.

The main tasks for this exercise are as follows:

1. Examine DNS records related to replication.
2. Examine the DNS application directory partition.

► Task 1: Examine DNS records related to replication

1. Run **DNS Manager** as an administrator, with the user name **Pat.Coleman_Admin** and the password **Pa\$\$w0rd**.
2. Examine the service locator records in **_tcp.HEADQUARTERS._sites.contoso.com**
3. Examine the service locator records in **_tcp.BRANCHA._sites.contoso.com**.

► Task 2: Examine the DNS application directory partition

1. Click **Start>Administrative Tools >ADSI Edit** and enter administrative credentials when prompted. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
2. In the console tree, right-click **ADSI Edit**, and then click **Connect To**.
3. In the **Select a well known naming context** drop-down list, select **Configuration**.
4. Accept all other defaults. Click **OK**.
5. In the console tree, click **Configuration**, and then expand it.
6. In the console tree, click **CN=Configuration, DC=contoso, DC=com**, and then expand it.
7. In the console tree, click **CN=Partitions**.
8. Right-click **ADSI Edit**, and then click **Connect To**.
9. Click **Select or type a distinguished name or naming context**.
10. In the combo box, type **DC=DomainDnsZones,DC=contoso,DC=com**. Click **OK**.

11. In the console tree, click **Default Naming Context**, and then expand it.
12. Click on **DC=DomainDnsZones,DC=contoso,DC=com**, and then expand it.
13. Click on **CN=MicrosoftDNS**, and then expand it.
14. Click **DC=contoso.com**.
15. Examine the objects in this container. Compare the records to the DNS records you examined in the previous exercise.

Results: After this exercise, you should have explored the DNS records and the application directory partition for DNS in the contoso.com domain.



Important: Do not shut down the virtual machines once you are finished with this lab as the settings you have configured here will be used in subsequent labs in this module.

Lab Review Questions

Question: Describe the relationship between the records you viewed in ADSI Edit and the records you viewed in DNS Manager.

Question: When you examined the DNS records in _tcp.BRANCHA._sites.contoso.com, what domain controller was registering service locator records in the site? Explain why it did so.

Lesson 3

Configure Replication

- Understand Active Directory Replication
- Intrasite Replication
- Site Links
- Replication Transport Protocols
- Bridgehead Servers
- Site Link Transitivity and Bridges
- Control Intersite Replication
- Monitor and Manage Replication

In Lesson 1, you learned how to create site and subnet objects that enable Active Directory and its clients to localize authentication and directory access; you decided where domain controllers should be placed. In Lesson 2, you configured GC servers and application directory partitions; you managed what will replicate between domain controllers. In this lesson, you will learn how and when replication occurs. You'll discover why the default configuration of Active Directory supports effective replication and why you might modify that configuration so that replication is equally effective but more efficient, based on your network topology.

Objectives

After completing this lesson, you will be able to:

- Create connection objects to configure replication between two domain controllers.
- Implement site links and site link costs to manage replication between sites.
- Designate preferred bridgehead servers.

- Understand notification and polling.
- Report and analyze replication with repadmin.exe.
- Perform Active Directory replication health checks with dcdiag.exe.

Understand Active Directory Replication

- **Multimaster replication's balancing act: "loose coupling"**
 - Accuracy (integrity)
 - Consistency (convergence)
 - Performance (keeping replication traffic to a reasonable level)
- **Key characteristics of Active Directory Replication**
 - Multimaster replication
 - Pull replication
 - Store-and-forward
 - Partitions
 - Automatic generation of an efficient & robust replication topology
 - Attribute level replication
 - Distinct control of intrasite and intersite replication
 - Collision detection and remediation

Key Points

In previous lessons, you learned how to place domain controllers in network locations and how to represent those locations with site and subnet objects. You also learned about the replication of directory partitions (schema, configuration, and domain), the partial attribute set (GC), and application partitions. The most important thing to remember as you learn about Active Directory replication is that it is designed so that, in the end, each replica on a domain controller is consistent with the replicas of that partition hosted on other domain controllers. It is not likely that all domain controllers will have exactly the same information in their replicas at any one moment in time because changes are constantly being made to the directory. However, Active Directory replication ensures that all changes to a partition are transferred to all replicas of the partition. Active Directory replication balances accuracy (or integrity) and consistency (called *convergence*) with performance (keeping replication traffic to a reasonable level). This balancing act is described as loose coupling.

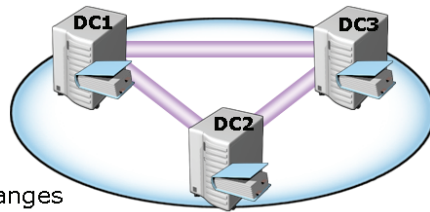
Key characteristics of Active Directory replication are:

- **Multimaster replication.** Any domain controller can initiate and commit a change to Active Directory.
- **Pull replication.** A domain controller requests, or "pulls," changes from other domain controllers. As you learn more about replication, it may become easy to forget this, because a DC *notifies* its replication partners that it has changes to the directory, or a DC can *poll* its partners to see if they have changes to the directory. But the changes themselves are, in the end, requested or "pulled" by the target DC.
- **Store-and-forward replication.** A domain controller can pull changes from one partner, and then make those changes available to another partner. For example, domain controller B can pull changes initiated by domain controller A. Then domain controller C can pull the changes from domain controller B.
- **Partitioning of the data store.** Domain controllers in a domain host only the domain naming context for their domain, which helps keep replication to a minimum, particularly in multidomain forests. Other data, including application directory partitions and the partial attribute set (GC), are not replicated to every domain controller in the forest, by default.
- **Automatic generation of an efficient and robust replication topology.** By default, Active Directory will configure an effective, two-way replication topology so that the loss of any one domain controller does not impede replication. This topology is automatically updated as domain controllers are added, removed, or moved between sites.
- **Attribute-level replication.** When an attribute of an object is modified, only that attribute, and minimal metadata that describes that attribute, is replicated. The entire object is not replicated except when the object is created.
- **Distinct control of intrasite replication** (within a single site) **and intersite replication** (between sites). Replication can be distinctly controlled in both of these situations.
- **Collision detection and management.** It is possible, although rare, that an attribute will have been modified on two different domain controllers during a single replication window. In such an event, the two changes will have to be reconciled. Active Directory has resolution algorithms that satisfy almost every such situation.

It is easier to understand Active Directory replication by examining each of its components. The following sections examine the components of Active Directory replication.

Intrasite Replication

- Connection object: inbound replication to a DC
- Knowledge consistency checker (KCC) creates topology
 - Efficient (maximum three hop) & robust (two-way) topology
 - Runs automatically, but you can “Check Replication Topology”
 - Few reasons to manually create connection objects
 - Standby operations masters should have connections to masters
- Replication
 - Notification: DC tells its downstream partners change is available (15 seconds)
 - Polling: DC checks with its upstream partners (1 hour) for changes
 - Downstream DC directory replication agent (DRA) replicates changes
 - Changes to all partitions held by both DCs are replicated



Key Points

This section includes discussion of the following key point topics:

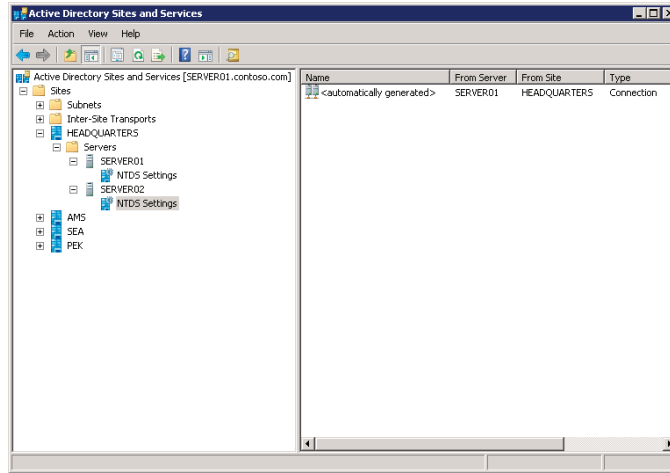
- Connection Objects
- The Knowledge Consistency Checker
- Intrasite Replication
- Notification
- Polling

Connection Objects

A domain controller replicates changes from another domain controller because of AD DS connection objects, also called simply *connection objects*.

Connection objects appear in the administrative tools in the Active Directory Sites and Services snap-in as objects contained in the NTDS Settings container of a domain controller's server object.

The following screen shot shows an example: A connection object in SERVER02 configures replication from SERVER01 to SERVER02. A connection object represents a replication path from one domain controller to another.



Connection objects are one-way, representing inbound-only replication. Replication in Active Directory is always a pull technology. In the domain illustrated above, SERVER02 pulls changes from SERVER01. SERVER02 is considered, in this example, a downstream replication partner of SERVER01. SERVER01 is the upstream partner. Changes from SERVER01 flow to SERVER02.



Note: Force replication. You can force replication between two domain controllers by right-clicking the connection object and choosing Replicate Now. Remember replication is inbound only, so to replicate both domain controllers, you will need to replicate the inbound connection object of each domain controller.

The Knowledge Consistency Checker

The replication paths built between domain controllers by connection objects create the replication topology for the forest. Luckily, you do not have to create the replication topology manually. By default, Active Directory creates a topology that ensures effective replication. The topology is two-way so that if any one domain controller fails, replication will continue uninterrupted. The topology also ensures that there are no more than three hops between any two domain controllers.

You'll notice in the previous screen shot that the connection object indicates it was automatically generated. On each domain controller, a component of Active Directory called the knowledge consistency checker (KCC) helps generate and optimize the replication automatically between domain controllers within a site. The KCC evaluates the domain controllers in a site and creates connection objects to build the two-way, three-hop topology described earlier. If a domain controller is added to or removed from the site, or if a domain controller is not responsive, the KCC rearranges the topology dynamically, adding and deleting connection objects to rebuild an effective replication topology.

You can manually create connection objects to specify replication paths that should persist. Manually created connection objects are not deleted by the KCC.

To create a connection object:

1. In **Active Directory Sites and Services**, locate the server object for the downstream replication partner—the DC that will receive changes from a source DC. Right-click the NTDS Settings container in the server object and choose **New Active Directory Domain Services Connection**.
2. In the **Find Active Directory Domain Controllers** dialog box, select the upstream replication partner, and then click **OK**.
3. Give the new connection object a name, and then click **OK**.
4. Open the properties of the connection object; use the **Description** field to indicate the purpose of any manually created connection object.

Within a site, there are very few scenarios that would require creating a connection object. One such scenario is standby operations masters. Operations masters are discussed in Module 11. It is recommended that you select domain controllers as standby operations masters to be used in the event that the operations master role must be transferred or seized. A standby operations master should be a direct replication partner with the current operations master. Thus, if a domain controller named DC01 is the RID master, and DC02 is the system that will take the RID master role if DC01 is taken offline, then a connection object should be created in DC02 so that it replicates directly from DC01.

Intrasite Replication

After connection objects between the domain controllers in a site have been established—automatically by the KCC or manually—replication can take place. Intrasite replication involves the replication of changes within a single site.

Notification

Consider the site shown in the previous screen shot. When SERVER01 makes a change to a partition, it queues the change for replication to its partners. SERVER01 waits 15 seconds, by default, to notify its first replication partner, SERVER02, of the change. Notification is the process by which an upstream partner informs its downstream partners that a change is available. SERVER01 waits three seconds, by default, between notifications to additional partners. These delays, called the initial notification delay and the subsequent notification delay, are designed to stagger network traffic caused by intrasite replication.

Upon receiving the notification, the downstream partner, SERVER02, requests the changes from SERVER01, and the directory replication agent (DRA) performs the transfer of the attribute from SERVER01 to SERVER02. In this example, SERVER01 made the initial change to Active Directory. It is the originating domain controller and the change it made originates the change. When SERVER02 receives the change from SERVER01, it makes the change to its directory. The change is not called a replicated change, but it is a change nonetheless. SERVER02 queues the change for replication to its own downstream partners.

SERVER03 is a downstream replication partner of SERVER02. After 15 seconds, SERVER02 notifies SERVER03 that it has a change. SERVER03 makes the replicated change to its directory and then notifies its downstream partners. The change has made two hops, from SERVER01 to SERVER02 and from SERVER02 to SERVER03. The replication topology will ensure that there are no more than three hops before all domain controllers in the site have received the change. At approximately 15 seconds per hop, that means the change will have fully replicated in the site within one minute.

Polling

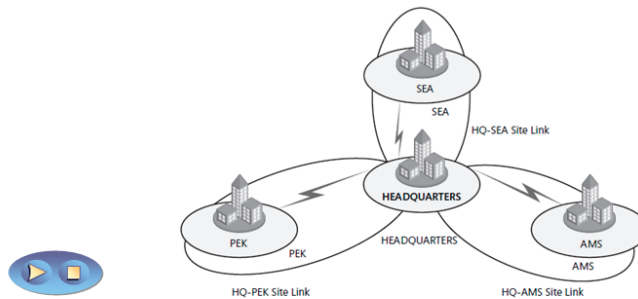
It is possible that SERVER01 might not make any changes to its replicas for quite a long time, particularly during off hours. In this case, SERVER02, its downstream replication partner, will not receive notifications from SERVER01. It is also possible that SERVER01 might be offline, which would also prevent it from sending notifications to SERVER02. So it's important for SERVER02 to know that its upstream partner is online and simply does not have any changes.

This is achieved through a process called polling. Polling involves the downstream replication partner contacting the upstream replication partner with a query as to whether any changes are queued for replication. By default, the polling interval for intrasite replication is once per hour. It is possible, although not recommended, to configure the polling frequency from the properties of a connection object by clicking Change Schedule.

If an upstream partner fails to respond to repeated polling queries, the downstream partner launches the KCC to check the replication topology. If the upstream server is indeed offline, the site's replication topology is rebuilt to accommodate the change.

Site Links

- Intersite topology generator (ISTG) builds replication topology *between* sites
- Site links
 - Contain sites
 - Within a site link, a connection object can be created between any two DCs
 - Not always appropriate given your network topology!

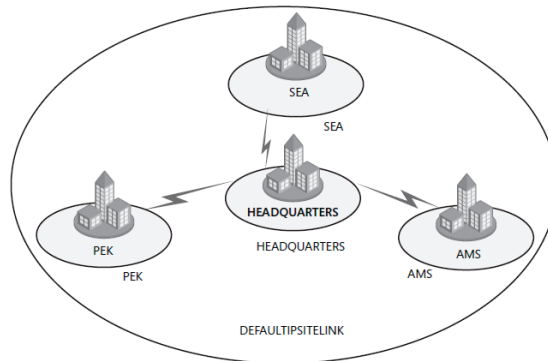


Key Points

The KCC assumes that within a site, all domain controllers can reach each other. It builds an intrasite replication topology that is agnostic to the underlying network connectivity. Between sites, however, you can represent the network paths over which replication should occur by creating site link objects. A site link contains two or more sites. The intersite topology generator (ISTG), a component of the KCC, builds connection objects between servers in each of the sites to enable intersite replication—replication between sites.

Site links are greatly misunderstood, and the important thing to remember about a site link is that it represents an available path for replication. A single site link does not control the network routes that are used. When you create a site link and add sites to it, you are telling Active Directory that it can replicate between any of the sites associated with the site link. The ISTG will create connection objects, and those objects will determine the actual path of replication. Although the replication topology built by the ISTG will effectively replicate Active Directory, it might not be efficient, given your network topology.

An example will illustrate this concept. When you create a forest, one site link object is created: DEFAULTIPSITELINK. By default, each new site that you add is associated with the DEFAULTIPSITELINK. Consider an organization with a data center at the headquarters and three branch offices. The three branch offices are each connected to the data center with a dedicated link. You create sites for each branch office, Seattle (SEA), Amsterdam (AMS), and Beijing (PEK). The network and site topology is shown in the following figure.

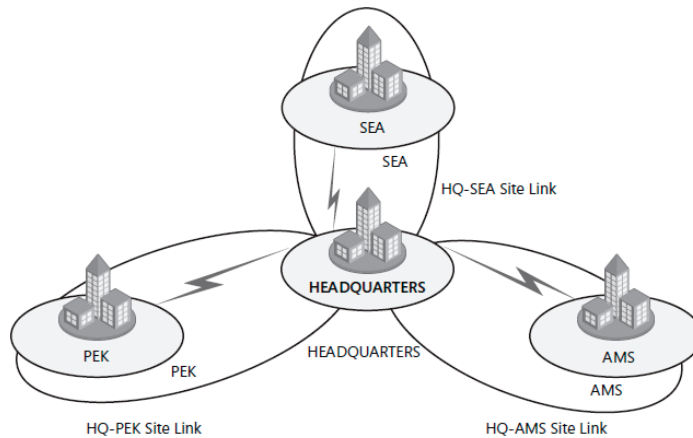


Because all four sites are on the same site link, you are instructing Active Directory that all four sites can replicate with each other. That means it is possible that Seattle will replicate changes from Amsterdam, Amsterdam will replicate changes from Beijing, and Beijing will replicate changes from Headquarters, which in turn replicates changes from Seattle. In several of these replication paths, the replication traffic on the network flows from one branch through the headquarters on its way to another branch. With a single site link, you have not created a hub-and-spoke replication topology even though your network topology is hub-and-spoke.

Therefore, it is recommended that you manually create site links that reflect your physical network topology. Continuing the preceding example, you would create three site links:

- HQ-AMS, including the Headquarters and Amsterdam sites
- HQ-SEA, including the Headquarters and Seattle sites
- HQ-PEK, including the Headquarters and Beijing sites

You would then delete the DEFAULTIPSITELINK. The resulting topology is shown in the following figure.



After you have created site links, the ISTG will use the topology to build an intersite replication topology connecting each site. Connection objects will be built to configure the intersite replication paths. These connection objects are created automatically, and although you can create connection objects manually, there are few scenarios that require manually creating intersite connection objects.

Replication Transport Protocols

- **Directory Service Remote Procedure Call (DS-RPC)**
 - Appears as **IP** in Active Directory Sites and Services
 - The default and preferred protocol for intersite replication
- **Inter-Site Messaging—Simple Mail Transport Protocol (ISM-SMTP)**
 - Appears as **SMTP** in Active Directory Sites and Services
 - Rarely used in the real world
 - Requires a certificate authority
 - Cannot replicate the domain naming context—only schema and configuration
 - Any site that uses SMTP to replicate must be in a separate domain within the forest

Key Points

You'll notice, in the Active Directory Sites And Services snap-in, that site links are contained within a container named IP that itself is inside the Inter-Site Transports container. Changes are replicated between domain controllers, using one of two protocols:

Directory Service Remote Procedure Call (DS-RPC)

DS-RPC appears in the Active Directory Sites and Services snap-in as IP. IP is used for all intrasite replication and is the default, and preferred, protocol for intersite replication.

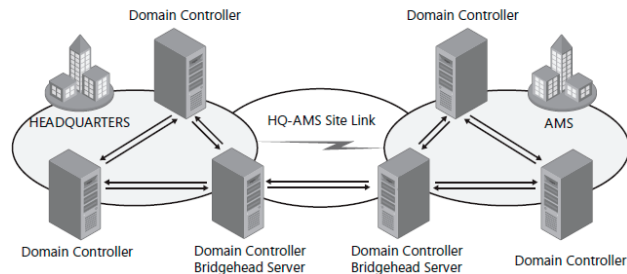
Inter-Site Messaging—Simple Mail Transport Protocol (ISM-SMTP)

Also known simply as SMTP, this protocol is used only when network connections between sites are unreliable or are not always available.

In general, you can assume you will use IP for all intersite replication. Very few organizations use SMTP for replication because of the administrative overhead required to configure and manage a certificate authority (CA) and because SMTP replication is not supported for the domain naming context, meaning that if a site uses SMTP to replicate to the rest of the enterprise, that site must be its own domain.

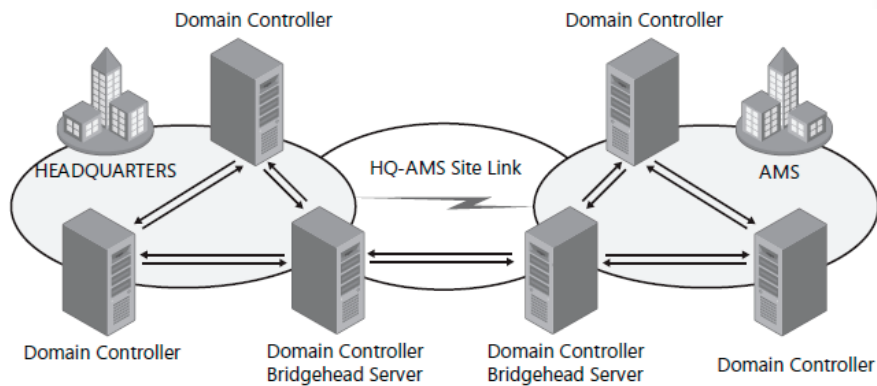
Bridgehead Servers

- Replicates changes from bridgeheads in all other sites
- Polled for changes by bridgeheads in all other sites
- Selected automatically by ISTG
- Or you can configure preferred bridgehead servers
 - Firewall considerations
 - Performance considerations



Key Points

The ISTG creates a replication topology between sites on a site link. To make replication more efficient, one domain controller is selected to be the bridgehead server. The bridgehead server is responsible for all replication into and out of the site for a partition. For example, if a data center site contains five DCs, one of the DCs will be the bridgehead server for the domain naming context. All changes made to the domain partition within the data center will replicate to all DCs in the site. When the changes reach the bridgehead server, those changes will be replicated to bridgehead servers in branch offices, which in turn replicate the changes to DCs in their sites. Similarly, any changes to the domain naming context in branch offices will be replicated from the branches' bridgehead servers to the bridgehead server in the data center, which in turn replicates the changes to other DCs in the data center. The following figure illustrates intrasite replication within two sites and the intersite replication using connection objects between the bridgehead servers in the sites.



To summarize, the bridgehead server is the server responsible for replicating changes to a partition from other bridgehead servers in other sites. It is also polled by bridgehead servers in other sites to determine when it has changes that they should replicate.

Bridgehead servers are selected automatically, and the ISTG creates the intersite replication topology to ensure that changes are replicated effectively between bridgeheads sharing a site link. Bridgeheads are selected per partition, so it is possible that one DC in a site might be the bridgehead server for the schema and another might be for the configuration. However, you will usually find that one domain controller is the bridgehead server for all partitions in a site unless there are domain controllers from other domains or application directory partitions, in which case, bridgeheads will be chosen for those partitions.

Preferred Bridgehead Servers

You can also designate one or more preferred bridgehead servers.

To designate a domain controller as a preferred bridgehead server:

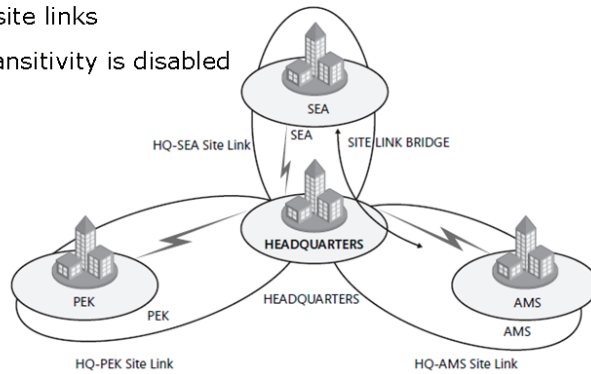
1. Open the properties of the server object in the **Active Directory Sites and Services** snap-in.
2. Select the transport protocol, which will almost always be IP, and then click **Add**.

You can configure more than one preferred bridgehead server for a site, but only one will be selected and used as the bridgehead. If that bridgehead fails, one of the other preferred bridgehead servers will be used.

It's important to understand that if you have specified one or more bridgehead servers and none of the bridgeheads is available, no other server is automatically selected, and replication does not occur for the site even if there are servers that could act as bridgehead servers. In an ideal world, you should not configure preferred bridgehead servers. However, performance considerations might suggest that you assign the bridgehead server role to domain controllers with greater system resources. Firewall considerations might also require that you assign a single server to act as a bridgehead instead of allowing Active Directory to select and possibly reassign bridgehead servers over time.

Site Link Transitivity and Bridges

- **Site link transitivity (default)**
 - ISTG can create connection objects between site links
 - Disable transitivity in the properties of the IP transport
- **Site link bridges**
 - Manually transitive site links
 - Useful only when transitivity is disabled



Key Points

After you have created site links and the ISTG has generated connection objects to replicate partitions between bridgehead servers that share a site link, your work might be complete. In many environments, particularly those with straightforward network topologies, site links might be sufficient to manage intersite replication. In more complex networks, however, you can configure additional components and properties of replication.

Site Link Transitivity

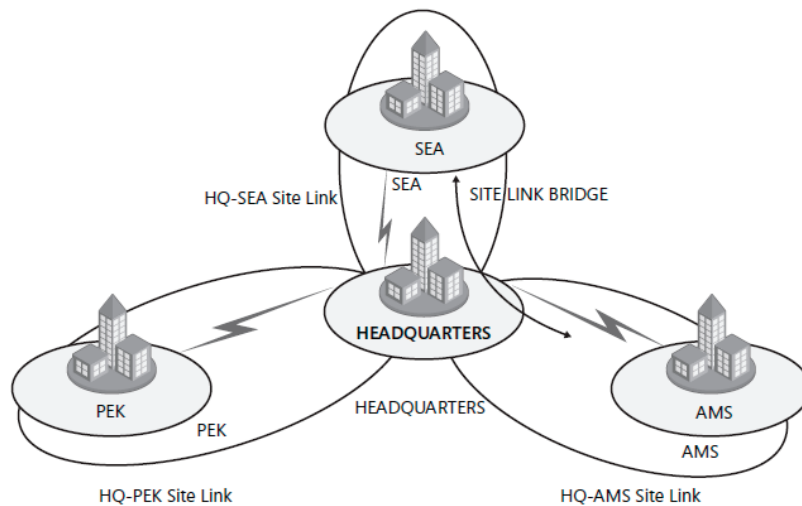
By default, site links are transitive. That means, continuing the example from earlier, that if Amsterdam and Headquarters sites are linked, and Headquarters and Seattle sites are linked, then Amsterdam and Seattle are transitively linked. This means, theoretically, that the ISTG could create a connection object directly between a bridgehead in Seattle and a bridgehead in Amsterdam, again working around the hub-and-spoke network topology.

You can disable site link transitivity by opening the properties of the IP transport in the Inter-Site Transports container and deselecting Bridge All Site Links. Before you do this in a production environment, be sure to spend time reading the technical resources about replication in the Windows Server technical libraries on Microsoft TechNet at <http://technet.microsoft.com>.

Site Link Bridges

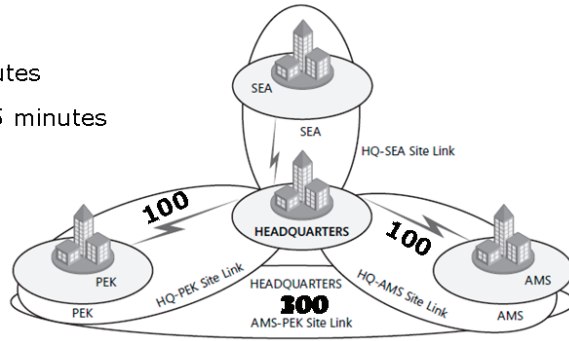
A site link bridge connects two or more site links in a way that creates a transitive link. Site link bridges are necessary only when you have cleared the Bridge All Site Links option for the transport protocol. Remember that site link transitivity is enabled by default, in which case, site link bridges have no effect.

The following figure illustrates the use of a site link bridge in a forest in which site link transitivity has been disabled. By creating a site link bridge, AMS-HQ-SEA, that includes the HQ-AMS and HQ-SEA site links, those two site links become transitive, so a replication connection can be made between a domain controller in Amsterdam and a domain controller in Seattle.



Control Intersite Replication

- **Site link costs**
 - Replication uses the connections with the lowest cost
- **Replication**
 - Notifications off by default. Bridgeheads do not notify partners
 - Polling. Downstream bridgehead polls upstream partners
 - Default: 3 hours
 - Minimum: 15 minutes
 - Recommended: 15 minutes
 - Replication schedules
 - 24 hours a day
 - Can be scheduled



Key Points

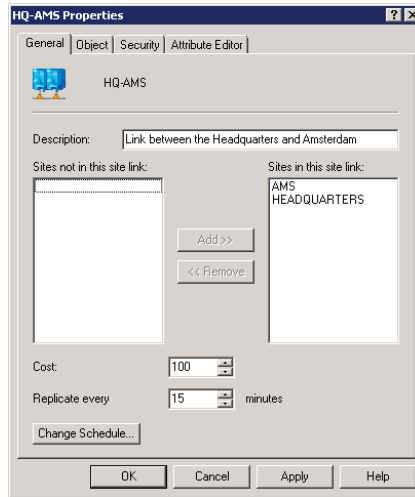
Key points in this section include:

- Site Link Costs
- Replication Frequency
- Replication Schedules

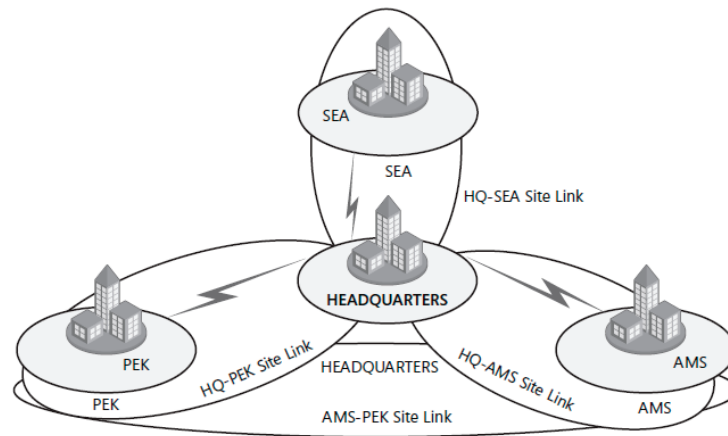
Site Link Costs

Site link costs are used to manage the flow of replication traffic when there is more than one route for replication traffic. You can configure site link cost to indicate that a link is faster, more reliable, or is preferred. Higher costs are used for slow links, and lower costs are used for fast links. Active Directory replicates using the connection with the lowest cost.

By default, all site links are configured with a cost of 100. To change the site link cost, open the properties of a site link and change the value in the Cost spin-box, shown in the following screen shot.



Returning to the example used earlier in the lesson, imagine if a site link was created between the Amsterdam and Beijing sites, as shown in the following figure.



Such a site link could be configured to allow replication between domain controllers in those two sites in the event that the links to the headquarters became unavailable. You might want to configure such a topology as part of a disaster recovery plan, for example.

With the default site link cost of 100 assigned to the AMS-PEK site link, Active Directory will replicate changes directly between Amsterdam and Beijing. If you configure the site link cost to 300, changes will replicate between Amsterdam and the Headquarters, then between the Headquarters and Beijing at a cost of 200 rather than directly over the AMS-PEK site link at a cost of 300.

Replication Frequency

Intersite replication is based only on polling; there is no notification. Every three hours, by default, a bridgehead server will poll its upstream replication partners to determine whether changes are available. This replication interval is too long for organizations that want changes to the directory to replicate more quickly. You can change the polling interval for each site link.

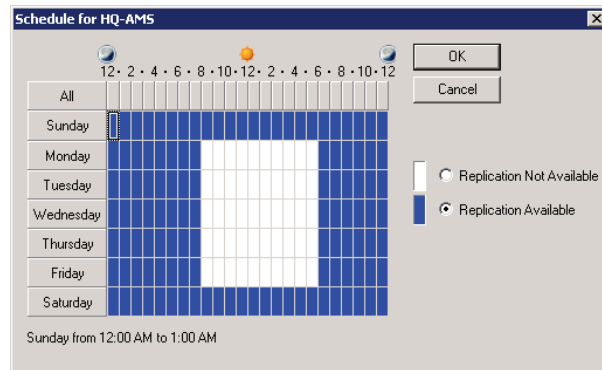
To change the polling interval for a site link:

- Open the site link's properties and change the value in the **Replicate Every** spin-box, shown in the previous screen shot.

The minimum polling interval is 15 minutes. That means, using Active Directory's default replication configuration, a change made to the directory in one site will take several minutes before the change is replicated to domain controllers in another site.

Replication Schedules

By default, replication occurs 24 hours a day. However, you can restrict intersite replication to specific times by changing the schedule attributes of a site link. Open the properties of a site link and click the Change Schedule button. Using the Schedule For dialog box shown in the following screen shot, you can select the times during which the link is available for replication. The link shown in the figure does not replicate from 8:00 A.M. to 6:00 P.M. Monday through Friday.



You must be careful when scheduling site link availability. It is possible to schedule windows of availability that do not overlap, at which point, replication will not happen. It's generally not recommended to configure link availability. If you do not require link scheduling, you should select the Ignore Schedules option in the properties of the IP transport protocol. This option causes any schedules for site link availability to be ignored, ensuring replication 24 hours a day over all site links.

Monitor and Manage Replication

- RepAdmin
 - **repadmin /showrepl** hqdc01.contso.com
 - **repadmin /showconn** hqdc01.contoso.com
 - **repadmin /showobjmeta** hqdc01 "cn=Linda Miller,ou=..."
 - **repadmin /kcc**
 - **repadmin /replicate** hqdc02 hqdc01 dc=contoso,dc=com
 - **repadmin /syncall** hqdc01.contoso.com /A /e
- DCDiag /test:testName
 - **FrsEvent** or **DFSREvent**
 - **Intersite**
 - **KccEvent**
 - **Replications**
 - **Topology**

Key Points

After you have implemented your replication configuration, you must be able to monitor replication for ongoing support, optimization, and troubleshooting. Two tools are particularly useful for reporting and analyzing replication: the Replication Diagnostics tool (Repadmin.exe) and Directory Server Diagnosis (Dcdiag.exe). This lesson introduces you to these powerful tools.

Repadmin.exe

The Replication Diagnostics tool, Repadmin.exe, is a command-line tool that enables you to report the status of replication on each domain controller. The information produced by Repadmin.exe can help you spot a potential problem before it gets out of control and troubleshoot problems with replication in the forest. You can view levels of detail down to the replication metadata for specific objects and attributes, enabling you to identify where and when a problematic change was made to Active Directory. You can even use Repadmin.exe to create the replication topology and force replication between domain controllers.

Like other command-line tools, you can type **repadmin /?** to see the usage information for the tool. Its basic syntax is as follows:

```
repadmin command arguments...
```

Repadmin.exe supports a number of commands that perform specific tasks. You can learn about each command by typing **repadmin /?:command**. Most commands require arguments. Many commands take a *DSA_LIST* parameter, which is simply a network label (DNS or NetBIOS name or IP address) of a domain controller. Some of the replication monitoring tasks you can perform with Repadmin are:

- **Display the replication partners for a domain controller.** To display the replication connections of a domain controller, type **repadmin /showrepl *DSA_LIST***. By default, Repadmin.exe shows only intersite connections. Add the **/repsto** argument to see intersite connections as well.
- **Display connection objects for a domain controller.** Type **repadmin /showconn *DSA_LIST*** to show the connection objects for a domain controller.
- **Display metadata about an object, its attributes, and replication.** You can learn a lot about replication by examining an object on two different domain controllers to find out which attributes have or have not replicated. Type **repadmin /showobjmeta *DSA_LIST Object***, where *DSA_LIST* indicates the domain controller(s) to query. (You can use an asterisk [*] to indicate all domain controllers.) *Object* is a unique identifier for the object, its DN or GUID, for example.

You can also make changes to your replication infrastructure by using Repadmin. Some of the management tasks you can perform are:

- **Launching the KCC.** Type **repadmin /kcc** to force the KCC to recalculate the inbound replication topology for the server.
- **Forcing replication between two partners.** You can use Repadmin to force replication of a partition between a source and a target domain controller. Type **repadmin /replicate *Destination_DSA_LIST Source_DSA_Name Naming_Context***.
- **Synchronizing a domain controller with all replication partners.** Type **repadmin /syncall *DSA /A /e*** to synchronize a domain controller with all its partners, including those in other sites.

Dcdiag.exe

The Directory Service Diagnosis tool, Dcdiag.exe, performs a number of tests and reports on the overall health of replication and security for Active Directory Domain Services. Run by itself, dcdiag.exe performs summary tests and reports the results. On the other extreme, **dcdiag.exe /c** performs almost every test. The output of tests can be redirected to files of various types, including XML. Type **dcdiag /?** for full usage information.

You can also specify one or more tests to perform using the **/test:Test Name** parameter. Tests that are directly related to replication include:

- **FrsEvent.** Reports any operation errors in the file replication system (FRS).
- **DFSREvent.** Reports any operation errors in the DFS replication (DFS-R) system.
- **Intersite.** Checks for failures that would prevent or delay intersite replication.
- **KccEvent.** Identifies errors in the knowledge consistency checker.
- **Replications.** Checks for timely replication between domain controllers.
- **Topology.** Checks that the replication topology is fully connected for all DSAs.
- **VerifyReplicas.** Verifies that all application directory partitions are fully instantiated on all domain controllers hosting replicas.

See the Help & Support Center for more information about Repadmin.exe and Dcdiag.exe.

Lab C: Configure Replication

- Exercise 1: Create a Connection Object
- Exercise 2: Create Site Links
- Exercise 3: Move Domain Controllers into Sites
- Exercise 4: Designate a Preferred Bridgehead Server
- Exercise 5: Configure Intersite Replication

Logon information

Virtual machine	6425B-HQDC01-B	6425-HQDC02-B	6425B-HQDC03-B	6425B-BRANCHDC01-B
Logon user name	Pat.Coleman	Do not log on	Do not log on	Do not log on
Administrative user name	Pat.Coleman_Admin			
Password	Pa\$\$w0rd			

Estimated time: 30 minutes

Scenario

You are the administrator of Contoso, Ltd. You want to optimize replication of AD DS by aligning replication with your network topology and domain controller roles and placement.

Exercise 1: Create a Connection Object

It is a best practice to configure direct replication between a domain controller that will be a standby operations master and the domain controller that is currently the operations master. Then, if the current operations master needs to be taken offline, the standby operations master is as up to date as possible with the operations master. In this exercise, you will create a connection object between HQDC01 and HQDC02, where HQDC02, the standby operations master, replicates from HQDC01, the current operations master.

The main tasks for this exercise are as follows:

1. Prepare for the lab.
2. Create a connection object.

► Task 1: Start and log on to the virtual machines

The virtual Machines should already be started and available after completing Labs A and B. However, if they are not, you should complete the below steps then step through Exercises 1 to 3 in Labs A and B before continuing.

- Start 6425B-HQDC01-B, and log on as **Pat.Coleman** with the password **Pa\$\$w0rd**. This virtual machine may take several minutes to start.
- After logging on to HQDC01, start 6425B-HQDC02-B but do not log on.
- After HQDC02 has completed startup, start 6425B-HQDC03-B but do not log on.
- After HQDC03 has completed startup, start BRANCHDC01-B but do not log on.
- Wait for BRANCHDC01 to finish startup before continuing to the next task.

► **Task 2: Create a connection object**

- Run **Active Directory Sites and Services** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
- In the console tree, expand **HEADQUARTERS, Servers**, and **HQDC02**, and then click the **NTDS Settings** node below **HQDC02**.
- Right-click **NTDS Settings** and click **New Active Directory Domain Services Connection**.
- In the **Find Active Directory Domain Controllers** dialog box, select **HQDC01**, and then click **OK**, and answer **Yes** to the warning message.
- In the **New Object – Connection** dialog box, type the name **HQDC01 - OPERATIONS MASTER**, and click **OK**.

Results: After this exercise, you should have created a connection object to replicate changes from HQDC01 to HQDC02.

Exercise 2: Create Site Links

In this exercise, you will create site links between the headquarters and the other sites, creating a hub-and-spoke replication topology.

The main tasks for this exercise are as follows:

- Create site links.

► Task 1: Create site links

- Rename the **DEFAULTIPSITELINK** to **HQ-HQB2**, and modify it so that it includes only the **HEADQUARTERS** and **HQ-BUILDING-2** sites.
- Create a new IP site link named **HQ-BRANCHA** that includes the **HEADQUARTERS** and **BRANCHA** sites.

Results: After this exercise, you should have two site links, one that links the **HEADQUARTERS** and **HQ-BUILDING-2** sites, and one that links **HEADQUARTERS** and **BRANCHA**.

Exercise 3: Move Domain Controllers into Sites

When you promote a domain controller, you can select the site for the DC and, by default, it will be in the site associated with the DC's IP address. If you modify sites and subnets after domain controllers are already in place, you must move the existing domain controllers into the correct sites. In this exercise, you will move domain controllers into the sites you have created in this module's Labs.

The main tasks for this exercise are as follows:

- Move domain controllers to new sites.

► Task 1: Move domain controllers to new sites

- Move BRANCHDC01 into the **BRANCHA** site.

Results: After this exercise, you should have moved BRANCHDC01 to the BRANCHA site.

Exercise 4: Designate a Preferred Bridgehead Server

You can designate a preferred bridgehead server that will handle replication to and from its site. This is useful when you want to assign the role to a domain controller in a site with greater system resources or when firewall considerations require that the role be assigned to a single, fixed system. In this exercise, you will designate a preferred bridgehead server for the site.

The main tasks for this exercise are as follows:

- Designate a preferred bridgehead server.
-
- ▶ **Task 1: Designate a preferred bridgehead server**
 - Configure HQDC02 as a preferred bridgehead server. When you do so, a lengthy warning message appears. Read the message. You will discuss it at the end of the Lab. Then click **OK**.

Results: After this exercise, you should have designated HQDC02 as a preferred bridgehead server.

Exercise 5: Configure Intersite Replication

After you have created site links and, optionally, designated bridgehead servers, you can continue to refine and control replication by configuring properties of the site link. In this exercise, you will reduce the intersite replication polling frequency, and you will increase the cost of a site link.

The main tasks for this exercise are as follows:

- Configure Intersite Replication.

► Task 1: Configure Intersite Replication

- Configure the replication interval for the **HQ-HQB2** site link to **15** minutes.
- Configure the replication interval for the **HQ-BRANCHA** site link to **15** minutes, and the cost to **200**.
- Examine the replication schedule for the **HQ-BRANCHA** site link. Experiment with configuring the schedule but click **Cancel** when you are finished.

Results: After this exercise, you should have configured the intersite replication interval to 15 minutes for all site links.



Note: After completing this exercise, turn off all virtual machines and discard undo disks.

Lab Review Questions

Question: Explain the warning message that appeared when you designated HQDC02 as a preferred bridgehead server.

Question: What are the advantages of reducing the intersite replication interval? What are the disadvantages?

Question: Is the procedure you performed in Exercise 2 enough to create a "hub and spoke" replication topology, which ensures that all changes from branches are replicated to the headquarters before being replicated to other branches? If not, what must still be done?

MCT USE ONLY. STUDENT USE PROHIBITED

Module 13

Directory Service Continuity

Contents:

Lesson 1: Monitor Active Directory	13-4
Lab A: Monitor Active Directory Events and Performance	13-29
Lesson 2: Manage the Active Directory Database	13-45
Lab B: Manage the Active Directory Database	13-64
Lesson 3: Back Up and Restore AD DS and Domain Controllers	13-72
Lab C: Back Up and Restore Active Directory	13-86

Module Overview

- Monitor Active Directory
- Manage the Active Directory Database
- Back Up and Restore AD DS and Domain Controllers

As an IT professional supporting Windows Server 2008 and AD DS, the health of your career is tied closely to the health of your domain. If the domain goes down, so does your job. In this module, you will learn about the technologies and tools that are available to help ensure the health and longevity of the directory service. You will explore tools that help you monitor performance in real time, and you will learn to log performance over time so that you can keep an eye on performance trends in order to spot potential problems. You'll also learn how to optimize and protect your directory service so that if a domain controller does fail, you can get it up and running as quickly as possible.

Objectives

After completing this module, you will be able to:

- Monitor real-time performance and events with Task Manager, Event Viewer, and Windows Reliability and Performance Monitor.
- Leverage new features of Event Viewer in Windows Server 2008, including custom views and event subscriptions.

- Monitor real-time and logged performance with Performance Monitor, data collection sets, and reports.
- Identify sources of performance and event information for AD DS domain controllers.
- Create alerts based on events and performance metrics.
- Maintain and optimize the Active Directory database.
- Back up and restore AD DS and domain controllers.
- Recover deleted objects and attributes.

Lesson 1

Monitor Active Directory

- Understand Performance and Bottlenecks
- Task Manager
- Resource Manager
- Event Viewer
- Demonstration: Event Viewer
- Custom Views
- Subscriptions
- Demonstration: Configure Custom Views and Subscriptions
- Windows Reliability and Performance Monitor (WRPM)
- Demonstration: Windows Reliability and Performance Monitor (WRPM)
- Reliability Monitor
- Performance Monitor
- Data Collector Sets
- Demonstration: Monitor AD DS
- Monitoring Best Practices

Performance problems happen: that's the reality. What matters most is how you respond to, evaluate, and remediate those problems. In this lesson, you will learn how to use performance and event monitoring tools in Windows Server 2008 to reactively and proactively keep tabs on the health of your domain controllers and of AD DS.

Objectives

After completing this lesson, you will be able to:

- Monitor real-time performance with Task Manager, Resource Monitor, and Performance Monitor.
- Examine events and changes with Reliability Monitor and Event Viewer.
- Leverage new features of Event Viewer in Windows Server 2008, including custom views and event subscriptions.

- Monitor real-time and logged performance with Performance Monitor, data collection sets, and reports.
- Identify sources of performance and event information for AD DS domain controllers.
- Create alerts based on events and performance metrics.

Understand Performance and Bottlenecks

- Key system resources
 - CPU
 - Disk
 - Memory
 - Network
- Bottleneck: Resource that is *currently* at peak utilization
- Tools
 - Task Manager
 - Event Viewer
 - Resource Monitor
 - Reliability Monitor
 - Performance Monitor
 - System Center Operations Manager

Key Points

Poor system performance can usually be attributed to insufficient system resources. The four key system resources are the processor (CPU), disk subsystem, memory, and network.

Identifying and remediating bottlenecks involves close examination of system logs and performance counters to determine which resource is currently constrained. Once that resource has been augmented, it is likely that performance will improve, but performance will reach a plateau when it hits a new bottleneck due to limitations in another system resource.

In this lesson, you will examine a variety of tools that can be used to monitor real-time performance as well as examine system changes and events that may have, over time, led to performance degradation.

Task Manager

- Starting taskmgr.exe
 - CTRL+SHIFT+ESC
 - CTRL+ALT+DEL
 - Right-click taskbar
 - Start taskmgr.exe
- Real-time performance
 - Applications
 - Processes
 - Services
 - Performance
 - High-level CPU, network, memory
 - No disk counters
 - Logged-on users
- Entry point to Resource Monitor

Key Points

Windows Task Manager should be a familiar tool to any IT professional. Windows Server 2008 has significantly augmented the capabilities of Task Manager. In addition to the familiar Applications and Processes tabs, Windows Server 2008 provides details about services, and a high-level view of performance of three system resources: CPU, network, and memory. Task Manager does not expose real-time performance counters for disk performance. Finally, Task Manager is where you can see a list of currently logged-on users without having to open the terminal services management snap-in.

To open Tasks Manager, do one of the following:

- Press CTRL+SHIFT+ESC.
- Press CTRL+ALT+DEL, and then click **Task Manager**.
- Right-click the taskbar, and then click **Task Manager**.
- Click the **Start** button, and then in the **Start Search** box, type **taskmgr.exe**.

On the Processes tab, you can click Show Processes From All Users for detailed information about processes running under the system context, or running under other user contexts.

On the Performance tab, click Resource Monitor to open the new and very useful view of real-time performance.

Resource Monitor

- Full view of key system components
 - Click each graph to expand/collapse the component
- Launching Resource Monitor
 - Task Manager → Performance → Resource Monitor
 - Start perfmon /res
 - Home view of Windows Reliability and Performance Monitor (WRPM) snap-in

Key Points

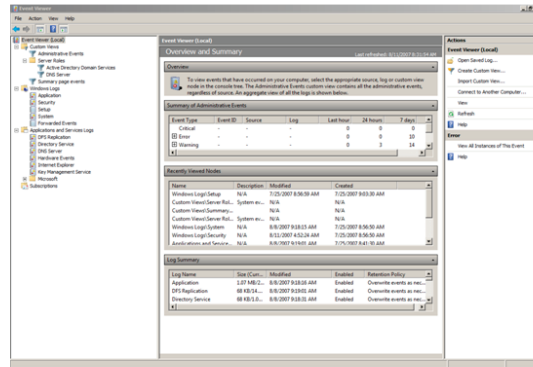
Resource Monitor is like Task Manager, but greatly enhanced. It provides a detailed view of the performance of each of the key system components (CPU, disk, network, and memory) in both a graphical and a detailed report form. If you need to troubleshoot real-time performance, or to identify why a system is running slowly, Resource Monitor is the first tool you should turn to.

To launch Resource Monitor, do one of the following:

- Open **Task Manager**, click the **Performance** tab, and then click **Resource Monitor**.
- Click the **Start** button, and then in the **Start Search** box, type **perfmon /res**, and then press ENTER.
- Click the root of the Windows Reliability and Performance Monitor snap-in.

Event Viewer

- What you see
 - Many more logs
 - Summary and custom views based on cross-log queries
 - Role-based views in Server Managers
 - More detailed events
- What you can do
 - Integrate with Task Scheduler: E-mails or actions based on event
 - Subscribe to events from other computers



Key Points

While developing Windows Server 2008, Microsoft® rewrote Event Viewer from the ground up. Behind the scenes, events are stored in a new event log file format (.elf). Events are exposed both in classic Windows logs such as Application, Security, and System, as well as in dozens of new logs dedicated to monitoring events from specific system components.

To help you make sense of all of these new events and logs, Event Viewer provides summary views that roll up events across multiple logs. It also allows you to create custom views to aggregate events for multiple logs. When you open Service Manager, you will also see role-specific events exposed in the home view for each role.

And the events themselves have improved. You will find that events provide far more detail than in the past, meaning that there will be fewer times in which an event leaves you guessing as to what it really means.

Perhaps most excitingly, the event subsystem has been integrated with other Windows components. Now, thanks to integration with Task Scheduler, you can trigger an action based on a specific event. The action may include sending an e-mail message. That's right: Windows can now send you an e-mail alert (and thereby potentially a text message or page) when something goes wrong. You might also trigger a specific script or executable in response to an event—for example, a script that restarts a service when that service stops.

Another major component that has been integrated with the event subsystem is Windows Remote Management (WinRM), a set of Web services used to manage Windows systems. This integration allows you to aggregate events for multiple computers to a single location, by subscribing to events on remote systems. When a remote system logs an event that matches your specified criteria, that event is forwarded to an event log on the collector machine.

Additional Reading

- Event Viewer
<http://go.microsoft.com/fwlink/?LinkId=168451>

Demonstration: Event Viewer

In this demonstration, we will

- Explore Event Viewer
- Identify the Active Directory logs
 - Directory Service
 - Domain Name System (DNS)
 - Distributed File System Replication (DFSR)
 - Group Policy Operational log
- Discover the new features in the Windows Server 2008 Event Viewer

Key Points

In this demonstration, your instructor will show you some of the features of Event Viewer that were described in the previous slide. This will be an opportunity to provide some extra tips, and to ensure that you are familiarized with Event Viewer.

You will have the opportunity to perform similar tasks hands on in the Lab for this module.

Your instructor will also point out four logs that are particularly important for monitoring domain controllers:

- Directory Service
- DNS
- DFSR
- Group Policy Operational log

Demonstration Steps

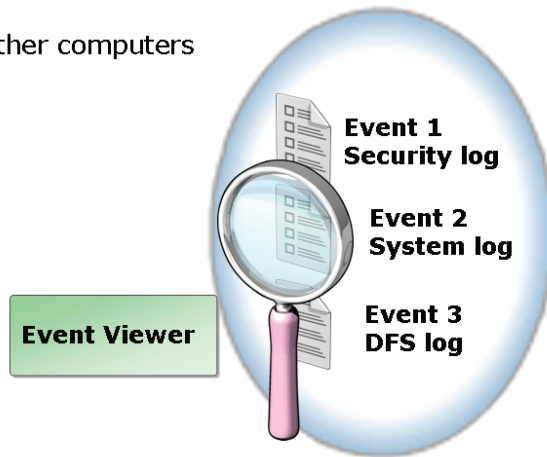
1. Open **Event Viewer** and observe the new look of the **Microsoft® Management Console (MMC)**.
2. Notice the default summary view, then expand custom views and display the default custom views.
3. Expand **Windows Logs**, and then display the traditional logs and the new logs.
4. Open any of the logs, and observe the options available in the Actions pane.
Please note that it is possible to attach a task to an event using the Create a Basic Task Wizard.
It is also possible to copy an event's details as text into Notepad.
5. Double-click any event to show the details.
6. Expand the **Microsoft Windows** folder to display the logs.
7. It is also possible to connect to another computer.



Reminder: Remote event-log management must be enabled on the remote computer's firewall. Working with the firewall is part of the upcoming lab for this lesson.

Custom Views

- Aggregate events from multiple logs
- Filter
- Reuse
- Export for import to other computers



Key Points

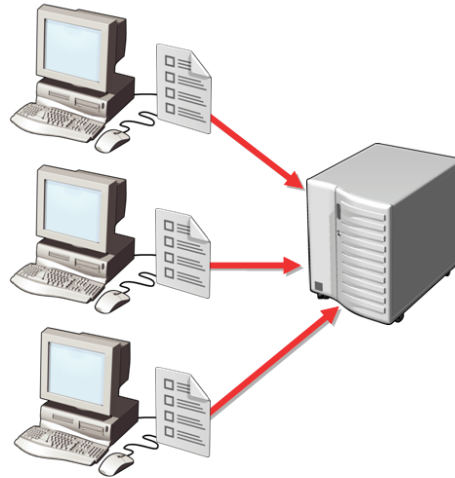
Custom views are filters that are named and saved. After creating and saving a custom view, you are able to reuse it without recreating its underlying filter. To reuse a custom view, navigate to the Custom Views category in the console tree, and select the custom view's name. By selecting the custom view, you apply the underlying filter, and the results are displayed. You can import and export custom views, enabling you to share them between users and computers.

Additional Reading

- Create and Manage Custom Views
<http://go.microsoft.com/fwlink/?LinkId=168452>

Subscriptions

- Collect events from one or more computers
- Store the events locally
- Use Windows Remote Management (WinRM)
- Require WinRM exceptions in firewall



Key Points

Using the Event Viewer snap-in, you can connect to a single remote computer to examine its event logs. However, troubleshooting an issue effectively may require that you examine events stored on multiple computers.

In Windows Server 2008, Event Viewer allows you to subscribe to specific events on one or more remote computers, to collect those events, and to store them locally. After you create an event subscription, events are forwarded from source computers to the collector computer, at which point the events can be viewed and manipulated just as if they were local events.

Additional Reading

- Event Subscriptions
<http://go.microsoft.com/fwlink/?LinkId=168453>

Demonstration: Configure Custom Views and Subscriptions

In this demonstration, we will:

- Create a custom view, and then add the AD DS-specific logs to the view
- Create a subscription to collect logs from multiple domain controllers

Key Points

In this demonstration, your instructor will show you some of the features of Custom Views and Event Subscriptions that were described in the previous slide. This will be an opportunity to receive some extra tips, and to ensure that you are familiar with these features.

You will have the opportunity to perform similar tasks yourself in the lab for this module.

Demonstration Steps

Create a Custom View

1. We will create a new custom view that captures error events from some Active Directory-related logs;
2. Export the view to an XML file; and
3. Delete the original custom view, and then import the XML file.

Create a Subscription

1. For this, we need to ensure that we are logged on to all collector and source computers as administrator.
2. On each source computer, at an elevated command prompt, type **winrm quickconfig**.
3. On the collector computer, at an elevated command prompt, type **Wecutil qc**.
4. Add the computer account of the collector computer to the local **Administrators** group on each of the source computers.
5. Create the subscription.
6. Filter events to show only errors from the system log.

Additional Reading

- Create a Custom View
<http://go.microsoft.com/fwlink/?LinkId=99511>
- Configure Computers to Forward and Collect Events
<http://go.microsoft.com/fwlink/?LinkId=99513>

Windows Reliability and Performance Monitor (WRPM)

- Track system changes (Reliability Monitor)
- Display real-time or logged performance data (Performance Monitor)
 - Generate reports or graphical views of performance
 - Generate alerts
 - Take action when thresholds are reached
- Collect data (Data Collector Sets and Reports)
 - Generate reports
 - Generate graphical views of logged performance

Key Points

Windows Reliability and Performance Monitor (WRPM) is a suite of new and improved snap-ins that greatly enhance your ability to both reactively and proactively monitor the health and performance of your Windows servers.

Reliability Monitor tracks system changes, including software install and uninstall. Performance Monitor generates graphical or reports-based views of performance using either real-time or logged performance data. And Data Collector Sets and Reports enable you to manage the collection and review of performance data.

You will learn about each of these tools in this module, and then you'll have the chance to work with them yourself in the lab for this module.

Additional Reading

- Windows Reliability and Performance Monitor
<http://go.microsoft.com/fwlink/?LinkId=168454>

Demonstration: Windows Resource and Performance Monitor (WRPM)

In this demonstration we will:

- Explore Windows Reliability and Performance Monitor (WRPM)

Key Points

In this demonstration, your instructor will give you a quick tour of WRPM, so that you are exposed to the various snap-ins and nodes in this powerful suite of administrative tools.

Demonstration Steps

1. Open **Reliability and Performance Monitor**.
2. Observe the resource overview screen. Expand some sections to show details.
3. Open **Performance Monitor**. This feature has not changed significantly from Windows Server 2003.
4. Open **Reliability Monitor**. Browse through and observe some details.
5. Open **Reports**, and note the system reports that are available.

Reliability Monitor

- Tracks system changes
 - Software install/uninstall
 - Application failures
 - Windows failures
 - Hardware failures

Key Points

Reliability Monitor provides a view of system stability and the events and changes that impact the overall integrity of a system. It tracks software installation and uninstallation, Windows failures, application failures, and hardware failures.

Reliability Monitor calculates a System Stability Index that reflects in graph form whether unexpected problems reduced the system's reliability. The accompanying System Stability Report provides details to help identify the specific changes that reduced reliability.

Additional Reading

- Using Reliability Monitor
<http://go.microsoft.com/fwlink/?LinkId=168455>

Performance Monitor

- Useful counters in any server baseline
 - Memory \ Pages/sec
 - PhysicalDisk \ Avg. Disk Queue Length
 - Processor \ %Processor Time
- Useful counters for monitoring Active Directory
 - NTDS\ DRA Inbound Bytes Total/sec
 - NTDS\ DRA Inbound Object
 - NTDS\ DRA Outbound Bytes Total/sec
 - NTDS\ DRA Pending Replication Synchronizations
 - NTDS \ Kerberos Authentications/sec
 - NTDS\ NTLM Authentications

Key Points

Performance Monitor enables you to view report-based or graphical displays of system performance. Whereas Resource Monitor displays performance related to system components (CPU, disk, memory, and network), Performance Monitor allows you to examine performance at a deeper level. Even with system components, Performance Monitor reveals more detail: disk utilization per physical volume or partition, CPU utilization per core, and specific types of packets being sent or received, for example.

Performance Monitor also exposes performance counters for numerous more granular components, roles, services, and features. Windows components can register performance counters with Performance Monitor during installation. For example, when you add the AD DS role to a server, the NT Directory Service (NTDS) performance object is registered, which itself exposes dozens of counters related to directory service performance.

With Performance Monitor, you can interactively create a collection of counters to monitor in real time. Alternately, you can save counters as part of a Data Collector Set that can be reused at any time to view real-time performance, or that can be launched at a later date to log performance.

The most useful counters to monitor for any server are the following, which can reveal performance bottlenecks in key system components:

- Memory \ Pages/sec
- PhysicalDisk \ Avg. Disk Queue Length
- Processor \ %Processor Time

On a domain controller, you should also monitor at least the following performance counters exposed by the NT Directory Service (NTDS) object:

- NTDS\ DRA Inbound Bytes Total/sec
- NTDS\ DRA Inbound Object
- NTDS\ DRA Outbound Bytes Total/sec
- NTDS\ DRA Pending Replication Synchronizations
- NTDS \ Kerberos Authentications/sec
- NTDS\ NTLM Authentications

Windows Server 2008 allows performance to be viewed and logged by users without requiring those users to be members of the local Administrators group. If you want to enable a non-administrative user to use Performance Monitor, add the user to the Performance Log Users group. The Performance Log Users group must also have the Logon as a batch file user right, which is assigned to the group by default.

Additional Reading

- Using Performance Monitor
<http://go.microsoft.com/fwlink/?LinkId=168456>

Data Collector Sets

- Collections of data points
 - Performance counters
 - Event trace data
 - System configuration information (registry keys)
- Use to
 - View real-time performance with Performance Monitor
 - Create a log (manually invoked or scheduled) and then view Reports
 - Generate alerts based on thresholds
 - Use by other applications
- Create
 - Start from a template; role templates added by Windows
 - Save an existing set of counters in a Performance Monitor view
 - Manually specify and configure data collectors in a set
 - Export/import data collector set as XML

Key Points

Although it is possible to interactively add counters to a Performance Monitor view, doing so repeatedly will become tedious and, in the long term across multiple systems, unmanageable. In addition, there are information sources other than performance counters, such as registry settings and event traces, that can provide insight into the performance and health of a system.

A Data Collector Set is the building block of monitoring and reporting in WRPM. A Data Collector Set organizes performance counters and registry settings, and presents this data from a single component that can then be used to view real-time performance or to log performance on a manually triggered or scheduled basis. A Data Collector Set and the information that it has logged can then be viewed as a report or can be loaded into Performance Monitor or one of several Microsoft or non-Microsoft applications. Data Collector Sets can also be configured to generate alerts when thresholds are reached, or to trigger Windows Management Instrumentation (WMI) actions.

Additional Reading

- Creating Data Collector Sets
<http://go.microsoft.com/fwlink/?LinkId=168457>

Demonstration: Monitor AD DS

In this demonstration, we will:

- Configure AD DS monitoring by using Data Collector Sets

Key Points

In this demonstration, your instructor will configure an AD DS Data Collector Set, demonstrating some of the concepts and tools introduced in the previous slide.

You will have the opportunity to review and practice similar procedures in the lab for this lesson.

Demonstration Steps

Create a new Data Collector Set named Custom Active Directory.

1. Add the server baseline counters.
2. Add some of the Active Directory counters, and then start the **Data Collector Set**.
3. Perform some activity to generate statistics. For example, create, modify and/or delete several user or group accounts.

4. Stop the **Data Collector Set**, and then look at the user-defined report.
5. In the system container, start the **Active Directory Diagnostics Data Collector Set**.
6. Perform some activity to generate statistics. For example, create, modify and/or delete several user or group accounts.
7. Stop **the Data Collector Set**, and then look at the system-defined report.

Monitoring Best Practices

1. Monitor *early* to establish baselines!
 - Document performance when things are working well
 - Include server and role-related counters during idle and busy times
2. Monitor *often* to identify potential problems
 - Compare to baseline and watch for troublesome deviation
3. Know how to monitor and interpret performance *before* a meltdown
 - Establish Data Collector Sets
 - Build the skills to interpret performance counters
4. Capture *appropriately*
 - Don't overcapture
 - Degrades performance
 - Creates "noise," making it difficult to identify real problems

Key Points

To establish an effective monitoring framework, follow these guidelines:

Monitor Early to Establish Baselines

It's critical that you monitor performance while a system is performing normally. This allows you to establish a baseline, so that you have documented the expected ranges of performance counters. To create a baseline, monitor performance counters during both busy and idle times.

Monitor Often to Identify Potential Problems

Establish a regular monitoring routine, perhaps using scheduled Data Collector Sets, and compare the logs and reports to your baselines. Look for unusual deviations from expected values in order to identify potential problems before those problems are manifested in your directory service.

Know How to Monitor and Interpret Performance before a Meltdown

When a real problem arises, you do not want to have to take time to learn how to capture and interpret performance counters and events. So take the time to learn how to use the tools, and determine which counters provide the most meaningful insight into the performance of your enterprise. Establish Data Collector Sets that will make it easy for you to capture performance during a crisis, and be sure to export those Data Collector Sets to back them up, in case the system that is down is the system you normally use for monitoring.

Capture Appropriately

Don't go overboard with monitoring. If you try to monitor every counter, every event trace, and every registry entry, you will create such a mass of performance information that it will be difficult to identify real problems. Additionally, monitoring performance degrades performance, slightly, on the system. Align your monitoring activities with your business requirements for monitoring.

Lab A: Monitor Active Directory Events and Performance

- Exercise 1: Monitor Real-Time Performance Using Task Manager and Resource Monitor
- Exercise 2: Use Reliability Monitor and Event Viewer to Identify Performance-Related Events
- Exercise 3: Monitor Events on Remote Computers with Event Subscriptions
- Exercise 4: Attach Tasks to Event Logs and Events
- Exercise 5: Monitor AD DS with Performance Monitor
- Exercise 6: Work with Data Collector Sets

Logon information

Virtual machine	6425B-HQDC01-B	6425B-HQDC02-B
Logon user name	Pat.Coleman	Pat.Coleman
Administrative user name	Pat.Coleman_Admin	Pat.Coleman_Admin
Password	Pa\$\$w0rd	Pa\$\$w0rd

Estimated time: 60 minutes

Scenario

Last month, the only domain controller in the branch office failed, causing Contoso's call center to be offline for an entire day and costing the company a significant amount of money in lost revenue. You were hired to replace the administrator who had configured a critical location without redundant authentication or monitoring. This week, you are working to configure monitoring to ensure that performance and reliability can be watched on an ongoing basis for any signs of trouble.

Exercise 1: Monitor Real-Time Performance Using Task Manager and Resource Monitor

In this exercise, you will use Task Manager and Resource Monitor to examine real-time performance at a high level, which can help you to identify performance bottlenecks and processes or services that are consuming too many system resources.

The main tasks for this exercise are as follows:

1. Prepare for the lab.
2. Monitor real-time performance with Task Manager.
3. Monitor real-time performance with Resource Monitor.

► Task 1: Prepare for the lab

- Start 6425B-HQDC01-B and log on as **Pat.Coleman** with the password **Pa\$\$w0rd**.
- Run **D:\Labfiles\Lab13a\Lab13a_Setup.bat** with administrative credentials. Use the account **Administrator** with the password **Pa\$\$w0rd**.
- The lab setup script runs. When it is complete, press any key to continue.
- Close the Windows Explorer window, **Lab13a**.
- Start 6425B-HQDC02-B.
- Log on to HQDC02 as **Pat.Coleman** with the password **Pa\$\$w0rd**.

► Task 2: Monitor real-time performance with Task Manager

1. On HQDC01, press CTRL+SHIFT+ESC to launch Task Manager.
2. Click the **Processes** tab and examine the commands available when you right-click **taskmgr.exe**. Examine the properties of a process by opening the **Properties** dialog box for **taskmgr.exe**.
3. Show processes from all users, which requires administrative credentials. Authenticate as **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
4. On the **Services** tab, stop and then start the **Dnscache** service.
5. Right-click the **Dnscache** service, and then click **Go to Process**.

Question: What process is hosting the DNS Client service?

6. Right-click the process and choose **Go to Service(s)**.

Question: The Services tab exposes a subset of the most-used functionality of which administrative snap-in?

7. Click the **Services** button. The **Services** console appears. Close the **Services** console.
8. Click the **Users** tab. This tab displays users who have either local (console) or remote desktop connections to the server.
9. Click the **Networking** tab.

This tab provides an overview of performance for each available network adapter.

10. Click the **Performance** tab.

This tab provides an overview of performance for CPU utilization and memory.

Question: Which major system component is *not* shown by task manager?

► **Task 3: Monitor real-time performance with Resource Monitor**

1. In Task Manager, on the **Performance** tab, click the **Resource Monitor** button.
If you are prompted for administrative credentials, use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
2. Resource Monitor appears. Maximize the **Resource Monitor** window and close Task Manager.
3. Click the **CPU** graph. How much CPU utilization is being generated by Reliability and Performance Monitor itself?
4. Click the **CPU** graph again. The **CPU** section collapses.

5. Click the **Disk** graph. Which file is experiencing the most Read activity? Which process is causing the Read activity for that file? Which file is experiencing the most Write activity? Which process is causing the Write activity for that file?

To view the activity of the page file, click the File column label. If C:\pagefile.sys is not listed, open an application such as Server Manager, which should generate some paging activity.

Question: How many processes are reading from or writing to pagefile.sys?

Question: If the pagefile Read and Write activity is consistently high, what system component should be augmented?

6. Close Resource Manager. Click the **Start** button and run **perfmon** as an administrator with the user name **Pat.Coleman_Admin** and the password **Pa\$\$w0rd**.

Users, members of the Performance Monitor Users group, members of the Performance Log Users group, and members of the local Administrators group, are able to access increasing levels of functionality from WRPM.

The home view for the console is the Resource Overview, equivalent to Resource Monitor. Note that the console tree contains each of the WRPM snap-ins. Close Reliability and Performance Monitor.

7. Click the **Start** button and run **perfmon /res** as an **Administrator**, with the user name **Pat.Coleman_Admin** and the password **Pa\$\$w0rd**. This is an alternate way to open Resource Monitor, which you have opened from Task Manager, and which is the home view of the Reliability and Performance Monitor console. Close Resource Monitor.

Results: After this exercise, you will have used both Task Manager and Resource Monitor to monitor real-time performance of processes, services, and system components including disk, memory, network and CPU.

Exercise 2: Use Reliability Monitor and Event Viewer to Identify Performance-Related Events

In this exercise, you will use Reliability Monitor to examine stability-related events. You will then use Event Viewer to identify events related to performance and reliability, and you will learn how to work with custom views.

The main tasks for this exercise are as follows:

1. Monitor stability-related events with Reliability Monitor.
2. Identify role-related events with Server Manager.
3. Examine the event logs.
4. Create a custom view.
5. Export a custom view.
6. Import a custom view.

► Task 1: Monitor stability-related events with Reliability Monitor

1. Run **Server Manager** as an administrator, with the user name **Pat.Coleman_Admin** and the password **Pa\$\$w0rd**.
2. Use Reliability Monitor to examine stability-related events that occurred on Sept 9, 2009.

► Task 2: Identify role-related events with Server Manager

1. In the root node of **Server Manager**, in the **Roles Summary** section, notice what icons appear next to the **ADDS** and **DNS Server** roles.
2. Click the link to the **ADDS** role in the **Roles Summary** section and examine the information in the **Events** section.
3. Click the **Filter Events** link in the **Events** section and remove **Information** events from the view.
4. Double-click an event to open its details, examine the event, and then close the event.
5. Note the information shown in the **System Services** section.

► **Task 3: Examine the event logs**

1. In the root of the Server Manager Event Viewer snap-in, in the **Summary of Administrative Events** section, expand the **Error** events summary. Double-click a summary row with **ActiveDirectory** as the source.
2. If you do not see a row in the summary with **ActiveDirectory** as the source, double-click another row in the **Error** events summary.

The Summary page events view opens in the details pane. This view "drills down" to show the events that were summarized on the row of the Error events summary.

Examine the logs in the Windows Logs and Applications and Services Logs nodes of the console tree.

Examine the events in the Administrative Events view. Right-click Administrative Events, and then click Properties. Note that the Description indicates that the view shows Critical, Error, and Warning events from all administrative logs. Click the Edit Filter button and note that this custom view cannot be modified—it is Read Only. Note also that it is difficult to know exactly which logs are being included in the Event Logs list. The information is truncated. Click the XML tab. Can you identify which logs are included using the information on the XML tab? In each XML Select element, what do you think Level refers to? Click Cancel twice to close the open dialog boxes.

► **Task 4: Create a custom view**

- In the **Custom Views** folder, create a custom view that displays **Critical**, **Warning**, and **Error** messages for the following logs: **DFS Replication**, **Directory Service**, and **DNS Server**. Name the log **Custom Directory Service Event View**.

► **Task 5: Export a custom view**

- Export the **Custom Directory Service Event View** as **D:\Data\DSEventView.xml**.

► **Task 6: Import a custom view**

1. On HQDC02, import the custom view \\HQDC01\Data\DSEventView.xml and name it **Custom Directory Service Event View**.
2. A **Query Error** message appears, because HQDC02 is not a DNS server and therefore has no **DNS Server** log. Click **OK**.

Results: After this exercise, you will have identified several places in Server Manager that expose events related to server roles and performance. You will also have created a custom view and imported that view to Event Viewer on another computer.

Exercise 3: Monitor Events on Remote Computers with Event Subscriptions

In this exercise, you will use the new event forwarding and subscription functionality of Windows Server 2008 to collect events from remote systems for centralized monitoring.

The main tasks for this exercise are as follows:

1. Configure computers to forward and collect events.
2. Create a subscription to collect events.
3. Generate events.
4. View forwarded events.

► Task 1: Configure computers to forward and collect events

1. On HQDC01, run the command prompt as an administrator, with the user name **Pat.Coleman_Admin** and the password **Pa\$\$w0rd**. Type **wecutil qc**, then press ENTER, then press **Y**, then press ENTER to configure event collection.
2. On HQDC02, run the command prompt as an administrator, with the user name **Pat.Coleman_Admin** and the password **Pa\$\$w0rd**. Type **winrm quickconfig**, then press ENTER, then press **Y**, then press ENTER to configure Windows Remote Management.

► Task 2: Create a subscription to collect events

1. On HQDC01, in the Server Manager Event Viewer snap-in, create a new subscription named **DC Services** that collects events from HQDC02. Configure the subscription to collect System log events with Event ID 7036. The subscription should use the user name **CONTOSO\Pat.Coleman_Admin**, and the password **Pa\$\$w0rd**. It should be configured to **Minimize Latency**. If Event Viewer messages appear when you complete the configuration, click **Yes**.
2. Confirm that in the **Subscriptions** folder, the new **DC Services** subscription shows a status of **Active**.

► **Task 3: Generate events**

- On HQDC02, at the command prompt, type **net stop dfsr** and press ENTER, then type **net start dfsr** and press ENTER.

► **Task 4: View forwarded events**

1. Switch to HQDC01.
2. In the Server Manager console tree, under **Event Viewer\Windows Logs**, click **Forwarded Events**.

Forwarded events may take several minutes to appear. If the events do not appear right away, wait a few minutes, start and stop the Distributed File System Replication (DFSR) service on HQDC02 again, then wait a few more minutes.

Results: After this exercise, you will have configured event subscriptions so that you can view events from HQDC02 on HQDC01.

Exercise 4: Attach Tasks to Event Logs and Events

In this exercise, you will invoke tasks when an event log is updated or when an event is generated.

The main tasks for this exercise are as follows:

1. Attach a task to an event log and to an event.
2. Prepare to view event viewer task messages.
3. Confirm that event viewer tasks are functioning.

► Task 1: Attach a task to an event log and to an event

1. On HQDC01, right-click the **Forwarded Events** event log and attach a task to the log. The task should display a message with the title, **Forwarded Event Received** and with the message, **A forwarded event was received**.
2. In the **Forwarded Events** event log, right-click one of the 7036 events and attach a task to the event. The task should display a message with the title, **DC Service Event** and with the message, **A service was started or stopped**.

► Task 2: Prepare to view event viewer task messages

When you choose to display a message in a task, because messages are displayed on the desktop of the user whose account is used to create the event viewer task (Pat.Coleman_Admin), you will need to log on interactively as Pat.Coleman_Admin to fully experience this simulation.

- Log off of HQDC01 and log on as **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.

► Task 3: Confirm that event viewer tasks are functioning

1. On HQDC02, at the Command Prompt, type **net stop dfsr** and press ENTER, then type **net start dfsr** and press ENTER.
2. On HQDC01, wait for the event viewer task messages to appear.

Results: After this exercise, you will have configured tasks to launch when an event is received in the Forwarded Events log and when a service is started or stopped on a remote machine.

Exercise 5: Monitor AD DS with Performance Monitor

In this exercise, you will use Performance Monitor to monitor the real-time performance of AD DS, to save performance counters, and to view a log of saved performance counters.

The main tasks for this exercise are as follows:

1. Configure Performance Monitor to monitor AD DS.
2. Create a Data Collector Set from Performance Monitor counters.
3. Start a Data Collector Set.
4. View a Data Collector Set report.

► Task 1: Configure Performance Monitor to monitor AD DS

1. On HQDC02, in Server Manager, open the **Performance Monitor** snap-in.
2. Add the following object performance counters:
 - **DirectoryServices\DRS Inbound Bytes Total/sec**
 - **DirectoryServices\DRS Outbound Bytes Total/sec**
 - **DirectoryServices\DS Threads In Use**
 - **DirectoryServices\DS Directory Reads/sec**
 - **DirectoryServices\DS Directory Writes/sec**
 - **DirectoryServices\DS Directory Searches/sec**
 - **Security System-Wide Statistics\Kerberos Authentications**
 - **DNS\UDP Query Received/sec**
3. Watch performance for a few moments. Then, in the counter list below the graph, select **UDP Query Received/sec**. Click the **Highlight** button in the toolbar to highlight that counter in the graph. Then click the **Highlight** button in the toolbar again to turn off the highlight.
4. Spend a few moments exploring the functionality of Performance Monitor. Do not add or remove counters, however.

► **Task 2: Create a Data Collector Set from Performance Monitor counters**

- Create a new Data Collector Set from the current view of Performance Monitor. Name the Data Collector Set **Custom ADDS Performance Counters**. Make a note of the default root directory in which the Data Collector Set will be saved.

► **Task 3: Start a Data Collector Set**

1. Click the **Data Collector Sets\User Defined** node, then right-click **Custom ADDS Performance Counters** and then click **Start**.
2. The **Custom ADDS Performance Counters** node is automatically selected. You can identify the individual data collectors in the Data Collector Set. In this case, only one data collector (the System Monitor Log performance counters) is contained in the Data Collector Set. You can also identify where the output from the data collector is being saved.
3. In the console tree, right-click the **Custom ADDS Performance Counters** data collector set, and then click **Stop**.

► **Task 4: View a Data Collector Set report**

- In the console tree, expand **Custom ADDS Performance Counters**, and then click **System Monitor Log.blg**. The graph of the log's performance counters is displayed.

Results: After this exercise, you will have created a Data Collector Set, allowed the Data Collector Set to run, and then viewed the data it contains.

Exercise 6: Work with Data Collector Sets

In this exercise, you will examine and run a Data Collector Set that is predefined when you add the AD DS role to a server. You will then create a custom Data Collector Set, configure its schedule and data management policies, run it, and examine its data.

The main tasks for this exercise are as follows:

1. Examine a predefined Data Collector Set.
2. Create a Data Collector Set.
3. Configure start conditions for a Data Collector Set.
4. Configure stop conditions for a Data Collector Set.
5. Configure data management for a data collector.
6. View the results of data collection.

► Task 1: Examine a predefined Data Collector Set

1. Select the **Active Directory Diagnostics** Data Collector Set under **Reliability and Performance\Data Collector Sets\System**. Notice what data collectors are part of the Data Collector Set.
2. Start the Data Collector Set.
3. Expand **Reports**, **System**, and **Active Directory Diagnostics**, and then click the report. The **Report Status** indicates that data is being collected for 300 seconds (five minutes). Wait five minutes or wait at least one minute, and then right-click **Active Directory Diagnostics** under **Data Collector Sets\System** and choose **Stop**.
4. Spend a few moments examining the sections of the report. Right-click the report and, using the **View** menu, examine the **Performance Monitor**, **Report**, and **Folder** views.
5. In the Folder view, double-click **Performance Counter** in the details pane. A new instance of WPRM is opened to display the log. The new instance may be minimized, in which case you can bring it to the front by clicking its button in the task bar. Examine the window, then close WPRM.

6. In the Server Manager console tree, select the **Performance Monitor** node. Click the **View Log Data** button, and configure the source for Performance Monitor to be **C:\PerfLogs\ADDS\report\Performance Counter**, where *report* is the same name as the report you just generated.

Note that no counters are immediately visible. Click the **Add** counter button, and add the following DirectoryServices object counters to the display: **DS Directory Reads/sec**, **DS Directory Searches/sec**, and **DSDirectoryWrites/sec**.

► Task 2: Create a Data Collector Set

1. In the Server Manager console tree, select the **User Defined** node underneath **Data Collector Sets**.
2. Create a new Data Collector Set named **Custom ADDS Diagnostics** using the predefined **Active Directory Diagnostics** Data Collector Set as a template. Save the new Data Collector Set in the **C:\ADDS Data Collector Sets** folder. Run the data collector set as **CONTOSO\Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.

In a production environment, the account you use should be a unique domain account. It must be a member of the Performance Log Users group and must have the Logon as a batch job user logon right. By default, the Performance Log Users group has this right, so you can simply create a domain account and make it a member of the group.

► Task 3: Configure start conditions for a Data Collector Set

- Configure the schedule for the new Data Collector Set to begin today, with an expiration date in one week. Configure the start time to a time five minutes from now. Make a note of the start time you configure. When prompted for credentials with which to run the scheduled task, use the user name **CONTOSO\Pat.Coleman_Admin** and the password **Pa\$\$w0rd**.

► Task 4: Configure stop conditions for a Data Collector Set

- Configure the Stop Condition for the task to be an overall duration of two minutes. In a production environment, you would likely run a data collector for a longer period of time. Select the option to **Stop when all data collectors have finished**.

► **Task 5: Configure data management for a data collector**

- Configure the data manager resource policy to delete the oldest items and, every day, to copy cab files to \\hqdc01\ADDS_Diag_Reports. Ensure that **Create cab file** and **Delete data file** are selected. When prompted for credentials with which to run the scheduled task, use the user name **CONTOSO\Pat.Coleman_Admin** and the password **Pa\$\$w0rd**.

► **Task 6: View the results of data collection**

1. Wait until the time that you configured as the start time for the Data Collector Set passes. Select the report under **Reports\User Defined\Custom ADDS Diagnostics** and note that the **Report Status** indicates that data is being collected for 120 seconds (two minutes). After data collection has completed, the **Report Status** indicates that the report is being generated.

Spend a few moments examining the report.

2. Right-click the report in the console tree, then point to **View**, and then select **Folder**. Double-click **Performance Counter** in the details pane.

A new instance of Reliability and Performance Monitor opens, with Performance Monitor displaying the logged data in the **Performance Counter** log. Spend a few moments examining the performance graph, and then close the window.

Results: After this exercise, you will have examined a predefined Data Collector Set, created a custom Data Collector Set, run the set on a schedule, and viewed its results.



Note: Do not shut down the virtual machines once you are finished with this lab as the settings you have configured here will be used in subsequent labs in this module.

Lab Review Questions

Question: In what situations do you currently use, or can you envision using, event subscriptions as a monitoring tool?

Question: To what events or performance counters would you consider attaching e-mail notifications or actions? Do you use notifications or actions currently in your enterprise monitoring?

Lesson 2

Manage the Active Directory Database

- Active Directory Database Files
- NTDSUtil
- Perform Database Maintenance
- Demonstration: AD DS Database Maintenance
- Active Directory Snapshots
- Restore Deleted Objects
- Demonstration: Using Snapshots and Object Reanimation





You learned in Module 1 that, in the end, Active Directory is a database supported by a number of services. The Active Directory database is fairly self maintaining. However, there may be occasions that require you to perform maintenance on the database files themselves. In this lesson, you will learn how to maintain the Active Directory database and, along the way, how to recover an accidentally deleted object.

Objectives

After completing this lesson, you will be able to:

- Describe the components and functionality of Active Directory database files.
- Use NTDSUtil to perform Active Directory database maintenance tasks, including offline defragmentation.
- Create and mount snapshots of Active Directory.
- Recover a deleted user.

Active Directory Database Files

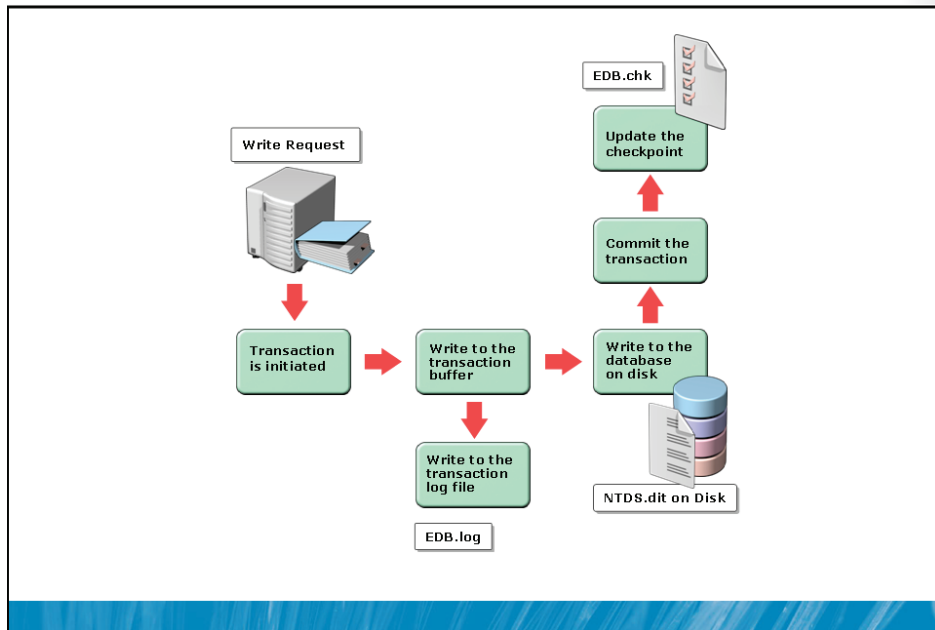
File	Description
 NTDS.dit	<ul style="list-style-type: none">• The AD DS database file• All AD DS partitions and objects on the domain controller• Default location: systemroot\NTDS
 EDB*.log	<ul style="list-style-type: none">• Transaction log• Default transaction log: EDB.log• Overflow logs: Edb000x.log
 EDB.chk	<ul style="list-style-type: none">• Checkpoint file• Pointer into transaction log: which transactions have or have not been committed
 ebdres00001.jrs ebdres00002.jrs	<ul style="list-style-type: none">• Reserved transaction log files• Used if disk runs out of space, so that transaction logs do not crash

Key Points

The Active Directory database is stored as a file named NTDS.dit. When you install and configure AD DS, you can specify the location of the file. The default location is %systemroot%\NTDS. Within NTDS.dit are all of the partitions hosted by the domain controller: the forest schema and configuration, the domain naming context, and (depending on the server configuration) the partial attribute set and application partitions.

In the NTDS folder, there are other files that support the Active Directory database. The Edb.log file is the transaction log for Active Directory. When a change needs to be made to the directory, it is first written to the log file. The change is committed to the directory as a transaction. If the transaction fails, it can be rolled back.

The slide here illustrates this process:



Under normal operations, the transaction log will eventually wrap around, with new transactions overwriting old transactions that had already been committed. However, if a large number of transactions are made within a short period of time, Active Directory will create additional transaction log files, so you may see several EDB*.log files if you look in the NTDS folder of a particularly busy domain controller. Over time, those files are removed automatically.

The EDB.chk file acts like a bookmark into the log files, marking the location before which transactions have been successfully committed to the database, and after which transactions remain to be committed.

If a disk drive runs out of space, it is highly problematic for the server. It is even more problematic if that disc is hosting the Active Directory database, because transactions that may be pending cannot be written to the logs. Therefore, Active Directory maintains two additional log files, edbres0001.jrs and edbres0002.jrs. These are empty files of 10 MB each. When a disk runs out of space for normal transaction logs, Active Directory will recruit the space used by these two files in order to continue writing transactions. Of course, it will be important for an administrator to remediate the low disk space problem as quickly as possible. The file simply provides a temporary solution to prevent the directory service from refusing new transactions.

Additional Reading

- How the Data Store Works
<http://go.microsoft.com/fwlink/?LinkId=101077>

NTDSUtil

- Manage and control single master operations (Module 11)
- Perform AD DS database maintenance (Module 13)
 - Perform offline defragmentation
 - Create and mount snapshots
 - Move database files
- Clean domain controller metadata
 - Domain controller removal or demotion while not connected to domain
- Reset Directory Services Restore Mode password
 - set dsrm

Key Points

In previous modules, you have used the NTDSUtil command to perform actions on the directory service. In Module 11, the command was used to seize operations master roles. In this module, you will use the command to perform database maintenance, including the creation of snapshots, offline defragmentation, and the relocation of the database files.

NTDSUtil is also used to clean up domain controller metadata. If a domain controller is demoted (removed from the domain) while offline, it is unable to remove important information from the directory service. You can then use NTDSUtil to clean out the remnants of the domain controller, and it is very important that you do so.

Finally, NTDSUtil can reset the password used to logon to the Directory Services Restore Mode (DSRM). This password is initially configured during the configuration of a domain controller. If you forget the password, `ntds set dsrm` can reset it.

Additional Reading

- Data Store Tools and Settings
<http://go.microsoft.com/fwlink/?LinkId=101078>
- How to remove data in Active Directory after an unsuccessful domain controller demotion
<http://go.microsoft.com/fwlink/?LinkId=168459>

Perform Database Maintenance

- Garbage collection
 - Scavenging: Removing deleted items that have reached their tombstone lifetime
- Defragmentation
 - Online defrag (part of garbage collection): reclaims unused space
 - Offline defrag (manual): releases unused space, reduces file size
 - Use NTDSUtil
- Restartable AD DS
 - You can stop AD DS in Services just like any other service
 - For applying updates that affect AD DS files
 - Before performing offline defragmentation

Key Points

The Active Directory database is fairly self maintaining. Every 12 hours, by default, each domain controller runs a process called *garbage collection*. Garbage collection does two things. First, it removes deleted objects that have outlived their tombstone lifetime. When an object is deleted, it is moved to the Deleted Objects container and stripped of almost all of its attributes. The object remains in the directory service portrait of time defined by the tombstone lifetime, 180 days by default on Windows Server 2008. This allows an enterprise to reanimate, or restore, the object using procedures that you will learn later in this lesson. Once the tombstone life has been reached, garbage collection zeros out the object's row in the database.

As objects are deleted, the zeroed out rows create a type of fragmentation that can impact performance. The garbage collection process reorganizes the rows of the database so that the blank rows are contiguous, very much like disk fragmentation reorganizes sectors of a disk so that free space is contiguous. However, this process, called online defragmentation, does not reduce the file size of the database. It simply optimizes the internal order of the database.

In many environments, this is sufficient. However, it may be necessary to reduce the file size of NTDS.dit in organizations that delete significant numbers of objects from the directory. To do this, you must perform offline defragmentation using NTDSUtil. The procedures for doing so are discussed later in this lesson.

In previous versions of Windows, domain controllers maintained a lock on the Active Directory database. In order to perform database maintenance, you had to restart the server in the DSRM. In Windows Server 2008, AD DS has been architected as a service and, just like any other service, it can be stopped or started on demand from the Services snap-in. Now, if you want to perform offline defragmentation, you can simply stop the AD DS service, perform the maintenance, and then restart the service.

Demonstration: AD DS Database Maintenance

In this demonstration, we will:

- Stop the AD DS service
- Simulate compacting the database
- Simulate moving the database to a new volume
- Restart the AD DS service

Key Points

In this demonstration, your instructor will show you how to stop and start the AD DS service, how to compact the database, and how to move database files to another volume.

Procedures for these steps can be found in the Lab Answer Key for this module. You will have the opportunity to practice many of these procedures in the lab.

Demonstration Steps

To stop the AD DS service:

- Open the Services console then right-click **Active Directory Domain Services**, and then select **Stop** from the context menu.

To perform an offline defrag of the Advanced Directory database while in an AD DS stopped state:

1. In the command window, type **ntdsutil**, and then press ENTER.
2. At the ntdsutil: prompt, type **Activate Instance NTDS**, and then press ENTER.
3. At the ntdsutil: prompt, type **files**, and then press ENTER.
4. At the file maintenance: prompt, type **compact to drive:\ LocalDirectoryPath** (where drive:\ LocalDirectoryPath is the path to a location on the local computer). After a short while, press CTRL+C to break the process. This process can take a long time to complete.
5. After the process has completed itself, you would need to copy NTDS.dit to a “backup” location, along with the logs (*.log), and then you would delete the logs (*.log).
6. Best Practices recommend that we lastly check the integrity of the newly compacted database. Type **"integrity"** to check the integrity of the newly compacted database. This process, like a compact, takes a long time to complete. Press CTRL+C at any time to break the process and move on to the next part of the demo.

To move the AD DS database:

1. In the File Maintenance command window, type **move db to pathname**. As above, we will not wait for this process to complete.
2. Press CTRL+C to break the process at any time.

Please know that the NTDS.dit file would be moved to the new location and permissions would be set accordingly had we waited for the entire process to complete itself.

Lastly, restart AD DS:

- In the Services MMC, right-click **Active Directory Domain Services**, and then click **Start**.

Stick a fork in yourself - you're done!

Question: Why is it necessary to stop AD DS before defragmenting?

Question: Why is it necessary to compact the database to a temporary directory first?

Additional Reading

- Compact the Directory Database File (Offline Defragmentation)
<http://go.microsoft.com/fwlink/?LinkId=101083>

Active Directory Snapshots

- Create a snapshot of Active Directory
 - NTDSUtil
- Mount the snapshot to a unique port
 - NTDSUtil
- Expose the snapshot
 - Right-click the root node of Active Directory Users and Computers and choose Connect to Domain Controller
 - Enter serverFQDN:port
- View (read-only) snapshot
 - Cannot directly restore data from the snapshot
- Recover data
 - Manually re-enter data or
 - Restore a backup from the same date as the snapshot

Key Points

NTDSUtil in Windows Server 2008 has the capability to create and mount snapshots of Active Directory. A snapshot is a form of historical backup—it captures the exact state of the directory service at the time of the snapshot. Unlike a backup, a snapshot cannot be used to restore data. However, you can use tools to explore the contents of the snapshot in order to examine the state of the directory service at the time the snapshot was made.

To create a snapshot:

1. Open an elevated command prompt.
2. Type **ntdsutil**, and then press ENTER.
3. Type **snapshot**, and then press ENTER.
4. Type **activate instance ntds**, and then press ENTER.

5. Type **create**, and then press ENTER.

The command returns a message indicating that the snapshot set was generated successfully.

The GUID that is displayed is important for commands in later tasks. Make a note of the GUID or, alternatively, copy it to the Clipboard.

6. Type **quit**, and then press ENTER.

It is recommended that you schedule snapshots of Active Directory on a regular basis. You can use the Task Scheduler to execute a batch file with the appropriate NTDSUtil commands.

In order to view the contents of a snapshot, you must mount the snapshot as a new instance of AD DS. This is also accomplished with NTDSUtil.

To mount a snapshot:

1. Open an elevated command prompt.
2. Type **ntdsutil**, and then press ENTER.
3. Type **activate instance ntds**, and then press ENTER.
4. Type **snapshot**, and then press ENTER.
5. Type **list all**, and then press ENTER.

The command returns a list of all snapshots.

6. Type **mount {GUID}**, where **GUID** is the GUID returned by the create snapshot command, and then press ENTER.
7. Type **quit**, and then press ENTER.
8. Type **quit**, and then press ENTER.
9. Type **dsamain -dbpath c:\\$snap_<datetime>_volume{GUID}\windows\ntds\ntds.dit -ldapport 50000**, and then press ENTER.

The port number, 50000, can be any open and unique TCP port number.

A message indicates that Active Directory Domain Services startup is complete..

10. Do not close the command prompt window and leave the command you just ran, Dsamain.exe, running while you continue to the next step.

After the snapshot has been mounted, you can use tools to connect to and explore the snapshot. Even Active Directory Users and Computers can connect to the instance.

To connect to a snapshot with Active Directory Users and Computers:

1. Open **Active Directory Users and Computers**.
2. Right-click the root node, and then click **Change Domain Controller**.

The Change Directory Server dialog box appears.

3. Click **<Type a Directory Server name[:port] here>**.
4. Type **HQDC01:50000**, and then press ENTER.

HQDC01 is the name of the domain controller on which you mounted the snapshot, and 50000 is the TCP port number you configured for the instance and you are now connected to the snapshot.

5. Click **OK**.

Note that snapshots are Read Only. You cannot modify the contents of a snapshot. Nor are there direct methods with which to move, copy, or restore objects or attributes from the snapshot to the production instance of Active Directory.

To unmount the snapshot:

1. Switch to the command prompt in which the snapshot is mounted.
2. Press CTRL+C to stop DSAMain.exe.
3. Type **ntdsutil**, and then press ENTER.
4. Type **activate instance ntds**, and then press ENTER.
5. Type **snapshot**, and then press ENTER.
6. Type **unmount GUID**, where **GUID** is the GUID of the snapshot, and then press ENTER.
7. Type **quit**, and then press ENTER.
8. Type **quit**, and then press ENTER.

Additional Reading

- Active Directory Domain Services Database Mounting Tool (Snapshot Viewer or Snapshot Browser) Step-by-Step Guide
<http://go.microsoft.com/fwlink/?LinkId=168460>

Restore Deleted Objects

- When an object is deleted
 - Stripped of almost every attribute except
 - SID, objectGUID, lastKnownParent, sAMAccountName
 - Moved to Deleted Objects container, marked as isDeleted
- You can restore (“reanimate”) deleted (“tombstoned”) objects when
 - Domain functional level is Windows Server 2003 or greater
 - Deleted object has not yet been scavenged
- Steps
 - LDP.exe
 - Modify isDeleted
 - Provide distinguished name (DN)
 - Repopulate all other attributes

Key Points

As mentioned earlier, when an object is deleted, it is moved to the Deleted Objects container and stripped of almost all of its attributes. In fact, the only attributes that remain are the object's SID, objectGUID, lastKnownParent, and sAMAccountName.

As long as the domain functional level is Windows Server 2003 or greater, and as long as the object has not yet been scavenged by the garbage collection process after reaching the end of its tombstone lifetime, you can restore or reanimate the deleted object.

To restore a deleted object:

1. Click the **Start** button, then in the **Start Search** box, type **LDP.exe** and press CTRL+SHIFT+ENTER, which executes the command as an administrator.
The User Account Control dialog box appears.
2. Click **Use another account**.
3. In **User name**, type the username of an administrator.

4. In **Password**, type the password for the administrative account, and then press ENTER.
LDP opens.
5. Click the **Connection** menu, then click **Connect**, and then click **OK**.
6. Click the **Connection** menu, then click **Bind**, and then click **OK**.
7. Click the **Options** menu, and then click **Controls**.
8. In the **Load Predefined** list, click **Return Deleted Objects**, and then click **OK**.
9. Click the **View** menu, then click **Tree**, and then click **OK**.
10. Expand the domain and then double-click **CN=Deleted Objects,DC=contoso,DC=com**.
11. Right-click the deleted object, and then click **Modify**.
12. In the **Attribute** box, type **isDeleted**.
13. In the **Operation** section, click **Delete**.
14. Click the ENTER button.
15. In the **Attribute** box, type **distinguishedName**.
16. In the **Values** box, type the distinguished name of the object in the parent container or organizational unit into which the object should be restored. For example, type the distinguished name of the object before it was deleted.
17. In the **Operation** section, click **Replace**.
18. Click the ENTER button.
19. Select the **Extended** check box.
20. Click the **Run** button.
21. Click the **Close** button.
22. Close LDP.
23. Use Active Directory Users and Computers to repopulate attributes of the object, reset the password (for a user object), and enable the object (if disabled).

Additional Reading

- End-to-End Scenario That Uses the Active Directory Database Mounting Tool
<http://go.microsoft.com/fwlink/?LinkId=168462>

Demonstration: Using Snapshots and Object Reanimation

In this demonstration, we will:

- Create a snapshot
- Delete a user
- Mount the snapshot
- Expose the snapshot
- Reanimate the tombstoned user object
- Repopulate the user's attributes
- Unmount the snapshot

Key Points

In this demonstration, your instructor will create a snapshot, delete an object (a user, perhaps), mount the snapshot with NTDSutil, and use LDP or ADSIedit to view the deleted object in the snapshot..

You will have the opportunity to review and practice similar procedures in the lab shortly for this lesson.

For specific steps for these demos please refer to the previous two topics **Active Directory Snapshots** and **Restore Deleted Objects**. These contain detailed steps to create a snapshot, mount a snapshot, connect to a snapshot with Active Directory Users and Computers, to unmount the snapshot and to restore a deleted object.

Question: When would it be useful to mount multiple snapshots simultaneously?

Question: Why is it necessary to specify different LDAP, SSL, and global catalog ports for each mounted instance of the database?

Additional Reading

- End-to-End Scenario That Uses the Active Directory Database Mounting Tool:
<http://go.microsoft.com/fwlink/?LinkId=168818>

Lab B: Manage the Active Directory Database

- Exercise 1: Perform Database Maintenance
- Exercise 2: Work with Snapshots and Recovering a Deleted User

Logon information

Virtual machine	6425B-HQDC01-B	6425B-HQDC02-B
Logon user name	Pat.Coleman	Pat.Coleman
Administrative user name	Pat.Coleman_Admin	Pat.Coleman_Admin
Password	Pa\$\$w0rd	Pa\$\$w0rd

Estimated time: 30 minutes

Scenario

You are the administrator of Contoso, Ltd., an online university. At the end of the semester, 65 days ago, you deleted 835 user accounts for students who have graduated or will no longer return to the program. You now want to compact your Active Directory database to reclaim the space released by that many deleted objects. Additionally, you were notified that yesterday, one user account, Adriana Giorgi, was deleted by accident. You want to recover that account with a snapshot you have scheduled to run each night at 1:00 a.m.

Exercise 1: Perform Database Maintenance

In this exercise, you will perform maintenance on the Active Directory database. To do so, you will need to stop the AD DS service and restart it when the maintenance is complete.

The main tasks for this exercise are as follows:

1. Prepare for the lab.
2. Prepare to compact the Active Directory database.
3. Stop the AD DS service.
4. Compact the Active Directory database.
5. Replace the Active Directory database with the compacted copy.
6. Verify the integrity of the compacted database.
7. Start the AD DS service.

► Task 1: Prepare for the lab

The virtual machines should already be started and available after completing Lab A. However, if they are not, you should complete the below steps.

1. Start 6425B-HQDC01-B and log on as **Pat.Coleman** with the password **Pa\$\$w0rd**.
2. Start 6425B-HQDC02-B but do not log on.

► Task 2: Prepare to compact the Active Directory database

1. Run the command prompt as an administrator, with the user name **Pat.Coleman_Admin** and the password **Pa\$\$w0rd**.
2. From the command prompt, create two folders: **D:\NTDSCompact** and **D:\NTDSOriginal**.

► Task 3: Stop the AD DS service

1. Run the **Services** console as an administrator, with the user name **Pat.Coleman_Admin** and the password **Pa\$\$w0rd**.
2. Stop the AD DS service.

► **Task 4: Compact the Active Directory database**

- Use **NTDSUtil** to activate the NTDS instance and to compact the database file to **D:\NTDSCompact**.

► **Task 5: Replace the Active Directory database with the compacted copy**

1. Move the old version of **NTDS.dit** and all *.log files from **%systemroot%\NTDS** to **D:\NTDSOriginal** to preserve them in the event that the compaction did not succeed or caused corruption.
2. Copy the compacted **NTDS.dit** from **D:\NTDSCompact** to **%systemroot%\NTDS\ntds.dit**.

► **Task 6: Verify the integrity of the compacted database**

- Use **NTDSUtil** to activate the NTDS instance, to perform an integrity check, and to perform a semantic database analysis in fixup mode.

► **Task 7: Start the AD DS service**

1. Switch to the **Services** console.
2. Start the AD DS service.
3. Close the **Services** console.

Results: After this exercise, you will have stopped AD DS, compacted the Active Directory database, performed integrity and semantic checking, and restarted AD DS.

Exercise 2: Work with Snapshots and Recover a Deleted User

In this exercise, you will create and mount an Active Directory snapshot, and you will use the information to help you repopulate attributes of a deleted user object.

The main tasks for this exercise are as follows:

1. Create a snapshot of Active Directory.
2. Make a change to Active Directory.
3. Mount an Active Directory snapshot and create a new instance.
4. Explore a snapshot with Active Directory Users and Computers.
5. Use LDP to restore a deleted object (OPTIONAL).

► Task 1: Create a snapshot of Active Directory

- From the elevated command prompt, type the following commands:

```
ntdsutil  
snapshot  
activate instance ntds  
create  
quit  
quit
```

The command returns a message indicating that the snapshot set was generated successfully. The GUID that is displayed is important for commands in later tasks. Make a note of the GUID or, alternatively, copy it to the Clipboard.

► Task 2: Make a change to Active Directory

1. Run Active Directory Users and Computers as an administrator, with the user name **Pat.Coleman_Admin** and the password **Pa\$\$w0rd**.
2. Delete **Adriana Giorgi's** account in the **User Accounts\Employees** organizational unit (OU).

► **Task 3: Mount an Active Directory snapshot and create a new instance**

1. From the elevated command prompt, type the following commands:

```
ntdsutil  
activate instance ntds  
snapshot  
list all
```

The command returns a list of all snapshots.

2. Type the following commands:

```
mount guid  
quit  
quit
```

where *guid* is the GUID of the snapshot you created.

3. Start an instance of Active Directory using the snapshot by typing the following command, all on one line.

```
dsamain -dbpath c:\$snap_datetime_volumec$\windows\ntds\ntds.dit -  
ldapport 50000
```

Note that *datetime* will be a value that is unique for you. There should only be one folder on your drive C with a name that begins with *\$snap*.

A message indicates that Active Directory Domain Services startup is complete. Leave Dsamain.exe running. Do not close the command prompt.

► **Task 4: Explore a snapshot with Active Directory Users and Computers**

1. Switch to **Active Directory Users and Computers**. Right-click the root node of the snap-in and choose **Change Domain Controller**. Type the directory server name and port **HQDC01:50000**, and then press ENTER. Click **OK**.
2. Locate **Adriana Giorgi's** object in the **User Accounts\Employees** OU. Note that **Adriana Giorgi's** object is displayed because the snapshot was taken prior to deleting it.

► **Task 5 (Optional): Use LDP to restore a deleted object**

Restoring a deleted user account is a task that is not directly related to snapshots. You use the Ldp.exe command to reanimate objects from the Deleted Objects container of Active Directory. A deleted object is stripped of most of its attributes, so a snapshot can be helpful to examine attributes of the object prior to its deletion.

1. Click the **Start** button. In the **Start Search** box, type **LDP.exe** and press CTRL+SHIFT+ENTER, which executes the command as an administrator.
The User Account Control dialog box appears.
2. Click **Use another account**.
3. In **User name**, type **Pat.Coleman_Admin**.
4. In **Password**, type **Pa\$\$w0rd**, and then press ENTER.
LDP opens.
5. Click the **Connection** menu, then click **Connect**, and then click **OK**.
6. Click the **Connection** menu, then click **Bind**, and then click **OK**.
7. Click the **Options** menu, and then click **Controls**.
8. In the **Load Predefined** list, click **Return Deleted Objects**, and then click **OK**.
9. Click the **View** menu, then click **Tree**, and then click **OK**.
10. In the console tree, expand **DC=contoso,DC=com**, and then double-click **CN=Deleted Objects,DC=contoso,DC=com**.
11. Right-click **CN=Adriana Giorgi**, and then click **Modify**.
12. In the **Attribute** box, type **isDeleted**.
13. In the **Operation** section, click **Delete**.
14. Click the ENTER button.
15. In the **Attribute** box, type **distinguishedName**.
16. In the **Values** box, type **CN=Adriana Giorgi,OU=Employees,OU=User Accounts,DC=contoso,DC=com**.
17. In the **Operation** section, click **Replace**.
18. Click the ENTER button.
19. Select the **Extended** check box.

20. Click the **Run** button.
21. Click the **Close** button.
22. Close LDP.
23. Run **Active Directory Users and Computers** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
24. In the console tree, expand the **contoso.com** domain, and the **User Accounts** OU, and then click the **Employees** OU.
25. Note that Adriana Giorgi's account is restored; however, all attributes are missing, including the description and the password. Because the password is missing, the account has been disabled.
26. Switch to the instance of Active Directory Users and Computers that is displaying the snapshot data.
27. Note that you can use the attributes contained in the snapshot to manually re-populate attributes in Active Directory.
28. Close both instances of Active Directory Users and Computers.

► **Task 6: Unmount an Active Directory snapshot**

1. In the command prompt, press CTRL+C to stop **DSAMain.exe**.
2. Type the following commands:

```
ntdsutil  
activate instance ntds  
snapshot  
unmount guid quit  
quit
```

where guid is the GUID of the snapshot.

Results: After this exercise, you will have created, mounted, and examined a snapshot of Active Directory and, optionally, restored a deleted user account.



Note: Do not shut down the virtual machines once you are finished with this lab as the settings you have configured here will be used in subsequent labs in this module.

Lab Review Questions

Question: In what other situations might it be useful to mount a snapshot of Active Directory?

Question: What are the disadvantages of restoring a deleted object with a tool such as LDP?

Lesson 3

Back Up and Restore AD DS and Domain Controllers

- Backup and Recovery Tools
- Overview of AD DS and Domain Controller Backup
- Demonstration: Backing Up AD DS
- Other Backup and Recovery Tools
- Active Directory Restore Options
- Nonauthoritative Restore
- Authoritative Restore

Even with the most effective monitoring plan and technologies, it is still possible for a domain controller to fail, or for Active Directory to be damaged or corrupted, intentionally or accidentally. In such an event, you must be prepared to restore the domain controller, the directory, or objects within the directory. In this lesson, you will learn how to use Windows Server Backup and Directory Services Restore Mode to effectively backup and restore AD DS and domain controllers.

Objectives

After completing this lesson, you will be able to:

- Back up an AD DS domain controller.
- Schedule domain controller backup jobs.
- Restore AD DS

Backup and Recovery Tools

- Windows Server Backup snap-in (use locally or remotely)
 - Back up a full server (all volumes)
 - Back up selected volume(s)
 - Back up system state (includes all critical volumes)
 - Recover volumes, folders, files, or system state
- wbadmin.exe
- Perform manual or automated backup
- Back up to CD/DVD/HDD
 - No tape!
 - Use a dedicated HDD for backup: recommended or required

Key Points

Windows Server Backup is the new and greatly improved feature of Windows Server 2008 that enables you to back up and restore a server, its roles, and its data. Windows Server Backup is installed as a feature in Server Manager.

Windows Server Backup provides a snap-in administrative tool and the WBAAdmin command (wbadmin.exe). Both the snap-in and the command line allow you to perform manual or automated backups to an internal or external disk volume, a remote share, or optical media. Backing up to tape is no longer supported by Windows Server Backup.

Windows Server Backup allows you to perform one of the following types of backups:

- Full server
- Selected volumes
- System state

You cannot use Windows Server Backup to back up individual files or folders. However, Windows Server Backup does allow you to restore individual files or folders.

If you choose to back up to a local or external disk volume, it is recommended or required (depending on your configuration) that the volume be dedicated to backups. In other words, you should not use the volume to store any other types of data.

Note that the legacy backup tool, NTBackup, is no longer supported. Furthermore, Windows Server Backup is unable to restore backups made by NTBackup. You can download a version of NTBackup that is compatible with Windows Server 2008 and supported for restoring legacy backup files onto Windows Server 2008 when you need to recover data. However, NTBackup should not be used to perform any new backup operations.

There are several nuances and requirements for using Windows Server Backup in certain scenarios and configurations. If you will be using Windows Server Backup as your backup utility, be sure to read the articles listed under "Additional Reading" below.

Additional Reading

- Backup and Recovery Overview for Windows Server 2008
<http://go.microsoft.com/fwlink/?LinkId=168463>
- Windows Server Backup
<http://go.microsoft.com/fwlink/?LinkId=168464>
- Windows Server Backup Step-by-Step Guide for Windows Server 2008
<http://go.microsoft.com/fwlink/?LinkId=168465>
- Backing Up Your Server
<http://go.microsoft.com/fwlink/?LinkId=168466>

Overview of AD DS and Domain Controller Backup

- You must back up all critical volumes
 - System volume: The volume that contains boot files
 - Boot volume: The volume that contains the Windows operating system and the registry
 - Volume(s) hosting SYSVOL, AD DS database (NTDS.dit), logs
 - *Do not store other data* on these volumes as it will increase backup and restore times
- Windows Server Backup (wbadmin.exe)

Key Points

In previous versions of Windows, backing up Active Directory entailed creating a backup of the System State, which was a small collection of files that included the Active Directory database and the registry.

In Windows Server 2008, the System State concept still exists, but it is much larger. Because of interdependencies between server roles, physical configuration, and Active Directory, the System State is now a subset of a Full Server backup and, in some configurations, might be just as big. In order to back up a domain controller, you must back up all critical volumes fully.

You can use Windows Server Backup (the snap-in or wbadmin.exe) perform a System State backup.

Additional Reading

- AD DS Backup and Recovery Step-by-Step Guide
<http://go.microsoft.com/fwlink/?LinkId=168467>

Demonstration: Backup AD DS

In this demonstration we will:

- Back up a domain controller

Key Points

In this demonstration, your instructor will show you how to back up Active Directory. You will have the opportunity to perform a similar procedure in the lab for this module.

Demonstration Steps

To perform an interactive backup of Active Directory:

1. Open the **Windows Server Backup** snap-in.
2. Click the **Backup Once** link. The Backup Once Wizard appears.
3. On the **Backup** options page, ensure that **Different options** is selected, and then click **Next**.
4. On the **Select backup configuration** page, click **Custom**, and then click **Next**.
5. On the **Select backup items** page, ensure that the **Enable system recovery** check box is selected, and click **Next**.
6. On the **Specify destination type** page, click **Next**.

7. On the **Select backup destination** page, click **Next**.
8. On the **Specify advanced option** page, click **VSS full backup**, and then click **Next**.
9. On the **Confirmation** page, click **Backup**.

Other Backup and Recovery Tools

- Active Directory Snapshots
- PowerShell cmdlets
- Windows Recovery Environment
 - Boot to Windows Server 2008 DVD and choose System Recovery Options
 - Install locally as a boot option
 - Useful for full system recovery
- Microsoft System Center Data Protection Manager 2007

Key Points

Windows Server 2008 provides several additional tools that are related to backup and recovery of Active Directory Domain Services.

In the previous lesson, you learned how to create snapshots of Active Directory. The snapshots, although they are Read Only, are a valuable piece of the recovery picture. First, you can easily browse snapshots to identify at what point in time a problem was introduced in the directory, and then you can restore the correct backup accordingly. Second, while Windows provides no method for copying or storing information from a snapshot into the production instance of Active Directory, there are scripts and third-party tools that will allow you to do some of that.

Windows Server Backup adds several Windows PowerShell cmdlets that allow you to script backup and recovery operations.

Finally, the Windows Recovery Environment (WinRE) is extraordinarily helpful in certain recovery scenarios. WinRE is a memory-resident version of Windows derived from the Windows Preinstallation Environment (WinPE). You can launch WinRE by booting with the Windows Server 2008 DVD and, when prompted, choosing System Recovery Options. A command prompt opens, at which you have full access to unencrypted disk volumes on the system. You can use wbadm to perform backup or restore operations, and you can use many other command-line troubleshooting operations.

It is recommended that you install WinRE as a boot option on a server, in case the primary operating system fails. This allows you to boot directly to WinRE without needing the Windows Server 2008 installation media.

You can learn more about WinRE and the other tools on this slide in the article listed under "Additional Reading."

Additional Reading

- Backup and Recovery Overview for Windows Server 2008
<http://go.microsoft.com/fwlink/?LinkId=168449>

Active Directory Restore Options

- **Nonauthoritative (normal) restore**
 - Restore domain controller to previously known good state of Active Directory
 - Domain controller will be updated using standard replication from up-to-date partners
- **Authoritative restore**
 - Restore domain controller to previously known good state of Active Directory
 - "Mark" objects that you want to be authoritative
 - Windows sets the version numbers very high
 - Domain controller is updated from its up-to-date-partners
 - Domain controller sends authoritative updates to its partners
- **Full Server Restore**
 - Typically performed in Windows Recovery Environment
- **Alternate Location Restore**

Key Points

When a domain controller or its directory is corrupted, damaged, or failed, you have several options with which to restore the system.

The first such option is called "normal restore" or "nonauthoritative restore." In a normal restore operation, you restore a backup of Active Directory as of a known good date. Effectively, you roll the domain controller back in time. When AD DS restarts on the domain controller, the domain controller contacts its replication partners and requests all subsequent updates. Effectively, the domain controller "catches up" with the rest of the domain using standard replication mechanisms.

Normal restore is useful when the directory on a domain controller has been damaged or corrupted but the problem has not spread to other domain controllers. What about a situation in which damage has been done, and the damage has been replicated? For example, what if you delete one or more objects, and that deletion has been replicated?

In these situations, a normal restore is not sufficient. If you restore a known good version of Active Directory and restart the domain controller, the deletion (which happened subsequent to the backup) will simply replicate back to the domain controller, and you will be right where you started.

That's where authoritative restore is necessary. In an authoritative restore, you restore the known good version of Active Directory just as you do in a normal restore, but before restarting the domain controller you mark the objects that you wish to retain (the accidentally deleted objects) as authoritative, so that they will replicate *from* the restored domain controller *to* its replication partners. Behind the scenes, when you mark objects as authoritative, Windows increments the version number of all object attributes to be so high that the version is guaranteed to be higher than the version number on all other domain controllers. When the restored domain controller is restarted, it replicates from its replication partners all changes that have been made to the directory, but it also notifies its partners that it has changes, the version numbers of which ensure that partners take the changes and replicate them throughout the directory service.

The third option for restoring the directory service is to restore the entire domain controller. This is done by booting to the Windows Recovery Environment and restoring a full server backup of the domain controller. By default, this is a normal restore. If you also need to mark objects as authoritative, you must restart the server in Directory Services Restore Mode and set those objects as authoritative prior to booting the domain controller into normal operation.

Finally, you can restore a backup of the System State to an alternate location. This allows you to examine files and, potentially, to mount the NTDS.dit file as you learned how to do in the previous lesson. You should absolutely not copy the files from an alternate restore location over the production versions of those files. Do not do a piecemeal restore of Active Directory. This option is also used if you want to use the Install From Media option for creating a new domain controller.

Nonauthoritative Restore

- Restart the domain controller in DSRM
 - Locally: Press F8 on restart
 - Remotely using remote desktop:
 - Configure restart in DSRM: `bcdedit /set safeboot dsarepair`
 - Restart: `shutdown -t 0 -r`
- Log on with the Administrator account and the DSRM password
- Perform the nonauthoritative restore
 - Use Windows Server Backup (wbadmin.exe) to restore AD DS
- Restart
 - Set normal restart: `bcdedit /deletevalue safeboot dsarepair`
 - Restart: `shutdown -t 0 -r`
- Domain controller replicates all changes since date of backup from its partners

Key Points

In order to perform a non-authoritative or authoritative restore of Active Directory, you must have full access to the files on the domain controller. This requires restarting the domain controller in Directory Services Restore Mode (DSRM).

If you are restarting a domain controller locally, press F8 on startup and choose Directory Services Restore Mode from the boot menu.

Alternatively, you can configure the domain controller to automatically restart in DSRM. This method must be used if you are accessing the domain controller remotely with remote desktop.

To configure a domain controller to restart in DSRM:

1. Open an elevated command prompt, type the following command, and then press ENTER:

```
bcdedit /set safeboot dsrepair
```


2. Type the following command, and then press ENTER:

```
shutdown -t 0 -r
```

3. To restart the server normally after you perform the restore operation, type the following command, and then press ENTER:

```
bcdedit /deletevalue safeboot dsrepair  
shutdown -t 0 -r
```

When you start a domain controller in DSRM, you will log on as Administrator with the DSRM password.

You can then use Windows Server Backup to restore the directory database.

1. Open a Command Prompt.
2. Type **wbadmin get versions -backuptarget:D: -machine:HQDC01**, and then press ENTER.

Where D: is the volume on which backups are stored and HQDC01 is the name of the domain controller that you are restoring.
3. Note the version information that is returned.
4. Type **wbadmin start systemstaterecovery -version:version**, where *version* is the number that you recorded in the previous step, and then press ENTER.
5. Type **Y**, and then press ENTER.

After the restore operation is complete, restart the server. The domain controller will "catch up" with the rest of the domain by pulling from its replication partners the changes to the directory that have occurred since the date of the backup.

Authoritative Restore

- Restart the domain controller in DSRM
- Log on with the Administrator account and the DSRM password
- Perform the nonauthoritative restore
 - Use Windows Server Backup (wbadmin.exe) to restore AD DS
- Mark selected objects as authoritative
 - `restore [object/subtree] "objectDN"`
 - Authoritative changes have a higher version number than on partners
- Restart
- Restored domain controller replicates changes since date of backup
- Partners see authoritative changes with high version numbers
 - Partners pull the authoritative changes from the restored domain controller

Key Points

Most of the procedures involved in performing an authoritative restore are identical to those of a non-authoritative restore.

First, restart the domain controller in DSRM. Log on with the Administrator account and the DSRM password. Restore the directory with Windows Server Backup, as described on the previous slide.

But before restarting the domain controller, you must mark as authoritative the objects that you wish to persist after restart—that is, the deleted objects that you are trying to restore.

To mark an object as authoritative, at the Command Prompt, type the following commands:

```
ntdsutil
authoritative restore
restore object "object DN"
```

To mark an OU or container, and all of its subobjects as authoritative, at the command prompt, type the following commands:

```
ntdsutil  
authoritative restore  
restore subtree "object DN"
```

Restart the domain controller. The domain controller will replicate from its partners all of the changes that have occurred to the directory since the date of the backup. However, for the objects that were marked authoritative, every attribute of those objects was given a very high version number. Therefore, these objects will be replicated from the restored domain controller to the rest of the directory service.

Lab C: Back Up and Restore Active Directory

- Exercise 1: Back up Active Directory
- Exercise 2: Restore Active Directory and a Deleted OU

Logon information

Virtual machine	6425B-HQDC01-B	6425B-HQDC02-B
Logon user name	Pat.Coleman	Pat.Coleman
Administrative user name	Pat.Coleman_Admin	Pat.Coleman_Admin
Password	Pa\$\$w0rd	Pa\$\$w0rd

Estimated time: 30 minutes

Scenario

As administrator of Contoso, it is your responsibility to ensure that the directory service is backed up. Today, you noticed that last night's backup did not run as scheduled. You therefore decided to perform an interactive backup. Shortly after the backup, a domain administrator accidentally deletes the Employees OU. Luckily, you are able to restore the OU with the backup you just made.

Exercise 1: Back Up Active Directory

In this exercise, you will install the Windows Server Backup feature, and then use it to schedule a backup of Active Directory. You also will perform an interactive backup of the system volume.

The main tasks for this exercise are as follows:

1. Prepare for the lab.
2. Install the Windows Server Backup feature.
3. Create a scheduled backup.
4. Perform an interactive backup.

► Task 1: Prepare for the lab

The virtual machines should already be started and available after completing Labs A and B. However, if they are not, you should complete the below steps.

1. Start 6425B-HQDC01-B and log on as **Pat.Coleman** with the password **Pa\$\$w0rd**.
2. Start 6425B-HQDC02-B and log on as **Pat.Coleman** with the password **Pa\$\$w0rd**.

► Task 2: Install the Windows Server Backup feature

1. On HQDC01, run Server Manager as an administrator, with the user name **Pat.Coleman_Admin** and the password **Pa\$\$w0rd**.
2. Install all of the Windows Server Backup features.

► Task 3: Create a scheduled backup

1. Run **Windows Server Backup** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
2. In the Actions pane, click the **Backup Schedule** link.
The Backup Schedule Wizard appears.
3. On the **Getting Started** page, click **Next**.
4. On the **Select backup configuration** page, click **Custom**, and then click **Next**.

5. On the **Select backup items** page, clear the **6425B (D:)** drive check box, and then click **Next**.
6. On the **Specify backup time** page, select **Once a day**.
7. In the **Select time of day** list, select **12:00 am**.
8. Click **Next**.
9. On the **Select destination disk** page, click **Show All Available Disks**.
The Show All Available Disks dialog box appears.
10. Select the **Disk 1** check box, and then click **OK**.
11. On the **Select destination disk** page, select the **Disk 1** check box, and then click **Next**.
The Windows Server Backup dialog box appears, informing you that all data on the disk will be deleted.
12. Click **Yes** to continue.
13. On the **Label destination disk** page, click **Next**.
14. On the **Confirmation** page, click **Cancel** to avoid formatting drive D.

► **Task 4: Perform an interactive backup**

1. In the Windows Server Backup window, in the Actions pane, click **Backup Once**.
2. Configure the backup to use the following settings:
 - **Backup type:** Custom
 - **Backup items:** C: drive only with Enable system recovery
 - **Advanced option:** VSS full backup
3. The backup will take about 10 to 15 minutes to complete. When the backup is complete, close Windows Server Backup.

Results: After this exercise, you will have installed the Windows Server Backup feature and used it to schedule a backup of the AD DS information, and to perform an interactive backup.

Exercise 2: Restore Active Directory and a Deleted OU

In this exercise, you will perform an authoritative restore of the AD DS database. You will then verify that the data is restored successfully.

The main tasks are as follows:

1. Delete the Employees OU.
2. Restart in Directory Services Restore Mode (DSRM).
3. Restore System State data.
4. Mark the restored information as authoritative and restart the server.
5. Verify that the deleted data has been restored.

► Task 1: Delete the Employees OU

1. Run **Active Directory Users and Computers** as an administrator, with the user name **Pat.Coleman_Admin** and the password **Pa\$\$w0rd**.
2. Delete the **Contractors** OU within the **User Accounts** OU.
3. On HQDC02, run **Active Directory Users and Computers** as an administrator, with the user name **Pat.Coleman_Admin** and the password **Pa\$\$w0rd**.
4. Verify that the domain controller has replicated the deletion of the **Contractors** OU.

► Task 2: Restart in Directory Services Restore Mode (DSRM)

1. On HQDC01, run the command prompt as an administrator, with the user name **Pat.Coleman_Admin** and the password **Pa\$\$w0rd**.
2. Type **bcdedit /set safeboot dsrepair** to configure the server to start in Directory Services Restore Mode (DSRM).
3. Restart HQDC01.

► **Task 3: Restore System State data**

1. Log on as **Administrator** using the password **Pa\$\$w0rd**.
2. Run the command prompt as an administrator.
3. Type **wbadmin get versions -backuptarget:D: -machine:HQDC01** to get the version information for the backup.
4. Restore the System State information by typing **wbadmin start systemstaterecovery -version:version -backuptarget:D: -machine:HQDC01**.
i.e. **wbadmin start systemstaterecovery -version:10/14/2009-01:11 -backuptarget:D: -machine:HQDC01**
The restore will take about 30-35 minutes.

► **Task 4: Mark the restored information as authoritative, and then restart the server**

1. At the command prompt, use NTDS to perform an authoritative restore of **"OU=Contractors,OU=User Accounts,DC=contoso,DC=com"**.
2. To restart the server normally after you perform the restore operation, type **bcdedit /deletevalue safeboot**, and then press ENTER.
3. Restart the server.

► **Task 5: Verify that the deleted data has been restored**

1. After the server restarts, log on as **Pat.Coleman** with the password **Pa\$\$w0rd**.
2. Run Active Directory Users and Computers as an administrator, with the user name **Pat.Coleman_Admin** and the password **Pa\$\$w0rd**.
3. On HQDC02, refresh the view of **Active Directory Users and Computers**. Verify that the **Contractors** OU has also been restored on this domain controller.

Results: After this exercise, you will have performed an authoritative restore of Active Directory data to recover from the accidental deletion of an OU.



Note: After completing this exercise, turn off all virtual machines and discard undo disks.

Lab Review Questions

Question: What type of domain controller and directory service backup plan do you have in place? What do you expect to put in place after having completed this lesson and this Lab?

Question: When you restore a deleted user (or an OU with user objects) using authoritative restore, will the objects be exactly the same as before? What attributes might not be the same?

MCT USE ONLY. STUDENT USE PROHIBITED

Module 14

Manage Multiple Domains and Forests

Contents:

Lesson 1: Configure Domain and Forest Functional Levels	14-4
Lab A: Raise Domain and Forest Functional Levels	14-16
Lesson 2: Manage Multiple Domains and Trust Relationships	14-23
Lab B: Administer a Trust Relationship	14-68

Module Overview

- Configure Domain and Forest Functional Levels
- Manage Multiple Domains and Trust Relationships

In Module 1, you learned that AD DS provides the foundation for an identity and access management solution, and you explored the creation of a simple AD DS infrastructure consisting of a single forest and a single domain. In subsequent modules, you mastered the details of managing an AD DS environment. Now you are ready to return to the highest level of an AD DS infrastructure and consider the model and functionality of your domains and forests. In this module, you will learn how to raise the domain and forest functionality levels within your environment, how to design the optimal AD DS infrastructure for your enterprise, how to migrate objects between domains and forests, and how to enable authentication and resources access across multiple domains and forests.

Objectives

After completing this module, you will be able to:

- Understand domain and forest functional levels.
- Raise domain and forest functional levels.
- Identify capabilities added by each functional level.

- Design an effective domain and tree structure for AD DS.
- Identify the role of the Active Directory Migration Tool, and the issues related to object migration and domain restructure.
- Understand trust relationships.
- Configure, administer, and secure trust relationships.

Lesson 1

Configure Domain and Forest Functional Levels

- Understand Functional Levels
- Domain Functional Levels
- Forest Functional Levels

As you introduce Windows Server® 2008 domain controllers into your domains and forest, you can begin to take advantage of new capabilities in Active Directory directory service. Domain and forest functional levels are operating modes of domains and forests, respectively. Functional levels determine the versions of Windows® that you can use as domain controllers and the availability of Active Directory features.

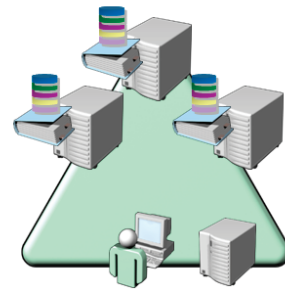
Objectives

After completing this lesson, you will be able to:

- Understand domain and forest functional levels.
- Raise domain and forest functional levels.
- Identify capabilities added by each functional level.

Understand Functional Levels

- Domain functional levels
- Forest functional levels
- New functionality requires that *domain controllers (DCs)* are running a particular version of Windows®
 - Windows 2000
 - Windows Server® 2003
 - Windows Server 2008
- Active Directory Domains and Trusts
- Cannot raise functional level while DCs are running previous versions of Windows
- Cannot add DCs running previous versions of Windows after raising functional level



Key Points

Functional levels are like switches that enable new functionality offered by each version of Windows. Windows Server 2003 added several features to Active Directory, and Windows Server 2008 continues the evolution of Active Directory Domain Services (AD DS). These features are not backward compatible, so if you have domain controllers (DCs) running Windows 2000 Server, you cannot enable the functionality offered by later versions of Windows; the newer functionality is disabled. Similarly, until all DCs are running Windows Server 2008, you cannot implement its enhancements to AD DS. Raising the functional level entails two major requirements:

1. All domain controllers must be running the correct version of Windows Server.
2. You must manually raise the functional level. It does not happen automatically.

Remember that *only domain controllers determine your ability to set a functional level*. You can have member servers and workstations running any version of Windows within a domain or forest at any functional level.

It's important to note that raising a functional level is a one-way operation: you cannot lower a domain or forest functional level. Therefore, once you have raised the domain functional level to Windows Server 2008, for example, you cannot at a later date add a domain controller running at Windows Server 2003 to the same domain.

It's also important to note that a forest can have domains running at different functional levels, but once the forest functional level has been raised, you cannot add a domain controller running a lower version of Windows to any domain in the forest.

Domain Functional Levels

- Windows 2000 Native
- Windows Server 2003
 - Domain controller rename
 - Default user and computer container redirection
 - lastLogonTimestamp attribute
 - Selective authentication on external trust relationships
- Windows Server 2008
 - Distributed File System Replication (DFS-R) of SYSVOL
 - Last interactive logon information
 - Fine-grained password policy
 - Advanced Encryption Services (AES 128 and AES 256) for Kerberos

Key Points

The domain functional level affects the Active Directory features available within the domain and determines the versions of Windows that are supported for domain controllers within the domain. In previous versions of Windows, domain functional levels and modes, as they were called in Windows 2000 Server, supported domain controllers running Windows NT® 4.0. That support has ended with Windows Server 2008. All domain controllers must be running Windows 2000 Server or later before you can add the first Windows Server 2008 domain controller to the domain. Windows Server 2008 Active Directory supports three domain functional levels:

- Windows 2000 Native
- Windows Server 2003
- Windows Server 2008

Windows 2000 Native

The Windows 2000 Native domain functional level is the lowest functional level that supports a Windows Server 2008 domain controller. The following operating systems are supported for domain controllers:

- Windows 2000 Server
- Windows Server 2003
- Windows Server 2008

If you have domain controllers running Windows 2000 Server or Windows Server 2003, or if you expect that you might add one or more domain controllers running those previous versions of Windows, you should leave the domain at the Windows 2000 Native functional level.

Windows Server 2003

After you have removed or upgraded all domain controllers running Windows 2000 Server, the domain functional level can be raised to Windows Server 2003. At this functional level, the domain can no longer support domain controllers running Windows 2000 Server, so all domain controllers must be running one of the following two operating systems:

- Windows Server 2003
- Windows Server 2008

The Windows Server 2003 domain functional level adds a number of new features to those offered at the Windows 2000 Native domain functional level. These features include the following:

- **Domain controller rename.** The domain management tool, netdom.exe, can be used to prepare for domain controller rename.
- **The lastLogonTimestamp attribute.** When a user or computer logs on to the domain, the lastLogonTimestamp attribute is updated with the logon time. This attribute is replicated within the domain.
- **The userPassword attribute.** Security principals in Active Directory include users, computers, and groups. A fourth object class, inetOrgPerson, is similar to a user and is used to integrate with several non-Microsoft directory services. At the Windows Server 2003 domain functional level, you can set the userPassword attribute as the effective password on both inetOrgPerson and user objects. This attribute is Write Only. You cannot retrieve the password from the userPassword attribute.

- **Default user and computer container redirection.** In Module 5, you learned that you can use the `redirusr.exe` and `redircmp.exe` commands to redirect the default user and computer containers. Doing so causes new accounts to be created in specific organizational units rather than in the Users and Computers containers.
- **Authorization Manager policies.** Authorization Manager, a tool that can be used to provide authorization by applications, can store its authorization policies in AD DS.
- **Constrained delegation.** Applications can take advantage of the secure delegation of user credentials by means of the Kerberos authentication protocol. Delegation can be configured to be allowed only to specific destination services.
- **Selective authentication.** In Lesson 2 of this module, you will learn to create trust relationships between your domain and another domain or forest. Selective authentication enables you to specify the users and groups from the trusted domain or forest who are allowed to authenticate to servers in your forest.
- **Read-Only domain controllers (RODCs).** A domain must be at the Windows Server 2003 domain functional level before an RODC can be added. In addition, you must run `adprep /rodcprep`, and at least one writable Windows Server 2003 domain controller must be in place.

Windows Server 2008

When all domain controllers are running Windows Server 2008, and you are confident that you will not need to add domain controllers running previous versions of Windows, you can raise the domain functional level to Windows Server 2008. The Windows Server 2008 domain functional level supports domain controllers running only one operating system:

- Windows Server 2008

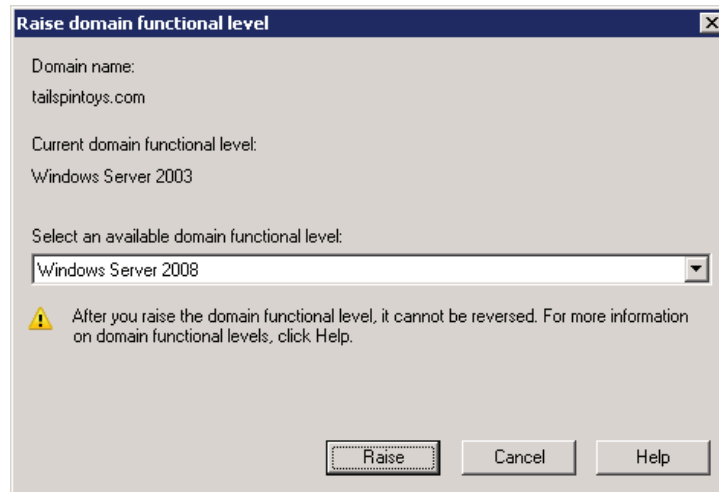
The Windows Server 2008 domain functional level adds four domain-wide features to AD DS:

- **DFS-R replication of SYSVOL.** In Module 11, you learned to configure SYSVOL so that it is replicated with DFS-R instead of File Replication Service (FRS). DFS-R provides a more robust and detailed replication of SYSVOL contents.

- **Advanced Encryption Services.** You can increase the security of authentication with Advanced Encryption Services (AES 128 and AES 256) support for the Kerberos protocol. AES replaces the RC4-HMAC (Hash Message Authentication Code) encryption algorithm.
- **Last interactive logon information.** When a user logs on to the domain, several attributes of the user object are updated with the time, the workstation to which the user logged on, and the number of failed logon attempts since the last logon.
- **Fine-grained password policies.** In Module 8, you learned about fine-grained password policies, which enable you to specify unique password policies for users or groups in the domain.

Raising the Domain Functional Level

You can raise the domain functional level after all domain controllers are running a supported version of Windows and when you are confident you will not have to add domain controllers running unsupported versions of Windows. To raise the domain functional level, open the Active Directory Domains and Trusts snap-in, right-click the domain, and choose Raise Domain Functional Level. The dialog box shown here enables you to select a higher domain functional level.





Note: One-way operation. Raising the domain functional level is a one-way operation. You cannot roll back to a previous domain functional level.

You can also raise the domain functional level by using the Active Directory Users and Computers snap-in. Right-click the domain and choose Raise Domain Functional Level or right-click the root node of the snap-in and choose Raise Domain Functional Level from the All Tasks menu.

Forest Functional Levels

- Windows 2000
- Windows Server 2003
 - Forest trusts
 - Domain rename
 - Linked-value replication
 - Support for Read-Only domain controllers (RODCs)
 - Requires adprep /rodcprep and one writeable Windows Server 2008 DC
 - Improved Knowledge Consistency Checker (KCC) algorithms and scalability
 - Conversion of inetOrgPerson objects to user objects
 - Support for dynamicObject auxiliary class
 - Support for application basic groups and Lightweight Directory Access Protocol (LDAP) query groups
 - Deactivation and redefinition of attributes and object classes
- Windows Server 2008
 - No new features; sets minimum level for all new domains

Key Points

Just as domain functional levels enable certain domain-wide functionality and determine the versions of Windows that are supported for domain controllers in the domain, forest functional levels enable forest-wide functionality and determine the operating systems supported for domain controllers in the entire forest. Windows Server 2008 Active Directory supports three forest functional levels:

- Windows 2000
- Windows Server 2003
- Windows Server 2008

Each functional level is described in the following sections.

Windows 2000

The Windows 2000 forest functional level is the baseline, default functional level. At the Windows 2000 functional level, domains can be running at any supported domain functional level:

- Windows 2000 Native
- Windows Server 2003
- Windows Server 2008

You can raise the forest functional level after all domains in the forest have been raised to the equivalent domain functional level.

Windows Server 2003

After all domains in the forest are at the Windows Server 2003 domain functional level, and when you do not expect to add any new domains with Windows 2000 Server domain controllers, you can raise the forest functional level to Windows Server 2003. At this forest functional level, domains can be running at the following domain functional levels:

- Windows Server 2003
- Windows Server 2008

The following features are enabled at the Windows Server 2003 forest functional level:

- **Forest trusts.** In Lesson 2, you will learn to create trust relationships between forests.
- **Domain rename.** You can rename a domain within a forest.
- **Linked-value replication.** At the Windows 2000 forest functional level, a change to a group's membership results in the replication of the entire multivalued member attribute of the group. This can lead to increased replication traffic on the network and the potential loss of membership updates when a group is changed concurrently at different domain controllers. It also leads to a recommended cap of 5,000 members in any one group. Linked-value replication, enabled at the Windows Server 2003 forest functional level, replicates an individual membership change rather than the entire member attribute. This uses less bandwidth and prevents you from losing updates when a group is changed concurrently at different domain controllers.

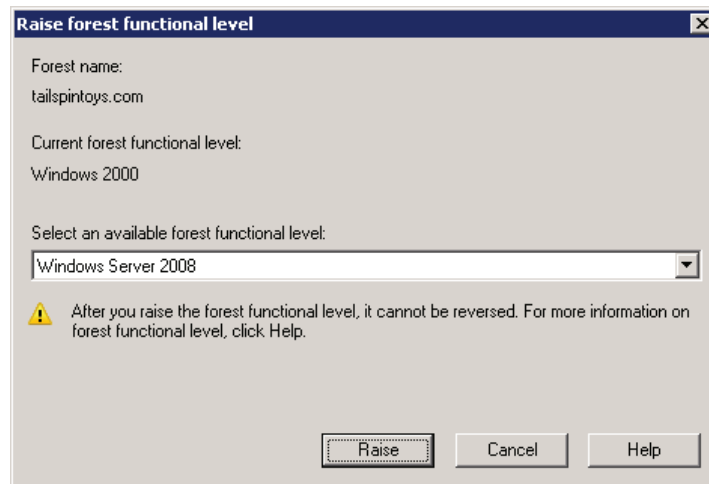
- **Support for Read-Only domain controllers (RODCs).** Module 8 discussed RODCs. RODCs are supported at the Windows Server 2003 forest functional level. Of course, the RODC itself must be running Windows Server 2008.
- **Improved Knowledge Consistency Checker (KCC) algorithms and scalability.** The intersite topology generator (ISTG) uses algorithms that enable AD DS to support replication in forests with more than 100 sites. At the Windows 2000 forest functional level, you must manually intervene to create replication topologies for forests with hundreds of sites. Additionally, the election of the ISTG uses an algorithm that is more efficient than at the Windows 2000 forest functional level.
- **Conversion of inetOrgPerson objects to user objects.** You can convert an instance of an inetOrgPerson object, used for compatibility with certain non-Microsoft directory services, into an instance of class user. You can also convert a user object to an inetOrgPerson object.
- **Support for dynamicObject auxiliary class.** The schema allows instances of the dynamic auxiliary class in domain directory partitions. This object class can be used by certain applications and by developers.
- **Support for application basic groups and LDAP query groups.** Two new group types, called application basic groups and LDAP query groups, can be used to support role-based authorization in applications that use Authorization Manager.
- **Deactivation and redefinition of attributes and object classes.** Although you cannot delete an attribute or object class in the schema, at the Windows Server 2003 functional level, you can deactivate or redefine attributes or object classes.

Windows Server 2008

The Windows Server 2008 forest functional level does not add new forest-wide features. However, after the forest is configured to the Windows Server 2008 forest functional level, new domains added to the forest will operate at Windows Server 2008 domain functional level by default. At this forest functional level, all domains must be at the Windows Server 2008 domain functional level, which means that all domain controllers must be running Windows Server 2008.

Raising the Forest Functional Level

Use the Active Directory Domains and Trusts snap-in to raise the forest functional level. Right-click the root node of the snap-in, Active Directory Domains and Trusts, and choose Raise Forest Functional Level. The dialog box shown here enables you to choose a higher forest functional level.



Raise the forest functional level only when you are confident that you will not add new domains at unsupported domain functional levels. You cannot roll back to a previous forest functional level after raising it.

Lab A: Raise Domain and Forest Functional Levels

- Exercise 1: Raise the Domain Functional Level to Windows Server 2003
- Exercise 2: Raise the Forest Functional Level to Windows Server 2003
- Exercise 3: Raise the Domain Functional Level to Windows Server 2008

Logon information

Virtual machine	6425B-TSTDC01-A
Logon user name	Sara.Davis
Administrative user name	Sara.Davis_Admin
Password	Pa\$\$w0rd

Estimated time: 30 minutes

Scenario

You are the domain administrator of Tailspin Toys. A branch office was the last location with a Windows 2000 domain controller, and you have just upgraded it to Windows Server 2008. You want to take advantage of functionality provided by higher domain and forest functional levels.

Exercise 1: Raise the Domain Functional Level to Windows Server 2003

In this exercise, you will attempt to take advantage of capabilities supported at the Windows Server 2003 domain functional level. You will see that these capabilities are not supported at lower domain functional levels. You will then raise the domain functional level. Finally, you will test the advanced capabilities to verify that they are now supported.

The main tasks for this exercise are as follows:

1. Prepare for the lab.
2. Confirm that the current domain functional level is Windows 2000 Native.
3. Experience functionality not supported by the Windows 2000 Native domain functional level.
4. Raise the domain functional level to Windows Server 2003.
5. Verify functionality supported by the Windows Server 2003 domain functional level.

► Task 1: Prepare for the lab

- Start 6425B-TSTDC01-A and log on as **Sara.Davis** with the password **Pa\$\$w0rd**.

► Task 2: Confirm that the current domain functional level is Windows 2000 Native

1. On TSTDC01, run **Active Directory Domains and Trusts** as an administrator, with the user name **Sara.Davis_Admin** and the password **Pa\$\$w0rd**
2. Confirm that the current domain functional level is Windows 2000 Native, but *do not raise the functional level*. Instead, cancel out of the dialog box.

► **Task 3: Experience functionality not supported by the Windows 2000 Native domain functional level**

1. Run Command Prompt as an administrator, with the user name **Sara.Davis_Admin** and the password **Pa\$\$w0rd**.
2. Type **redircmp.exe "ou=Client Computers,dc=tailspintoys,dc=com"** and press ENTER. A message appears indicating that redirection was not successful. This is because the domain functional level is not at least Windows Server 2003.
3. Type **redirusr.exe "ou=User Accounts,dc=tailspintoys,dc=com"** and press ENTER. A message appears indicating that redirection was not successful. This is because the domain functional level is not at least Windows Server 2003.

► **Task 4: Raise the domain functional level to Windows Server 2003**

- In **Active Directory Domains and Trusts**, raise the domain functional level to Windows Server 2003.

► **Task 5: Verify functionality supported by Windows Server 2003 domain functional level**

1. Run the Command Prompt as an administrator, with the user name **Sara.Davis_Admin** and the password **Pa\$\$w0rd**.
2. Type **redircmp.exe "ou=Client Computers,dc=tailspintoys,dc=com"** and press ENTER. A message appears indicating that redirection was successful.
3. Type **redirusr.exe "ou=User Accounts,dc=tailspintoys,dc=com"** and press ENTER. A message appears indicating that redirection was successful.

Results: After this exercise, you will have raised the domain functional level to Windows Server 2003 and confirmed that new functionality is enabled.

Exercise 2: Raise the Forest Functional Level to Windows Server 2003

In this exercise, you will attempt to take advantage of capabilities supported at the Windows Server 2003 forest functional level. You will see that these capabilities are not supported at lower forest functional levels. You will then raise the forest functional level. Finally, you will test the advanced capabilities to verify that they are now supported.

The main tasks for this exercise are as follows:

1. Confirm that the current forest functional level is Windows 2000 Native.
2. Experience functionality not supported by the Windows 2000 Native forest functional level.
3. Raise the forest functional level to Windows Server 2003.
4. Verify functionality supported by the Windows Server 2003 forest functional level.

► Task 1: Confirm that the current forest functional level is Windows 2000 Native

1. On TSTDC01, run **Active Directory Domains and Trusts** as an administrator, with the user name **Sara.Davis_Admin** and the password **Pa\$\$w0rd**.
2. Confirm that the current domain functional level is Windows 2000 Native, but *do not raise the functional level*. Instead, cancel out of the dialog box.

► Task 2: Experience functionality not supported by the Windows 2000 Native forest functional level

1. Run **Active Directory Users and Computers** as an administrator, with the user name **Sara.Davis_Admin** and the password **Pa\$\$w0rd**.
2. Right-click the **Domain Controllers** OU and attempt to create a new Read-Only domain controller account. Accept all defaults in the Active Directory Domain Services Installation Wizard.

You are prevented from creating an RODC account, and you are informed that the forest functional level must be Windows Server 2003 or higher.

- ▶ **Task 3: Raise the forest functional level to Windows Server 2003**
 - In **Active Directory Domains and Trusts**, raise the forest functional level to Windows Server 2003.

- ▶ **Task 4: Verify functionality supported by the Windows Server 2003 forest functional level**
 - In **Active Directory Users and Computers**, create a Read-Only domain controller account named **TSTDC03** in the **Domain Controllers** OU. Accept all default values in the Active Directory Domain Services Installation Wizard.

Exercise 3: Raise the Domain Functional Level to Windows Server 2008

In this exercise, you will attempt to take advantage of capabilities supported at the Windows Server 2008 domain functional level. You will see that these capabilities are not supported at lower domain functional levels. You will then raise the domain functional level. Finally, you will test the advanced capabilities to verify that they are now supported.

The main tasks for this exercise are as follows:

1. Confirm that the current domain functional level is lower than Windows Server 2008.
2. Confirm that DFS-R is not available at domain functional levels lower than Windows Server 2008.
3. Raise the domain functional level.
4. Confirm that DFS-R replication is available at the Server 2008 domain functional level.

► **Task 1: Confirm that the current domain functional level is lower than Windows Server 2008**

1. On TSTDC01, run **Active Directory Domains and Trusts** as an administrator, with the user name **Sara.Davis_Admin** and the password **Pa\$\$w0rd**.
2. Confirm that the current domain functional level is Windows Server 2003, but *do not raise the functional level*. Instead, cancel out of the dialog box.

► **Task 2: Confirm that DFS-R replication is not available at domain functional levels lower than Windows Server 2008**

1. Run the Command Prompt as an administrator, with the user name **Sara.Davis_Admin** and the password **Pa\$\$w0rd**.
2. Type **dfsrmig /getglobalstate** and press ENTER. A message appears informing you that dfsrmig is supported only on domains at the Windows Server 2008 functional level.

► **Task 3: Raise the domain functional level**

- In **Active Directory Domains and Trusts**, raise the domain functional level to Windows Server 2008.
- Close Active Directory Domains and Trusts.

► **Task 4: Confirm that DFS-R replication is available at the Windows Server 2008 domain functional level**

- Switch to the command prompt. Type `dfsrmig /getglobalstate` and then press ENTER. A message appears informing you that DFS-R migration has not yet been initialized. This indicates that the feature is now available, but has not yet been initialized.

Results: After this exercise, you will have raised the domain functional level to Windows Server 2008 and confirmed that new functionality is available.



Note: Do not shut down the virtual machines once you are finished with this lab as the settings you have configured here will be used in subsequent labs.

Lab Review Questions

Question: Can you raise the domain functional level to Windows Server 2008 when your Microsoft Exchange server is still running Windows Server 2003?

Question: Can you raise the domain functional level of a domain to Windows Server 2008 when other domains contain domain controllers running Windows Server 2003?

Lesson 2

Manage Multiple Domains and Trust Relationships

- Define Your Forest and Domain Structure
- Move Objects Between Domain and Forests
- Understand Trust Relationships
- Characteristics of Trust Relationships
- How Trusts Work Within a Forest
- Demonstration: Create a Trust
- Shortcut Trusts
- External Trusts and Realm Trusts
- Forest Trusts
- Administer Trust Relationships
- Domain Quarantine
- Resource Access for Users from Trusted Domains

Previous modules in this course have prepared you to configure, administer, and manage a single domain. However, your enterprise's Active Directory infrastructure might include a multidomain forest or even more than one forest. You might need to move objects between domains or restructure your domain model entirely. You might also encounter requirements to enable authentication and access to resources across domains and forests. In this lesson, you will learn the skills required to support multiple domains and forests.

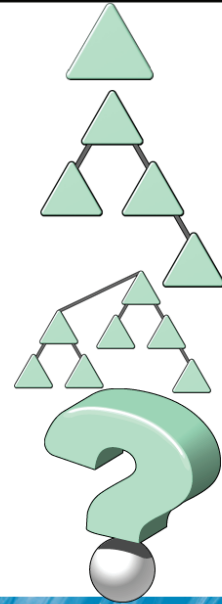
Objectives

After completing this lesson, you will be able to:

- Design an effective domain and tree structure for AD DS.
- Identify the role of the Active Directory Migration Tool and the issues related to object migration and domain restructure.
- Understand trust relationships.
- Configure, administer, and secure trust relationships.

Define Your Forest and Domain Structure

- Dedicated forest root domain
- Single-domain forest
 - Single domain partition, replicated to all DCs
 - Single Kerberos policy
 - Single Domain Name System (DNS) namespace
- Multiple-domain forest
 - Increased hardware and administrative cost
 - Increased security risk
- Multiple trees
- Multiple forests

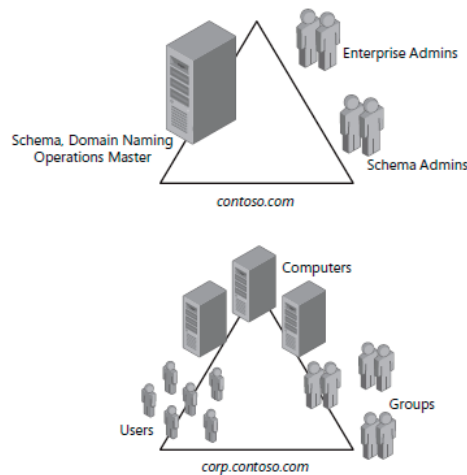


Key Points

With the perspective you have gained from the previous modules of this course, you are prepared to consider the design of your Active Directory forest, trees, and domains. Interestingly, the best practices guidance regarding forest and domain structure has evolved as enterprises around the world have put Active Directory into production in every conceivable configuration and as the Active Directory feature set has grown.

Dedicated Forest Root Domain

In the early days of Active Directory, the recommendation was to create a dedicated forest root domain. You'll recall from Module 1 that the forest root domain is the first domain in the forest. A dedicated forest root domain's exclusive purpose is to administer the forest infrastructure. It contains, by default, the single master operations for the forest. It also contains highly sensitive groups, such as Enterprise Admins and Schema Admins, that can have a far-reaching impact on the forest. The theory was that the dedicated forest root would enhance the security around these forest-wide functions. The dedicated forest root domain would also be less likely to become obsolete and would provide easier transfer of ownership. Underneath the dedicated forest root, according to early recommendations, would be a single global child domain with all the objects one thinks of in a domain: users, groups, computers, and so on. The structure would look something like the figure below.



A Single-Domain Forest



Note: No longer recommended for most enterprises. Implementation of a dedicated forest root domain is no longer recommended for most enterprises. A single domain forest is the most common design recommendation. There is no single design that is appropriate for every organization, so you must examine the characteristics of your enterprise against the design criteria presented later in this lesson.

After ten years on the market, Active Directory is better understood, and the former recommendation no longer applies. For most organizations, building a forest with a single domain is now recommended. The experience and knowledge that have led to the change in guidance include the following points:

- There are risks and costs associated with any multidomain forest, as you'll learn later in this lesson. A single domain bears the lowest hardware and support cost and reduces certain risks.
- There are not yet tools that enable an enterprise to perform pruning and grafting of Active Directory trees. In other words, you cannot break a domain off of your tree and transplant it in the forest of another enterprise. If that were possible, a dedicated forest root that you could maintain while transferring domains in and out of your forest would make more sense.
- You can implement least-privilege security within a single domain that is at least as secure as, if not more secure than, security in a forest with a dedicated forest root and a child domain.

Therefore, when you consider your domain design, you should begin with the assumption that you will have a single domain in your forest.

Multiple-Domain Forest

In some scenarios, a multiple-domain forest is required. The important point to remember is that you should never create a multiple-domain forest simply to reflect the organizational structure of your business. That structure—the business units, divisions, departments, and offices—will change over time. The logical structure of your directory service should not be dependent solely on organizational characteristics.

Instead, your domain model should be derived from the characteristics of domains themselves. There are certain properties of a domain that affect all objects within the domain, and if that consistent effect is not appropriate for your business requirements, you must create additional domains. A domain is characterized by the following:

- **A single domain partition, replicated to all domain controllers.** The domain naming context contains the objects for users, computers, groups, policies, and other domain resources. It is replicated to every domain controller in the domain. If you need to partition replication for network topology considerations, you must create separate domains. Consider, however, that Active Directory replication is extremely efficient and can support large domains over connections with minimal bandwidth.

If there are legal or business requirements that restrict replication of certain data to locations where you maintain domain controllers, you need to either avoid storing that data in the domain partition or create separate domains to segregate replication. In such cases, you should also ensure that the global catalog (GC) is not replicating that data.

Because legal and technical issues surrounding replication tend to affect the global catalog and potentially other data stores, organizations with these concerns are increasingly turning to multiple forest models.

- **A single Kerberos policy.** The default Kerberos policy settings in AD DS are sufficient for most enterprises. If, however, you need distinct Kerberos policies, you will require distinct domains.
- **A single DNS namespace.** An Active Directory domain has a single DNS domain name. If you need multiple domain names, you would need multiple domains. However, give serious consideration to the costs and risks of multiple domains before modeling your directory service domains to match arbitrary DNS name requirements.

In domains running domain functional levels lower than Windows Server 2008, a domain can support only one password and account lockout policy. Therefore, in prior versions of Windows, an organization requiring multiple password policies would need multiple domains to support that requirement. This is no longer the case in Windows Server 2008, which, at the Windows Server 2008 domain functional level, can support *fine-grained password policies*.

Adding domains to a forest increases administrative and hardware costs. Each domain must be supported by at least two domain controllers, which must be backed up, secured, and managed. Even more domain controllers might be required to support cross-domain resource access in a geographically distributed enterprise. Additional domains can result in the need to move users between domains, which is more complicated than moving users between OUs. Group Policy objects and access control settings that are common for the enterprise will have to be duplicated for each domain.

These are just a few of the costs associated with a multiple-domain environment. There are also *security risks involved with having multiple domains*. Most of these risks relate to the fact that a domain is not a security boundary—a forest is the security boundary. Within a forest, service administrators can cause forest-wide damage. There are several categories of vulnerability whereby a compromised administrative account, or an administrator with bad intent, could cause denial of service or damage to the integrity of the forest.

For example, an administrator in any domain can create universal groups, the membership of which is replicated to the GC. By creating multiple universal groups and overpopulating the member attribute, excessive replication could lead to denial of service on domain controllers acting as domain controllers in other domains. An administrator in any domain could also restore an outdated backup of the directory, which could corrupt the forest.

Additional Reading

- For more information about the security considerations related to domain and forest design, see “Best Practices for Delegating Active Directory Administration” at: <http://go.microsoft.com/fwlink/?LinkId=168833>

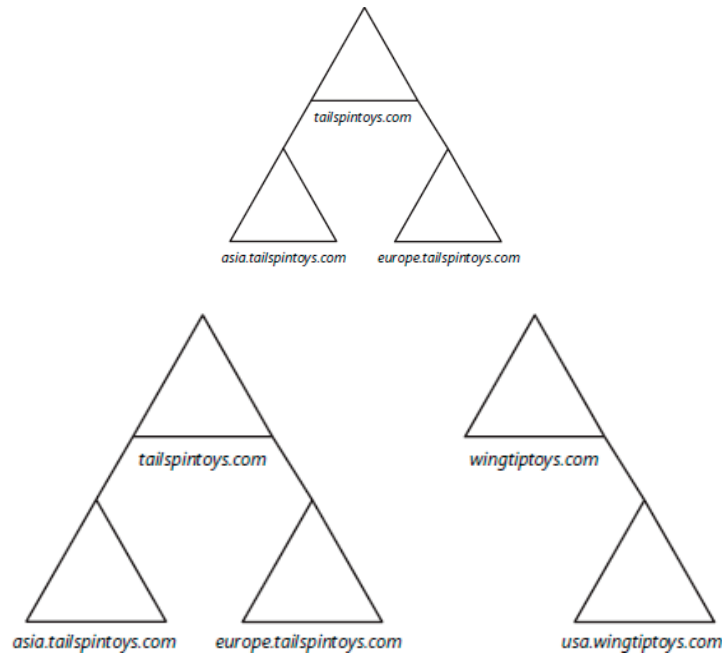


Important: Given the costs and risks of multiple domains, the construction of a single-domain forest is highly recommended. The most common driver to multiple-domain forests is a significant requirement related to the replication of the domain naming context.

In a multidomain forest, it might make sense to create a dedicated forest root domain as an empty domain to act as the trust root for the forest. Trust roots will be discussed later in this lesson.

Multiple Trees

Remember that a tree is defined as a contiguous DNS namespace. If you have more than one domain, you can decide whether those domains share a contiguous DNS namespace and form a single tree, as shown in the first figure here, or are in a noncontiguous DNS namespace, thus forming multiple trees, as shown in the second figure.



Multiple Forests

A forest is an instance of Active Directory. All domains and domain controllers in a forest share replicas of the schema and configuration. Domain controllers that are GC servers host partial attribute sets for all objects in other domains in the forest. Domains in a forest share transitive, two-way trusts, meaning that all users in the domain belong to the Authenticated Users special identity in every domain. The forest's Enterprise Admins, Schema Admins, and Administrators groups in the forest root domain wield significant power over all objects in the forest.

If any of these characteristics of a forest are at odds with your business requirements, you might need multiple forests. In fact, given the market's current concerns with security, many consultants are recommending that organizations design either a single-domain forest or use multiple forests. Cross-forest trusts, discussed later in this lesson, and Active Directory Federation Services (AD FS) make it easier to manage authentication in multiple-forest enterprises.

Additional Reading

- For more information about planning the architecture of an AD DS enterprise see <http://go.microsoft.com/fwlink/?LinkId=168826>

Move Objects Between Domains and Forests

- Inter-forest migration: Copy objects
- Intra-forest migration: Move objects
- Active Directory Migration Tool (ADMT)
 - Console, command line, scriptable APIs
 - “Simulation” mode: Test the migration settings and migrate later
- Security identifiers, security descriptors, and migration
 - sIDHistory
 - Security Translation: NTFS, printers, SMB shares, registry, rights, profiles, group memberships
- Group membership

Key Points

In multidomain scenarios, you might need to move users, groups, or computers between domains or forests to support business operations. You might need to move large quantities of users, groups, or computers between domains or forests to implement mergers and acquisitions or to restructure your domain model.

In each of these tasks, you move or copy the accounts from one domain (the source domain) into another domain (the target domain). Domain restructuring terminology, concepts, and procedures apply to inter-forest migration between a Windows NT 4.0 or Active Directory source domain and an Active Directory target domain in a separate forest and to intra-forest migration—that is, the restructuring or moving of accounts between domains in the same forest.

An inter-forest domain restructure preserves the existing source domain and clones (or copies) accounts into the target domain. This nondestructive method enables an enterprise to time the transition and even migrate in phases. Operations go uninterrupted because both domains are maintained in parallel to support operations for users in either domain. This method also provides a level of rollback because the original environment remains unaltered in any significant way. After the migration is complete, you can simply decommission the source domain by moving any remaining accounts, member servers, and workstations into the new domain and then taking source DCs offline, at which point you can redeploy those DCs for roles in the new domain.

An intra-forest migration involves moving objects from the source domain to the target domain without decommissioning the source domain. After you have migrated objects, you can restructure your domains to consolidate operations and build a domain and OU structure that more accurately reflects your administrative model. Many organizations consolidate multiple domains into one Active Directory domain. This consolidation can result in cost savings and simplified administration by reducing administrative complexity and the cost of supporting your Active Directory environment.

Understanding the ADMT

The Active Directory Migration Tool version 3 (ADMT v3) can perform object migration and security translation tasks. You can download the ADMT v3 from <http://go.microsoft.com/fwlink/?LinkID=75627>. On that page, you will also find a detailed guide to the tool.

You can use the ADMT to migrate objects between a source and a target domain. The migration can take place between domains in the same forest (an intra-forest migration) or between domains in different forests (an inter-forest migration). The ADMT provides wizards that automate migration tasks such as migrating users, groups, service accounts, computers, and trusts, and performing security translation. You can perform these tasks by using the ADMT console or the command line, at which you can simplify and automate the `admt.exe` command with option files that specify parameters for the migration task. Then, with a simple text file, you can list objects to migrate rather than having to enter each object on the command line. The ADMT also provides interfaces that enable you to script migration tasks with languages such as Microsoft Visual Basic® Scripting Edition (VBScript). Run the ADMT console and open the online Help function for details about how to use the ADMT from the command line and about scripting the ADMT.

When you are performing migration tasks, the ADMT enables you to simulate the migration so that you can evaluate potential results and errors without making changes to the target domain. Wizards provide the Test The Migration Settings And Migrate Later option. You can then configure the migration task, test the settings, and review the log files and wizard-generated reports. After identifying and resolving any problems, you can perform the migration task. You will repeat this process of testing and analyzing results as you migrate users, groups, and computers and perform security translations.

Security Identifiers and Migration

Uninterrupted resource access is the primary concern during any migration. Further, to perform a migration, you must be comfortable with the concepts of security identifiers (SIDs), tokens, access control lists (ACLs), and *sidHistory*.

SIDs are domain-unique values that are assigned to the accounts of security principals—users, groups, and computers, for example—when those accounts are created. When a user logs on, a token is generated that includes the primary SID of the user account and the SIDs of groups to which the user belongs. The token thus represents the user with all the SIDs associated with the user and the user's group memberships.

Resources are secured using a security descriptor (SD) that describes the permissions, ownership, extended rights, and auditing of the resource. Within the SD are two ACLs. The system ACL (SACL) describes auditing. The discretionary ACL (DACL) describes resource access permissions. Many administrators and documents refer to the DACL as the ACL. The DACL lists permissions associated with security principals. Within the list, individual access control entries (ACEs) link a specific permission with the SID of a security principal. The ACE can be an Allow or Deny permission.

When a user attempts to access a resource, the Local Security Authority Subsystem (LSASS) compares the SIDs in the user's token against the SIDs in the ACEs in the resource's ACL.

When you migrate accounts to a new domain, the accounts are copied or cloned from the source domain to the target domain. New SIDs are generated for the accounts in the target domain, so the SIDs of new accounts will not be the same as the SIDs of the accounts in the source domain. That is, even though the cloned accounts have the same name and many of the same properties, because the SIDs are different, the accounts are technically different and will not have access to resources in the source domain. You have two ways to address this problem: *sidHistory* or security translation.

sIDHistory

Enterprises typically prefer to take advantage of the sIDHistory attribute to perform effective domain restructuring. The capitalization, which appears odd, reflects the capitalization of the attribute in the Active Directory schema. An Active Directory security principal (which can be a user, group, or computer) has a principal SID and a sIDHistory attribute, which can contain one or more SIDs that are also associated with the account. When an account is copied to a target domain, the unique principal SID is generated by Active Directory in the target domain. Optionally, the sIDHistory attribute can be loaded with the SID of the account in the source domain. When a user logs on to an Active Directory domain, the user's token is populated with the principal SID and the sIDHistory of the user account and groups to which the user belongs. The LSASS uses the SIDs from the sIDHistory just like any other SID in the token to maintain the user's access to resources in the source domain.

Security Translation

Security translation is the process of examining each resource's SD, including its ACLs, identifying each SID that refers to an account in the source domain, and replacing that SID with the SID of the account in the target domain. The process of re-mapping ACLs (and other elements in the SD) to migrated accounts in the target domain is also called re-ACLing. As you can imagine, security translation or re-ACLing would be a tedious process to perform manually in anything but the simplest environment. Migration tools such as the ADMT automate security translation. The ADMT can translate the SDs and policies of resources in the source domain to refer to the corresponding accounts in the target domain. Specifically, the ADMT can translate:

- File and folder permissions
- Printer permissions
- Share permissions
- Registry permissions
- User rights
- Local profiles, which involves changing file, folder, and registry permissions
- Group memberships

In most domain restructuring and migration projects, sIDHistory is used to maintain access and functionality during the migration; then, security translation is performed.

Additional Reading

- For more information about domain migration, SIDs, and SID history, see the “Domain Migration Cookbook” at: <http://go.microsoft.com/fwlink/?LinkId=168829>

Group Membership

The final concern related to resource access is that of group membership. Global groups can contain members only from the same domain. Therefore, if you clone a user to the target domain, the new user account cannot be a member of the global groups in the source domain to which the source user account belonged.

To address this issue in an inter-forest migration, first migrate global groups to the target domain. Those global groups will maintain the source groups’ SIDs in their `sidHistory` attributes, thus maintaining resource access. Then, migrate users. As you migrate users, the ADMT evaluates the membership of the source account and adds the new account to the same group in the target domain. If the group does not yet exist in the target domain, the ADMT can create it automatically. In the end, the user account in the target domain will belong to global groups in the target domain. The user and the user’s groups will contain the SIDs of the source accounts in their `sidHistory` attributes. Therefore, the user will be able to access resources in the source domain that have permissions assigned to the source accounts.

In an intra-forest migration, the process works differently. A global group is created in the target domain as a universal group so that it can contain users from both the source and the target domain. The new group gets a new SID, but its `sidHistory` is populated with the SID of the global group in the source domain, thereby maintaining resource access for the new group. After all users have been migrated from the source to the target domain, the scope of the group is changed back to global.

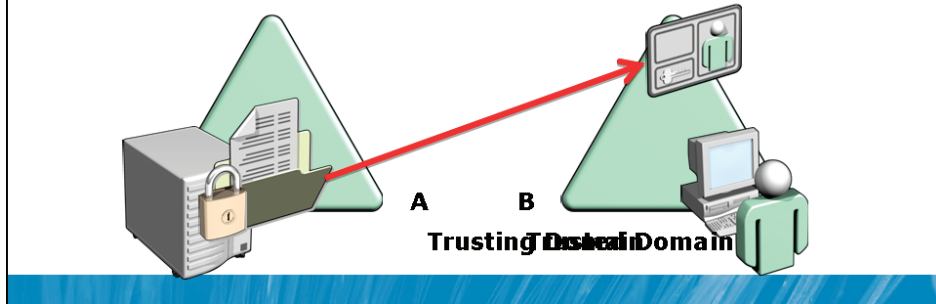
Other Migration Concerns

There are a number of issues that you must address in planning for and executing the migration of objects between domains and forests. Each of the concerns is detailed in the ADMT user guide, available from the ADMT download page listed earlier. Among the greatest concerns are:

- **Password migration.** The ADMT supports migrating user passwords; however, it cannot confirm that those passwords comply with the policies of the target domain regarding password length and complexity. Nonblank passwords will migrate regardless of the target domain password policy, and users will be able to log on with those passwords until they expire, at which time a new, compliant password must be created. If you are concerned about locking down the environment at the time of migration, this might not be a satisfactory process. You might instead want to let the ADMT configure complex passwords, or script an initial password, and then force the user to change the password at the first logon.
- **Service accounts.** Services on domain computers might use domain-based user accounts for authentication. As those user accounts are migrated to the target domain, services must be updated with the new service account identity. The ADMT automates this process.
- **Objects that cannot be migrated.** Some objects cannot be seamlessly migrated. The ADMT cannot migrate built-in groups such as Domain Admins or the domain local Administrators group. The user guide provides details for working around this limitation.

Understand Trust Relationships

- Extends concept of trusted identity store to another domain
- Trusting domain (with the resource) trusts the identity store and authentication services of the trusted domain.
- A trusted user can authenticate to, and be given access to resources in, the trusting domain
- Within a forest, each domain trusts all other domains
- Trust relationships can be established with external domains



Key Points

Whenever you are implementing a scenario involving two or more AD DS domains, it is likely that you will be working with trust relationships, or trusts. It is important that you understand the purpose, functionality, and configuration of trust relationships.

Trust Relationships within a Domain

In Module 1, you were guided through what happens when a domain member server or workstation joins a domain. While in a workgroup, the computer maintains an identity store in the security accounts manager (SAM) database, it authenticates users against that identity store, and it secures system resources only with identities from the SAM database. When the computer joins a domain, it forms a trust relationship with the domain. The effect of that trust is that the computer allows users to be authenticated not by the local system and its local identity store but by the authentication services and identity store of the domain: AD DS. The domain member also allows domain identities to be used to secure system resources. For example, Domain Users is added to the local Users group, giving Domain Users the right to log on locally to the system. Also, domain user and group accounts can be added to ACLs on files, folders, registry keys, and printers on the system. All domain members have similar trust relationships with the domain, enabling the domain to be a central store of identity and a centralized service providing authentication.

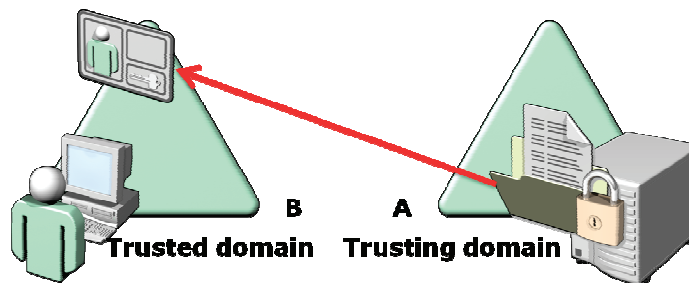
Trust Relationships between Domains

With that foundation, you can extend the concept of trust relationships to other domains. A trust relationship between two domains enables one domain to trust the authentication service and the identity store of another domain and to use those identities to secure resources. In effect, a trust relationship is a logical link established between domains to enable pass-through authentication.

There are two domains in every trust relationship: a trusting domain and a trusted domain. The trusted domain holds the identity store and provides authentication for users in that identity store. When a user in the directory of the trusted domain logs on to or connects to a system in the trusting domain, the trusting domain cannot authenticate that user because the user is not in its data store, so it passes the authentication to a domain controller in the trusted domain. The trusting domain, therefore, trusts the trusted domain to authenticate the identity of the user. The trusting domain extends trust to the authentication services and the identity store of the trusted domain.

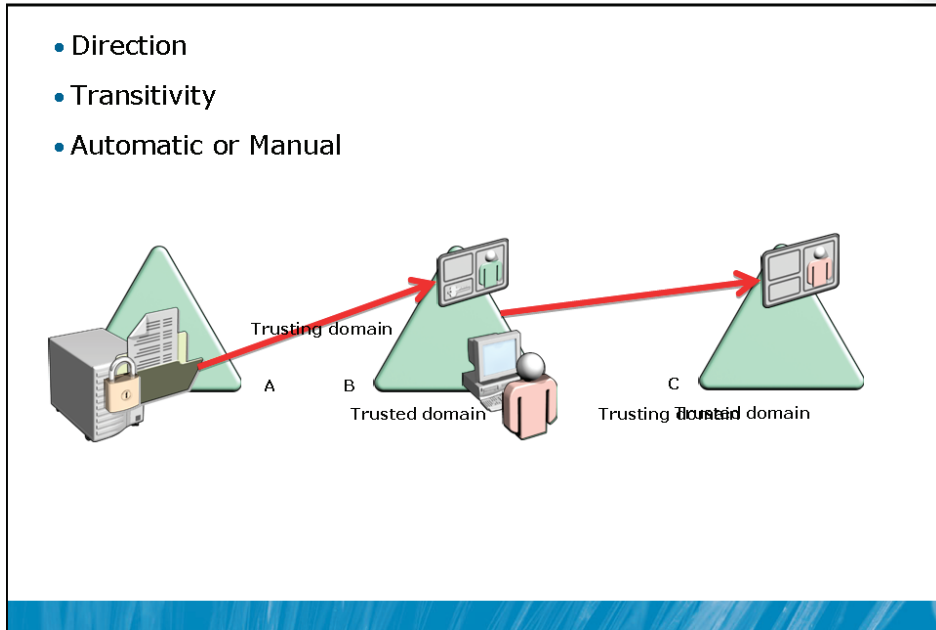
Because the trusting domain trusts the identities in the trusted domain, the trusting domain can use the trusted identities to grant access to resources. Users in a trusted domain can be given user rights such as the right to log on to workstations in the trusting domain. Users or global groups in the trusted domain can be added to domain local groups in the trusting domain. Users or global groups in the trusted domain can be given permissions to shared folders by adding the identities to ACLs in the trusting domain.

The terminology can be confusing, and it is often easier to understand trust relationships when you look at an illustration. The diagram here shows a simple trust relationship. Domain A trusts Domain B. That makes Domain A the trusting domain and Domain B the trusted domain. If a user in Domain B connects to or logs on to a computer in Domain A, Domain A will pass the authentication request to a domain controller in Domain B. Domain A can also use the identities from Domain B—users and groups, for example—to grant user rights and resource access in Domain A. A user or group in Domain B can, therefore, be added to an ACL on a shared folder in Domain A. A user or group in Domain B can also be added to a domain local group in Domain A.



Characteristics of Trust Relationships

- Direction
- Transitivity
- Automatic or Manual



Key Points

Trust relationships between domains can be characterized by three attributes of the trust: direction, transitivity, and automatic or manual.

Direction

A trust relationship can be one-way or two-way. In a one-way trust, such as the trusts illustrated above, users in the trusted domain can be given access to resources in the trusting domain, but users in the trusting domain cannot be given access to resources in the trusted domain. In most cases, you can create a second, one-way trust in the opposite direction to achieve that goal. For example, you can create a second trust relationship in which Domain B trusts Domain A. Some trust relationships are by nature two-way. In a two-way trust, both domains trust the identities and authentication services of the other domain.

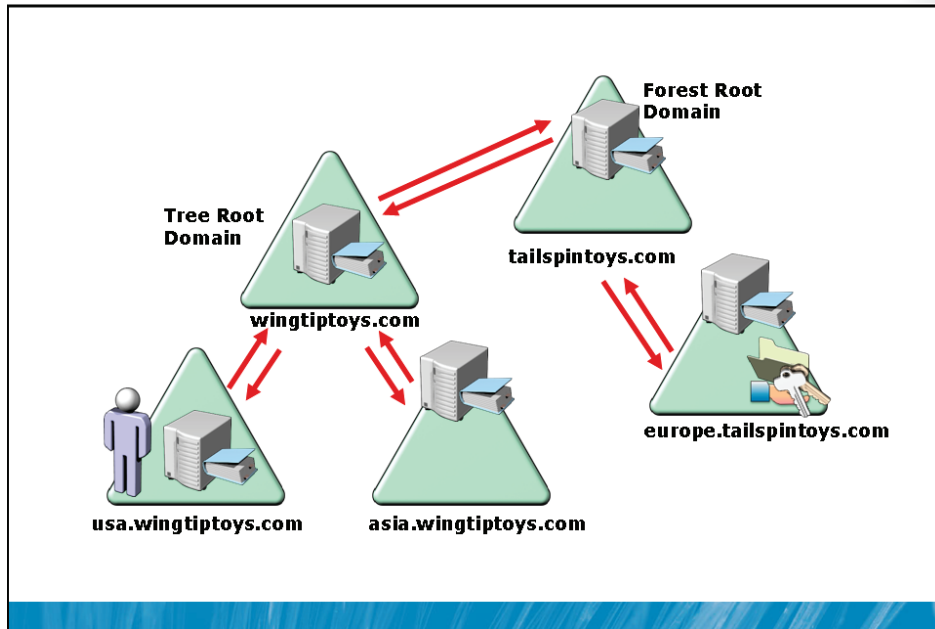
Transitivity

Some trusts are not transitive, and others are transitive. In the figure above, Domain A trusts Domain B, and Domain B trusts Domain C. If the trusts are transitive, then Domain A trusts Domain C. If they are not transitive, then Domain A does not trust Domain C. In most cases, you could create a third trust relationship, specifying that Domain A trusts Domain C. With transitive trusts, that third relationship is not necessary; it is implied.

Automatic or Manual

Some trusts are created automatically. Other trusts must be created manually.

How Trusts Work Within a Forest



Key Points

Within a forest, all domains trust each other. That is because the root domain of each tree in a forest trusts the forest root domain—the first domain installed in the forest—and each child domain trusts its parent domain. All trusts automatically created should never be deleted and are transitive and two-way. The net result is that a domain trusts the identity stores and authentication services of all other domains in its forest. Users and global groups from any domain in the forest can be added to domain local groups, can be given user rights, and can be added to ACLs on resources in any other domain in the forest. Trusts to other forests and to domains outside the forest must be manually established. With that summary, you can look at the details of trusts within and outside of an Active Directory forest.

Authentication Protocols

Windows Server 2008 Active Directory authenticates users with one of two protocols—Kerberos version 5 (v5) or NTLM. Kerberos v5 is the default protocol used by computers running Windows Server 2008, Windows Vista®, Windows Server 2003, Windows XP, and Windows 2000 Server. If a computer involved in an authentication transaction does not support Kerberos v5, the NTLM protocol is used instead. Group Policies can be used to disable NTLM authentication

Kerberos Authentication within a Domain

When a user logs on to a client running Kerberos v5, the authentication request is forwarded to a domain controller. Each Active Directory domain controller acts as a key distribution center (KDC), a core component of Kerberos. After validating the identity of the user, the KDC on the domain controller gives the authenticated user what is known as a ticket-granting ticket (TGT).

When the user needs to access resources on a computer in the same domain, the user must first obtain a valid session ticket for the computer. Session tickets are provided by the KDC of a domain controller, so the user returns to a domain controller to request a session ticket. The user presents the TGT as proof that he or she has already been authenticated. This enables the KDC to respond to the user's session ticket request without having to re-authenticate the user's identity. The user's session ticket request specifies the computer and the service the user wants to access. The KDC identifies that the service is in the same domain based on the service principal name (SPN) of the requested server. The KDC then provides the user a session ticket for the service.

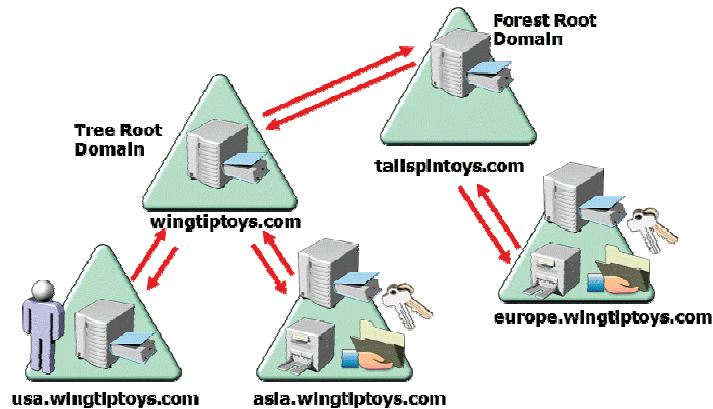
The user then connects to the service and presents the session ticket. The server is able to determine that the ticket is valid and that the user has been authenticated by the domain. This happens through private keys, a topic that is beyond the scope of this lesson. The server, therefore, does not need to authenticate the user; it accepts the authentication and identity provided by the domain with which the computer has a trust relationship.

All these Kerberos transactions are handled by Windows clients and servers and are transparent to users themselves.

Kerberos Authentication across Domains in a Forest

Each child domain in a forest trusts its parent domain with an automatic, two-way, transitive trust called a parent-child trust. The root domain of each tree in a domain trusts the forest root domain with an automatic, two-way, transitive trust called a tree-root trust.

These trust relationships create what is referred to as the trust path or trust flow in a forest. The trust path is easy to understand with a diagram, shown the next illustration. The forest consists of two trees, the tailspintoys.com tree and the wingtip toys.com tree. The tailspintoys.com domain is the forest root domain. The illustration indicates that the wingtip toys.com tree root domain trusts the tailspintoys.com domain.



Kerberos authentication uses the trust path to provide a user in one domain a session ticket to a service in another domain. If a user in **usa.wingtip toys.com** requests access to a shared folder on a server in **europe.tailspintoys.com**, the following transactions occur:

1. The user logs on to a computer in **usa.wingtip toys.com** and is authenticated by a domain controller in **usa.wingtip toys.com**, using the authentication process described in the previous section. The user obtains a TGT for the domain controller in **usa.wingtip toys.com**.

The user wants to connect to a shared folder on a server in **europe.tailspintoys.com**.

2. The user contacts the KDC of a domain controller in **usa.wingtip toys.com** to request a session ticket for the server in **europe.tailspintoys.com**.

3. The domain controller in usa.wingtiptoys.com identifies, based on the SPN, that the desired service resides in europe.tailspintoys.com, not in the local domain.

The job of the KDC is to act as a trusted intermediary between a client and a service. If the KDC cannot provide a session ticket for the service because the service is in a trusted domain and not in the local domain, the KDC will provide the client a referral to help it obtain the session ticket it is requesting.

The KDC uses a simple algorithm to determine the next step. If the KDC domain is trusted directly by the service's domain, the KDC gives the client a referral to a domain controller in the service's domain. If not, but if a transitive trust exists between the KDC and the service's domain, the KDC provides the client a referral to the next domain in the trust path.

4. The usa.wingtiptoys.com domain is not trusted directly by europe.tailspintoys.com, but a transitive trust exists between the two domains, so the KDC in the usa.wingtiptoys.com domain gives the client a referral to a domain controller in the next domain in the trust path, wingtiptoys.com.
5. The client contacts the KDC in the referral domain, wingtiptoys.com.
6. Again, the KDC determines that the service is not in the local domain and that europe.tailspintoys.com does not trust wingtiptoys.com directly, so it returns a referral to a domain controller in the next domain in the trust path, tailspintoys.com.
7. The client contacts the KDC in the referral domain, tailspintoys.com.
8. The KDC determines that the service is not in the local domain and that europe.tailspintoys.com trusts tailspintoys.com directly, so it returns a referral to a domain controller in the europe.tailspintoys.com domain.
9. The client contacts the KDC in the referral domain, europe.tailspintoys.com.
10. The KDC in europe.tailspintoys.com returns to the client a session ticket for the service.
11. The client contacts the server and provides the session ticket; the server provides access to the shared folder based on the permissions assigned to the user and the groups to which the user belongs.

This process might seem complicated, but recall that it is handled in a way that is completely transparent to the user.

The reverse process occurs if a user from `usa.wingtiptoy.com` logs on to a computer in the `europa.tailspintoy.com` domain. The initial authentication request must traverse the trust path to reach a KDC in the `usa.wingtiptoy.com` domain to authenticate the user.

Although it is not necessary to master the details of Kerberos authentication between domains in a forest for the 70-640 exam, it can help you in the real world to have a basic understanding that cross-domain authentication in a forest follows a trust path.

Demonstration: Create a Trust

In this demonstration, we will:

- Create a trust using Active Directory Domains and Trusts and the New Trust Wizard

Key Points

The steps for creating trusts are similar across categories of trusts. You must be a member of the Domain Admins or Enterprise Admins group to create a trust successfully.

To create a trust relationship:

1. Open the **Active Directory Domains and Trusts** snap-in.
2. Right-click the domain that will participate in one side of the trust relationship, and choose **Properties**.

You must be running Active Directory Domains and Trusts with credentials that have permissions to create trusts in this domain.

3. Click the **Trusts** tab.
4. Click the **New Trust** button.

The New Trust Wizard guides you through the creation of the trust.

5. On the **Trust Name** page, type the DNS name of the other domain in the trust relationship, and then click **Next**.
6. If the domain you entered is not within the same forest, you will be prompted to select the type of trust, which will be one of the following:
 - **Forest**
 - **External**
 - **Realm**

If the domain is in the same forest, the wizard knows it is a shortcut trust.

7. If you are creating a realm trust, you will be prompted to indicate whether the trust is transitive or non-transitive. (Realm trusts are discussed later in this lesson.)
8. On the **Direction Of Trust** page, select one of the following:
 - **Two-Way**. This establishes a two-way trust between the domains.
 - **One-Way: Incoming**. This establishes a one-way trust in which the domain you selected in step 2 is the trusted domain, and the domain you entered in step 5 is the trusting domain.
 - **One-Way: Outgoing**. This establishes a one-way trust in which the domain you selected in step 2 is the trusting domain, and a domain you entered in step 5 is the trusted domain.
9. Click **Next**.
10. On the **Sides Of Trust** page, select one of the following:
 - **Both this domain and the specified domain**. This establishes both sides of the trust. This requires that you have permission to create trusts in both domains.
 - **This domain Only**. This creates the trust relationship in the domain you selected in step 2. An administrator with permission to create trusts in the other domain must repeat this process to complete the trust relationship.

The next steps will depend on the options you selected in steps 8 and 10. The steps will involve one of the following:

- If you selected **Both this domain and the specified domain**, you must enter a user name and password with permissions to create the trust in the domain specified in step 5.
 - If you selected **This Domain Only**, you must enter a trust password. A trust password is entered by administrators on each side of a trust to establish the trust. The passwords should not be the administrators' user account passwords. Instead, each should be a unique password used only for the purpose of creating this trust. The passwords are used to establish the trust, and then the domains change them immediately.
11. If the trust is an outgoing trust, you are prompted to choose one of the following:
 - **Selective Authentication**
 - **Domain-Wide Authentication** or **Forest-Wide Authentication**, depending on whether the trust type is an external trust or a forest trust, respectively.
 12. The New Trust Wizard summarizes your selections on the **Trust Selections Complete** page. Click **Next**.
The wizard creates the trust.
 13. The **Trust Creation Complete** page appears. Verify the settings, and then click **Next**.

You will then have the opportunity to confirm the trust. This option is useful if you have created both sides of the trust or if you are completing the second side of a trust.

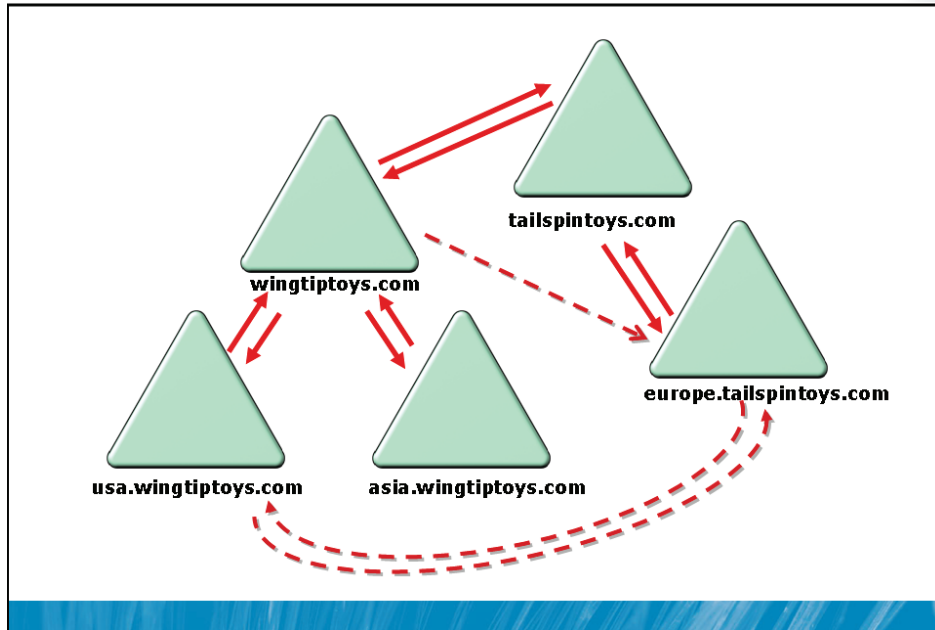
If you selected Both This Domain And The Specified Domain in step 8, the process is complete. If you selected This Domain Only in step 8, the trust relationship will not be complete until an administrator in the other domain completes the process:

- If the trust relationship you established is a one-way outgoing trust, an administrator in the other domain must create a one-way incoming trust.
- If the trust relationship you established is a one-way incoming trust, an administrator in the other domain must create a one-way outgoing trust.
- If the trust relationship you established is a two-way trust, an administrator in the other domain must create a two-way trust.

Additional Reading

- Detailed procedures for creating each type of trust are available at:
<http://go.microsoft.com/fwlink/?LinkId=168830>

Shortcut Trusts



Key Points

Four types of trusts must be created manually:

- Shortcut trusts
- External trusts
- Realm trusts
- Forest trusts

Each of these types of trusts will be discussed in the following sections.

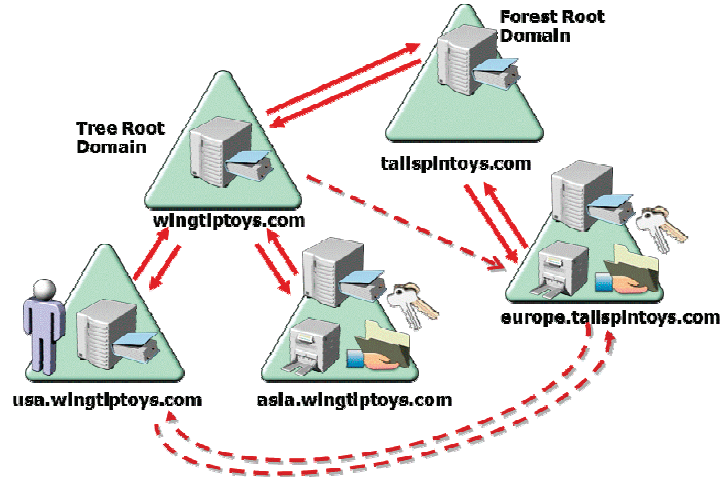
Shortcut Trusts

In an earlier section, there were the 11 steps of the process used to grant a session ticket for a client to access a resource in another domain within a forest. Most of those steps involved referrals to domains on the trust path between the user's domain and the domain of the shared folder. When a user from one domain logs on to a computer in another domain, the authentication request must also traverse the trust path. This can affect performance and, if a domain controller is not available in a domain along the trust path, the client will not be able to authenticate or to access the service.

Shortcut trusts are designed to overcome those problems by creating a trust relationship directly between child domains in the forest trust path.

Shortcut trusts optimize authentication and session ticket requests between domains in a multidomain forest. By eliminating the trust path, they eliminate the time required to traverse the trust path and thereby can significantly improve performance of session ticket requests.

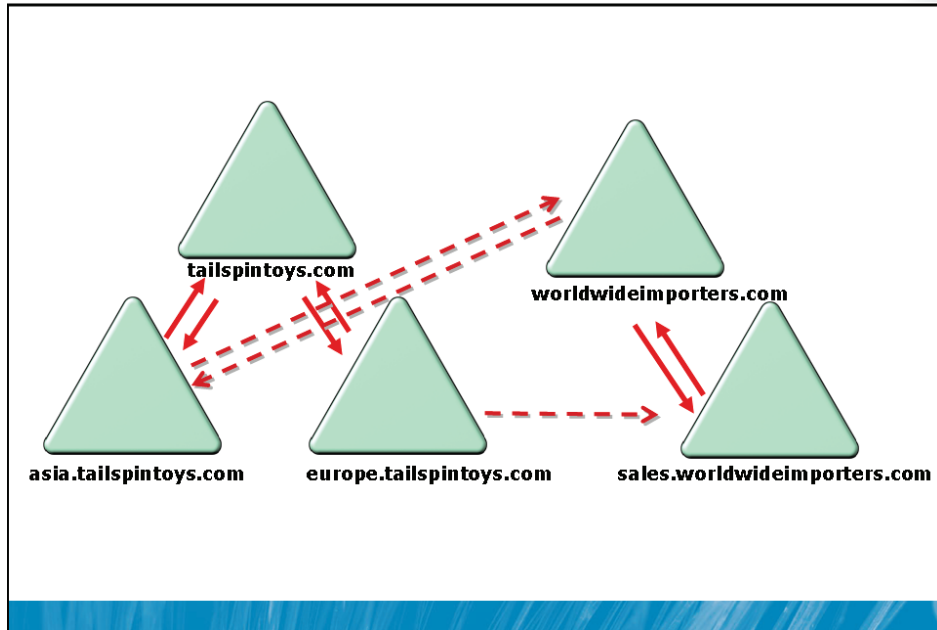
Shortcut trusts can be one-way or two-way. In either case, the trust is transitive. In the illustration here, a one-way shortcut trust exists whereby wingtip toys.com trusts europe.tailspintoys.com.



When a user from europe.tailspintoys.com logs on to a computer in wingtiptoy.com or requests a resource in wingtiptoy.com, the request can be referred directly to a domain controller in the trusted domain, asia.wingtiptoy.com. However, the reverse is not true. If a user in wingtiptoy.com logs on to a computer in europe.tailspintoys.com, the authentication request will traverse the trust path up to tailspintoys.com and down to wingtiptoy.com.

A two-way shortcut trust is illustrated between usa.wingtiptoy.com and europe.tailspintoys.com. Users in both domains can be authenticated by and can request resources from computers in the other domain, and the shortcut trust path will be used.

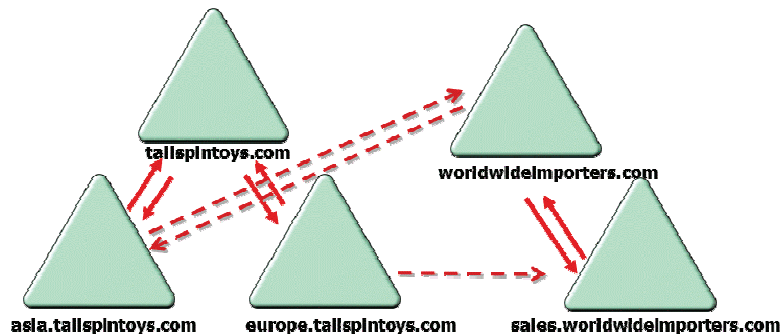
External Trusts and Realm Trusts



Key Points

External Trusts

When you need to work with a domain that is not in your forest, you might need to create an external trust. An external trust is a trust relationship between a domain in your forest and a Windows domain that is not in your forest. Examples are shown in the illustration.



You can see a one-way trust between the sales.worldwideimporters.com domain and the europe.tailspintoys.com domain. The Europe domain trusts the Sales domain, so users in the Sales domain can log on to computers in the Europe domain or connect to resources in the Europe domain.

The illustration shows a two-way trust between the worldwideimporters.com domain and the asia.tailspintoys.com domain. Users in each domain can be given access to resources in the other domain. Technically, all external trusts are non-transitive, one-way trusts. When you create a two-way external trust, you are actually creating two one-way trusts, one in each direction.

When you create an outgoing external trust, Active Directory creates a foreign security principal object for each security principal in the trusted domain. Those users, groups, and computers can then be added to domain local groups or to ACLs on resources in the trusting domain.

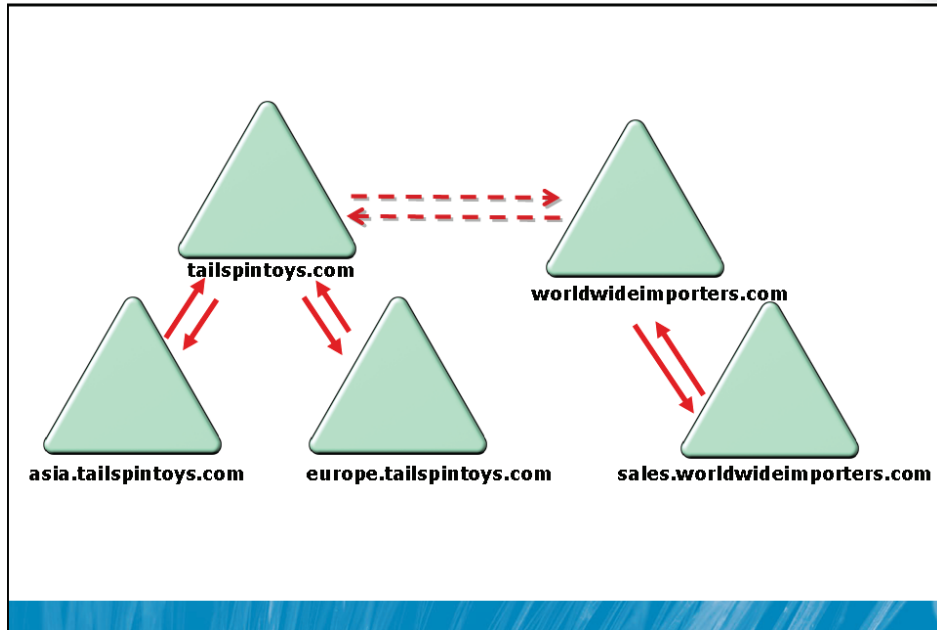
To increase the security of an external trust relationship, you can choose Selective Authentication on the Outgoing Trust Authentication Level page of the New Trust Wizard. Additionally, domain quarantine, also called SID filtering, is enabled by default on all external trusts.

Realm Trusts

When you need cross-platform interoperability with security services based on other Kerberos v5 implementations, you can establish a realm trust between your domain and a UNIX Kerberos v5 realm. Realm trusts are one-way, but you can establish one-way trusts in each direction to create a two-way trust. By default, realm trusts are non-transitive, but they can be made transitive.

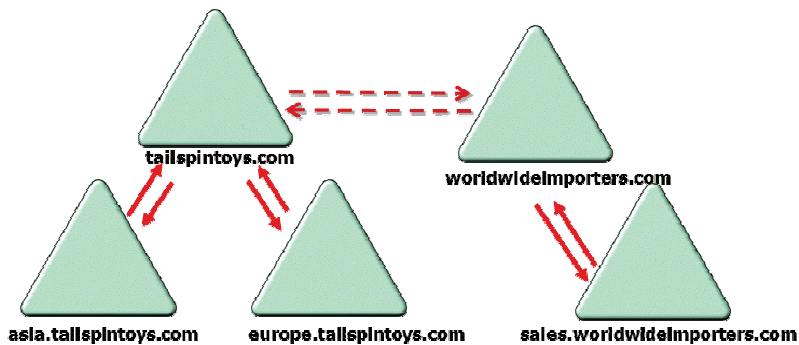
If a non-Windows Kerberos v5 realm trusts your domain, the realm trusts all security principals in your domain. If your domain trusts a non-Windows Kerberos v5 realm, users in the realm can be given access to resources in your domain; however, the process is indirect. When users are authenticated by a non-Windows Kerberos realm, Kerberos tickets do not contain all the authorization data needed for Windows. Therefore, an account mapping system is used. Security principals are created in the Windows domain and are mapped to a foreign Kerberos identity in the trusted non-Windows Kerberos realm. The Windows domain uses only these proxy accounts to evaluate access to domain objects that have security descriptors. All Windows proxy accounts can be used in groups and on ACLs to control access on behalf of the non-Windows security principal. Account mappings are managed through Active Directory Users and Computers.

Forest Trusts



Key Points

When you require collaboration between two separate organizations represented by two separate forests, you can consider implementing a forest trust. A forest trust is a one-way or two-way transitive trust relationship between the forest root domains of two forests. The illustration shows an example of a forest trust between the **tailspintoys.com** forest and the **worldwideimporters.com** forest.



A single forest trust relationship allows the authentication of a user in any domain by any other domain in either forest, assuming that the forest trust is two-way. If the forest trust is one-way, any user in any domain in the trusted forest can be authenticated by computers in the trusting forest. Forest trusts are significantly easier to establish, maintain, and administer than are separate trust relationships between each of the domains in the forests. Forest trusts are particularly useful in scenarios involving cross-organization collaboration or mergers and acquisitions, or within a single organization that has more than one forest to isolate Active Directory data and services.

When you establish a forest trust relationship, domain quarantine, also called SID filtering, is enabled by default. Domain quarantine is discussed in the “Domain Quarantine” section.

You can specify whether the forest trust is one-way, incoming or outgoing, or two-way. As mentioned earlier, a forest trust is transitive, allowing all domains in a trusting forest to trust all domains in a trusted forest.

However, forest trusts are not themselves transitive. For example, if the tailspintoys.com forest trusts the worldwideimporters.com forest, and the worldwideimporters.com forest trusts the northwindtraders.com forest, those two trust relationships do not allow the tailspintoys.com forest to trust the northwindtraders.com forest. If you want those two forests to trust each other, you must create a specific forest trust between them.

Several requirements must be met before you can implement a forest trust. The forest functional level must be Windows Server 2003 or later. In addition, you must have a specific DNS infrastructure to support a forest trust.

Additional Reading

- You can learn about the DNS requirements for a forest trust at <http://go.microsoft.com/fwlink/?LinkId=168831>

Administer Trust Relationships

- **Validate a trust relationship**
 - Active Directory Domains and Trusts
 - `netdom trust TrustingDomainName /domain:TrustedDomainName /verify`
- **Remove a manually created trust relationship**
 - Active Directory Domains and Trusts
 - `netdom trust TrustingDomainName /domain:TrustedDomainName /remove [/force] /UserD:User /PasswordD:*`
 - UserD is a user in the Enterprise Admins or Domain Admins group of the trusted domain

Key Points

If you are concerned that a trust relationship is not functioning, you can validate a trust relationship between any two Windows domains. You cannot validate a trust relationship to a Kerberos v5 realm. To validate a trust relationship, complete the following steps:

1. Open **Active Directory Domains and Trusts**.
2. In the console tree, right-click the domain that contains the trust that you want to validate, and then click **Properties**.
3. Click the **Trusts** tab.
4. Select the trust you want to validate.
5. Click **Properties**.
6. Click **Validate**.

7. Do one of the following, and then click **OK**:
 - Click **Yes, Validate The Incoming Trust**. Enter credentials that are members of the Domain Admins or Enterprise Admins groups in the reciprocal domain.
 - Click **No, Do Not Validate The Incoming Trust**. It is recommended that you repeat this procedure for the reciprocal domain.

You can also verify a trust from the command prompt by typing the following command:

```
netdom trust TrustingDomainName /domain:TrustedDomainName /verify
```

There can also be reason to remove a manually created trust. To do so, follow these steps:

1. Open **Active Directory Domains and Trusts**.
2. In the console tree, right-click the domain that contains the trust you want to validate, and then click **Properties**.
3. Click the **Trusts** tab.
4. Select the trust you want to remove.
5. Click **Remove**.
6. Do one of the following, and then click **OK**:
 - Click **Yes, Remove The Trust From Both The Local Domain And The Other Domain**. Enter credentials that are members of the Domain Admins or Enterprise Admins groups in the reciprocal domain.
 - Click **No, Remove The Trust From The Local Domain Only**. It is recommended that you repeat this procedure for the reciprocal domain.

To delete a manually created trust from the command prompt, use the netdom.exe command with the following syntax:

```
netdom trust TrustingDomainName /domain:TrustedDomainName  
/remove [/force] /UserD:User /PasswordD:*
```

The UserD parameter is a user with credentials in the Enterprise Admins or Domain Admins group of the trusted domain. Specifying the PasswordD:* parameter causes netdom.exe to prompt you for the password to the account. The /force switch is required when removing a realm trust.



Note: The Windows Domain Manager, `netdom.exe`, and other command-line tools can be used to manage and test trust relationships. See: <http://go.microsoft.com/fwlink/?LinkId=168832> for details regarding these commands.

Domain Quarantine

- Filters out trusted user SIDs that come from a domain other than the trusted domain
- If a user was migrated into the trusted domain
 - User account may have SIDs from user's previous domain in the sIDHistory attribute
 - Those SIDs are included in the user's privilege attribute certificate (PAC) that is part of the Kerberos ticket the user presents to the trusted domain
 - These SIDs are discarded
- Enabled by default on all new outgoing trusts to external domains/forests
- Disable if necessary

```
netdom trust TrustingDomainName /domain:TrustedDomainName  
/quarantine:[Yes|No]
```

Key Points

By default, domain quarantine, also called SID filtering, is enabled on all external and forest trusts. When a user is authenticated in a trusted domain, the user presents authorization data that includes the SIDs of the user's account in the groups to which the user belongs. Additionally, the user's authorization data includes security identifiers from other attributes of the user and his or her groups.

Some of the SIDs presented by the user from the trusted domain might not have been created in the trusted domain. For example, if a user is migrated from one domain into another, a new SID is assigned to the migrated account. The migrated account will, therefore, lose access to any resources that had permissions assigned to the SID of the user's former account. To enable the user to continue to access such resources, an administrator performing a migration can specify that the sIDHistory attribute of the user's migrated account will include the former account's SID. When the user attempts to connect to the resource, the original SID in the sIDHistory attribute will be authorized for access.

In a trusted domain scenario, it is possible that a rogue administrator could use administrative credentials in the trusted domain to load SIDs into the `sidHistory` attribute of a user that are the same as SIDs of privileged accounts in your domain. That user would then have inappropriate levels of access to resources in your domain.

Domain quarantine prevents this problem by enabling the trusting domain to filter out SIDs from the trusted domain that are not the primary SIDs of security principals. Each SID includes the SID of the originating domain, so when a user from a trusted domain presents the list of the user's SIDs and the SIDs of the user's groups, SID filtering instructs the trusting domain to discard all SIDs without the domain SID of the trusted domain.

Domain quarantine is *enabled by default for all outgoing trusts to external domains and forests*. Disable domain quarantine only if one or more of the following are true:

- You have extremely high levels of confidence in the administrators of the trusted domain.
- Users or groups have been migrated to the trusted domain with their SID histories preserved, and you want to grant those users or groups permissions to resources in the trusting domain based on the `sidHistory` attribute.

To disable domain quarantine, type the following command:

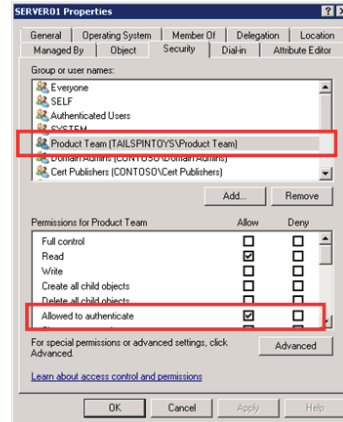
```
netdom trust TrustingDomainName /domain:TrustedDomainName  
/quarantine:no
```

To re-enable domain quarantine, type this command:

```
netdom trust TrustingDomainName /domain:TrustedDomainName  
/quarantine:yes
```

Resource Access for Users from Trusted Domains

- Giving trusted users access to resources
 - Authenticated Users
 - Add trusted identities to trusting domain's domain local groups
 - Add trusted identities to ACLs
- Selective authentication
 - Reduces the risk of exposure--for example, to Authenticated Users
 - You specify which trusted users are allowed to authenticate on a server-by-server (computer-by-computer) basis
 - Enable selective authentication in the properties of the trust
 - Give users Allowed To Authenticate permission on the computer object in Active Directory



Key Points

When you configure a trust relationship that enables your domain to trust another domain, you open up the possibility for users in the trusted domain to gain access to resources in your domain. The following sections examine components related to the security of a trusting domain's resources.

Authenticated Users

A trust relationship itself does not grant access to any resources; however, it is likely that by creating a trust relationship, users in the trusted domain will have immediate access to a number of your domain's resources. This is because many resources are secured with ACLs that give permissions to the Authenticated Users group.

Membership in Domain Local Groups

As you learned in Module 4, the best practice for managing access to a resource is to assign permissions to a domain local group. You can then nest users and groups from your domain into the domain local group and, thereby, grant them access to the resource. Domain local security groups can also include users and global groups from trusted domains as members. Therefore, the most manageable way to assign permissions to users in a trusted domain is to make them or their global groups members of a domain local group in your domain.

Add trusted identities to ACLs

You can also add users and global groups from a trusted domain directly to the ACLs of resources in a trusting domain. This approach is not as manageable as the previous method, using a domain local group, but it is possible.

Transitivity

When you create a realm trust, the trust is nontransitive by default. If you make it transitive, you open up the potential for users from domains and realms trusted by the Kerberos v5 realm to gain access to resources in your domain. It is recommended that you use nontransitive trusts unless you have a compelling business reason for a transitive realm trust.

Selective Authentication

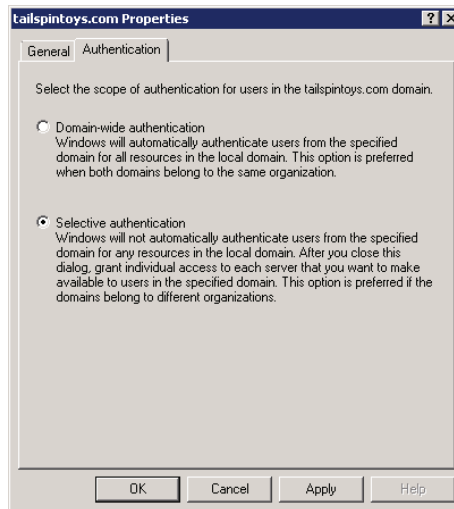
When you create an external trust or a forest trust, you can control the scope of authentication of trusted security principals. There are two modes of authentication for an external or forest trust:

- Selective authentication
- Domain-wide authentication (for an external trust) or forest-wide authentication (for a forest trust)

If you choose domain-wide or forest-wide authentication, all trusted users can be authenticated for access to services on all computers in the trusting domain. Trusted users can, therefore, be given permission to access resources anywhere in the trusting domain. With this authentication mode, you must have confidence in the security procedures of your enterprise and in the administrators who implement those procedures so that inappropriate access is not assigned to trusted users. Remember, for example, that users from a trusted domain or forest are considered Authenticated Users in the trusting domain, so any resource with permissions granted to Authenticated Users will be immediately accessible to trusted domain users if you choose domain-wide or forest-wide authentication.

If, however, you choose selective authentication, all users in the trusted domain are trusted identities; however, they are allowed to authenticate only for services on computers that you have specified. For example, imagine that you have an external trust with a partner organization's domain. You want to ensure that only users from the marketing group in the partner organization can access shared folders on only one of your many file servers. You can configure selective authentication for the trust relationship and then give the trusted users the right to authenticate only for that one file server.

To configure the authentication mode for a new outgoing trust, use the Outgoing Trust Authentication Level page of the New Trust Wizard. Configure the authentication level for an existing trust, open the properties of the trusting domain in Active Directory Domains and Trusts, select the trust relationship, click Properties, and then click the Authentication tab, shown in the illustration.

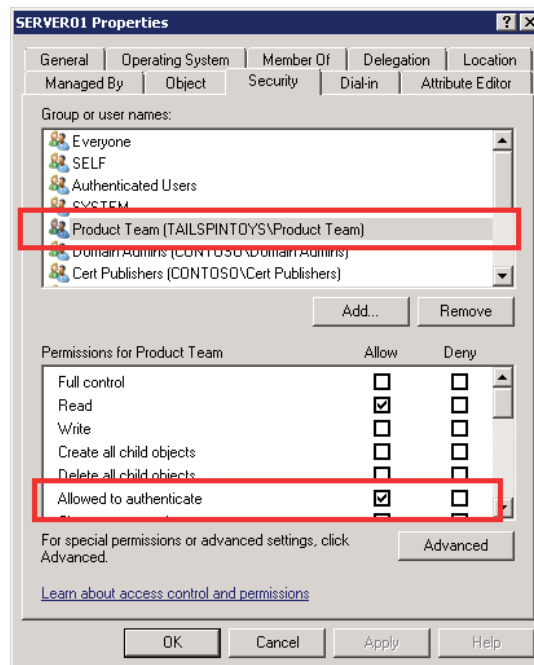


After you have selected Selective Authentication for the trust, no trusted users will be able to access resources in the trusting domain, even if those users have been given permissions.

The users must also be assigned the Allowed To Authenticate permission on the computer object in the domain.

To assign this permission

1. Open the **Active Directory Users and Computers** snap-in and make sure that **Advanced Features** is selected in the **View** menu.
2. Open the properties of the computer to which trusted users should be allowed to authenticate—that is, the computer that trusted users will log on to or that contains resources to which trusted users have been given permissions.
3. On the **Security** tab, add the trusted users or a group that contains them and select the **Allow** check box for the **Allowed to authenticate** permission, as shown in the next illustration.



Lab B: Administer a Trust Relationship

- Exercise 1: Configure DNS
- Exercise 2: Create a Trust Relationship
- Exercise 3: Validate a Trust Relationship
- Exercise 4: Assign Permissions to Trusted Identities
- Exercise 5: Implement Selective Authentication

Logon information

Virtual machine	6425B-HQDC01-A	6425B-TSTDC01-A
Logon user name	Pat.Coleman	Sara.Davis
Administrative user name	Pat.Coleman_Admin	Sara.Davis_Admin
Password	Pa\$\$w0rd	Pa\$\$w0rd

Estimated time: 45 minutes

Scenario

Contoso, Ltd. is forming a partnership with Tailspin Toys. A team of product developers at Tailspin Toys requires access to a shared folder in the Contoso domain. You must configure your domain to support this business requirement. Additionally, the inexperienced domain administrator at Tailspin Toys requires assistance configuring the reciprocal side of the trust relationship.

Exercise 1: Configure DNS

It is important for DNS to be functioning properly before you create trust relationships. Each domain must be able to resolve names in the other domain. In Module 10, you learned how to configure name resolution. There are several ways to support name resolution between two forests. In this exercise, you will create a stub zone in the contoso.com domain for the tailspintoys.com domain and a conditional forwarder in the tailspintoys.com domain to resolve contoso.com.

The main tasks for this exercise are as follows:

1. Prepare for the lab.
2. Configure DNS in contoso.com.
3. Configure DNS in tailspintoys.com.

► Task 1: Prepare for the lab

1. Start 6425B-HQDC01-A and log on as **Pat.Coleman** with the password **Pa\$\$w0rd**.
2. Start 6425B-TSTDC01-A and log on as **Sara.Davis** with the password **Pa\$\$w0rd**.

► Task 2: Configure DNS in contoso.com

1. On HQDC01, run DNS Management as an administrator, with the user name **Pat.Coleman_Admin** and the password **Pa\$\$w0rd**.
2. Create a stub zone for tailspintoys.com that refers to the IPv4 address **10.0.0.31** as the master server.

► Task 3: Configure DNS in tailspintoys.com

1. On TSTDC01, run **DNS Management** as an administrator, with the user name **Sara.Davis_Admin** and the password **Pa\$\$w0rd**.
2. Create a conditional forwarder for contoso.com that forwards to the IPv4 address **10.0.0.11**.

Results: After this exercise, you will have configured DNS name resolution between the contoso.com and tailspintoys.com domains.

Exercise 2: Create a Trust Relationship

In this exercise, you will create the trust relationship to enable authentication of Tailspin Toys users in the Contoso domain.

The main tasks for this exercise are as follows:

1. Identify the trusted and trusting domains.
2. Initiate the trust in the trusted domain.
3. Complete the trust in the trusting domain.

► Task 1: Identify the trusted and trusting domains

- Users in tailspintoys.com require access to a shared folder in contoso.com. Answer the following questions:
 - Which domain is the trusting domain, and which is the trusted domain?
 - Which domain has an outgoing trust, and which has an incoming trust?

► Task 2: Initiate the trust in the trusted domain

1. On HQDC01, run **Active Directory Domains and Trusts** as an administrator, with the user name **Pat.Coleman_Admin** and the password **Pa\$\$w0rd**.
2. Create a one-way, outgoing external trust relationship with tailspintoys.com. Configure the trust to use domain-wide authentication, and to use **Pa\$\$w0rd** as the initial trust relationship password.

► Task 3: Complete the trust in the trusting domain

1. On TSTDC01, run **Active Directory Domains and Trusts** as an administrator, with the user name **Sara.Davis_Admin** and the password **Pa\$\$w0rd**.
2. Create a one-way, incoming external trust relationship with contoso.com. Configure the trust to use domain-wide authentication, and to use **Pa\$\$w0rd** as the initial trust relationship password.

Results: After this exercise, you will have established a trust relationship between the contoso.com and tailspintoys.com domains, in which contoso.com is the trusted domain.

Exercise 3: Validate a Trust Relationship

In the previous exercise, you had the opportunity to confirm the trust relationship. You can also confirm or validate an existing trust relationship. In this exercise, you will validate the trust between contoso.com and tailspintoys.com.

The main task for this exercise is as follows:

- Validate a trust relationship.
-
- **Task 1: Validate a trust relationship**
 - On HQDC01, use **Active Directory Domains and Trusts** to validate the trust between contoso.com and tailspintoys.com.

Results: After this exercise, you will have validated the trust between contoso.com and tailspintoys.com.

Exercise 4: Assign Permissions to Trusted Identities

In this exercise, you will provide access to a shared folder in the Contoso domain to the product team from Tailspin Toys.

The main task for this exercise is as follows:

- Assign permissions to trusted groups.

► Task 1: Assign permissions to trusted groups

1. On TSTDC01, run **Active Directory Users and Computers** as an administrator, with the user name **Sara.Davis_Admin** and the password **Pa\$\$w0rd**.
2. In the **User Accounts** OU, create a user account for **Pat Coleman** with the user logon name **Pat.Coleman** and the password **Pa\$\$w0rd**. Configure the password so that it does not have to be changed at first logon.
3. In the **tailspintoys.com** domain, create an OU named **Groups**.
4. In the **Groups** OU, create a global security group named **Product Team**.
5. On HQDC01, run **Active Directory Users and Computers** as an administrator, with the user name **Pat.Coleman_Admin** and the password **Pa\$\$w0rd**.
6. In the **Groups\Role** OU, create a global security group named **Product Developers**.
7. In the **Groups\Access** OU, create a domain local group named **ACL_Product Information_Modify**.
8. Create a folder named **Product Information** on drive C of HQDC01.
9. Give the **ACL_Product Information_Modify** group **Modify** permission to the **Product Information** folder.

10. Open the properties of the **ACL_ Product Information _Modify** group. Add the **Contoso Product Developers** and the **Tailspin Toys Product Team** as members.

When you do so, a Windows Security dialog box appears. Because the trust is one-way, your user account as the administrator of contoso.com (Pat.Coleman_Admin) does not have permissions to read the directory of the tailspintoys.com domain. You must have an account in tailspintoys.com to read its directory. If the trust were a two-way trust, this message would not have appeared. Your standard user account in the tailspintoys.com domain will be used to provide you Read Access to the directory service.

In the **User Name** box, type **TAILSPINTOYS\Pat.Coleman**. In the **Password** box, type **Pa\$\$w0rd**.

11. Note that the two global groups from the two domains are now members of the domain local group in the contoso.com domain that has access to the Product Information folder.

Results: After this exercise, you will have assigned resource access permissions to the Product Information folder in the Contoso domain to groups in both the Contoso and Tailspin Toys domains.

Exercise 5: Implement Selective Authentication

In this exercise, you will restrict the ability of users from the tailspintoys.com domain to authenticate with computers in the contoso.com domain.

The main task for this exercise is as follows:

- Implement selective authentication.

► Task 1: Implement selective authentication

- On HQDC01, use **Active Directory Domains and Trusts** to enable selective authentication for the trust between contoso.com and tailspintoys.com.

With selective authentication enabled, users from a trusted domain cannot authenticate against computers in the trusting domain, even if they've been given permissions to a folder. Trusted users must also be given the **Allowed To Authenticate** permission on the computer itself.

- In **Active Directory Users and Computers**, ensure that **Advanced Features** are enabled. Then open the properties of HQDC01 and give the **TAILSPINTOYS\Product Team** the **Allowed to Authenticate** permission.

When you do so, a Windows Security dialog box appears. Because the trust is one-way, your user account as the administrator of contoso.com (Pat.Coleman_Admin) does not have permissions to read the directory of the tailspintoys.com domain. You must have an account in tailspintoys.com to read its directory. If the trust were a two-way trust, this message would not have appeared. Your standard user account in the tailspintoys.com domain will be used to provide you Read Access to the directory service.

In the **User Name** box, type **TAILSPINTOYS\Pat.Coleman**. In the **Password** box, type **Pa\$\$w0rd**.



Note: After completing this exercise, turn off all virtual machines and discard undo disks.

Lab Review Questions

Question: You have given the Research and Development group from Tailspin Toys Modify permission to the Product Information folder on HQDC01. However, of the ten users in the group, only one user (who happens to also be a member of the Product Team group) has access. The others cannot access the folder. What must be done?

Question: A user from Contoso attempts to access a shared folder in the Tailspin Toys domain and receives an Access Denied error. What must be done to provide access to the user?

MCT USE ONLY. STUDENT USE PROHIBITED

Module 1: Introducing Active Directory® Domain Services (AD DS)

Lab: Install an AD DS DC to Create a Single Domain Forest

Exercise 1: Perform Post-Installation Configuration Tasks

► Task 1: Prepare for the lab

1. Start 6425B-HQDC01-D.
2. Press ALT+DELETE, which sends the secure key sequence (CTRL+ALT+DELETE) to the virtual machine guest.
3. With the user name of Administrator present, In **Password**, type Pa\$\$w0rd, then press ENTER or click the log on arrow.

The Windows desktop appears and, after a moment, the Initial Configuration Tasks window opens.

► Task 2: Configure the display resolution

1. Minimize (do not close) the Initial Configuration Tasks window.
2. Right-click the desktop and choose **Personalize**.
3. Click **Display Settings**.
4. Drag the **Resolution** slider to **1024 by 768**.
5. Click **OK**.

You are prompted with the message *Do you want to keep these display settings?*

6. Click **Yes**.
7. Close the Personalization window.

► **Task 3: Configure the time zone**

1. Maximize the Initial Configuration Tasks window.
2. In the Initial Configuration Tasks window, click the **Set time zone** link.
3. Click **Change time zone**.
4. From the **Time zone** drop-down list, select the time zone that is appropriate for your location, and then click **OK**.
5. Click **OK** again.

► **Task 4: Change IP configuration**

1. In the Initial Configuration Tasks window, click the **Configure networking** link.
The Network Connections window appears.
2. Right-click **Local Area Connection** and choose **Properties**.
The Local Area Connection Properties dialog box appears.
3. Click **Internet Protocol Version 4 (TCP/IPv4)**, and then click **Properties**.
Note that Windows Server 2008 also provides native support for Internet Protocol Version 6 (TCP/IPv6).
4. Click **Use the following IP address**. Enter the following configuration:
 - IP Address: **10.0.0.11**
 - Subnet Mask: **255.255.255.0**
 - Default Gateway: **10.0.0.1**
 - Preferred DNS Server: **10.0.0.11**
5. Click **OK**, and then click **Close**.
6. Close the Network Connections window.

► **Task 5: Rename the server HQDC01**

1. In the Initial Configuration Tasks window, click the **Provide computer name and domain** link.

The System Properties dialog box appears.

2. Click **Change**.
3. In the **Computer name** box, type **HQDC01**. Click **OK**.

You are prompted with the message *You must restart your computer to apply these changes*.

4. Click **OK**.
5. Click **Close**.

You are prompted with the message *You must restart your computer to apply these changes*.

6. Click **Restart Later**. If you accidentally click **Restart Now**, wait for the server to restart, and then log on as **Administrator** with the password **Pa\$\$w0rd**.

► **Task 6: Restart the server**

1. In the Initial Configuration Tasks window, note the **Add roles** and **Add features** links.

In the next exercise, you will use Server Manager to add roles and features to HQDC01. These links are another way to perform the same tasks.

By default, the Initial Configuration Tasks window will appear each time you log on to the server.

2. Select the **Do not show this window at logon** check box to prevent the window from appearing.

If you need to open the Initial Configuration Tasks window in the future, you do so by running the Oobe.exe command.

3. Click the **Close** button at the bottom of the window.

Server Manager appears.

Server Manager enables you to configure and administer the roles and features of a server running Windows Server 2008. You will use Server Manager in the next exercise.

At the bottom of the Server Manager window, a status message informs you, *Console cannot refresh until computer is restarted.*

4. Click the **Restart** link next to the status message.

You are prompted with the message *Do you want to restart now?*

5. Click **Yes**.

The computer restarts.

Exercise 2: Install a New Windows Server 2008 Forest with the Windows Interface

► Task 1: Add the Active Directory Domain Services role to HQDC01

1. Log on to HQDC01 as **Administrator** with the password **Pa\$\$w0rd**.
The Windows desktop appears and, after a moment, Server Manager opens.
If Server Manager does not open, click the Server Manager link in the Quick Launch next to the Start button.
2. In the **Roles Summary** section of the Server Manager home page, click **Add Roles**.
The Add Roles Wizard appears.
3. Click **Next**.
4. On the **Select Server Roles** page, select the check box next to **Active Directory Domain Services**. Click **Next**.
5. On the **Active Directory Domain Services** page, click **Next**.
6. On the **Confirm Installation Selections** page, click **Install**.
The Installation Progress page reports the status of installation tasks.
7. On the **Installation Results** page, confirm the installation succeeded, and then click **Close**.

In the Roles Summary section of Server Manager's home page, you'll notice an error message indicated by a red circle with a white "x." You'll also notice a message in the Active Directory Domain Services section of the Roles page. Both of these links will take you to the Active Directory Domain Services role page of Server Manager. The message shown reminds you that it is necessary to run `dcpromo.exe`, which you will do in the next task.

► **Task 2: Configure a new Windows Server 2008 forest named contoso.com with HQDC01 as the first domain controller**

1. In Server Manager, expand the **Roles** node in the tree pane, and then click **Active Directory Domain Services**.
2. Click the **Run the Active Directory Domain Services Installation Wizard (dcpromo.exe)** link.

The Active Directory Domain Services Installation Wizard appears.

3. Click **Next**.
4. On the **Operating System Compatibility** page, review the warning about the default security settings for Windows Server 2008 domain controllers, and then click **Next**.
5. On the **Choose a Deployment Configuration** page, click **Create a new domain in a new forest**, and then click **Next**.
6. On the **Name the Forest Root Domain** page, type **contoso.com**, and then click **Next**.

The system performs a check to ensure that the DNS and NetBIOS names are not already in use on the network.

7. On the **Set Forest Functional Level** page, choose **Windows Server 2008**, and then click **Next**.

The Additional Domain Controller Options page appears.

Each of the functional levels is described in the Details box on the page. Choosing Windows Server 2008 forest functional level ensures that all domains in the forest operate at the Windows Server 2008 domain functional level, which enables several new features provided by Windows Server 2008.

In a production environment, you would choose Windows Server 2008 forest functional level when creating a new forest if you require the features provided by the Windows Server 2008 domain functional level and if you will not be adding any domain controllers running operating systems prior to Windows Server 2008.

DNS Server is selected by default. The Active Directory Domain Services Installation Wizard will create a DNS infrastructure during AD DS installation.

The first domain controller in a forest must be a global catalog server and cannot be a read-only domain controller (RODC).

8. Click **Next**.

A Static IP assignment warning appears.

Because discussion of IPv6 is beyond the scope of this training kit, you did not assign a static IPv6 address to the server in Exercise 2. You did assign a static IPv4 address in Exercise 1, and other labs in this course will use IPv4. You can therefore ignore this error in the context of the exercise.

9. Click **Yes, the computer will use a dynamically assigned IP address (not recommended)**.

A warning appears that informs you that a delegation for the DNS server cannot be created.

In the context of this exercise, you can ignore this error. Delegations of DNS domains will be discussed later in this course.

10. Click **Yes** to close the Active Directory Domain Services Installation Wizard warning message.

11. On the **Location for Database, Log Files, and SYSVOL** page, accept the default locations for the database file, the directory service log files, and the SYSVOL files, and then click **Next**.

The best practice in a production environment is to store these files on three separate volumes that do not contain applications or other files not related to AD DS. This best practice design improves performance and increases the efficiency of backup and restore.

12. On the **Directory Services Restore Mode Administrator Password** page, type a **Pa\$\$w0rd** in both the **Password** and **Confirmed Password** boxes. Click **Next**.

In a production environment, you should use a very strong password for the Directory Services Restore Mode Administrator Password. Do not forget the password you assign to the Directory Services Restore Mode Administrator.

13. On the **Summary** page, review your selections.

If any settings are incorrect, click **Back** to make modifications.

14. Click **Next**.

Configuration of AD DS begins. After several minutes of configuration, the Completing the Active Directory Domain Services Installation Wizard page appears.

15. Click **Finish**.
16. Click **Restart Now**.
The computer restarts.
17. Continue with Task 3 (optional) or skip to Task 4.

► **Task 3: Examine the default configuration of the contoso.com forest and domain (OPTIONAL)**

1. Log on to HQDC01 as **Administrator** with the password **Pa\$\$w0rd**.
The Windows desktop appears and, after a moment, Server Manager opens.
2. Expand the **Roles** node in the tree pane, and expand the **Active Directory Domain Services** node.
3. Expand **Active Directory Users and Computers** and the **contoso.com** domain node.
4. Click the **Users** container in the tree.
The users and groups you see are available to any computer in the domain. For example, the domain's Administrator account can be used to log on to any computer in the domain, by default, and the Domain Users group is a member of the local Users group on each computer in the domain.
5. Click the **Builtin** container in the tree.
The groups you see are shared by and available to domain controllers, but not to member servers or workstations. For example, members of the Backup Operators group can perform backup and restore tasks on domain controllers only, and the Administrators group in the Builtin container represents the administrators of all domain controllers.
6. Select the **Computers** container in the tree.
It is empty. This is the default container for member servers and workstations.
7. Select the **Domain Controllers** organizational unit (OU) in the tree.
This is the OU into which domain controllers are placed. The computer object for HQDC01 appears in this OU.

► **Task 4: Shut down the virtual machine**

1. If you are not already logged on to HQDC01, log on to HQDC01 as **Administrator** with the password **Pa\$\$w0rd**.
2. If you are not already logged on to HQDC01, log on to HQDC01 as **Administrator** with the password **Pa\$\$w0rd**.
The Windows desktop appears and, after a moment, Server Manager opens.
3. Shut down HQDC01 and discard changes you made while doing this lab exercise.



Note: After completing this exercise, turn off all virtual machines and discard undo disks.

MCT USE ONLY. STUDENT USE PROHIBITED

Module 2: Secure and Efficient Administration of Active Directory®

Lab A: Create and Run a Custom Administrative Console

► Log on to a virtual machine

Unless otherwise instructed, use the following steps to log on to a virtual machine.

1. Press ALT+DELETE.
This sends the secure key sequence (CTRL+ALT+DELETE) to the virtual machine. If you press CTRL+ALT+DELETE, you send the secure key sequence to the host operating system.
2. Click **Switch User**.
3. Click **Other User**.
4. In **User name**, type the username.
5. In **Password**, type the password.
6. Press ENTER or click the log on arrow.

The Windows® desktop appears.

Exercise 1: Perform Basic Administrative Tasks Using the Active Directory Users and Computers Snap-in

► Task 1: Prepare for the lab

1. Start 6425B-HQDC01-A.
2. Log on to HQDC01 as **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
Pat.Coleman_Admin is a member of Domain Admins.
Server Manager opens automatically.
3. Close **Server Manager**.
4. Open **D:\Labfiles\Lab02a**.
5. Right-click **Lab02a_Setup.bat**, and then click **Run as administrator**.
A User Account Control dialog box appears.
6. Click **Continue**.
7. The lab setup script runs. When it is complete, press any key to continue.
8. Close the Windows Explorer window, **Lab02a**.

► Task 2: View objects

1. Click **Start**, and then click **Control Panel**.
2. If **Control Panel** is in the **Classic** view, double-click **Administrative Tools**.
If **Control Panel** is in the **Category** view, click **System and Maintenance** and then click **Administrative Tools**.
3. Double-click **Active Directory Users and Computers**.
A User Account Control dialog box appears.
4. Click **Continue**.
5. In the console tree, expand the **contoso.com** domain and the **User Accounts** OU, and then click the **Employees** OU.

► **Task 3: Refresh the view**

1. In the console tree, click the **Employees** OU.
2. Click the **Refresh** button in the snap-in toolbar or press **F5**.

► **Task 4: Create objects**

1. In the console tree, right-click **contoso.com**, then point to **New**, and then click **Organizational Unit**.
2. In the **Name** box, type **6425B**, and then click **OK**.

► **Task 5: Configure object attributes**

1. In the console tree, click the **Employees** OU.
2. In the details pane, right-click **Pat Coleman**, and then click **Properties**.
3. Click the **General** tab.
4. In **Office**, replace the current value with **Redmond**.
5. Click **OK**.

► **Task 6: View all object attributes**

1. In the console tree, click the **Employees** OU.
2. In the details pane, right-click **Pat Coleman**, and then click **Properties**.
3. Confirm that the **Attribute Editor** tab is not visible, and that there is no input control for the **division** property on any of the tabs.
4. Close the **Properties** dialog box.
5. Click the **View** menu, and then select the **Advanced Features** option.
6. In the console tree, expand the **User Accounts** OU, and then click the **Employees** OU.
7. In the details pane, right-click **Pat Coleman**, and then click **Properties**.
8. Click the **Attribute Editor** tab.

9. Double-click the **division** attribute.
10. Enter **6425B** and then click **OK**.
11. Click **OK** to close the **Pat Coleman Properties** dialog box.
12. Close Active Directory Users and Computers.

Exercise 2: Create a Custom Active Directory Administrative Console

► Task 1: Create a custom MMC console with the Active Directory Users and Computers snap-in

1. Click **Start**, and in the **Start Search** box type **mmc.exe**, and then press ENTER.
A User Account Control dialog box appears.
2. Click **Continue**.
An empty MMC console appears. By default, the new console window is not maximized.
3. Maximize the MMC console.
4. Click the **File** menu, and then click **Add/Remove Snap-in**.
The Add or Remove Snap-ins dialog box appears.
5. In the **Available snap-ins** list, click **Active Directory Users and Computers**, and then click **Add**.
6. Click **OK** to close the **Add or Remove Snap-ins** dialog box.
7. Click the **File** menu, and then click **Save**.
8. In the **Save As** dialog box, browse to drive **C**.
9. Click the **Create New Folder** button on the toolbar and name the new folder **AdminTools**.
10. Open the new **AdminTools** folder.
11. In the **File name** box, type **MyConsole**.
12. Click **Save**.

► Task 2: Add other Active Directory snap-ins to the console

1. Click the **File** menu, and then click **Add/Remove Snap-in**.
The Add or Remove Snap-ins dialog box appears.
2. In the **Available snap-ins** list, click **Active Directory Sites and Services**, and then click **Add**.

3. In the **Available snap-ins** list, click **Active Directory Domains and Trusts**, and then click **Add**.
4. Click **OK** to close the **Add or Remove Snap-ins** dialog box.
5. In the console tree, right-click **Console Root**, and then click **Rename**.
6. Type **Active Directory Administrative Tools** and press ENTER.
7. Click the **File** menu, and then click **Save**.

► **Task 3: Add the Active Directory Schema snap-in to a custom MMC console**

1. Click the **File** menu, and then click **Add/Remove Snap-in**.
The Add or Remove Snap-ins dialog box appears.
2. In the **Add or Remove Snap-ins** dialog box, examine the **Available snap-ins** list. Note that **Active Directory Schema** is not available.

The Active Directory Schema snap-in is installed with the Active Directory Domain Services role, and with the Remote Server Administration Tools (RSAT), but it is not registered, so it does not appear.

3. Click **OK** to close the **Add or Remove Snap-ins** dialog box.
4. Click **Start**, then right-click **Command Prompt**, and then click **Run as administrator**.

A User Account Control dialog box appears.

5. Click **Continue**.

The Administrator: Command Prompt window appears.

6. In the command prompt, type the command **regsvr32.exe schmmgmt.dll**.

This command registers the dynamic link library (DLL) for the Active Directory Schema snap-in. This is necessary to do one time on a system before you can add the snap-in to a console.

A prompt appears that indicates the registration was successful.

7. Click **OK**.
8. Close the Command Prompt window.

9. Return to your customized MMC console. Click the **File** menu, and then click **Add/Remove Snap-in**.

The Add or Remove Snap-ins dialog box appears.

10. In the **Available snap-ins** list, click **Active Directory Schema**, and then click **Add**.
11. Click **OK** to close the **Add or Remove Snap-ins** dialog box.
12. Click the **File** menu, and then click **Save**.

► **Task 4: Manage snap-ins in a custom MMC console (optional)**

- Open the **Add or Remove Snap-ins** dialog box and use the **Move Up**, **Move Down**, and **Remove** buttons to rearrange your console. For future labs, you will need the console in the condition it was in at the end of Task 3, so do not save your changed console. Instead, close the console without saving changes.

Exercise 3: Perform Administrative Tasks with Least Privilege, Run As Administrator, and User Account Control

- ▶ **Task 1: Log on with credentials that do not have administrative privileges**
 1. Log off of HQDC01.
 2. Log on to HQDC01 as **Pat.Coleman** with the password, **Pa\$\$w0rd**.

Pat.Coleman is a member of Domain Users and has no administrative privileges.

- ▶ **Task 2: Run Server Manager as an administrator**
 1. Click the **Server Manager** icon in the **Quick Launch**, next to the **Start** button.

A User Account Control dialog box appears.

Because your user account is not a member of Administrators, the dialog box requires you to enter administrative credentials: a username and a password.

If you do not see the User Name and Password boxes, make sure that you are logged on as Pat.Coleman and *not* as Pat.Coleman_Admin.
 2. In the **User name** box, type **Pat.Coleman_Admin**.
 3. In the **Password** box, type **Pa\$\$w0rd** and press ENTER.

Server Manager opens.

- ▶ **Task 3: Examine the credentials used by running processes**
 1. Right-click the taskbar and click **Task Manager**.

Task Manager opens.
 2. Click the **Processes** tab.

3. Click **Show processes from all users**.

A User Account Control dialog box appears.

Task Manager can run without administrative credentials, but it will show only those processes running under the current user account. Therefore, the User Account Control dialog box includes an option to authenticate using the same credentials with which you are logged on: Pat.Coleman.

4. Click **Use another account**.
5. In the **User name** box, type **Pat.Coleman_Admin**.
6. In the **Password** box, type **Pa\$\$w0rd** and press ENTER.
Task Manager closes and re-opens using the new credentials.
7. If Task Manager opens in a minimized state, click Task Manager on the taskbar to restore the window.
8. Click the **Processes** tab.
9. Click the **User Name** column header to sort by username.
10. Expand the **User Name** column so that it is wide enough to see the full width of usernames.
11. Scroll down to see the processes being run as Pat.Coleman and Pat.Coleman_Admin.

Question: Which processes are running as Pat.Coleman_Admin? What applications do the processes represent?

Answer: Task Manager (taskmgr.exe) and Server Manager (which appears in the Processes list as mmc.exe) are running as Pat.Coleman_Admin.

► **Task 4: Run the command prompt as an administrator**

1. Click **Start**, then right-click **Command Prompt**, and then click **Run as administrator**.
A User Account Control dialog box appears.
2. Click **Use another account**.
3. In the **User name** box, type **Pat.Coleman_Admin**.

4. In the **Password** box, type **Pa\$\$w0rd** and press ENTER.
The Administrator: Command Prompt window appears.
5. Close the Command Prompt window.
6. Click **Start**, and in the **Start Search** box, type **cmd.exe**, and then press CTRL+SHIFT+ENTER.
In the Start Search box, the keyboard shortcut CTRL+SHIFT+ENTER runs the specified command as an administrator.
A User Account Control dialog box appears.
7. Click **Use another account**.
8. In the **User name** box, type **Pat.Coleman_Admin**.
9. In the **Password** box, type **Pa\$\$w0rd** and press ENTER.
The Administrator: Command Prompt window appears.

► **Task 5: Run administrative tools as an administrator**

1. Click the **Show Desktop** icon in the **Quick Launch**, next to the **Start** button.
2. Click **Start**, then point to **Administrative Tools**, then right-click **Active Directory Users and Computers**, and then click **Run as administrator**.
A User Account Control dialog box appears.
3. Click **Use another account**.
4. In the **User name** box, type **Pat.Coleman_Admin**.
5. In the **Password** box, type **Pa\$\$w0rd** and press ENTER.

► **Task 6: Run a custom administrative console as an administrator**

1. Close all open windows on your desktop.
2. Open the **C:\AdminTools** folder.
3. Right-click **MyConsole** and click **Run as administrator**.
A User Account Control dialog box appears.
4. Click **Use another account**.

5. In the **User name** box, type **Pat.Coleman_Admin**.
6. In the **Password** box, type **Pa\$\$w0rd** and press ENTER.
7. Log off of HQDC01. Do not shut down or reset the virtual machine.



Note: Do not shut down the virtual machines once you are finished with this lab as the settings you have configured here will be used in the Lab B.

Lab Review Questions

Question: Which snap-in are you most likely to use on a day-to-day basis to administer Active Directory?

Answer: The correct answer will be based on your own experience and situation.

Question: When you build a custom MMC console for administration in your enterprise, what snap-ins will you add?

Answer: The correct answer will be based on your own experience and situation.

Lab B: Find Objects in Active Directory

► Log on to a virtual machine

Unless otherwise instructed, use the following steps to log on to a virtual machine.

1. Press ALT+DELETE.

This sends the secure key sequence (CTRL+ALT+DELETE) to the virtual machine. If you press CTRL+ALT+DELETE, you send the secure key sequence to the host operating system.

2. Click **Switch User**.
3. Click **Other User**.
4. In **User name**, type the username.
5. In **Password**, type the password.
6. Press ENTER or click the log on arrow.

The Windows desktop appears.

► Run an application with administrative credentials

1. Right-click the application, and then click **Run as administrator**.

A User Account Control (UAC) dialog box appears.

2. The **UAC** dialog box will display one of three options. Do the steps based on the option you see:

If the UAC dialog box prompts you to continue or cancel:

- Click **Continue**.

If the UAC dialog box gives you the option to *Use another account*:

1. Click **Use Another Account**.
2. In **User Name**, type the username.
3. In **Password**, type the password.
4. Press ENTER or click **OK**.

If the UAC dialog box does not give you the option to use another account, and prompts you for a username and password:

1. In **User Name**, type the username.
2. In **Password**, type the password.
3. Press ENTER or click **OK**.

Exercise 1: Find Objects in Active Directory

► Task 1: Explore the behavior of the Select dialog box



Important Note: The steps in this task guide you through using several important Active Directory Users and Computers interfaces. You can think of this task as a "tour" of the interfaces and their features. The specific changes you are making are less important than the experience you gain with the nuances of these interfaces. **Follow the exact steps listed** and don't worry about *what* you are doing; instead **focus on how you are doing it** and how the user interfaces behave.

The virtual machine should already be started and available after completing Lab A. However, if it is not, you should launch it complete the exercises in Lab A before continuing.

1. Log on to HQDC01 as **Pat.Coleman** with the password **Pa\$\$w0rd**.
2. Run your custom console, **C:\AdminTools\MyConsole.msc** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
Alternately, run the pre-created console, **D:\AdminTools\ADConsole.msc** with administrative credentials.
3. In the console tree, expand the **Active Directory Users and Computers** snap-in, the **contoso.com** domain, and the **User Accounts** OU, and then click the **Employees** OU.
4. Right-click **Pat Coleman** and then click **Properties**.
5. Click the **Member Of** tab.
6. Click **Add**.
7. In the **Select** dialog box, type the name **Special**.
8. Click **OK**.
The name is resolved to Special Project.
9. Click **OK** again to close the **Properties** dialog box.
10. In the console tree, expand the **Groups** OU, and then click the **Role** OU.
11. In the details pane, right-click the **Special Project** group and then click **Properties**.

12. Click the **Members** tab.

13. Click **Add**.

The Select Users, Contacts, Computers, or Groups dialog box appears.

14. Type **linda;joan**, and then click the **Check Names** button.

The Select dialog box resolves the names to Linda Mitchell and Joanna Rybka and underlines the names to indicate visually that the names are resolved.

15. Click **OK**.

16. Click **Add**.

17. Type **carole**, and then click **OK**.

The Select dialog box resolves the name to Carole Poland and closes. You see Carole Poland on the Members list.

When you click the OK button, a “Check Names” operation is performed prior to closing the dialog box. It is not necessary to click the Check Names button unless you want to check names and remain in the Select dialog box.

18. Click **Add**.

19. Type **tony;jeff**, and then click **OK**.

Because there are multiple users matching “tony,” the Multiple Names Found box appears.

20. Click **Tony Krijnen** and then click **OK**.

Because there are multiple users matching “jeff,” the Multiple Names Found box appears.

21. Click **Jeff Ford** and then click **OK**. Click **OK** to close the **Special Project Properties** dialog box.

Whenever there is more than one object that matches the information you enter, the check names operation will give you the opportunity to choose the correct object.

22. In the console tree, click the **Application** OU under the **Groups** OU.

23. In the details pane, right-click the **APP_Office** group and then click **Properties**.

24. Click the **Members** tab.

25. Click **Add**.

26. In the **Select** dialog box, type **DESKTOP101**.

27. Click **Check Names**.

A Name Not Found dialog box appears, indicating that the object you specified could not be resolved.

28. Click **Cancel** to close the **Name Not Found** box.

29. In the **Select** dialog box, click **Object Types**.

30. Select the check box next to **Computers** and click **OK**.

31. Click **Check Names**.

The name will resolve now that the Select dialog box is including computers in its resolution.

32. Click **OK**.

33. Click **OK** to close the **APP_Office Properties** dialog box.

► **Task 2: Control the view of objects in the Active Directory Users and Computers snap-in**

1. In the console tree, expand the **contoso.com** domain and the **User Accounts** OU, and then click the **Employees** OU.
2. Click the **View** menu, and then click **Add/Remove Columns**.
3. In the **Available Columns** list, click **Last Name**, then click **Add**.
4. In the **Displayed columns** list, click **Last Name** and click **Move Up** two times.
5. In the **Displayed columns** list, click **Type** and click **Remove**.
6. Click **OK**.
7. In the console tree, expand the **contoso.com** domain and the **User Accounts** OU, and then click the **Employees** OU.
8. In the details pane, click the **Last Name** column header to sort alphabetically by last name.
9. Click the **View** menu, and then click **Add/Remove Columns**.

10. In the **Available Columns** list, click **Pre-Windows 2000 Logon**, and then click **Add**.
11. In the **Displayed columns** list, click **Pre-Windows 2000 Logon**, and then click **Move Up**.
12. Click **OK**.
13. In the console tree, expand the **contoso.com** domain and the **User Accounts** OU, and then click the **Employees** OU.

► **Task 3: Use the Find command**

1. In the console tree, click the **Employees** OU.
2. Click the **Find** button in the snap-in toolbar.
3. In the **Name** box, type **Dan** and then click **Find Now**.

Question: How many users are found?

Answer: There should be more than one user named Dan.

4. Close the **Find Users, Contacts, and Groups** dialog box.

► **Task 4: Determine where an object is located**

1. Click the **View** menu, and then select the **Advanced Features** option.
2. Click **Find**.
3. Click the **In** drop-down list, and then click **Entire Directory**.
4. In the **Name** box, type **Pat.Coleman**, and then click **Find Now**.
5. Double-click **Pat Coleman (Admin)**.

Question: Where is Pat's administrative account located?

Answer: In the Admin Identities OU inside the Admins OU.

Exercise 2: Use Saved Queries

► Task 1: Create a saved query that displays all domain user accounts

1. In the console tree, right-click **Saved Queries**, then point to **New**, and then click **Query**.
2. In the **New Query** dialog box, type **All User Objects** in the **Name** box.
3. Click **Define Query**.
4. From the **Name** drop-down list, choose **Has a value**. Click **OK** two times.

► Task 2: Create a saved query that shows all user accounts with non-expiring passwords

1. In the console tree, right-click **Saved Queries**, then point to **New**, and then click **Query**.
2. In the **New Query** dialog box, type **Non-Expiring Passwords** in the **Name** box.
3. Click **Define Query**.
4. Select the **Non expiring passwords** check box. Click **OK** two times.

Note that, for the purposes of maintaining a simple, single password for all users in this course, *all* user accounts are configured so that passwords do not expire. In a production environment, user accounts should not be configured with non-expiring passwords.

► Task 3: Transfer a query to another computer

1. In the console tree, right-click the **Non-Expiring Passwords** query, and then click **Export Query Definition**. The **Save As** dialog box appears.
2. In the **File name** box, type **C:\AdminTools\Query_NonExpPW.xml** and click **Save**.
3. Right-click the **Non-Expiring Passwords** query, and then click **Delete**.
A confirmation message appears.
4. Click **Yes** to confirm the deletion of the query.
5. Right-click **Saved Queries**, and then click **Import Query Definition**.

6. Double-click **Query_NonExpPW**.
The Edit Query dialog box appears.
7. Click **OK**.
8. Log off of HQDC01.



Note: Do not shut down the virtual machine once you are finished with this lab as the settings you have configured here will be used in the Lab C.

Lab Review Questions

Question: In your work, what scenarios require you to search Active Directory?

Answer: The correct answer will be based on your own experience and situation.

Question: What types of saved queries could you create to help you perform your administrative tasks more efficiently?

Answer: The correct answer will be based on your own experience and situation.

Lab C: Use DS Commands to Administer Active Directory

► Log on to a virtual machine

Unless otherwise instructed, use the following steps to log on to a virtual machine.

1. Press ALT+DELETE.

This sends the secure key sequence (CTRL+ALT+DELETE) to the virtual machine. If you press CTRL+ALT+DELETE, you send the secure key sequence to the host operating system.

2. Click **Switch User**.
3. Click **Other User**.
4. In **User name**, type the username.
5. In **Password**, type the password.
6. Press ENTER or click the log on arrow.

The Windows desktop appears.

► Run an application with administrative credentials

1. Right-click the application, and then click **Run as administrator**.

A User Account Control (UAC) dialog box appears.

2. The **UAC** dialog box will display one of three options. Do the steps based on the option you see:

If the UAC dialog box prompts you to continue or cancel:

- Click **Continue**.

If the UAC dialog box gives you the option to *Use another account*:

1. Click **Use Another Account**.
2. In **User Name**, type the username.
3. In **Password**, type the password.
4. Press ENTER or click **OK**.

If the UAC dialog box does not give you the option to use another account, and prompts you for a username and password:

1. In **User Name**, type the username.
2. In **Password**, type the password.
3. Press ENTER or click **OK**.

Exercise 1: Use DS Commands to Administer Active Directory

► Task 1: Prepare for the lab

The virtual machine should already be started and available after completing Lab A. However, if it is not, you should launch it complete the exercises in Lab A before continuing.

1. Log on to HQDC01 as **Pat.Coleman** with the password **Pa\$\$w0rd**.
2. Open **D:\Labfiles\Lab02c**.
3. Run **Lab02c_Setup.bat** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
4. The lab setup script runs. When it is complete, press any key to continue.
5. Close the Windows Explorer window, Lab02c.

► Task 2: Find objects with DSQuery

1. Open Command Prompt with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
The Administrator: Command Prompt window appears.
2. Type **dsquery user -name "*Mitchell"** and press ENTER.

► Task 3: Retrieve object attributes with DSGet

1. From the command prompt, get the e-mail address of Tony Krijnen.

```
dsget user "cn=Tony Krijnen,ou=Employees,ou=User  
Accounts,dc=contoso,dc=com" -email
```

2. From the command prompt, list the members of the Finance Managers group.
Do you know which attribute to use? Type "dsget group /?".

```
dsget group "cn=Finance  
Managers,ou=Role,ou=Groups,dc=contoso,dc=com" -members
```

► Task 4: Pipe DNs from DSQuery to other DS commands

Scott and Linda Mitchell are joining the Special Project team. They are the only two employees with the last name Mitchell who work at Contoso. They work in the Vancouver office.

1. Using a single command, add the Mitchells to the **Special Project** group.

Perform this step without typing the DN of the Mitchells' user accounts.

The DN of the Special Project group is "cn=Special Project,ou=Role,ou=Groups,dc=contoso,dc=com"

```
dsquery user -name "*Mitchell" | dsmod group "cn=Special Project,ou=Role,ou=Groups,dc=contoso,dc=com" -addmbr
```

If you receive an error that says, "The specified name is already a member of the group," use Active Directory Users and Computers to remove Scott Mitchell and Linda Mitchell from the Special Project group, then try again.

You may receive an Access Denied error. What is causing this error, and what can you do to work around it?

If you launched the command prompt without Run As Administrator, your user account (Pat.Coleman) does not have credentials to change the group membership.

2. Using a single command, retrieve the e-mail address of all users in the Vancouver office.

Users in the Vancouver office have the word **Vancouver** in the **Description** field.

If you don't know what attribute switch to use (**-desc**), type **dsquery user /?**.

```
dsquery user -desc "*Vancouver*"
```

If you receive a warning that your DSQuery has reached its limit, what can you do to ensure all results are returned?

```
dsquery user -desc "*Vancouver*" -limit 0
```

3. Using a single command, change the **office** attribute of the two users named Mitchell to **Vancouver**.

```
dsquery user -name "*Mitchell" | dsmod user -office "Vancouver"
```



Note: After completing this exercise, turn off all virtual machines and discard undo disks.

Lab Review Questions

Question: What can you do to avoid typing DNs of users, groups, or computers into DSGet, and other DS commands?

Answer: Create command files or batch files of commonly used commands.

Question: How are wildcard searches with DSQuery different than searches performed with the Find command in Active Directory Users and Computers? In other words, what kind of search have you performed in this lab that would not have been possible using the basic interface of the Find command?

Answer: DSQuery offers flexible wildcard searches with the * wildcard. The Find command can only do “Starts With” queries.

Module 3: Manage Users

Lab A: Create and Administer User Accounts

► Log on to a virtual machine

Unless otherwise instructed, use the following steps to log on to a virtual machine.

1. Press **ALT+DELETE**.

This sends the secure key sequence (CTRL+ALT+DELETE) to the virtual machine. If you press CTRL+ALT+DELETE, you send the secure key sequence to the host operating system.

2. Click **Switch User**.
3. Click **Other User**.
4. In **User name**, type the username.
5. In **Password**, type the password.
6. Press **ENTER** or click the log on arrow.

The Windows desktop appears.

► Run an application with administrative credentials

1. Right-click the application, and then click **Run as administrator**.

A User Account Control (UAC) dialog box appears.

2. The **UAC** dialog box will display one of three options. Do the steps based on the option you see:

If the UAC dialog box prompts you to continue or cancel:

- Click **Continue**.

If the UAC dialog box gives you the option to *Use another account*:

1. Click **Use Another Account**.
2. In **User Name**, type the username.

3. In **Password**, type the password.
4. Press ENTER or click **OK**.

If the UAC dialog box does not give you the option to use another account, and prompts you for a username and password:

1. In **User Name**, type the username.
2. In **Password**, type the password.
3. Press ENTER or click **OK**.

Exercise 1: Create User Accounts

► Task 1: Prepare for the lab

1. Start 6425B-HQDC01-A.
2. Log on to HQDC01 as **Pat.Coleman** with the password **Pa\$\$w0rd**.
3. Open **D:\Labfiles\Lab03a**.
4. Run **Lab03a_Setup.bat** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
5. The lab setup script runs. When it is complete, press any key to continue.
6. Close the Windows Explorer window, **Lab03a**.

► Task 2: Create a user account with Active Directory Users and Computers

1. Run **Active Directory Users and Computers** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
2. In the console tree, expand the **contoso.com** domain and the **User Accounts** OU, and then click the **Employees** OU.
3. Right-click the **Employees** OU, then point to **New**, and then click **User**.
4. In **First name**, type the user's first name: **Chris**.
5. In **Last name**, type the user's last name: **Mayo**.
6. In **User logon name**, type the user's logon name: **Chris.Mayo**.
7. In the **User logon name (pre-Windows 2000)** text box, type the pre-Windows 2000 logon name: **Chris.Mayo**.
8. Click **Next**.
9. Type **Pa\$\$w0rd** in the **Password** and **Confirm password** boxes.

In a production environment, you should use a unique, strong password for each user account that you create, even for the temporary password assigned to a new user.

10. Select **User must change password at next login**.
11. Click **Next**.
12. Review the summary and click **Finish**.

► **Task 3: Create a user account with the DSAdd command**

1. Run Command Prompt with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
2. If you are unsure which switches to use for the DSAdd command, type **dsadd user /?** and press ENTER.
3. Type the following command, and then press ENTER:

```
dsadd user "cn=Amy Strande,ou=Employees,ou=User  
Accounts,dc=contoso,dc=com" -samid Amy.Strande -upn  
Amy.Strande@contoso.com -fn Amy -ln Strande -display "Strande,  
Amy" -desc "Vice President, IT"
```

4. Switch to **Active Directory Users and Computers**.
5. In the console tree, expand the **contoso.com** domain and the **User Accounts** OU, and then click the **Employees** OU.
6. If Active Directory Users and Computers was already open prior to this task, click the **Refresh** button.
7. Right-click **Amy Strande** and then click **Properties**.
8. Examine the properties of the user account. Confirm that the attributes were set correctly, and then close the dialog box.

Exercise 2: Administer User Accounts

► Task 1: Administer a user account

The user account for Amy Strande is currently disabled, because no password was specified using the DSAdd command.

Question: What parameter could you have used with the DSAdd command to specify a password?

Answer: -pwd

1. Right-click **Amy Strande** and then click **Reset Password**.
2. In the **New password** and **Confirm password** boxes, type **Pa\$\$w0rd**.
3. Select the **User must change password at next logon** check box.
4. Click **OK**.
A message appears: "The password for Amy Strande has been changed."
5. Click **OK**.
6. Right-click **Amy Strande** and then click **Enable Account**.
A message appears: "Object Amy Strande has been enabled."
7. Click **OK**.

Question: What command could have been used at the command prompt to reset the password, specify that the password must be changed at the next logon, and enable the account? Write the command below, including all of the parameters.

Answer:

```
dsmod user "cn=Amy Strande,ou=Employees,ou=User  
Accounts,dc=contoso,dc=com" -pwd Pa$$w0rd -mustchpwd yes -disabled  
no
```

► **Task 2: Administer the lifecycle of a user account**

Contoso's policy for user account lifecycle management states the following:

- When a user leaves the organization for any reason, including leave of absence, the user's account must be disabled immediately and moved to the Disabled Accounts OU.
- Sixty days after the termination of a user, the user's account must be deleted.
 1. In console tree, click the **Employees** OU.
 2. Right-click **Chris Mayo**, and then click **Disable Account**.
A message appears: *Object Chris Mayo has been disabled*.
 3. Click **OK**.
 4. Right-click **Chris Mayo**, and then click **Move**.
 5. Click the **Disabled Accounts** OU, and then click **OK**.
 6. In the console tree, click the **Disabled Accounts** OU.
 7. Right-click **Chris Mayo** and then click **Delete**.
A prompt appears: "Are you sure you want to delete the User named 'Chris Mayo?'"
 8. Click **Yes**.
 9. Log off of HQDC01.



Note: Do not shut down the virtual machine once you are finished with this lab as the settings you have configured here will be used in the Lab B.

Lab Review Questions

Question: In this lab, which attribute(s) can be modified when you are creating a user account with the command prompt that cannot be modified when creating a user account with Active Directory Users and Computers?

Answer: Description, Display Name.

Question: What happens when you create a user account that has a password that does not meet the requirements of the domain?

Answer: The account is created, but it is disabled. It cannot be enabled until a password that meets the requirements of the domain is configured.

Lab B: Configure User Object Attributes

► Log on to a virtual machine

Unless otherwise instructed, use the following steps to log on to a virtual machine.

1. Press ALT+DELETE.

This sends the secure key sequence (CTRL+ALT+DELETE) to the virtual machine. If you press CTRL+ALT+DELETE, you send the secure key sequence to the host operating system.

2. Click **Switch User**.
3. Click **Other User**.
4. In **User name**, type the username.
5. In **Password**, type the password.
6. Press ENTER or click the log on arrow.

The Windows desktop appears. Run an Application with Administrative Credentials

7. Right-click the application, and then click **Run as administrator**.

A User Account Control (UAC) dialog box appears.

8. The **UAC** dialog box will display one of three options. Do the steps based on the option you see:

If the UAC dialog box prompts you to continue or cancel:

- Click **Continue**.

If the UAC dialog box gives you the option to *Use another account*:

1. Click **Use Another Account**.
2. In **User Name**, type the username.
3. In **Password**, type the password.
4. Press ENTER or click **OK**.

If the UAC dialog box does not give you the option to use another account, and prompts you for a username and password:

1. In **User Name**, type the username.
2. In **Password**, type the password.
3. Press ENTER or click **OK**.

Exercise 1: Examine User Object Attributes

► Task 1: Prepare for the lab

The virtual machine should already be started and available after completing Lab A. However, if it is not, you should launch it complete the exercises in Lab A before continuing

1. Start 6425B-HQDC01-A.
2. Log on to HQDC01 as **Pat.Coleman** with the password **Pa\$\$w0rd**.
3. Open **D:\Labfiles\Lab03b**.
4. Run **Lab03b_Setup.bat** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
5. The lab setup script runs. When it is complete, press any key to continue.
6. Close the Windows Explorer window, **Lab03b**.

► Task 2: Explore the properties of an Active Directory user object

1. Run **Active Directory Users and Computers** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
2. In the console tree, expand the **contoso.com** domain and the **User Accounts** OU, and then click the **Employees** OU.
3. Right-click **Tony Krijnen** and then click **Properties**.
4. Examine the **General**, **Address**, **Account** and **Organization** tabs.
5. Click **OK** to close the **Properties** dialog box.

► Task 3: Explore all attributes of an Active Directory user object

1. Click the **View** menu, and then select **Advanced Features**, so that the **Advanced Features** option is enabled.
2. In the console tree, expand the **contoso.com** domain and the **User Accounts** OU, and then click the **Employees** OU.
3. Right-click **Tony Krijnen** and then click **Properties**.
4. Click the **Attribute Editor** tab.

► **Task 4: Analyze the naming and display of user object attributes**

- For each of the following attributes in the **Tony Krijnen Properties** dialog box, identify the corresponding attribute name on the **Attribute Editor** tab:

Properties dialog box tab	Property name	Attribute name as shown on the Attribute Editor tab
General	First name	givenName
General	Last name	sn
General	Display name	displayName
General	Description	description
General	Office	physicalDeliveryOffice
General	Telephone number	telephoneNumber
General	E-mail	mail
Address	Street	streetAddress
Address	City	l
Address	Zip/Postal Code	postalCode
Address	Country	co
Organization	Job Title	title
Organization	Department	department
Organization	Company	company

Questions:

1. Use the Attribute Editor tab to answer the following questions.
 - Does the employeeID attribute, shown on the Attribute Editor tab, show up on a normal tab of the Properties dialog box? If so, which one? What about carLicense?
 - **Answer:** Neither employeeID nor carLicense appear on any other tab.
 - Looking at the Attribute Editor tab, what is the distinguished name (DN) of Tony Krijnen's object?
 - **Answer:**

```
cn=Tony Krijnen,ou=Employees,ou=User  
Accounts,dc=contoso,dc=com
```
 - Looking at the Attribute Editor tab, what is Tony's user principal name (UPN)? On which other tab does the attribute appear, and how is it labeled and displayed?
 - **Answer:** The Account tab shows the UPN as the User Logon Name. It is separated into two pieces: the logon name as a text box and the UPN suffix as a drop-down list.
2. Thought questions: Try to answer the following questions. However, it is possible that you may not come up with an answer. That is OK. Once you've tried to think of an answer, you can look at the Lab Answer Key.
 - Why might the sn attribute be named sn?
 - **Answer:** surname
 - What is the use of the c attribute?
 - **Answer:** The International Standards Organization (ISO) code for country

Exercise 2: Manage User Object Attributes

► Task 1: Modify the attributes of multiple user objects

1. In the Active Directory Users and Computers console tree, expand the **contoso.com** domain and the **User Accounts** OU, and then click the **Employees** OU.
2. Click **Adam Barr**. Then, hold the CTRL key and click **Adrian Lannin**, **Ajay Manchepalli**, **Ajay Solanki**, **Allan Guinot**, **Anav Silverman** and **András Tóth**.
3. Right-click any one of the selected users and then click **Properties**.
4. Select **Description**, and then type **Marketing Task Force** in the text box.
5. Select **Office**, and then type **Headquarters** in the text box.
6. Click the **Organization** tab.
7. Select **Manager**, and then click the **Change** button.
8. Type **Ariane Berthier**, and then click **OK**.
9. Click **OK**.
10. Double-click **Adam Barr**.
11. Click the **General** tab.
12. Examine the properties that you changed.
13. Click the **Organization** tab.
14. Examine the **Manager** property that you changed.
15. Close the **Properties** dialog box for **Adam Barr**.
16. Double-click **Ariane Berthier**.
17. Click the **Organization** tab.
18. Examine the values shown in the **Direct Reports** list.
19. Close the properties of **Ariane Berthier**.

► **Task 2: Manage user attributes from the command prompt**

1. Open the Command Prompt with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.

2. Type the command:

```
dsquery user -desc "Marketing Task Force" | dsget user -email
```

and press ENTER.

3. Type the command:

```
dsquery user -desc "Marketing Task Force" | dsmod user -hmdir  
"\\FILE01\TaskForceUsers\%username%" -hmdir U
```

and press ENTER.

4. In the Active Directory Users and Computers console tree, click the **Employees OU**.
5. In the details pane, right-click **Adam Barr**, and then click **Properties**.
6. Click the **Profile** tab.
7. Examine the **Home Folder** section, and then click **OK**.

Exercise 3: Create Users from a Template

► Task 1: Create a user account template for Sales

1. In the Active Directory Users and Computers console tree, expand the **contoso.com** domain and the **User Accounts** OU, and then click the **Employees** OU.
2. Right-click the **Employees** OU, point to **New**, and then click **User**.
3. Leave the **First Name** box empty.
4. Leave the **Last Name** box empty.
5. In the **Full Name** box, type **_Sales User**.
6. In **User Logon Name**, type: **Template.Sales**.
7. In the **User Logon Name (Pre-Windows 2000)** text box, enter the pre-Windows 2000 logon name: **Template.Sales**.
8. Click **Next**.
9. Type **Pa\$\$w0rd** in the **Password** and **Confirm password** boxes.
10. Select **User must change password at next logon**.
11. Select **Account is disabled**.
12. Click **Next**.
13. Review the summary and click **Finish**.
14. Right-click **_Sales User** and then click **Properties**.
15. Click the **Member Of** tab.
16. Click **Add**.
17. Type **Sales** and click **OK**.
The Multiple Names Found dialog box appears.
18. Click **Sales** and click **OK**.
19. Click the **Organization** tab.
20. In **Department**, type **Sales**.
21. In **Company**, type **Contoso, Ltd**.
22. Click the **Change** button in the **Manager** section.

23. Type **Anibal Sousa** and click **OK**.
24. Click the **Account** tab.
25. In the **Account Expires** section, click **End Of**, and then select the last day of the current year.
26. Click **OK**.

► **Task 2: Create a new user account based on a template**

1. Right-click **_Sales User**, and then click **Copy**.
2. In **First Name**, type **Rob**.
3. In **Last Name**, type **Young**.
4. In **User logon name**, type **Rob.Young**.
5. Confirm that the **User logon name (pre-Windows 2000)** is **Rob.Young**, and then click **Next**.
6. In **Password** and **Confirm password**, type **Pa\$\$w0rd**.
7. Clear **Account is disabled**.
8. Click **Next**.
9. Review the summary, and then click **Finish**.
10. Log off HQDC01.



Note: Do not shut down the virtual machine once you are finished with this lab as the settings you have configured here will be used in the Lab C.

Lab Review Questions

Question: What options have you learned for modifying attributes of new and existing users?

Answer: Multi-selecting users and opening the Properties dialog box, using the DSMod command, and creating a user account based on a user account template

Question: What are the advantages and disadvantages of each?

Answer: Each option gives you the chance to configure a slightly different set of attributes. No option provides the opportunity to configure all of the available attributes for more than one user. For example, DSMod allows you to change users' descriptions, but you cannot configure the description of a new user based on a template--the description attribute is not copied. DSMod allows you to reset passwords for multiple users, but you cannot do that when you select multiple users in Active Directory Users and Computers.

Lab C: Automate User Account Creation

Exercise 1: Export and Import Users with Comma Separated Value Directory Exchange (CSVDE)

► Task 1: Prepare for the lab

The virtual machine should already be started and available after completing Labs A and B. However, if it is not, you should launch it complete the exercises in Labs A and B before continuing.

1. Start 6425B-HQDC01-A.
2. Log on to HQDC01 as **Pat.Coleman** with the password **Pa\$\$w0rd**.
3. Open **D:\Labfiles\Lab03c**.
4. Run **Lab03c_Setup.bat** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
5. The lab setup script runs. When it is complete, press any key to continue.
6. Close the Windows Explorer window, **Lab03c**.

► Task 2: Export users with CSVDE

1. Open the **Command Prompt** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
2. Type the following command:

```
csvde -f D:\LABFILES\LAB03C\UsersNamedApril.csv -r "(name=April*)"
-l DN,objectClass,sAMAccountName,sn,givenName,userPrincipalName
```

then press ENTER.

3. Right-click the file **D:\LABFILES\LAB03C\UsersNamedApril.csv**, and then click **Open**.

A message appears: "Windows cannot open this file."

4. Click **Select a program from a list of installed programs**, and then click **OK**.
5. Click **Notepad**, and then click **OK**.
6. Examine the file, and then close it.

► **Task 3: Import users with CSVDE**

1. Open **D:\LABFILES\LAB03C\NewUsers.csv** with Notepad.
2. Examine the information about the users listed in the file.
3. Switch to the command prompt.
4. Type the following command:

```
csvde -i -f D:\LABFILES\LAB03C\NewUsers.csv -k
```

and then press ENTER.

The two users are imported.

5. Run **Active Directory Users and Computers** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
6. In the console tree, expand the **contoso.com** domain and the **User Accounts** OU, and then click the **Employees** OU.
7. Confirm that the users were created successfully.

If you have had the Active Directory Users and Computers snap-in open while importing the CSV file, you might have to refresh your view to see the newly created accounts.

8. Examine the accounts to confirm that first name, last name, user principal name, and pre-Windows 2000 logon name are populated according to the instructions in NewUsers.csv.
9. Right-click **Lisa Andrews** and then click **Reset Password**. In the **Password** and **Confirm Password** boxes, type **Pa\$\$w0rd**, and then click **OK**.
10. Right-click **Lisa Andrews** and then click **Enable Account**.
11. Right-click **David Jones** and then click **Reset Password**. In the **Password** and **Confirm Password** boxes, type **Pa\$\$w0rd**, and then click **OK**.
12. Right-click **David Jones** and then click **Enable Account**.
13. Close NewUsers.csv.

Exercise 2: Import Users with Lightweight Directory Access Protocol (LDAP) Data Interchange Format Directory Exchange (LDIFDE)

► Task 1: Import users with LDIFDE

1. Right-click the file **D:\LABFILES\LAB03C\NewUsers.ldf**, and then click **Open**.

A message appears: "Windows cannot open this file."

2. Click **Select a program from a list of installed programs**, and then click **OK**.
3. Click **Notepad**, and then click **OK**.
4. Examine the information about the users listed in the file.
5. Switch to the command prompt.
6. Type the following command:

```
ldifde -i -f D:\LABFILES\LAB03C\NewUsers.ldf -k
```

and then press ENTER.

The two users are imported.

7. Switch to Active Directory Users and Computers.
8. In the console tree, expand the **contoso.com** domain and the **User Accounts** OU, and then click the **Employees** OU.
9. Confirm that the users were created successfully.

If you have had the Active Directory Users and Computers snap-in open while importing the CSV file, you might have to refresh your view to see the newly created accounts.

10. Examine the accounts to confirm that user properties are populated according to the instructions in NewUsers.ldf.
11. Right-click **Bobby Moore** and then click **Reset Password**. In the **Password** and **Confirm Password** boxes, type **Pa\$\$w0rd**, and then click **OK**.
12. Right-click **Bobby Moore** and then click **Enable Account**.
13. Right-click **Bonnie Kearney** and then click **Reset Password**. In the **Password** and **Confirm Password** boxes, type **Pa\$\$w0rd**, and then click **OK**.

14. Right-click **Bonnie Kearney** and then click **Enable Account**.
15. Close NewUsers.ldf.
16. Log off HQDC01.



Note: After completing this exercise, turn off all virtual machines and discard undo disks.

Lab Review Question

Question: What scenarios lend themselves to importing users with CSVDE and LDIFDE?

Answer: If you are importing a large quantity of users, CSVDE and LDIFDE add significant value. Also, CSVDE and LDIFDE give you the ability to configure most user attributes, unlike templates and DSAdd, which support a very limited number of attributes.

MCT USE ONLY. STUDENT USE PROHIBITED

Module 4: Manage Groups

Lab A: Administer Groups

► Log on to a virtual machine

Unless otherwise instructed, use the following steps to log on to a virtual machine.

1. Press ALT+DELETE.

This sends the secure key sequence (CTRL+ALT+DELETE) to the virtual machine. If you press CTRL+ALT+DELETE, you send the secure key sequence to the host operating system.

2. Click **Switch User**.
3. Click **Other User**.
4. In **User name**, type the username.
5. In **Password**, type the password.
6. Press ENTER or click the log on arrow.

The Windows desktop appears.

► Run an application with administrative credentials

1. Right-click the application, and then click **Run as administrator**.

A User Account Control (UAC) dialog box appears.

2. The **UAC** dialog box will display one of three options. Do the steps based on the option you see:

If the UAC dialog box prompts you to continue or cancel:

- Click **Continue**.

If the UAC dialog box gives you the option to *Use another account*:

- a. Click **Use Another Account**.
- b. In **User Name**, type the username.
- c. In **Password**, type the password.
- d. Press ENTER or click **OK**.

If the UAC dialog box does not give you the option to use another account, and prompts you for a username and password:

1. In **User Name**, type the username.
2. In **Password**, type the password.
3. Press ENTER or click **OK**.

Exercise 1: Implement Role-Based Management Using Groups

► Task 1: Prepare for the lab

1. Start 6425B-HQDC01-A.
2. Log on to HQDC01 as **Pat.Coleman** with the password **Pa\$\$w0rd**.
3. Open **D:\Labfiles\Lab04a**.
4. Run **Lab04a_Setup.bat** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
5. The lab setup script runs. When it is complete, press any key to continue.
6. Close the Windows Explorer window, **Lab04a**.

► Task 2: Create role groups with Active Directory Users and Computers

1. Run **Active Directory Users and Computers** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
2. In the console tree, expand the **contoso.com** domain and the **Groups** OU, and then click the **Role** OU.
3. Right-click the **Role** OU, then point to **New**, and then click **Group**.
4. In the **Group name** box, type **Sales**.
5. Select the **Global** group scope and **Security** group type. Click **OK**.
6. Repeat steps 3 through 5 to create a global security group called **Consultants**.

► **Task 3: Create role groups with DSAdd**

1. Run Command Prompt with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
2. Type the following command on one line, and then press ENTER:

```
dsadd group "CN=Auditors,OU=Role,OU=Groups,DC=contoso,DC=com"  
-secgrp yes -scope g
```

3. In Active Directory Users and Computers, confirm that the group was created successfully in the **Role** OU, inside the **Groups** OU.
 - If the Active Directory Users and Computers snap-in was open prior to performing this task, refresh the view.

► **Task 4: Add users to the role group**

1. In the Active Directory Users and Computers console tree, click the **Role** OU.
2. Right-click the **Sales** group, and then click **Properties**.
3. Click the **Members** tab.
4. Click the **Add** button.
5. Type **Tony Krijnen** and click **OK**.
6. Click **OK** to close the **Properties** dialog box.
7. In the console tree, expand the **User Accounts** OU, and then click the **Employees** OU.
8. Right-click **Linda Mitchell**, and then click **Add to a group**.
9. Type **Sales** and press ENTER.

The **Multiple Names Found** box appears, because there are two groups with names that begin with *Sales*.

10. Click **Sales**, and then click **OK**.

A message appears: *The Add to Group operation was successfully completed.*

11. Click **OK**.

► **Task 5: Implement a role hierarchy in which Sales Managers are also part of the Sales role**

1. In the console tree, expand the **Groups** OU, and then click the **Role** OU.
2. Right-click the **Sales Managers** group, and then click **Properties**.
3. Click the **Member Of** tab.
4. Click the **Add** button.
5. Type **Sales** and click **OK**.

The Multiple Names Found box appears, because there are two groups with names that begin with *Sales*.

6. Click **Sales**, and then click **OK**.
7. Click **OK** to close the **Properties** dialog box.

► **Task 6: Create a resource access management group**

1. In the console tree, click the **Groups\Access** OU.
2. Right-click the **Access** OU, then point to **New**, and then click **Group**.
3. In the **Group Name** box, type **ACL_Sales Folders_Read**.
4. Select the **Domain local** group scope and **Security** group type. Click **OK**.

► **Task 7: Assign permissions to the resource access management group**

1. Create a folder in D:\Data named **Sales**. If you are prompted for credentials use username **Pat.Coleman_Admin** with password **Pa\$\$w0rd**.
2. Right-click the **Sales** folder, then click **Properties**, and then click the **Security** tab.
3. Click **Edit**, and then click **Add**.
4. Type **ACL_** and press ENTER.

Notice that when you use a prefix for group names, such as the ACL_ prefix for resource access groups, you can find them quickly.

5. Click **ACL_Sales Folders_Read**, and then click **OK**.
6. Confirm that the group has been given Read & Execute permission.
7. Click **OK** to close each open dialog box.

► **Task 8: Define which roles and users have access to a resource**

1. In the Active Directory users and Computers console tree, click the **Access OU**.
2. Right-click the **ACL_Sales Folders_Read** group, and then click **Properties**.
3. Click the **Members** tab.
4. Click **Add**.
5. Type **Sales;Consultants;Auditors** and click **OK**.
The Multiple Items Found box appears because there are two groups with names that start with *Sales*.
6. Click **Sales** and click **OK**.
7. Click **Add**.
8. Type **Bobby Moore** and click **OK**.
9. Click **OK** to close the **Properties** dialog box.

Exercise 2: Manage Group Membership from the Command Prompt

► Task 1: Modify group membership with DSMod

1. Switch to the command prompt. It should still be running with administrator credentials from the previous exercise.
2. Type the following command on one line, and then press ENTER.

```
dsmod group "CN=Auditors,OU=Role,OU=Groups,DC=contoso,DC=com"  
-addmbr "CN=Mike Danseglio,OU=Employees,OU=User Accounts,  
DC=contoso,DC=com" "CN=Finance Managers,OU=Role,  
OU=Groups,DC=contoso,DC=com"
```

3. In the Active Directory Users and Computers console tree, click the **Role** OU.
4. Right-click the **Auditors** group, and then click **Properties**.
5. Click the **Members** tab.
6. Confirm that Mike Danseglio and the Finance Managers group are members, and then close the **Properties** dialog box.

► Task 2: Retrieve group membership with DSGet

1. Switch to the command prompt.
2. List the direct members of the **Auditors** group by typing the following command, and then pressing ENTER:

```
dsget group "CN=Auditors,OU=Role,OU=Groups,DC=contoso,DC=com"  
-members
```

3. List the full list of members of the **Auditors** group by typing the following command, and then pressing ENTER:

```
dsget group "CN=Auditors,OU=Role,OU=Groups,DC=contoso,DC=com"  
-members -expand
```

4. List the full list of members of the **ACL_Sales Folders_Read** group by typing the following command, and then pressing ENTER:

```
dsget group "CN=ACL_Sales Folders_Read,OU=Access,  
OU=Groups,DC=contoso,DC=com" -members -expand
```

5. List the direct group membership of **Mike Danseglio** by typing the following command, and then pressing ENTER:

```
dsget user "CN=Mike Danseglio,OU=Employees,OU=User Accounts,  
DC=contoso,DC=com" -memberof
```

6. List the full group membership of **Mike Danseglio** by typing the following command on one line, and then pressing ENTER:

```
dsget user "CN=Mike Danseglio,OU=Employees,OU=User Accounts,  
DC=contoso,DC=com" -memberof -expand
```



Note: Do not shut down the virtual machines once you are finished with this lab as the settings you have configured here will be used in the Lab B.

Lab Review Questions

Question: Describe the purpose of global groups in terms of role-based management.

Answer: Global groups are generally used to define roles.

Question: What types of objects can be members of global groups?

Answer: Global groups can include as members users and other roles (global groups) from the same domain.

Question: Describe the purpose of domain local groups in terms of role-based management of resource access.

Answer: Domain local groups are generally used to define a scope of management, such as managing a level of access to a resource.

Question: What types of objects can be members of domain local groups?

Answer: Domain local groups can contain roles (global groups) and individual users from any trusted domain in the same forest or an external forest, as well as other domain local groups in the same domain. Finally, domain local groups can contain universal groups from anywhere in the forest.

Question: If you have implemented role-based management and are asked to report who can read the Sales folders, what command would you use to do so?

Answer: You would use the DSGet command.

Lab B: Best Practices for Group Management

► Log on to a virtual machine

Unless otherwise instructed, use the following steps to log on to a virtual machine.

1. Press **ALT+DELETE**.

This sends the secure key sequence (CTRL+ALT+DELETE) to the virtual machine. If you press CTRL+ALT+DELETE, you send the secure key sequence to the host operating system.
2. Click **Switch User**.
3. Click **Other User**.
4. In **User name**, type the username.
5. In **Password**, type the password.
6. Press **ENTER** or click the log on arrow.

The Windows desktop appears.

► Run an application with administrative credentials

1. Right-click the application, and then click **Run as administrator**.
A User Account Control (UAC) dialog box appears.
2. The **UAC** dialog box will display one of three options. Do the steps based on the option you see:

If the UAC dialog box prompts you to continue or cancel:

- Click **Continue**.

If the UAC dialog box gives you the option to *Use another account*:

1. Click **Use Another Account**.
2. In **User Name**, type the username.
3. In **Password**, type the password.
4. Press **ENTER** or click **OK**.

If the UAC dialog box does not give you the option to use another account, and prompts you for a username and password:

1. In **User Name**, type the username.
2. In **Password**, type the password.
3. Press ENTER or click **OK**.

Exercise 1: Implement Best Practices for Group Management

► Task 1: Prepare for the lab

1. The virtual machine should already be started and available after completing Lab A. However, if it is not, you should launch it and complete the exercises in Lab A before continuing.
2. Start 6425B-HQDC01-A.
3. Log on to HQDC01 as **Pat.Coleman** with the password **Pa\$\$w0rd**.

► Task 2: Create a well-documented group

1. Run **Active Directory Users and Computers** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
2. In the console tree, expand the **Groups** OU, and then click the **Access** OU.
3. Right-click the **ACL_Sales Folders_Read** group and then click **Properties**.
4. In the **Description** box, summarize the resource management rule represented by the group. Type **Sales Folders (READ)**.
5. In the **Notes** box, type the following paths to represent the folders that have permissions assigned to this group and click OK when finished:
 `\\contoso\teams\Sales (READ)`
 `\\file02\data\Sales (READ)`
 `\\file03\news\Sales (READ)`

► Task 3: Protect a group from accidental deletion

1. Click the **View** menu, and then select **Advanced Features**, so that the Advanced Features option is enabled.
2. In the console tree, click the **Groups\Access** OU.
3. Right-click the **ACL_Sales Folders_Read** group, and then click **Properties**.
4. Click the **Object** tab.
5. Select the **Protect object from accidental deletion** check box and click **OK**.

6. Right-click **ACL_Sales Folders_Read**, and then click **Delete**.

A message appears asking if you are sure.

7. Click **Yes**.

A message appears: *You do not have sufficient privileges to delete ACL_Sales Folders_Read, or this object is protected from accidental deletion.*

8. Click **OK**.

► **Task 4: Delegate group membership management**

1. In the console tree, click the **Role** OU.
2. Right-click the **Auditors** group, and then click **Properties**.
3. Click the **Managed By** tab.
4. Click the **Change** button.
5. Type **Mike Danseglio** and click **OK**.
6. Select the **Manager can update membership list** check box. Click **OK**.

► **Task 5: Validate the delegation of group membership management**

1. Log off HQDC01.
2. Log on to HQDC01 with the username **Mike.Danseglio** and the password **Pa\$\$w0rd**.
3. Click **Start**, and then click **Network**.
4. Click **Search Active Directory**.
5. Type **Auditors**.
6. Click **Find Now**.
7. Double-click the **Auditors** group.
8. Click the **Add** button.
9. Type **Executives**, and then click **OK**.
10. Click **OK**.
11. Log off of HQDC01.



Note: After completing this exercise, turn off all virtual machines and discard undo disks.

Lab Review Questions

Question: What are some benefits of using the Description and Notes fields of a group?

Answer: Better documented groups are easier to find and understand, and are less likely to be misused for purposes other than their intended purpose.

Question: What are the advantages and disadvantages of delegating group membership?

Answer: Delegating group membership allows IT to get "out of the middle." In most organizations, when a user needs access to a resource, he or she contacts IT, IT contacts the business owner to get approval, and then IT adds the user to the groups. Delegating allows the request to go straight to the business owner, who can then make the change to the group.

Module 5: Support Computer Accounts

Lab A: Create Computers and Joining the Domain

► Log on to a virtual machine

Unless otherwise instructed, use the following steps to log on to a virtual machine.

1. Press ALT+DELETE.

This sends the secure key sequence (CTRL+ALT+DELETE) to the virtual machine. If you press CTRL+ALT+DELETE, you send the secure key sequence to the host operating system.

2. Click **Switch User**.
3. Click **Other User**.
4. In **User name**, type the username.
5. In **Password**, type the password.
6. Press ENTER or click the log on arrow.

The Windows desktop appears.

► Run an application with administrative credentials

1. Right-click the application, and then click **Run as administrator**.

A User Account Control (UAC) dialog box appears.

2. The **UAC** dialog box will display one of three options. Do the steps based on the option you see:

If the UAC dialog box prompts you to continue or cancel:

- Click **Continue**.

If the UAC dialog box gives you the option to *Use another account*:

- a. Click **Use Another Account**.
- b. In **User Name**, type the username.
- c. In **Password**, type the password.
- d. Press ENTER or click **OK**.

If the UAC dialog box does not give you the option to use another account, and prompts you for a username and password:

1. In **User Name**, type the username.
2. In **Password**, type the password.
3. Press ENTER or click **OK**.

Exercise 1: Join a Computer to the Domain with the Windows® Interface

► Task 1: Prepare for the lab

1. Start 6425B-HQDC01-A.
2. Log on to HQDC01 as **Pat.Coleman** with the password **Pa\$\$w0rd**.
3. Open **D:\Labfiles\Lab05a**.
4. Run **Lab05a_Setup.bat** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
5. The lab setup script runs. When it is complete, press any key to continue.
6. Close the Windows Explorer window, **Lab05a**.
7. Start 6425B-SERVER01-B.

► Task 2: Identify and correct a DNS configuration error

1. Log on to SERVER01 as **Administrator** with the password **Pa\$\$w0rd**.
2. Open **System Properties** using one of the following methods:
 - Click **Start**, then right-click **Computer**, and then click **Properties**.
 - Open **System** from **Control Panel**.
 - Press the WINDOWS LOGO key and the PAUSE key.
3. In the **Computer name, domain and workgroup settings** section, click **Change Settings**.

The System Properties dialog box appears.

4. On the **Computer Name** tab, click **Change**.
5. In the **Member Of** section, click **Domain**.
6. Type **contoso.com**.

Be sure to use the fully qualified domain name, contoso.com, not the NetBIOS name of the domain, contoso.

7. Click **OK**.

A dialog box appears, informing you that "An Active Directory® Domain Controller for the domain contoso.com could not be contacted."

8. Click **OK** to close the warning.
9. Click **Cancel** to close the **Computer Name/Domain Changes** dialog box, and **Cancel again** to close the **System Properties** dialog box.
10. Click **Start**, then right-click **Network**, and then click **Properties**.
The Network and Sharing Center opens.
11. Click the **View status** link next to **Local Area Connection**.
12. Click **Properties**.
The Local Area Connection Properties dialog box appears
13. Click **Internet Protocol Version 4 (TCP/IPv4)**, and then click **Properties**.
14. In the **Preferred DNS server** box, type **10.0.0.11**, and then click **OK**.
15. Click the **Close** button two times.

Question: Why might the join have succeeded if you had used the domain name contoso instead of contoso.com? What might go wrong after the domain was successfully joined with DNS but incorrectly configured?

Answer: The use of the fully qualified name forced the name resolution process to use DNS, and because DNS failed, the domain join failed. The domain name "contoso" is a flat domain name that could be resolved through NetBIOS name resolution. Even though the domain join would be successful, the client would likely have problems locating domain controllers in other sites, and locating other resources in the domain. Performing the join with a fully qualified domain name ensures that DNS is functioning before joining the domain.

► **Task 3: Join SERVER01 to the domain**

1. Open **System Properties** using one of the following methods:
 - If it is still open from the previous tasks in this exercise, click its button on the task bar.
 - Click **Start**, then right-click **Computer**, and then click **Properties**.
 - Open **System** from **Control Panel**.
 - Press the WINDOWS LOGO key and the PAUSE key.

2. In the **Computer name, domain and workgroup settings** section, click **Change Settings**.

The System Properties dialog box appears.

3. On the **Computer Name** tab, click **Change**.
4. In the **Member Of** section, click **Domain**.
5. Type **contoso.com**.
6. Click **OK**.

A Windows Security dialog box appears.

7. In **User name**, type **Aaron.Painter**.
8. In **Password**, type **Pa\$\$w0rd**.
9. Click **OK**.

A message appears: "Welcome to the contoso.com domain."

Note that Aaron.Painter is a standard user in the contoso.com domain. He has no special rights or permissions, and yet he is able to join a computer to the domain. He does have to be logged on to the computer with an account that is a member of the computer's Administrators group.

10. Click **OK**.

A message appears informing you to restart.

11. Click **OK**.

12. Click **Close** to close the **System Properties** dialog box.

Another message appears informing you to restart.

13. Click **Restart Now**.

► Task 4: Verify the location of the SERVER01 account

1. Switch to HQDC01.
2. Run **Active Directory Users and Computers** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.

3. In the console tree, expand the **contoso.com** domain, and then click the **Computers** container.
4. Locate SERVER01 in the **Computers** container.

Question: In which OU or container does the account exist?

Answer: The Computers container

► **Task 5: Remove SERVER01 from the domain**

1. Log on to SERVER01 as **Administrator** with the password **Pa\$\$w0rd**.
2. Open **System Properties** using one of the following methods:
 - Click **Start**, then right-click **Computer**, and then click **Properties**.
 - Open **System** from **Control Panel**.
 - Press the WINDOWS LOGO key and the PAUSE key.
3. In the **Computer name, domain and workgroup settings** section, click **Change Settings**.

The System Properties dialog box appears.

4. On the **Computer Name** tab, click **Change**.
5. In the **Member Of** section, click **Workgroup**.
6. Type **WORKGROUP**.
7. Click **OK**.

A message appears: "Welcome to the WORKGROUP workgroup."

8. Click **OK**.

A message appears informing you to restart.

9. Click **OK**.
10. Click **Close** to close the **System Properties** dialog box.

Another message appears informing you to restart.
11. Click **Restart Now**.

► **Task 6: Delete the SERVER01 account**

1. Switch to HQDC01.
2. In the Active Directory Users and Computers console tree, click the **Computers** container, and then click the **Refresh** button on the snap-in toolbar.

Question: On HQDC01, refresh the view of the Computers container and examine the SERVER01 account. What is its status?

Answer: Disabled

Question: You were not prompted for domain credentials in Task 5, and yet a change was made to the domain: the computer account was reset and disabled. What credentials were used to do this? What credentials were used to change the workgroup/domain membership of SERVER01?

Answer: This is a tricky question! Domain credentials with appropriate permissions *are* required to make a change to the domain, such as resetting and disabling a computer account; and credentials that are in the local Administrators group on the client are required to change the computer's workgroup/domain membership.

You were logged on to SERVER01 as the local Administrator, so you were able to change the computer's workgroup/domain membership. Normally, you would have been prompted for domain credentials, but it just so happens that the local Administrator account's username, Administrator, and password, Pa\$\$w0rd, are identical to those of the domain Administrator account, which of course has permission to modify objects in the domain. Windows attempts to authenticate you behind the scenes, and only prompts you for domain credentials if that authentication fails. In this case, because of the similarity in credentials, you were actually authenticated as the domain's Administrator.

In a production environment, the domain's Administrator account should have a very long, complex, secure password that is *different* from the passwords used for domain member computer Administrator accounts.

3. Right-click SERVER01, and then click **Delete**.
You are prompted to confirm the deletion.
4. Click **Yes**.

Exercise 2: Secure Computer Joins

► Task 1: Redirect the default computer container

1. Still on HQDC01 run **Command Prompt** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
2. Type the following command:

```
redircmp "OU=New Computers,DC=contoso,DC=com"
```

and then press ENTER.

The output of the command indicates that it completed successfully.

3. Close the Command Prompt window.

► Task 2: Restrict unmanaged domain joins

1. Run **ADSI Edit** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
2. Right-click **ADSI Edit**, and then click **Connect To**.
The Connection Settings dialog box appears.
3. In the **Connection Point** section, click **Select A Well Known Naming Context**, and from the drop-down list choose **Default Naming Context**.
4. Click **OK**.
5. Click **Default naming context** in the console tree.
6. In the details pane, right-click the domain folder, **dc=contoso,dc=com**, and then click **Properties**.
7. Click **ms-DS-MachineAccountQuota** and click **Edit**.
8. Type **0**.
9. Click **OK**.
10. Click **OK** to close the **Attribute Editor**.
11. Close ADSI Edit.

► **Task 3: Validate the effectiveness of ms-DS-MachineAccountQuota**

1. Log on to SERVER01 as **Administrator** with the password **Pa\$\$w0rd**.
2. Open **System Properties** using one of the following methods:
 - Click **Start**, then right-click **Computer**, and then click **Properties**.
 - Open **System** from **Control Panel**.
 - Press the WINDOWS LOGO key and the PAUSE key.
3. In the **Computer name, domain and workgroup settings** section, click **Change Settings**.

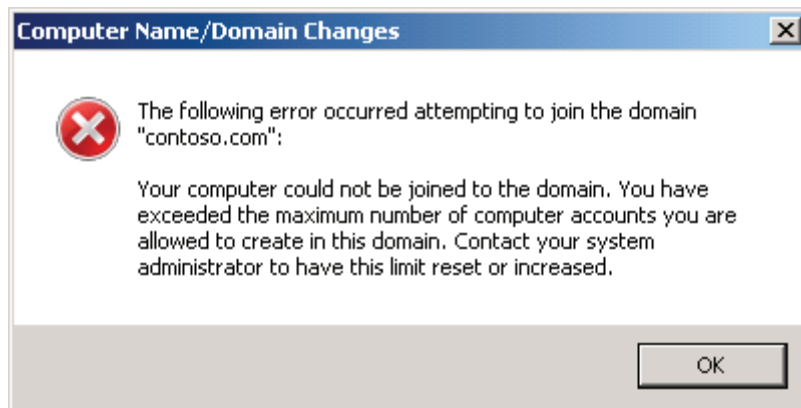
The System Properties dialog box appears.

4. On the **Computer Name** tab, click **Change**.
5. In the **Member Of** section, click **Domain**.
6. Type **contoso.com**.
7. Click **OK**.

A Windows Security dialog box appears.

8. In **User name**, type **Aaron.Painter**.
9. In **Password**, type **Pa\$\$w0rd**.
10. Click **OK**.

The message below appears:



11. Click **OK**.
12. Click **Cancel**.
13. Click **Cancel** to close the **System Properties** dialog box.

Exercise 3: Manage Computer Account Creation with Best Practices

► Task 1: Prestage a computer account

1. Switch to HQDC01.
2. In the Active Directory Users and Computers console tree, expand the **contoso.com** domain and the **Servers** OU, and then click the **File** OU.
3. Right-click the **File** OU, then point to **New**, and then click **Computer**.
The New Object - Computer dialog box appears.
4. In **Computer Name**, type **SERVER01**.
5. Click the **Change** button next to **User or Group**.
The Select User or Group dialog box appears.
6. Type **AD_Server_Deploy** and press ENTER.
7. Click **OK**.

► Task 2: Join a computer remotely to a prestaged account using NetDom

1. Run **Command Prompt** with administrative credentials. Use the account **Aaron.Painter_Admin** with the password **Pa\$\$w0rd**.
Aaron.Painter_Admin is a member of the **AD_Server_Deploy** group. In the previous task, you gave the group permission to join SERVER01 to the domain.
2. Type the command **whoami /groups** to list the group memberships of the current account (**Aaron.Painter_Admin**). Note that the user is a member of **AD_Server_Deploy** and is not a member of any other administrative group.

3. Type the following command on one line (the line can wrap), and then press ENTER:

```
netdom join SERVER01 /domain:contoso.com  
/UserO:Administrator /Password0:*  
/UserD:CONTOSO\Aaron.Painter_Admin /PasswordD:*  
/REBoot:5
```

You are prompted for the password associated with the domain user, CONTOSO\Aaron.Painter_Admin.

4. Type **Pa\$\$w0rd** and press ENTER.

You are prompted for the password associated with the object user, SERVER01\Administrator.

5. Type **Pa\$\$w0rd** and press ENTER.
6. The command completes successfully and SERVER01 restarts.
7. Log on to SERVER01 as **Pat.Coleman** with the password **Pa\$\$w0rd**.
This confirms that the server has successfully joined the domain.
8. Log off of SERVER01.



Note: Do not shut down the virtual machines once you are finished with this lab as the settings you have configured here will be used in the Lab B.

Lab B: Administer Computer Objects and Accounts

► Log on to a virtual machine

Unless otherwise instructed, use the following steps to log on to a virtual machine.

1. Press ALT+DELETE.

This sends the secure key sequence (CTRL+ALT+DELETE) to the virtual machine. If you press CTRL+ALT+DELETE, you send the secure key sequence to the host operating system.

2. Click **Switch User**.
3. Click **Other User**.
4. In **User name**, type the username.
5. In **Password**, type the password.
6. Press ENTER or click the log on arrow.

The Windows desktop appears.

► Run an application with administrative credentials

1. Right-click the application, and then click **Run as administrator**.

A User Account Control (UAC) dialog box appears.

2. The **UAC** dialog box will display one of three options. Do the steps based on the option you see:

If the UAC dialog box prompts you to continue or cancel:

- Click **Continue**.

If the UAC dialog box gives you the option to *Use another account*:

1. Click **Use Another Account**.
2. In **User Name**, type the username.
3. In **Password**, type the password.
4. Press ENTER or click **OK**.

If the UAC dialog box does not give you the option to use another account, and prompts you for a username and password:

- a. In **User Name**, type the username.
- b. In **Password**, type the password.
- c. Press ENTER or click **OK**.

Exercise 1: Administer Computer Objects Through Their Life Cycle

► Task 1: Prepare for the lab

The virtual Machines should already be started and available after completing Lab A. However, if they are not, you should complete steps 1 to 3 below and then step through exercises 1 to 3 in Lab A before continuing. You will be unable to successfully complete Lab B unless you have completed Lab A.

1. Start 6425B-HQDC01-A.
2. Log on to HQDC01 as **Pat.Coleman** with the password **Pa\$\$w0rd**.
3. Start 6425B-SERVER01-B.

► Task 2: Configure computer object attributes

1. On HQDC01 run **Active Directory Users and Computers** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
2. In the console tree, expand the **contoso.com** domain and the **Client Computers** OU, and then click **SEA**.
3. Right-click **LNO8538**, and then click **Properties**.
4. Click the **Managed By** tab.
5. Click the **Change** button.
6. Type **Linda Mitchell** and press ENTER.
Note that Linda's contact information is populated on the Managed By tab.
7. Click **OK** to close the computer **Properties** dialog box.
8. Repeat steps 3 through 8 to assign **LOT9179** to **Scott Mitchell**.
9. Click **LOT9179**.
10. Press and hold CTRL while you click **LNO8538**. You should now have both computers selected.

11. Right-click either of the highlighted items, **LNO8538** or **LOT9179**, and then click **Properties**.
12. Select the **Change the description text for all selected objects** check box.
13. Type **Scott and Linda Mitchell**.
14. Click **OK**.

► **Task 3: Add computers to software management groups**

1. In the console tree, click the **SEA** OU, then right-click **LOT9179** in the details pane, and then click **Add to a group**.
2. Type **APP_** and press ENTER.
The Multiple Items Found dialog box appears.
3. Click **APP_Project** and click **OK**.
A message appears: "The Add to Group operation was successfully completed."
4. Click **OK**.
5. In the console tree, expand the **Groups** OU, and then click **Application**.
6. Right-click **APP_Project**, and then click **Properties**.
7. Click the **Members** tab.
8. Click **Add**.
9. Type **LNO8538** and press ENTER.
The Name Not Found dialog box appears.
By default, the Select Users, Computers, or Groups interface does not search for computer objects.
10. Click **Object Types**.
11. Select the check box next to **Computers**, and then click **OK**.
12. Click **OK** to close the **Name Not Found** dialog box.
Both computers can now be seen on the **Members** tab.
13. Click **OK**.

► **Task 4: Move a computer between OUs**

1. In the **Client Computers\SEA OU**, click **LOT9179**.
2. Drag **LOT9179** into the **VAN OU**, visible in the console tree.
A message appears that reminds you to be careful about moving objects in Active Directory.
3. Click **Yes**.
4. Right-click **LNO8538**, and then click **Move**.
The Move dialog box appears.
5. Expand the **Client Computers** OU, and then click the **VAN OU**.
6. Click **OK**.

► **Task 5: Disable, enable, and delete computers**

1. In the **SEA OU**, right-click **DEP6152**, and then click **Disable Account**.
A confirmation message appears.
2. Click **Yes**.
A message appears: "Object DEP6152 has been disabled."
3. Click **OK**.
4. Right-click **DEP6152**, and then click **Enable Account**.
A message appears: "Object DEP6152 has been enabled."
5. Click **OK**.
6. Right-click **DEP6152**, and then click **Delete**.
A confirmation message appears.
7. Click **Yes**.

Exercise 2: Administer and Troubleshooting Computer Accounts

► Task 1: Reset a computer account

1. In the **VAN** OU, right-click **LOT9179**, and then click **Reset Account**.
A confirmation message appears.
2. Click **Yes**.
A message appears: "Account LOT9179 was successfully reset."
3. Click **OK**.

► Task 2: Experience a secure channel problem

1. Log on to SERVER01 as **Pat.Coleman** with the password **Pa\$\$w0rd**.
2. Click **Start**, then point to the arrow next to the **Lock** icon, and then click **Log Off**.
3. Switch to HQDC01.
4. In the Active Directory Users and Computers console tree, expand the **Servers** OU, and then click the **File** OU.
5. Right-click SERVER01, and then click **Reset Account**.
Because SERVER01 is currently joined to the domain correctly, this step effectively breaks the trust relationship by resetting the account password on the domain without involving or informing SERVER01 itself. The computer therefore does not know its new password.
A confirmation message appears.
6. Click **Yes**.
A message appears: "Account SERVER01 was successfully reset."
7. Click **OK**.
8. On SERVER01, attempt to log on as **Pat.Coleman** with the password **Pa\$\$w0rd**.
A message appears: "The trust relationship between this workstation and the primary domain failed."
9. Click **OK**.

► **Task 3: Reset the secure channel**

1. Switch to HQDC01.
2. In the Active Directory Users and Computers console tree, expand the **Servers** OU, and then click the **File** OU.
3. Right-click SERVER01, and then click **Reset Account**.

A confirmation message appears.

4. Click **Yes**.

A message appears: "Account SERVER01 was successfully reset."

5. Click **OK**.

After resetting the secure channel, you could move SERVER01 into a workgroup, and then rejoin the domain. It will join its reset account, thereby retaining its group memberships. Do not perform that step at this time.



Note: After completing this exercise, turn off all virtual machines and discard undo disks.

Module 6: Implement a Group Policy Infrastructure

Lab A: Implement Group Policy

► Log on to a virtual machine

Unless otherwise instructed, use the following steps to log on to a virtual machine.

1. Press ALT+DELETE.
This sends the secure key sequence (CTRL+ALT+DELETE) to the virtual machine. If you press CTRL+ALT+DELETE, you send the secure key sequence to the host operating system.
2. Click **Switch User**.
3. Click **Other User**.
4. In **User name**, type the user name.
5. In **Password**, type the password.
6. Press ENTER or click the logon arrow.
The Windows® desktop appears.

► Run an application with administrative credentials

1. Right-click the application, and then click **Run as administrator**.
A User Account Control (UAC) dialog box appears.
2. The **UAC** dialog box will display one of three options. Perform the steps based on the option you see:
If the UAC dialog box prompts you to continue or cancel:
 - Click **Continue**.
If the UAC dialog box gives you the option to use another account:
 - a. Click **Use Another Account**.
 - b. In **User Name**, type the username.
 - c. In **Password**, type the password.
 - d. Press ENTER or click **OK**.

If the UAC dialog box does not give you the option to use another account, and prompts you for a username and password:

1. In **User Name**, type the username.
2. In **Password**, type the password.
3. Press ENTER or click **OK**.

Exercise 1: Create, Edit, and Link Group Policy Objects

► Task 1: Prepare for the lab

1. Start 6425B-HQDC01-A.
2. Log on to HQDC01 as **Pat.Coleman** with the password **Pa\$\$w0rd**.
3. Start 6425B-DESKTOP101-A but do not log on to the system.

► Task 2: Create a GPO

1. Run **Group Policy Management** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
2. In the console tree, expand **Forest: contoso.com, Domains**, and **contoso.com**, and then click the **Group Policy Objects** container.
3. In the console tree, right-click the **Group Policy Objects** container, and then click **New**.
4. In **Name**: type **CONTOSO Standards**, and then click **OK**.

► Task 3: Edit the settings of a GPO

1. In the details pane of the Group Policy Management console (GPMC), right-click the **CONTOSO Standards** GPO, and then click **Edit**.
The Group Policy Management Editor (GPME) appears.
2. In the console tree, expand **User Configuration, Policies**, and **Administrative Templates**, and then click **System**.
3. Double-click the **Prevent access to registry editing tools** policy setting.
4. Click **Enabled**.
5. In the **Disable regedit from running silently?** drop-down list, select **Yes**.
6. Click **OK**.
7. In the console tree, expand **User Configuration, Policies, Administrative Templates**, and **Control Panel**, and then click **Display**.
8. In the details pane, click the **Screen Saver timeout** policy setting.
9. Note the explanatory text in the left margin of the console's details pane.

10. Double-click the **Screen Saver timeout** policy setting.
11. Review the explanatory text on the **Explain** tab.
12. Click the **Setting** tab and click **Enabled**.
13. In the **Seconds** box, type **600**, and click **OK**.
14. Double-click the **Password protect the screen saver** policy setting.
15. Click **Enabled**, and click **OK**.
16. Close the GPME.

Changes you make in the GPME are saved in real time. There is no Save command.

► **Task 4: Scope a GPO with a GPO link**

1. In the GPMC console tree, right-click the **contoso.com** domain, and then click **Link an Existing GPO**.
2. Select **CONTOSO Standards** and click **OK**.

► **Task 5: View the effects of Group Policy application**

1. Switch to DESKTOP101.
2. Log on to DESKTOP101 as **Pat.Coleman** with the password **Pa\$\$w0rd**.
3. Right-click the desktop, and then click **Personalize**.
4. Click **Screen Saver**.
5. Notice that the **Wait** control is disabled—you cannot change the timeout.
6. Notice that the **On resume, display logon screen** option is selected and disabled—you cannot disable password protection.
7. Click **OK** to close the **Screen Saver** dialog box.
8. Click **Start** and, in the **Start Search** box, type **regedit.exe**. Then press ENTER.
A message appears: “Registry editing has been disabled by your administrator.”
9. Click **OK**.

► **Task 6: Explore GPO settings**

1. Switch to HQDC01.
2. Right-click the **CONTOSO Standards** GPO, and then click **Edit**.
3. Spend time exploring the settings that are available in a GPO. Do not make any changes.



Note: Do not shut down the virtual machines once you are finished with this lab as the settings you have configured here will be used in subsequent labs.

Lab Review Questions

Question: What policy settings are already being deployed using Group Policy in your organization?

Answer: The correct answer will be based on your own experience and situation.

Question: What policy settings did you discover that you might want to implement in your organization?

Answer: The correct answer will be based on your own experience and situation.

Lab B: Manage Settings and GPOs

► Log on to a virtual machine

Unless otherwise instructed, use the following steps to log on to a virtual machine.

1. Press ALT+DELETE.

This sends the secure key sequence (CTRL+ALT+DELETE) to the virtual machine. If you press CTRL+ALT+DELETE, you send the secure key sequence to the host operating system.

2. Click **Switch User**.
3. Click **Other User**.
4. In **User name**, type the username.
5. In **Password**, type the password.
6. Press ENTER or click the logon arrow.

The Windows desktop appears.

► Run an application with administrative credentials

1. Right-click the application, and then click **Run as administrator**.

A User Account Control (UAC) dialog box appears.

2. The **UAC** dialog box will display one of three options. Perform the steps based on the option you see:

If the UAC dialog box prompts you to continue or cancel:

- Click **Continue**.

If the UAC dialog box gives you the option to use another account:

1. Click **Use Another Account**.
2. In **User Name**, type the username.
3. In **Password**, type the password.
4. Press ENTER or click **OK**.

If the UAC dialog box does not give you the option to use another account, and prompts you for a username and password:

1. In **User Name**, type the username.
2. In **Password**, type the password.
3. Press ENTER or click **OK**.

Exercise 1: Use Filtering and Commenting

► Task 1: Prepare for the lab

The virtual machine should already be started and available after completing Lab A. However, if it is not, you should complete the below steps then step through exercises 1 in Lab A before continuing.

1. Start 6425B-HQDC01-A.
2. Log on to HQDC01 as **Pat.Coleman** with the password **Pa\$\$w0rd**.

► Task 2: Search and filter policy settings

1. Run **Group Policy Management** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
2. In the console tree, expand **Forest: contoso.com**, **Domains**, and **contoso.com**, and then click the **Group Policy Objects** container.
3. In the details pane, right-click the **CONTOSO Standards** GPO, and then click **Edit**.

The Group Policy Management Editor appears.

4. In the console tree, expand **User Configuration** and **Policies**, and then click **Administrative Templates**.
5. Right-click **Administrative Templates**, and then click **Filter Options**.
6. Select the **Enable Keyword Filters** check box.
7. In the **Filter for word(s)** text box, type **screen saver**.
8. In the drop-down list next to the text box, select **Exact**, and click **OK**.

Administrative Templates policy settings are filtered to show only those that contain the words *screen saver*.

9. Spend a few moments examining the settings that you have found.
10. In the console tree, right-click **Administrative Templates** under **User Configuration**, and then click **Filter Options**.
11. Clear the **Enable Keyword Filters** check box.

12. In the **Configured** drop-down list, select **Yes**, and then click **OK**.
Administrative Template policy settings are filtered to show only those that have been configured (enabled or disabled).
13. Spend a few moments examining those settings.
14. In the console tree, right-click **Administrative Templates** under **User Configuration** and clear the **Filter On** option.

► **Task 3: Document GPOs and settings with comments**

1. In the console tree of the Group Policy Management Editor, right-click the root node, **CONTOSO Standards**, and then click **Properties**.
2. Click the **Comment** tab.
3. Type **Contoso corporate standard policies. Settings are scoped to all users and computers in the domain. Person responsible for this GPO: your name.**
This comment appears on the Details tab of the GPO in the GPMC.
4. Click **OK**.
5. In the console tree, expand **User Configuration, Policies, Administrative Templates**, and **Control Panel**, and then click **Display**.
6. Double-click the **Screen Saver** policy setting.
7. Click the **Comment** tab.
8. Type **Corporate IT Security Policy implemented with this policy in combination with Password Protect the Screen Saver**, and click **OK**.
9. Double-click the **Password protect the screen saver** policy setting.
10. Click the **Comment** tab.
11. Type **Corporate IT Security Policy implemented with this policy in combination with Screen Saver Timeout**, and click **OK**.

Exercise 2: Manage Administrative Templates

► Task 1: Explore the syntax of an administrative template

1. Click **Start**, then click **Run**, then type `%SystemRoot%\PolicyDefinitions` and then press ENTER.

The PolicyDefinitions folder opens.

2. Open the **en-us** folder or the folder for your region and language.
3. Double-click **ControlPanelDisplay.adml**.
4. Click the **Select a program from a list of installed programs** option and click **OK**.
5. Click **Notepad** and click **OK**.
6. Click the **Format** menu and select the **Word wrap** option, so that it is enabled.
7. Search for the text **ScreenSaverIsSecure**.

This is a definition of a string variable called ScreenSaverIsSecure.

8. Note the text between the `<string>` and `</string>` tags.
9. Note the name of the variable on the following line, **ScreenSaverIsSecure_Help**, and the text between the `<string>` and `</string>` tags.
10. Close the file.
11. Navigate up to the **PolicyDefinitions** folder.
12. Double-click **ControlPanelDisplay.admx**.
13. Click the **Select a program from a list of installed programs** option and click **OK**.
14. Click **Notepad** and click **OK**.
15. Search for the text, **ScreenSaverIsSecure**.

16. Examine the code in the file, also shown below:

```
<policy name="ScreenSaverIsSecure" class="User"
displayName="$(string.ScreenSaverIsSecure)"
explainText="$(string.ScreenSaverIsSecure_Help)"
key="Software\Policies\Microsoft\Windows\Control Panel\Desktop"
valueName="ScreenSaverIsSecure">
  <parentCategory ref="Display" />
  <supportedOn ref="windows:SUPPORTED_Win2kSP1" />
  <enabledValue>
    <string>1</string>
  </enabledValue>
  <disabledValue>
    <string>0</string>
  </disabledValue>
</policy>
```

17. Identify the parts of the template that define the following:
- The name of the policy setting that appears in the GPME
 - **Answer:** \$(string.ScreenSaverIsSecure)
 - The explanatory text for the policy setting
 - **Answer:** \$(string.ScreenSaverIsSecure_Help)
 - The registry key and value affected by the policy setting
 - class="User" (HKCU)
 - key="Software\Policies\Microsoft\Windows\Control Panel\Desktop"
 - valueName="ScreenSaverIsSecure"
 - The data put into the registry if the policy is enabled
 - <enabledValue><string>1</string></enabledValue>
 - The data put into the registry if the policy is disabled
 - <disabledValue><string>0</string></disabledValue>
18. Close the file, and then close the Windows Explorer window, **PolicyDefinitions**.

► **Task 2: Manage classic administrative templates (.ADM files)**

1. Switch to the GPME.
2. In the console tree, expand **User Configuration** and **Policies**, and then click **Administrative Templates**.
3. Right-click **Administrative Templates**, and then click **Add/Remove Templates**.
4. Click **Add**.
5. Browse to **D:\Labfiles\Lab06b\Office 2007 Administrative Templates**.
6. Open the **ADM** folder and then the **en-us** folder.
7. Click **office12.adm** and click **Open**.
8. Click **Close**.

The Classic Administrative Templates (ADM) node appears in the Administrative Templates tree.

9. In the console tree, expand **Administrative Templates**, **Classic Administrative Templates (ADM)** and **Microsoft Office 2007 System**.

Classic administrative templates (.ADM files) are provided primarily for enterprises that do not manage Group Policy with Windows Vista® or Windows Server® 2008 or later operating systems.

You should use a computer running the most recent version of Windows to manage Group Policy. By doing so, you will be able to view and modify all available policy settings, including those that apply to previous versions of Windows. If you have at least one computer running Windows Vista, Windows Server 2008, or later, you should use that computer to manage Group Policy, and then you will not need classic administrative templates (.ADM files) when .ADMX/.ADML files are available.

Note that the template format affects only the *management* of Group Policy. Settings will apply to versions of Windows as described in the Supported on or Requirements section of the policy setting properties.

10. Right-click **Administrative Templates**, and then click **Add/Remove Templates**.
11. Click **office12**, and then click **Remove**.
12. Click **Close**.

► **Task 3: Manage .ADMX and .ADML files**

1. Click **Start**, click **Run**, and then type **D:\Labfiles\Lab06b\Office 2007 Administrative Templates** and press **ENTER**.
2. Open the **ADMX** folder.
3. Select all .ADMX files and the **en-us** folder, or the appropriate folder for your language and region, and then press **CTRL+C** to copy the files and the folder.
4. Click **Start**, click **Run**, and then type **%SystemRoot%\PolicyDefinitions** and press **ENTER**.
5. Press **CTRL+V** to paste the files and the folder.
You are prompted to merge the en-us folder.
6. Select the **Do this for all current items** check box, and then click **Yes**.
You are prompted for administrative permissions.
7. Select the **Do this for all current items** check box, and then click **Continue**. A **User Account Control** dialog box appears.
8. In **User name**, type **Pat.Coleman_Admin**.
9. In **Password**, type **Pa\$\$word**.
10. Click **OK**.
11. Close Windows Explorer.
12. Close the GPME.
13. In the GPMC console tree, right-click **CONTOSO Standards**, and then click **Edit**. The GPME appears.
14. In the console tree, expand **User Configuration** and **Policies**, and then click **Administrative Templates**.
15. Note the addition of Microsoft® Office 2007 policy setting folders.

► **Task 4: Create the central store**

1. In the GPME, click the **Administrative Templates** node underneath **User Configuration\Policies**.
2. In the details pane heading, note the message, **Policy definitions (ADMX files) retrieved from the local machine**.

3. Close the GPME.
4. Run the command prompt with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
5. Type **md \\contoso.com\SYSVOL\contoso.com\Policies\PolicyDefinitions\en-us**, and then press ENTER.

If you are using another language or region, substitute *en-us* with the appropriate folder.

6. Type **xcopy %systemroot%\PolicyDefinitions\\contoso.com\SYSVOL\contoso.com\Policies\PolicyDefinitions**, and then press ENTER.

The .ADMX files are copied.

7. Type **xcopy %systemroot%\PolicyDefinitions\en-us\\contoso.com\SYSVOL\contoso.com\Policies\PolicyDefinitions\en-us**, and then press ENTER.

If you are using another language or region, substitute *en-us* with the appropriate folder.

The .ADML files are copied.

8. In the GPMC, right-click **CONTOSO Standards**, and then click **Edit**.
9. In the console tree, expand **User Configuration** and **Policies**, and then click **Administrative Templates**.
10. In the details pane heading, note the message, **Policy definitions (ADMX files) retrieved from the central store**.



Note: Do not shut down the virtual machines once you are finished with this lab as the settings you have configured here will be used in subsequent labs.

Lab Review Questions

Question: Describe the relationship between administrative template files (both .ADMX and .ADML files) and the GPME.

Answer: .ADMX files create the user interface for the GPME and determine the registry values that are applied when a policy setting is defined. .ADML files provide the language-specific elements (the text) in the user interface.

Question: When does an enterprise get a central store? What benefits does it provide?

Answer: A central store is manually created by adding a PolicyDefinitions folder to \\domain\\sysvol\\domain\\Policies.

Question: What are the advantages of managing Group Policy from a client running the latest version of Windows? Do settings you manage apply to previous versions of Windows?

Answer: If you manage Group Policy with a client running the latest version of Windows, you will be able to use the latest administrative templates, and you will be able to view settings that apply to this and all previous versions of Windows. The policy settings you configure will apply not based on the version of Windows from which you manage Group Policy, but rather based on the versions of Windows to which the policy setting can apply.

Lab C: Manage Group Policy Scope

► Log on to a virtual machine

Unless otherwise instructed, use the following steps to log on to a virtual machine.

1. Press ALT+DELETE.

This sends the secure key sequence (CTRL+ALT+DELETE) to the virtual machine. If you press CTRL+ALT+DELETE, you send the secure key sequence to the host operating system.

2. Click **Switch User**.
3. Click **Other User**.
4. In **User name**, type the username.
5. In **Password**, type the password.
6. Press ENTER or click the logon arrow.

The Windows desktop appears.

► Run an Application with Administrative Credentials

1. Right-click the application, and then click **Run as administrator**.

A User Account Control (UAC) dialog box appears.

2. The **UAC** dialog box will display one of three options. Perform the steps based on the option you see:

If the UAC dialog box prompts you to continue or cancel:

- Click **Continue**.

If the UAC dialog box gives you the option to use another account:

1. Click **Use Another Account**.
2. In **User Name**, type the username.
3. In **Password**, type the password.
4. Press ENTER or click **OK**.

If the UAC dialog box does not give you the option to use another account, and prompts you for a username and password:

1. In **User Name**, type the username.
2. In **Password**, type the password.
3. Press ENTER or click **OK**.

Exercise 1: Configure GPO scope with links

► Task 1: Prepare for the lab

The virtual machines should already be started and available after completing Labs A and B. However, if they are not, you should complete the below steps then step through the exercises in Labs A and B before continuing.

1. Start 6425B-HQDC01-A.
2. Log on to HQDC01 as **Pat.Coleman** with the password **Pa\$\$w0rd**.
3. Start 6425B-DESKTOP101-A but do not log on to the system.

► Task 2: Create a GPO with a policy setting that takes precedence over a conflicting setting

1. Run **Active Directory Users and Computers** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
2. In the console tree, expand the **contoso.com** domain and the **User Accounts** OU, and then click the **Employees** OU.
3. Right-click the **Employees** OU, point to **New**, and then click **Organizational unit**.
4. Type **Engineers**, and then click **OK**.
5. Close **Active Directory Users and Computers**.
6. Run the **Group Policy Management** console with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
The **Group Policy Management** console opens.
7. In the console tree, expand **Forest: contoso.com**, **Domains**, **contoso.com**, **User Accounts**, and **Employees**, and then click the **Engineers** OU.
8. Right-click the **Engineers** OU, and then click **Create a GPO in this domain and Link it here**.
9. Type **Engineering Application Override** and press **ENTER**.
10. Right-click the **Engineering Application Override** GPO, and then click **Edit**.
The **Group Policy Management Editor** appears.

11. In the console tree, expand **User Configuration, Policies, Administrative Templates**, and **Control Panel**, and then click **Display**.
12. Double-click the **Screen Saver timeout** policy setting.
13. Click **Disabled**, and click **OK**.
14. Close the GPME.
15. In the GPMC console tree, click the **Engineers OU**.
16. Click the **Group Policy Inheritance** tab.
17. Notice that the **Engineering Application Override** GPO has higher precedence than the **CONTOSO Standards** GPO.

The screen saver timeout policy setting you just configured in the Engineering Application Override GPO will be applied after the setting in the CONTOSO Standards GPO. Therefore, the new setting will overwrite the standards setting, and will "win." Screen saver timeout will be disabled for users within the scope of the Engineering Application Override GPO.

► **Task 3: View the effect of an enforced GPO link**

1. In the GPMC console tree, click the **Domain Controllers** OU, and then click the **Group Policy Inheritance** tab.
2. Notice that the GPO named **6425B** has the highest precedence. Settings in this GPO will override any conflicting settings in any of the other GPOs.

The Default Domain Controllers GPO specifies, among other things, which groups are given the right to log on locally to domain controllers. To enhance the security of domain controllers, standard users are not given the right to log on locally. In order to allow a nonprivileged user account such as Pat.Coleman to log on to domain controllers in this course, the 6425B GPO gives Domain Users the right to log on locally to a computer. The 6425B GPO is linked to the domain, so its settings would normally be overridden by settings in the Default Domain Controllers GPO. Therefore, the 6425B GPO link to the domain is configured as Enforced. In this way, the conflict in user rights assignment between the two GPOs is "won" by the 6425B GPO.

► **Task 4: Apply Block Inheritance**

1. In the GPMC console tree, click the **Engineers** OU, and then click the **Group Policy Inheritance** tab.
2. Examine the precedence and inheritance of GPOs.
3. Right-click the **Engineers** OU, and then click **Block Inheritance**.

Question: What GPOs continue to apply to users in the Engineers OU? Where are those GPOs linked? Why did they continue to apply?

Answer: The Engineering Application Override GPO, which is linked to the Engineers OU itself, and the 6425B GPO, linked to the domain, continue to apply. The 6425B GPO continues to apply to users in this OU because its link is Enforced.

4. Right-click the **Engineers** OU, and then clear **Block Inheritance**.

Exercise 2: Configure GPO Scope with Filtering

► Task 1: Configure policy application with security filtering

1. Switch to Active Directory Users and Computers.
2. In the console tree, expand the **contoso.com** domain and the **Groups** OU, and then click the **Configuration** OU.
3. Right-click the **Configuration** OU, then point to **New**, and then click **Group**.
4. Type **GPO_Engineering Application Override_Apply**, and then press ENTER.
5. Switch to the Group Policy Management console.
6. In the console tree, expand the **Engineers** OU, and then click the link of the **Engineering Application Override** GPO underneath the **Engineers** OU.
A message appears.
7. Read the message, then click **Do not show this message again**, and then click **OK**.
8. Notice in the **Security Filtering** section that the GPO applies by default to all authenticated users.
9. In the **Security Filtering** section, click **Authenticated Users**.
10. Click the **Remove** button. A confirmation prompt appears.
11. Click **OK**.
12. Click the **Add** button.
The Select User, Computer, or Group dialog box appears.
13. Type **GPO_Engineering Application Override_Apply** and press ENTER.

► Task 2: Configure an exemption with security filtering

1. Switch to Active Directory Users and Computers.
2. In the console tree, expand the **contoso.com** domain and the **Groups** OU, then click the **Configuration** OU.
3. Right-click the **Configuration** OU, then point to **New**, and then click **Group**.
4. Type **GPO_CONTOSO Standards_Exempt**, and then press ENTER.

5. Switch to the Group Policy Management console.
6. In the console tree, click the link of the **CONTOSO Standards** GPO to the **contoso.com** domain.
7. In the **Security Filtering** section, notice that the GPO applies by default to all authenticated users.
8. Click the **Delegation** tab.
9. Click the **Advanced** button.

The CONTOSO Standards Security Settings dialog box appears.
10. Click the **Add** button.

The Select User, Computer, or Group dialog box appears.
11. Type **GPO_CONTOSO Standards_Exempt** and press ENTER.
12. Click the check box below **Deny** and next to **Apply group policy**.
13. Click **OK**.

A warning message appears to remind you that deny permissions override allow permissions.
14. Click **Yes**.
15. Notice that the permission appears on the **Delegation** tab as **Custom**.

Exercise 3: Configure Loopback Processing

► Task 1: Configure loopback processing

1. In the GPMC console tree, expand the **Kiosks** OU, and then click the **Conference Rooms** OU.
2. Right-click the **Conference Rooms** OU and then click **Create a GPO in this domain, and Link it here**.
3. In **Name**, type **Conference Room Policies**, and then press ENTER.
4. In the console tree, expand **Conference Rooms**, and then click the **Conference Room Policies** GPO.
5. Click the **Scope** tab.
6. Confirm that the GPO is scoped to apply to **Authenticated Users**.
7. Right-click the **Conference Room Policies** GPO in the console tree, and then click **Edit**.

The Group Policy Management Editor appears.

8. In the GPME console tree, expand **User Configuration, Policies, Administrative Templates**, and then click **Control Panel**, and then click **Display**.
9. Double-click the **Screen Saver** timeout policy setting.
10. Click **Enabled**.
11. In the **Seconds** box, type **2700**, and click **OK**.
12. In the console tree, expand **Computer Configuration, Policies, Administrative Templates**, and then click **System**, and then click **Group Policy**.
13. Double-click the **User Group Policy loopback processing mode** policy setting.
14. Click **Enabled**.

15. In the **Mode** drop-down list, select **Merge**, and click **OK**.
16. Close the Group Policy Management Editor.



Note: Do not shut down the virtual machines once you are finished with this lab as the settings you have configured here will be used in subsequent labs.

Lab Review Questions

Question: Many organizations rely heavily on security group filtering to scope GPOs, rather than linking GPOs to specific OUs. In these organizations, GPOs are typically linked very high in the Active Directory® logical structure: to the domain itself or to a first-level OU. What advantages are gained by using security group filtering rather than GPO links to manage the scope of the GPO?

Answer: The fundamental problem of relying on OUs to scope the application of GPOs is that an OU is a fixed, inflexible structure within Active Directory, and that a single user or computer can only exist within one OU. As organizations get larger and more complex, configuration requirements are difficult to match in a one-to-one relationship with any container structure. With security groups, a user or computer can exist in as many groups as necessary, and can be added and removed easily without impacting the security or management of the user or computer account.

Question: Why might it be useful to create an exemption group—a group that is denied the Apply Group Policy permission—for every GPO that you create?

Answer: There are very few scenarios in which you can be guaranteed that all of the settings in a GPO will always need to apply to all users and computers within its scope. By having an exemption group, you will always be able to respond to situations in which a user or computer must be excluded. This can also help in troubleshooting compatibility and functionality problems. Sometimes, specific GPO settings can interfere with the functionality of an application. In order to test whether the application works on a "pure" installation of Windows, you might need to exclude the user or computer from the scope of GPOs, at least temporarily for testing.

Question: Do you use loopback policy processing in your organization? In what scenarios and for what policy settings can loopback policy processing add value?

Answer: Answers will vary. Scenarios including conference rooms, kiosks, virtual desktop infrastructures, and other "standard" environments should certainly be mentioned.

Lab D: Troubleshoot Policy Application

► Log on to a virtual machine

Unless otherwise instructed, use the following steps to log on to a virtual machine.

1. Press ALT+DELETE.

This sends the secure key sequence (CTRL+ALT+DELETE) to the virtual machine. If you press CTRL+ALT+DELETE, you send the secure key sequence to the host operating system.

2. Click **Switch User**.
3. Click **Other User**.
4. In **User name**, type the username.
5. In **Password**, type the password.
6. Press ENTER or click the logon arrow.

The Windows desktop appears.

► Run an application with administrative credentials

1. Right-click the application, and then click **Run as administrator**.

A User Account Control (UAC) dialog box appears.

2. The **UAC** dialog box will display one of three options. Perform the steps based on the option you see:

If the UAC dialog box prompts you to continue or cancel:

- Click **Continue**.

If the UAC dialog box gives you the option to use another account:

1. Click **Use Another Account**.
2. In **User Name**, type the username.
3. In **Password**, type the password.
4. Press ENTER or click **OK**.

If the UAC dialog box does not give you the option to use another account, and prompts you for a username and password:

1. In **User Name**, type the username.
2. In **Password**, type the password.
3. Press ENTER or click **OK**.

Exercise 1: Perform RSoP Analysis

► Task 1: Prepare for the lab

The virtual machines should already be started and available after completing Labs A, B and C. However, if they are not, you should complete the below steps then step through the exercises in Labs A, B and C before continuing.

1. Start 6425B-HQDC01-A.
2. Log on to HQDC01 as **Pat.Coleman** with the password **Pa\$\$w0rd**.
3. Start 6425B-DESKTOP101-A.
4. Log on to DESKTOP101 as **Pat.Coleman** with the password **Pa\$\$w0rd**.

► Task 2: Refresh Group Policy

1. On the DESKTOP101 virtual machine run the command prompt with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
2. Type **gpupdate.exe /force**.
3. Wait for the command to complete.
4. Make a note of the current system time, which you will need to know for a task later in this lab.
5. Restart DESKTOP101.
6. Wait for DESKTOP101 to restart before proceeding with the next task. Do not log on to DESKTOP101.

► Task 3: Create a Group Policy results RSoP report

1. Switch to HQDC01.
2. Run **Group Policy Management** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
3. In the console tree, expand **Forest: contoso.com**, and then click **Group Policy Results**.
4. Right-click **Group Policy Results**, and click **Group Policy Results Wizard**.
5. On the **Welcome to the Group Policy Results Wizard** page, click **Next**.

6. On the **Computer Selection** page, click **Another computer**, and then type **DESKTOP101** in the text box. Click **Next**.
7. On the **User Selection** page, click **Display policy settings for**, then click **Select a specific user**, and then select **CONTOSO\Pat.Coleman**. Click **Next**.
8. On the **Summary Of Selections** page, review your settings, and then click **Next**.
9. Click **Finish**. The RSoP report appears in the details pane of the console.
10. If you are prompted by an Internet Explorer® security message that refers to **about:security_mmc.exe**, then click **Add**. In the **Trusted sites** dialog box, click **Add**, and then click **Close**.
11. Review the **Group Policy Summary** results. For both user and computer configuration, identify the time of the last policy refresh and the list of allowed and denied GPOs. Identify the components that were used to process policy settings.
12. Click the **Settings** tab. Review the settings that were applied during user and computer policy application and identify the GPO from which the settings were obtained.
13. Click the **Policy Events** tab and locate the event that logs the policy refresh you triggered with the **GPUpdate** command in Task 1.
14. Click the **Summary** tab, right-click the page, and then click **Save Report**.
15. Save the report as an HTML file to drive D with a name of your choice.
16. Open the saved RSoP report from drive D. Examine the RSoP report, and then close it.

► **Task 4: Analyze RSoP with GPResults**

1. Log on to DESKTOP101 as **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
2. Run the command prompt with administrative credentials.
3. Type **gpresult /r** and press ENTER.

RSoP summary results are displayed.

The information is very similar to the Summary tab of the RSoP report produced by the Group Policy Results Wizard.

4. Type **gpresult /v** and press ENTER.
A more detailed RSoP report is produced.
Notice many of the Group Policy settings applied by the client are listed in this report.
5. Type **gpresult /z** and press ENTER.
The most detailed RSoP report is produced.
6. Type **gpresult /h:"%userprofile%\Desktop\RSOP.html"** and press ENTER.
An RSoP report is saved as an HTML file to your desktop.
7. Open the saved RSoP report from your desktop.
8. Compare the report, its information, and its formatting to the RSoP report you saved in the previous task.

Exercise 2: Use the Group Policy Modeling Wizard

► Task 1: Perform Group Policy results modeling

1. Switch to HQDC01.
2. In the Group Policy Management console tree, expand **Forest:Contoso.com**, and then click **Group Policy Modeling**.
3. Right-click **Group Policy Modeling**, and then click **Group Policy Modeling Wizard**.

The Group Policy Modeling Wizard appears.

4. Click **Next**.
5. On the **Domain Controller Selection** page, click **Next**.
6. On the **User And Computer Selection** page, in the **User Information** section, click the **User** option button, and then click **Browse**.

The Select User dialog box appears.

7. Type **Mike.Danseglio** and then press ENTER.
8. In the **Computer Information** section, click the **Computer** option button, and then click **Browse**.

The Select Computer dialog box appears.

9. Type **DESKTOP101** and then press ENTER.
10. Click **Next**.
11. On the **Advanced Simulation Options** page, select the **Loopback Processing** check box and then click **Merge**.

Even though the Conference Room Polices GPO specifies the loopback processing, you must instruct the Group Policy Modeling Wizard to consider loopback processing in its simulation.

12. Click **Next**.
13. On the **Alternate Active Directory Paths** page, click the **Browse** button next to **Computer location**.

The Choose Computer Container dialog box appears.

14. Expand **contoso.com** and **Kiosks**, and then click **Conference Rooms**.

You are simulating the effect of DESKTOP101 as a conference room computer.

15. Click **OK**.
16. Click **Next**.
17. On the **User Security Groups** page, click **Next**.
18. On the **Computer Security Groups** page, click **Next**.
19. On the **WMI Filters for Users** page, click **Next**.
20. On the **WMI Filters for Computers** page, click **Next**.
21. Review your settings on the **Summary of Selections** page, and then click **Next**.
22. Click **Finish**.
23. On the **Summary** tab, scroll to and expand, if necessary, **User Configuration, Group Policy Objects**, and **Applied GPOs**.
24. Will the **Conference Room Policies** GPO apply to Mike Danseglio as a User policy when he logs on to DESKTOP101 if DESKTOP101 is in the Conference Rooms OU?

If not, check the scope of the Conference Room Policies GPO. It should be linked to the Conference Rooms OU with security group filtering that applies the GPO to the Authenticated Users special identity. You can right-click the modeling query to rerun the query. If the GPO is still not applying, try deleting and re-building the Group Policy Modeling report, and be very careful to follow each step precisely.
25. Click the **Settings** tab.
26. Scroll to, and expand if necessary, **User Configuration, Policies, Administrative Templates** and **Control Panel/Display**.
27. Confirm that the screen saver timeout is 2700 seconds (45 minutes), the setting configured by the **Conference Room Policies** GPO that overrides the 10-minute standard configured by the **CONTOSO Standards** GPO.

Exercise 3: View Policy Events

► Task 1: View policy events

1. Switch to DESKTOP101.
2. Click **Start**, and then click **Control Panel**.
3. Click **System and Maintenance**.
4. Click **Administrative Tools**.
5. Double-click **Event Viewer**.

A User Account Control dialog box appears.

6. Click **Continue**.

Event Viewer opens.

7. In the console tree, expand **Windows Logs**, and then click the **System** log.
8. Locate events with **GroupPolicy** as the **Source**.

You can even click the Filter Current Log link in the Actions pane and then select GroupPolicy in the Event Sources drop-down list.

9. Review the information associated with **GroupPolicy** events.
10. In the console tree, click the **Application** log.
11. Sort the **Application** log by the **Source** column.
12. Review the events and identify the Group Policy events that have been entered in this log. Which events are related to Group Policy application, and which are related to the activities you have been performing to manage Group Policy?

Depending on how long the virtual machine has been running you may not have any Group Policy Events in the application log

13. In the console tree, expand **Applications and Services Logs, Microsoft, Windows**, and **GroupPolicy**, and then click **Operational**.
14. Locate the first event related in the **Group Policy** refresh you initiated in Exercise 1, with the **GPUpdate** command. Review that event and the events that followed it.



Note: After completing this exercise, turn off all virtual machines and discard undo disks.

Lab Review Questions

Question: In what situations have you used RSoP reports to troubleshoot Group Policy application in your organization?

Answer: The correct answer will be based on your own experience and situation.

Question: In what situations have you used, or could you anticipate using, Group Policy modeling?

Answer: The correct answer will be based on your own experience and situation.

Question: Have you ever diagnosed a Group Policy application problem based on events in one of the event logs?

Answer: The correct answer will be based on your own experience and situation.

Module 7: Manage Enterprise Security and Configuration with Group Policy Settings

Lab A: Delegate the Support of Computers

► Log on to a virtual machine

Unless otherwise instructed, use the following steps to log on to a virtual machine.

1. Press ALT+DELETE.

This sends the secure key sequence (CTRL+ALT+DELETE) to the virtual machine. If you press CTRL+ALT+DELETE, you send the secure key sequence to the host operating system.

2. Click **Switch User**.
3. Click **Other User**.
4. In **User name**, type the username.
5. In **Password**, type the password.
6. Press ENTER or click the log on arrow.

The Windows desktop appears.

► Run an application with administrative credentials

1. Right-click the application, and then click **Run as administrator**.

A User Account Control (UAC) dialog box appears.

2. The **UAC** dialog box will display one of three options. Do the steps based on the option you see:

If the UAC dialog box prompts you to continue or cancel:

- Click **Continue**.

If the UAC dialog box gives you the option to *Use another account*:

3. Click **Use Another Account**.
4. In **User Name**, type the username.

5. In **Password**, type the password.
6. Press ENTER or click **OK**.

If the UAC dialog box does not give you the option to use another account, and prompts you for a username and password:

- a. In **User Name**, type the username.
7. In **Password**, type the password.
8. Press ENTER or click **OK**.

Exercise 1: Configure the Membership of Administrators by Using Restricted Groups Policies

► Task 1: Prepare for the lab

1. Start 6425B-HQDC01-A.
2. Log on to HQDC01 as **Pat.Coleman** with the password **Pa\$\$w0rd**.
3. Start 6425B-DESKTOP101-A but do not log on to the system.

► Task 2: Delegate the administration of all clients in the domain

1. On HQDC01 click **Start >Administrative Tools** and run **Group Policy Management** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
2. In the console tree, expand the **Forest:contoso.com, Domains and contoso.com**, and then click the **Group Policy Objects** container.
3. Right-click the **Group Policy Objects** container, and then click **New**.
4. In the **Name** box, type **Corporate Help Desk**, and then click **OK**.
5. In the details pane, right-click the **Corporate Help Desk**, and then click **Edit**.
The Group Policy Management Editor appears.
6. In the console tree, expand **Computer Configuration, Policies, Windows Settings, Security Settings**, and then click **Restricted Groups**.
7. Right-click **Restricted Groups**, and then click **Add Group**.
8. Click the **Browse** button.
The Select Groups dialog box appears.
9. Type **CONTOSO\Help Desk**, and then press ENTER.
10. Click **OK** to close the **Add Group** dialog box.
The CONTOSO\Help Desk Properties dialog box appears.
11. In the **This group is a member of** section, click the **Add** button.
The Group Membership dialog box appears.
12. Type **Administrators**, and then click **OK**.
13. Click **OK** again to close the **Properties** dialog box.

14. Close the **Group Policy Management Editor**.
15. In the **Group Policy Management** console tree, right-click the **Client Computers** OU, and then click **Link an Existing GPO**.
The Select GPO dialog box appears.
16. Select the **Corporate Help Desk** GPO, and then click **OK**.
17. Close the **Group Policy Management** console.

► **Task 3: Create a Seattle Support group**

1. Run **Active Directory Users and Computers** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
2. In the console tree, expand the **contoso.com** domain and the **Groups** OU, and then click the **Role** OU.
3. Right-click **Role**, point to **New**, and then click **Group**.
4. In the **Group Name** box, type **SEA Support**, and then click **OK**.
5. Close Active Directory Users and Computers.

► **Task 4: Delegate the administration of a subset of clients in the domain**

1. In the Group Policy Management console tree, expand **Forest:contoso.com**, **Domains**, and **contoso.com**, and then click the **Group Policy Objects** container.
2. Right-click the **Group Policy Objects** container, and then click **New**.
3. In the **Name** box, type **Seattle Support**, and then click **OK**.
4. In the details pane, right-click **Seattle Support**, and then click **Edit**.
The Group Policy Management Editor appears.
5. In the console tree, expand **Computer Configuration**, **Policies**, **Windows Settings**, and **Security Settings**, and then click **Restricted Groups**.
6. Right-click **Restricted Groups**, and then click **Add Group**.
7. Click the **Browse** button.
The Select Groups dialog box appears.

8. Type **CONTOSO\SEA Support**, and then press ENTER.
9. Click **OK** to close the **Add Group** dialog box.
The **CONTOSO\SEA Support Properties** dialog box appears.
10. In the **This group is a member of** section, click the **Add** button.
The **Group Membership** dialog box appears.
11. Type **Administrators**, and then click **OK**.
12. Click **OK** again to close the **Properties** dialog box.
13. Close the **Group Policy Management Editor**.
14. In the **Group Policy Management** console tree, expand the **Client Computers** OU, and then click the **SEA** OU.
15. Right-click **SEA**, and then click **Link an Existing GPO**.
The **Select GPO** dialog box appears.
16. Select the **Seattle Support** GPO, and then click **OK**.

► **Task 5: Confirm the cumulative application of Member Of policies**

1. In the **Group Policy Management** console tree, expand **Forest:contoso.com**, and then click the **Group Policy Modeling** node.
2. Right-click the **Group Policy Modeling** node, and then click **Group Policy Modeling Wizard**. The **Group Policy Modeling Wizard** appears.
3. Click **Next**.
4. On the **Domain Controller Selection** page, click **Next**.
5. On the **User and Computer Selection** page, in the **Computer Information** section, click the **Browse** button next to **Container**.
6. Expand the **contoso** domain and the **Client Computers** OU, and then click the **SEA** OU.
7. Click **OK**.
8. Select the **Skip to the final page of this wizard without collecting additional data** check box. Click **Next**.
9. On the **Summary of Selections** page, click **Next**.
10. Click **Finish**. The **Group Policy Modeling** report appears.

11. Click the **Settings** tab.
12. Scroll to, and expand if necessary, **Computer Configuration, Policies, Windows Settings, Security Settings, and Restricted Groups**.
13. Confirm that you see both the **Help Desk** and **SEA Support** groups listed.

Restricted Groups policies using the This Group Is A Member Of setting are cumulative.

Notice that the report does not specify that the listed groups are members of the Administrators group in particular. This is a limitation of the Group Policy Modeling report. After the policy has been applied to a computer, the Group Policy Results report (RSOP) would specify that the groups are members of Administrators.



Note: Do not shut down the virtual machine once you are finished with this lab as the settings you have configured here will be used in subsequent labs.

Lab Review Questions

Question: If you wanted to ensure that the *only* members of the local Administrators group on a client computer were the Help Desk in the site-specific Support group, and to remove any other members from the local Administrators group, how would you achieve that using only restricted groups policies?

Answer: This is a bit of a tricky question, and requires some creative thinking. You can configure a Members policy setting for the Administrators group that adds the Administrator account. This would have the effect of cleaning out all other group members, and of course the Administrator account is already a member of the Administrator forest and cannot be removed. Then, you can configure restricted group policy settings for the Help Desk and the site-specific Support groups, as you did in the Lab. Alternately, you could use a Local Group preference configured to delete all member users and groups.

Lab B: Manage Security Settings

► Log on to a virtual machine

Unless otherwise instructed, use the following steps to log on to a virtual machine.

1. Press ALT+DELETE.

This sends the secure key sequence (CTRL+ALT+DELETE) to the virtual machine. If you press CTRL+ALT+DELETE, you send the secure key sequence to the host operating system.

2. Click **Switch User**.
3. Click **Other User**.
4. In **User name**, type the username.
5. In **Password**, type the password.
6. Press ENTER or click the log on arrow.

The Windows desktop appears.

► Run an application with administrative credentials

1. Right-click the application, and then click **Run as administrator**.

A User Account Control (UAC) dialog box appears.

2. The **UAC** dialog box will display one of three options. Do the steps based on the option you see:

If the UAC dialog box prompts you to continue or cancel:

- Click **Continue**.

If the UAC dialog box gives you the option to *Use another account*:

- a. Click **Use Another Account**.
3. In **User Name**, type the username.
4. In **Password**, type the password.
5. Press ENTER or click **OK**.

If the UAC dialog box does not give you the option to use another account, and prompts you for a username and password:

- a. In **User Name**, type the username.
6. In **Password**, type the password.
7. Press ENTER or click **OK**.

Exercise 1: Manage Local Security Settings

► Task 1: Prepare for the lab

The virtual Machine should already be started and available after completing Lab A. However, if it is not, you should complete the below steps.

1. Start 6425B-HQDC01-A.
2. Log on to HQDC01 as **Pat.Coleman** with the password **Pa\$\$w0rd**.

► Task 2: Enable Remote Desktop on HQDC01

1. Click the **Server Manager** icon next to the Start button. The **User Account Control** dialog box appears.
2. In the **User name** box, type **Pat.Coleman_Admin**.
3. In the **Password** box, type **Pa\$\$w0rd**, and then press ENTER.
Server Manager opens.
4. In the **Server Summary** section, click **Configure Remote Desktop**.
The System Properties dialog box opens.
5. Click **Allow connections only from computers running Remote Desktop with Network Level Authentication (more secure)**.
6. Click **OK**.
7. Close **Server Manager**.

► Task 3: Create a global security group named SYS_DC Remote Desktop

1. Run **Active Directory Users and Computers** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
2. In the console tree, expand the **contoso.com** domain, the **Admins** OU, and the **Admin Groups** OU, and then click the **Server Delegation** OU.
3. Right-click **Server Delegation**, point to **New**, and then click **Group**.
4. Type **SYS_DC Remote Desktop**, and then click **OK**.

► **Task 4: Add SYS_DC Remote Desktop to the Remote Desktop Users group**

In order to connect using remote desktop, a user must have the user logon right to log on through Terminal Services, which you will grant to the SYS_DC Remote Desktop group in the next task.

Additionally, the user must have permission to connect to the RDP-Tcp connection. By default, the Remote Desktop Users group and the Administrators group has permission to connect to the RDP-Tcp connection. Therefore, you should add the user (or the SYS_DC Remote Desktop group in this case) to the Remote Desktop Users group.

1. Still on HQDC01 in Active Directory Users and Computers, in the console tree, click **Builtin**.
2. In the details pane, double-click **Remote Desktop Users**.
3. Click the **Members** tab.
4. Click the **Add** button.

The Select Users, Contacts, Computers or Groups dialog box appears.

5. Type **SYS_DC Remote Desktop**, and then press ENTER.
6. Click **OK**.
7. Close Active Directory Users and Computers.



Note: Instead of adding the group to Remote Desktop Users, you could add the SYS_DC Remote Desktop group to the access control list (ACL) of the RDP-Tcp connection, using the Terminal Services Configuration console. Right-click RDP-Tcp, and then click Properties; then click the Security tab, click the Add button, and type SYS_DC Remote Desktop. Click OK twice to close the dialog boxes.

► **Task 5: Configure the Local Security Policy to allow Remote Desktop connections by SYS_DC Remote Desktop**

1. On HQDC01 go to **Start >Administrative Tools** and run **Local Security Policy** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
2. In the console tree, expand **Local Policies**, and then click **User Rights Assignment**.
3. Double-click **Allow log on through Terminal Services**.
The Allow log on through Terminal Services Properties dialog box opens.
4. Click **Add User or Group**.
The Select Users, Computers, Or Groups dialog box appears.
5. Type **SYS_DC Remote Desktop**, and then press ENTER.
6. Click **OK**.
7. Close the **Allow log on through Terminal Services** dialog box.

► **Task 6: Revert the local security policy to its default setting**

You will now revert the policy to its default in preparation for following Exercises.

1. Double-click **Allow log on through Terminal Services**.
The Allow Log On Through Terminal Services Properties dialog box opens.
2. Click **CONTOSO\SYS_DC Remote Desktop**.
3. Click **Remove**.
4. Click **OK**.
5. Close **Local Security Policy**.

Exercise 2: Create a Security Template

► Task 1: Create a custom MMC console with the Security Templates snap-in

1. Still on HQDC01, click **Start** and in the search box type **mmc.exe** and press ENTER, when prompted supply administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
2. Click **File**, and then click **Add/Remove Snap-in**.
3. In the **Available snap-ins** list, select **Security Templates**, then click **Add**.
4. Click **OK**.
5. Click **File**, and then click **Save**.
The Save As dialog box appears.
6. Type **D:\Security Management**, and then press ENTER.

► Task 2: Create a security template

1. In the console tree, expand **Security Templates**.
2. Right-click **C:\Users\Pat.Coleman_Admin\Documents\Security\Templates**, and then click **New Template**.
3. Type **DC Remote Desktop**, and then click **OK**.
4. In the console tree, expand **C:\Users\Pat.Coleman_Admin\Documents\Security\Templates**, **DC Remote Desktop**, and **Local Policies**, and then click **User Rights Assignment**.
5. In the details pane, double-click **Allow log on through Terminal Services**.
The Allow log on through Terminal Services Properties dialog box appears.
6. Select **Define these policy settings in the template**.
7. Click **Add User or Group**.
The Add User or Group dialog box appears.
8. Click the **Browse** button.
The Select Users or Groups dialog box appears.

9. Type **SYS_DC Remote Desktop**, and then click **OK**.
10. Click **OK** to close the **Add User or Group** dialog box.
11. Click **OK** to close the Policy Properties dialog box.
12. In the console tree, click **Restricted Groups**.
13. Right-click **Restricted Groups**, and then click **Add Group**.
The Add Group dialog box appears.
14. Click the **Browse** button.
15. Type **SYS_DC Remote Desktop**, and then click **OK**.
16. Click **OK** again to close the **Add Group** dialog box.
The CONTOSO\SYS_DC Remote Desktop Properties dialog box appears.
17. In the **This group is a member of** section, click **Add Groups**.
The Group Membership dialog box appears.
18. Click the **Browse** button.
The Select Groups dialog box appears.
19. Type **Remote Desktop Users**, and then click **OK**.
20. Click **OK** to close the **Group Membership** dialog box.
21. Click **OK** to close the properties dialog box.
22. In the console tree, right-click **DC Remote Desktop**, and then click **Save**.

Exercise 3: Use Security Configuration and Analysis

► **Task 1: Add the Security Configuration and Analysis snap-in to a custom console**

1. Click **File**, and then click **Add/Remove Snap-in**.
2. In the **Available snap-ins** list, select **Security Configuration and Analysis**, then click the **Add** button.
3. Click **OK**.
4. On the **File** menu, click **Save**.

► **Task 2: Create a security database and import a security template**

1. In the console tree, click **Security Configuration and Analysis**.
2. Right-click **Security Configuration and Analysis**, and then click **Open Database**.
The Open database dialog box appears.
The Open Database command enables you to create a new security database.
3. Type **HQDC01Test**, and then click **Open**.
The Import Template dialog box appears.
4. Select the **DC Remote Desktop** template you created in Exercise 2, and then click **Open**.

► **Task 3: Analyze the configuration of a computer using the security database**

1. In the console tree, right-click **Security Configuration and Analysis**, and then click **Analyze Computer Now**.
2. Click **OK** to confirm the default path for the error log.
The snap-in performs the analysis.

3. In the console tree, expand **Security Configuration and Analysis** and **Local Policies**, and then click **User Rights Assignment**.

Notice that the Allow log on through Terminal Services policy is flagged with a red circle and an X. This indicates a discrepancy between the database setting and the computer setting.

4. Double-click **Allow log on through Terminal Services**.

Notice the discrepancies. The computer is not configured to allow the SYS_DC Remote Desktop Users group to log on through Terminal Services.

Notice also that the Computer setting currently allows Administrators to log on through Terminal Services. This is an important setting that should be incorporated into the database.

5. Confirm that the **Define this policy in the database** check box is selected.
6. Select the **Administrators** check box, under **Database Setting**.

This will add the right for Administrators to log on through Terminal Services to the database. It does not change the template, and it does not affect the current configuration of the computer.

7. Click **OK**.
8. In the console tree, select **Restricted Groups**.
9. In the details pane, double-click **CONTOSO\SYS_DC Remote Desktop**.
10. Click the **Member Of** tab.

Notice that the database specifies that the SYS_DC Remote Desktop group should be a member of Remote Desktop Users, but the computer is not currently in compliance with that setting.

11. Confirm that the **Define this group in the database** check box is selected.
12. Click **OK**.
13. Right-click **Security Configuration and Analysis**, and then click **Save**.

This saves the security database, which includes the settings imported from the template plus the change you made to allow Administrators to log on through Terminal Services.

The hint displayed in the status bar when you hover over the Save command suggests that you are saving the template. That is incorrect. You are saving the database.

14. Right-click **Security Configuration and Analysis**, and then click **Export Template**.

The Export Template To dialog box appears.

15. Select **DC Remote Desktop**, and then click **Save**.

You have now replaced the template created in Exercise 2 with the settings defined in the database of the Security Configuration and Analysis snap-in.

► **Task 4: Configure security settings by using a security database**

1. Close your Security Management console. If you are prompted to save your settings, click **Yes**.

Closing and reopening the console is necessary to refresh fully the settings shown in the Security Templates snap-in.

2. Run **D:\Security Management.msc** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.

3. In the console tree, expand **Security Templates**, **C:\Users\Pat.Coleman_Admin\Documents\Security\Templates**, **DC Remote Desktop**, **Local Policies**, and then click **User Rights Assignment**.

4. In the details pane, double-click **Allow log on through Terminal Services**.

Notice that both the Administrators and SYS_DC Remote Desktop groups are allowed to log on through Terminal Services in the security template.

5. Click **OK**.

6. Right-click **Security Configuration and Analysis**, and then click **Configure Computer Now**.

7. Click **OK** to confirm the error log path. The settings in the database are applied to the server. You will now confirm that the change to the user right was applied.

8. Run **Local Security Policy** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.

9. In the console tree expand **Local Policies**, and then click **User Rights Assignment**.

10. Double-click **Allow Log On Through Terminal Services**.

The Allow Log On Through Terminal Services Properties dialog box opens.

11. Confirm that both **Administrators** and **SYS_DC Remote Desktop** are listed.
The Local Security Policy console displays the actual, current settings of the server.
12. Close the **Local Security Policy** console.
13. Close your custom **Security Management** console.

Exercise 4: Use the Security Configuration Wizard

► Task 1: Create a security policy

1. Still on HQDC01 click **Start > Administrative Tools** and run the Security Configuration Wizard with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
2. On the **Welcome to the Security Configuration Wizard** page, click **Next**.
3. On the **Configuration Action** page, select **Create a new security policy**, and then click **Next**.
4. On the **Select Server** page, accept the default server name, **HQDC01**, and click **Next**.
5. On the **Processing Security Configuration Database** page, you can optionally click **View Configuration Database** and explore the configuration that was discovered on HQDC01.
6. Click **Next**.
7. On the **Role Based Service Configuration** section introduction page, click **Next**.
8. On the **Select Server Roles** page, you can optionally explore the settings that were discovered on HQDC01, but do not change any settings. Click **Next**.
9. On the **Select Client Features** page, you can optionally explore the settings that were discovered on HQDC01, but do not change any settings. Click **Next**.
10. On the **Select Administration And Other Options** page, you can optionally explore the settings that were discovered on HQDC01, but do not change any settings. Click **Next**.
11. On the **Select Additional Services** page, you can optionally explore the settings that were discovered on HQDC01, but do not change any settings. Click **Next**.
12. On the **Handling Unspecified Services** page, do not change the default setting, **Do not change the startup mode of the service**. Click **Next**.
13. On the **Confirm Service Changes** page, in the **View** list, choose **All Services**.
14. Examine the settings in the Current Startup Mode column, which reflect service startup modes on HQDC01, and compare them to the settings in the Policy Startup Mode column.

15. In the **View** list, select **Changed Services**.
16. Click **Next**.
17. On the **Network Security** section introduction page, click **Next**.
18. On the **Network Security Rules** page, you can optionally examine the firewall rules derived from the configuration of HQDC01. Do not change any settings. Click **Next**.
19. On the **Registry Settings** section introduction page, click **Next**.
20. On each page of the **Registry Settings** section, examine the settings, but do not change any of them, then click **Next**. Continue clicking **Next** at each page until you get to the **Registry Settings Summary** page appears, examine the settings and click **Next**.
21. On the **Audit Policy** section introduction page, click **Next**.
22. On the **System Audit Policy** page, examine but do not change the settings. Click **Next**.
23. On the **Audit Policy Summary** page, examine the settings in the **Current Setting** and **Policy Setting** columns. Click **Next**.
24. On the **Save Security Policy** section introduction page, click **Next**.
25. In the **Security Policy File Name** text box, click at the end of the file path and type **DC Security Policy**.
26. Click the **Include Security Templates** button.
27. Click **Add**.
28. Browse to locate the **DC Remote Desktop** template created in Exercise 3, located in the C:\Users\Pat.Coleman_Admin\Documents\Security\Templates folder. When you have located and selected the template, click **Open**.

Be careful that you add the Documents\Security\Templates\DC Remote Desktop.inf file and *not* the DC Security.inf default security template.
29. Click **OK** to close the **Include Security Templates** dialog box.
30. Click the **View Security Policy** button.

You are prompted to confirm the use of the ActiveX control.
31. Click **Yes**.
32. Examine the security policy. Notice that the DC Remote Desktop template is listed in the **Templates** section.

33. Close the window after you have examined the policy.
34. In the Security Configuration Wizard, click **Next**.
35. On the **Apply Security Policy** page, accept the **Apply Later** default setting, and then click **Next**.
36. Click **Finish**.

► **Task 2: Transform a security policy into a Group Policy object**

1. Run Command Prompt with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
2. Type **cd c:\windows\security\msscw\policies** and then press ENTER.
3. Type **scwcmd transform /?**, and then press ENTER.
4. Type **scwcmd transform /p:"DC Security Policy.xml" /g:"DC Security Policy"** and then press ENTER.
5. Run **Group Policy Management** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
6. In the console tree expand **Forest:contoso.com, Domains, contoso.com**, and **Group Policy Objects**, and then click **DC Security Policy**. This is the GPO created by the Scwcmd.exe command.
7. Click the **Settings** tab to examine the settings of the GPO.
8. Expand **Security Settings** and **Local Policies/User Rights Assignment**.
9. Confirm that the BUILTIN\Administrators and CONTOSO\SYS_DC Remote Desktop groups are given the **Allow log on through Terminal Services** user right.
10. Expand **Restricted Groups**.
11. Confirm that CONTOSO\SYS_DC Remote Desktop is a member of BUILTIN\Remote Desktop Users.

The GPO is not applied to DCs because it is not yet linked to the Domain Controllers OU. In this Lab, do not link the GPO to the domain, site, or any OU. In a production environment, you would spend more time examining, configuring, and testing security settings in the security policy before deploying it as a GPO to production domain controllers.



Note: Do not shut down the virtual machine once you are finished with this lab as the settings you have configured here will be used in subsequent labs.

Lab Review Question

Question: Describe the relationship between security settings on a server, Local Group Policy, security templates, the database used in Security Configuration and Analysis, the security policy created by the Security Configuration Wizard, and domain-based Group Policy.

Answer: Although some security settings can be modified directly—for example, file system ACLs or local group membership—many can only be configured directly on a system using Local Group Policy. Security templates allow you to create a security policy that can be easily transferred to another system and, using Security Configuration and Analysis, loaded into a database that can be used to analyze or configure a computer. The database used by Security Configuration and Analysis can be exported to a security template.

Security Configuration Wizard is a newer tool that enables the role-based configuration of services, network security settings, registry values, and audit policies. It creates an xml file that can incorporate a security template and that can then be applied to another system using the Security Configuration Wizard. The Security Configuration Wizard allows you to roll back a security policy if it does not produce the desired results. A security policy produced by the Security Configuration Wizard can be transformed into a domain-based Group Policy object that can then apply to multiple servers.

Lab C: Manage Software with GPSI

► Log on to a virtual machine

Unless otherwise instructed, use the following steps to log on to a virtual machine.

1. Press ALT+DELETE.

This sends the secure key sequence (CTRL+ALT+DELETE) to the virtual machine. If you press CTRL+ALT+DELETE, you send the secure key sequence to the host operating system.

2. Click **Switch User**.
3. Click **Other User**.
4. In **User name**, type the username.
5. In **Password**, type the password.
6. Press ENTER or click the log on arrow.

The Windows desktop appears.

► Run an application with administrative credentials

1. Right-click the application, and then click **Run as administrator**.

A User Account Control (UAC) dialog box appears.

2. The **UAC** dialog box will display one of three options. Do the steps based on the option you see:

If the UAC dialog box prompts you to continue or cancel:

- Click **Continue**.

If the UAC dialog box gives you the option to *Use another account*:

- a. Click **Use Another Account**.
3. In **User Name**, type the username.
4. In **Password**, type the password.
5. Press ENTER or click **OK**.

If the UAC dialog box does not give you the option to use another account, and prompts you for a username and password:

- a. In **User Name**, type the username.
6. In **Password**, type the password.
7. Press ENTER or click **OK**.

Exercise 1: Deploy Software with GPSI

► Task 1: Prepare for the lab

The virtual Machines should already be started and available after completing the previous labs. However, if they are not, you should complete the below steps.

1. Start 6425B-HQDC01-A.
2. Log on to HQDC01 as **Pat.Coleman** with the password **Pa\$\$wOrd**.
3. Start 6425B-SERVER01-A but do not log on.
4. Wait for SERVER01 to finish startup before continuing with the next task.

► Task 2: Create a software distribution folder

1. Switch to HQDC01.
2. Run **Active Directory Users and Computers** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$wOrd**.
3. In the console tree, expand the **contoso.com** domain and the **Groups** OU, and then click the **Application** OU.
4. Right-click the **Application** OU, point to **New**, and then click **Group**.
5. Type **APP_XML Notepad**, and then press ENTER.
6. In the console tree, expand the **contoso.com** domain and the **Servers** OU, and then click the **File** OU.
7. In the details pane, right-click **SERVER01**, and then click **Manage**.
The Computer Management console opens, focused on SERVER01.
8. In the console tree, expand **System Tools** and **Shared Folders**, and then click **Shares**.
9. Right-click **Shares**, and then click **New Share**. The Create A Shared Folder Wizard appears.
10. Click **Next**.
11. In the **Folder Path** box, type **C:\Software**, and then click **Next**.
A message appears asking if you want to create the folder.
12. Click **Yes**.

13. Accept the default Share name, **Software**, and then click **Next**.
14. Click **Customize permissions**, and then click the **Custom** button.
15. Click the **Security** tab.
16. Click **Advanced**.

The Advanced Security Settings dialog box appears.
17. Click **Edit**.
18. Clear the option, **Include inheritable permissions from this object's parent**.

A dialog box appears asking if you want to Copy or Remove inherited permissions.
19. Click **Copy**.
20. Select the first permission assigned to the **Users** group, and then click **Remove**.
21. Select the remaining permission assigned to the **Users** group, and then click **Remove**.
22. Select the permission assigned to **Creator Owner**, and then click **Remove**.
23. Click **OK** two times to close the **Advanced Security Settings** dialog boxes.
24. In the **Customize Permissions** dialog box, click the **Share Permissions** tab.
25. Select the check box next to **Full Control** and below **Allow**.

Security management best practice is to configure least privilege permissions in the ACL of the resource, which will apply to users regardless of how users connect to the resource, at which point you can use the Full Control permission on the SMB shared folder. The resultant access level will be the more restrictive permissions defined in the ACL of the folder.
26. Click **OK**.
27. Click **Finish**.
28. Click **Finish** to close the wizard.
29. Click **Start**, click **Run**, type `\\SERVER01\c$`, and then press ENTER.

The Connect to SERVER01 dialog box appears.
30. In the **User name** box, type `CONTOSO\Pat.Coleman_Admin`.

31. In the **Password** box, type **Pa\$\$w0rd**, and then press ENTER.
A Windows Explorer window opens, focused on the root of the C drive on SERVER01.
32. Open the **Software** folder.
33. Click the **File** menu, point to **New**, and then click **Folder**.
A new folder is created and is in "rename mode."
34. Type **XML Notepad**, and then press ENTER.
35. Right-click the **XML Notepad** folder, and then click **Properties**.
36. Click the **Security** tab.
37. Click **Edit**.
38. Click **Add**. The **Select Users, Computers, or Groups** dialog box appears.
39. Type **APP_XML Notepad**, and then press ENTER.
The group is given the default, Read & Execute permission.
40. Click **OK** twice to close all open dialog boxes.
41. Open the **XML Notepad** folder.
42. Open the **D:\Labfiles\Lab07b** folder in a new window.
43. Right-click **XMLNotepad.msi**, and then click **Copy**.
44. Switch to the Windows Explorer window displaying **\\server01\c\$\Software\XML Notepad**.
45. Right-click in the empty details pane, and then click **Paste**.
XML Notepad is copied into the folder on SERVER01.
46. Close all open Windows Explorer windows.
47. Close the Computer Management console.

► **Task 3: Create a software deployment GPO**

1. Run **Group Policy Management** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
2. In the console tree, expand **Forest:contoso.com**, **Domains** and **contoso.com**, and then click the **Group Policy Objects** container.

3. Right-click the **Group Policy Objects** container, and then click **New**.
4. In the **Name** box, type **XML Notepad**, and then click **OK**.
5. Right-click the **XML Notepad** GPO, and then click **Edit**.
6. In the console tree, expand **Computer Configuration, Policies, and Software Settings**, and then click **Software Installation**.
7. Right-click **Software Installation**, point to **New**, and then click **Package**.
8. In the **File name** text box, type the network path to the software distribution folder, **\\server01\software\XML Notepad**, and then press ENTER.
9. Select the Windows Installer package, **XmlNotepad.msi**, and then click **Open**.
After a few moments, the Deploy Software dialog box appears.
10. Click **Advanced**, and then click **OK**.
The XML Notepad 2007 Properties dialog box appears.
11. On the **General** tab, note that the name of the package includes the version, XML Notepad 2007.
12. Click the **Deployment** tab.
Note that when deploying software to computers, Assigned is the only option. Examine the options that would be available if you were assigning or publishing the application to users.
13. Select **Uninstall this application when it falls out of the scope of management**.
14. Click **OK**.
15. Close **Group Policy Management Editor**.
16. In the Group Policy Management console tree, expand **Group Policy Objects**, and then click the **XML Notepad** GPO.
17. In the details pane, click the **Scope** tab.
18. In the **Security Filtering** section, select **Authenticated Users**, and then click **Remove**. You are prompted to confirm your choice.
19. Click **OK**.
20. Click the **Add** button.

The Select User, Computer or Group dialog box appears.

21. Type **APP_XML Notepad**, and press ENTER.
The GPO is now filtered to apply only to the APP_XML Notepad group. However, the GPO settings will not apply until it is linked to an OU, to a site, or to the domain.
22. In the console tree, right-click the **Client Computers** OU, and then click **Link an Existing GPO**.
23. Select **XML Notepad** from the Group Policy Objects list, and then click **OK**.

► **Task 4: Deploy software to computers**

1. Switch to **Active Directory Users and Computers**.
2. In the console tree, expand **Groups**, and then click the **Application** OU.
3. In the details pane, double-click **APP_XML Notepad**.
4. Click the **Members** tab.
5. Click the **Add** button.
6. Click the **Object Types** button.
7. Select **Computers**, and then click **OK**.
8. Type **DESKTOP101**, and then press ENTER.
9. Click **OK**.
10. Start 6425B-DESKTOP101-A, but do not log on.

► **Task 5: Confirm the successful deployment of software**

1. Switch to DESKTOP101.
2. Log on to DESKTOP101 as **Pat.Coleman** with the password **Pa\$\$w0rd**.
3. Click the **Start** button, and then click **All Programs**.
4. Open **XML Notepad**.

If XML Notepad is not installed, restart DESKTOP101 and repeat steps 2-4.



Note: When verifying the deployment of the xml notepad and it may take two startups to be successful. I.e. if you do not see Notepad installed restart the virtual machine. You may need to do this a couple of times.

Exercise 2: Upgrade Applications with GPSI

► Task 1: Create an upgrade package by using GPSI

1. Switch to HQDC01.
2. In the **Group Policy Management** console tree, right-click the **XML Notepad** GPO in the **Group Policy Objects** container, and then click **Edit**.

The Group Policy Management Editor opens.

3. In the console tree, expand **Computer Configuration, Policies, Software Settings**, and then click **Software Installation**.
4. Right-click **Software Installation**, point to **New**, and then click **Package**.
5. In the **File name** text box, type the network path to the software distribution folder, **\\server01\software\XML Notepad**, and then press ENTER.

This exercise will use the existing XmlNotepad.msi file as if it is an updated version of XML Notepad.

6. Select the Windows Installer package, **XmlNotepad.msi**, and then click **Open**.

The Deploy Software dialog box appears.

7. Click **Advanced**, and then click **OK**.
8. On the **General** tab, change the name of the package to suggest that it is the next version of the application. Type **XML Notepad 2010**.
9. Click the **Deployment** tab. Because you are deploying the application to computers, **Assigned** is the only deployment type option.
10. Click the **Upgrades** tab.
11. Click the **Add** button.
12. Click the **Current Group Policy Object (GPO)** option.
13. In the **Package to upgrade** list, select the package for the simulated earlier version, **XML Notepad 2007**.
14. Click the **Uninstall the existing package and then select then install the upgrade package** option.
15. Click **OK**.

16. Click **OK**.

If this were an actual upgrade, the new package would upgrade the previous version of the application as clients applied the XML Notepad GPO. Because this is only a simulation of an upgrade, you can remove the simulated upgrade package.

17. Right-click **XML Notepad 2010**, which you just created to simulate an upgrade, point to **All Tasks**, and then select **Remove**.
18. In the **Remove Software** dialog box, click **Immediately uninstall the software from users and computers**, and then click **OK**.



Note: Do not shut down the virtual machines once you are finished with this lab as the settings you have configured here will be used in subsequent labs.

Lab Review Questions

Question: Consider the NTFS permissions you applied to the Software and XML Notepad folders on SERVER01. Explain why these least privilege permissions are preferred to the default permissions.

Answer: The default permissions on a new NTFS folder include inherited permissions that are not least privilege. First, the USERS group is given the ability to add files and folders. In a software distribution folder, only administrators who need to add new applications should have the ability to add files and folders. Second, CREATOR OWNER special identity is given full control. This means that whoever adds a file or folder gets an explicit permission that allows full control, which may or may not be appropriate for each file and folder added to a software deployment point. Third, the USERS group is also given the ability to read all files and folders, which will allow them to install any software in the software distribution folder. Because most software is licensed per computer or per user, you can improve your compliance by allowing only a specified group to read the installation files for each application. The SOFTWARE folder (the root) gives access (full control) only to Administrators and System. The application subfolder, for example, XML Notepad, gives read access to a group that is allowed to install the application, for example, APP_XML Notepad. Those users can get to the subfolder even though they do not have access to the SOFTWARE folder. Windows allows all authenticated users the "traverse folders" privilege by default, which allows users to navigate to a specific subfolder to which they have access even if they do not have permission to a parent folder. The least privilege ACLs used in this Lab are a perfect example of the value of this user right.

Question: Consider the methods used to scope the deployment of XML Notepad: Assigning the application to computers, filtering the GPO to apply to the APP_XML Notepad group that contains only computers, and linking the GPO to the Client Computers OU. Why is this approach advantageous for deploying most software? What would be the disadvantage of scoping software deployment to users rather than to computers?

Answer: Most software is licensed per computer, so it is important to deploy such applications scoped to computers, rather than to users. The result is the same—the application is deployed to the computers of the users who require the application. If you were to deploy an application to users, it would "follow" the users to whatever computers they logged on to. For example, if a user logged on to a conference room computer or to a colleague's computer, the application would be installed on those computers as well. By scoping to a group of computers, and linking the GPO to a high-level OU (or even to the domain), it gives you maximum flexibility to deploy the application to whatever computers require it.

Lab D: Audit File System Access

► Log on to a virtual machine

Unless otherwise instructed, use the following steps to log on to a virtual machine.

1. Press ALT+DELETE.

This sends the secure key sequence (CTRL+ALT+DELETE) to the virtual machine. If you press CTRL+ALT+DELETE, you send the secure key sequence to the host operating system.

2. Click **Switch User**.
3. Click **Other User**.
4. In **User name**, type the username.
5. In **Password**, type the password.
6. Press ENTER or click the log on arrow.

The Windows desktop appears.

► Run an application with administrative credentials

1. Right-click the application, and then click **Run as administrator**.

A User Account Control (UAC) dialog box appears.

2. The **UAC** dialog box will display one of three options. Do the steps based on the option you see:

If the UAC dialog box prompts you to continue or cancel:

- Click **Continue**.

If the UAC dialog box gives you the option to *Use another account*:

- a. Click **Use Another Account**.
3. In **User Name**, type the username.
4. In **Password**, type the password.
5. Press ENTER or click **OK**.

If the UAC dialog box does not give you the option to use another account, and prompts you for a username and password:

- a. In **User Name**, type the username.
6. In **Password**, type the password.
7. Press ENTER or click **OK**.

Exercise 1: Configure Permissions and Audit Settings

► Task 1: Prepare for the lab

The virtual Machines should already be started and available after completing the previous labs. However, if they are not, you should complete the below steps.

1. Start 6425B-HQDC01-A.
2. Log on to HQDC01 as **Pat.Coleman** with the password **Pa\$\$w0rd**.
3. Start 6425B-SERVER01-A but do not log on to the system.
4. Start 6425B-DESKTOP101-A but do not log on.
5. Wait for all virtual machines to complete startup before continuing to the next task.

► Task 2: Create and secure a shared folder

1. Switch to HQDC01.
2. Run **Active Directory Users and Computers** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
3. In the console tree, expand the **contoso.com** domain and the **Groups** OU, and then click the **Role** OU.
4. Right-click the **Role** OU, point to **New**, and then click **Group**.
5. Type **Consultants**, and then press ENTER.
6. Double-click the **Consultants** group.
7. Click the **Members** tab.
8. Click the **Add** button.

The Select Users, Contacts, Computers, or Groups dialog box appears.

9. Type **Mike.Danseglio**, and then press ENTER.
10. Click **OK**.
11. Click **Start**, click **Run**, type **\\SERVER01\\c\$**, and then press ENTER.
The Connect to SERVER01 dialog box appears.
12. In the **User name** box, type **CONTOSO\Pat.Coleman_Admin**.

13. In the **Password** box, type **Pa\$\$w0rd**, and then press ENTER.
A Windows Explorer window opens, focused on the root of the C drive on SERVER01.
14. Open the **Data** folder.
15. Click the **File** menu, point to **New**, and then click **Folder**.
A new folder is created in "rename mode."
16. Type **Confidential Data**, and then press ENTER.
17. Right-click **Confidential Data**, and then click **Properties**.
18. Click the **Security** tab.
19. Click **Edit**.
20. Click **Add**.
21. Type **Consultants**, and then click **OK**.
22. Select the **Deny** check box for the **Full Control** permission.
23. Click **Apply**.
24. Click **Yes** to confirm the use of a Deny permission.
25. Click **OK** to close all open dialog boxes.

► **Task 3: Configure auditing settings on a folder**

1. Right-click **Confidential Data**, and then click **Properties**.
2. Click the **Security** tab.
3. Click **Advanced**.
4. Click the **Auditing** tab.
5. Click **Edit**.
6. Click **Add**.
7. Type **Consultants**, and then click **OK**.
8. In the **Auditing Entry** dialog box, select the check box under **Failed**, next to **Full Control**.
9. Click **OK** to close all open dialog boxes.

Exercise 2: Configure Audit Policy

► Task 1: Enable auditing of file system access by using Group Policy

1. Run **Group Policy Management** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
2. In the console tree, expand **Forest:contoso.com**, **Domains**, and **contoso.com**, and then click the **Group Policy Objects** container.
3. Right-click the **Group Policy Objects** container, and then click **New**.
4. In the **Name** box, type **File Server Auditing**, and then click **OK**.
5. Right-click the **File Server Auditing** GPO, and then click **Edit**.

The Group Policy Management Editor opens.

6. In the console tree, expand **Computer Configuration**, **Policies**, **Windows Settings**, **Security Settings**, and **Local Policies**, and then click **Audit Policy**.
7. Double-click **Audit object access**.
8. Select **Define these policy settings**.
9. Select the **Failure** check box.
10. Click **OK**.
11. Close **Group Policy Management Editor**.
12. In the GPM console tree, expand the **Servers** OU, and then click the **File** OU.
13. Right-click the **File** OU, and then click **Link an Existing GPO**.

The Select GPO dialog box appears.

14. Select **File Server Auditing**, and then click **OK**.

Exercise 3: Examine Audit Events

► Task 1: Generate audit events

1. Switch to SERVER01.
2. Log on to SERVER01 as **Pat.Coleman** with the password **Pa\$\$w0rd**.
3. Run Command Prompt with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
4. Type **gpupdate.exe /force**, and then press ENTER.
5. Switch to DESKTOP101.
6. Log on to DESKTOP101 as **Mike.Danseglio** with the password **Pa\$\$w0rd**.
7. Click **Start**. In the **Start Search** box, type “**\\server01\data\Confidential Data**” and press ENTER.

A message appears to inform you that Windows cannot access
\\server01\data\Confidential Data.
8. Click **Cancel**.

► Task 2: Examine audit event log messages

1. Switch to SERVER01.
2. Run **Event Viewer** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
3. In the console tree, expand **Windows Logs**, and then click **Security**.
4. Locate the audit failure events related to Mike Danseglio's access to the Confidential Data folder.



Note: After completing this exercise, turn off all virtual machines and discard undo disks.

Lab Review Questions

Question: What are the three major steps required to configure auditing of file system and other object access?

Answer: 1) Configure auditing settings on the file/folder SACL. 2) Enable audit policy for object access, in a GPO scoped to the server. 3) Examine event log audit entries.

Question: What systems should have auditing configured? Is there a reason not to audit all systems in your enterprise? What types of access should be audited, and by whom should they be audited? Is there a reason not to audit all access by all users?

Answer: Auditing should reflect IT security and usage policies. Auditing not only puts a (small) burden on performance of a system, but also generates excessive “noise” that can make finding the “important” events even harder. What, who, and when auditing is performed should be aligned with why auditing is being performed—as driven by your business requirements.

Module 8: Secure Administration

Lab A: Delegate Administration

► Log on to a virtual machine

Unless otherwise instructed, use the following steps to log on to a virtual machine.

1. Press ALT+DELETE.

This sends the secure key sequence (CTRL+ALT+DELETE) to the virtual machine. If you press CTRL+ALT+DELETE, you send the secure key sequence to the host operating system.

2. Click **Switch User**.
3. Click **Other User**.
4. In **User name**, type the username.
5. In **Password**, type the password.
6. Press ENTER or click the log on arrow.

The Windows desktop appears.

► Run an application with administrative credentials

1. Right-click the application, and then click **Run as administrator**.

A User Account Control (UAC) dialog box appears.

2. The **UAC** dialog box will display one of three options. Do the steps based on the option you see:

If the UAC dialog box prompts you to continue or cancel:

- Click **Continue**.

If the UAC dialog box gives you the option to *Use another account*:

1. Click **Use Another Account**.
2. In **User Name**, type the username.
3. In **Password**, type the password.
4. Press ENTER or click **OK**.

If the UAC dialog box does not give you the option to use another account, and prompts you for a username and password:

1. In **User Name**, type the username.
2. In **Password**, type the password.
3. Press ENTER or click **OK**.

Exercise 1: Delegate Permission to Create and Support User Accounts

► Task 1: Prepare for the lab

1. Start 6425B-HQDC01-A.
2. Log on to HQDC01 as **Pat.Coleman** with the password **Pa\$\$w0rd**.
3. Open **D:\Labfiles\Lab08a**.
4. Run **Lab08a_Setup.bat** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
5. The lab setup script runs. When it is complete, press any key to continue.
6. Close the Windows Explorer window, **Lab08a**.

► Task 2: Create security groups for role-based management

1. On HQDC01 click **Start > Administrative Tools** and run **Active Directory Users and Computers** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
2. In the console tree, expand the **contoso.com** domain and the **Groups** OU, and then click the **Role** OU.
3. Right-click the **Role** OU, then point to **New**, and then click **Group**.
4. In **Group name**, type **Help Desk**.
5. Confirm that **Group scope** is **global** and **Group type** is **Security**.
6. Click **OK**.
7. Repeat steps 3 through 5 to create a global security group named **User Account Admins**.
8. Right-click **Help Desk**, and then click **Properties**.
9. Click the **Members** tab.
10. Click the **Add** button.
11. Type **Aaron.Painter_Admin**; **Elly.Nkya_Admin**; **Julian.Price_Admin**; **Holly.Dickson_Admin**, and then press ENTER.
12. Click **OK** to close the group **Properties** dialog box.

13. Right-click **User Account Admins**, and then click **Properties**.
14. Click the **Members** tab.
15. Click the **Add** button.
16. Type **Pat.Coleman_Admin;April.Meyer_Admin;Max.Stevens_Admin**, and then press ENTER.
18. Click **OK** to close the group **Properties** dialog box.
19. In the console tree, expand the **Admins** OU and the **Admin Groups** OU, and then click **AD Delegation**.
20. Right-click **AD Delegation**, then point to **New**, and then click **Group**.
21. In **Group name**, type **AD_User Accounts_Support**.
22. In **Group scope**, click **Domain local**.
23. Confirm that **Group type** is **Security**.
24. Click **OK**.
25. Right-click **AD Delegation**, then point to **New**, and then click **Group**.
26. In **Group name**, type **AD_User Accounts_Full Control**.
27. In **Group scope**, click **Domain local**.
28. Confirm that **Group type** is **Security**.
29. Click **OK**.
30. Right-click **AD_User Accounts_Support**, and then click **Properties**.
31. Click the **Members** tab.
32. Click the **Add** button.
33. Type **Help Desk**, and then press ENTER.
34. Click **OK** to close the group **Properties** dialog box.
35. Right-click **AD_User Accounts_Full Control**, and then click **Properties**.
36. Click the **Members** tab.
37. Click the **Add** button.
38. Type **User Account Admins**, and then press ENTER.
39. Click **OK** to close the group **Properties** dialog box.

► **Task 3: Delegate control of user support with the Delegation of Control Wizard**

1. In the console tree, right-click the **User Accounts** OU, and then click **Delegate Control**.

The Welcome to the Delegation of Control Wizard appears.

2. Click **Next**.
3. On the **Users or Groups** page, click the **Add** button.
The Select Users, Computers, or Groups dialog box appears.
4. Type **AD_User Accounts_Support**, and then press ENTER.
5. Click **Next**.
6. On the **Tasks to Delegate** page, select the **Reset user passwords and force password change at next logon** check box.
7. Click **Next**.
8. On the **Completing the Delegation of Control Wizard** page, click **Finish**.

► **Task 4: Delegate permission to create and delete users with the Access Control List Editor interface**

1. Click the **View** menu, and then select **Advanced Features**, so that the Advanced Features option is enabled.
2. In the console tree, right-click the **User Accounts** OU, and then click **Properties**.

The User Accounts Properties dialog box appears.

3. Click the **Security** tab.
4. Click the **Advanced** button.
The Advanced Security Settings for User Accounts dialog box appears.
5. Click the **Add** button.
The Select User, Computer, or Group dialog box appears.
6. Type **AD_User Accounts_ Full Control** and press ENTER.
The Permission Entry for User Accounts dialog box appears.

7. In the **Apply to** list, select **This object and all descendant objects**.
8. In the **Permissions** list, select the **Allow** check box next to **Create User objects**.
9. In the **Permissions** list, select the **Allow** check box next to **Delete User objects**.
10. Click **OK**.
11. Click the **Add** button.

The Select User, Computer, or Group dialog box appears.
12. Type **AD_User Accounts_ Full Control** and press ENTER.

The Permission Entry for User Accounts dialog box appears.
13. In the **Apply to** list, select **Descendant User objects**.
14. In the **Permissions** list, select the **Allow** check box next to **Full control**.
15. Click **OK**.
16. Click **OK** to close each remaining open dialog box.

► **Task 5: Validate the implementation of delegation**

1. Close Active Directory Users and Computers.
2. Run **Active Directory Users and Computers** with administrative credentials. Use the account **Aaron.Painter_Admin** with the password **Pa\$\$w0rd**.
3. In the console tree, expand the **contoso.com** domain and the **User Accounts** OU, and then click the **Employees** OU.
4. In the details pane, right-click **Jeff Ford**, and then click **Reset Password**.

The Reset Password dialog box appears.
5. In **New password**, type **Pa\$\$w0rd**.
6. In **Confirm password**, type **Pa\$\$w0rd**.
7. Notice that the **User must change password at next logon** check box is disabled.
8. Click **OK**.

A message appears: "The password for Jeff Ford has been changed."
9. Click **OK**.

10. Right-click **Jeff Ford**, and then click **Disable Account**. A message appears: "Windows cannot disable object Jeff Ford because: insufficient access rights to perform the operation."
11. Click **OK**.
12. In the console tree, expand the **contoso.com** domain and the **Admins** OU, and then click the **Admin Identities** OU.
13. In the details pane, right-click **Pat Coleman (Administrator)**, and then click **Reset Password**.

The Reset Password dialog box appears.
14. In **New password**, type **Pa\$\$w0rd**.
15. In **Confirm password**, type **Pa\$\$w0rd**.
16. Notice that the **User must change password at next logon** check box is disabled.
17. Click **OK**.

A message appears: "Windows cannot complete the password change for Pat Coleman (Administrator) because: Access is denied."
18. Close Active Directory Users and Computers.
19. Run **Active Directory Users and Computers** with administrative credentials. Use the account **April.Meyer_Admin** with the password **Pa\$\$w0rd**.
20. In the console tree, expand the **contoso.com** domain and the **User Accounts** OU, and then click **Employees**.
21. Right-click **Employees**, then point to **New**, and then click **User**. The **New Object - User** dialog box appears.
22. In **First name**, type your first name.
23. In **Last name**, type your last name.
24. In **User logon name**, type a username for yourself following the naming standard **FirstName.LastName**.
25. Click **Next**.

Note that user logon names can be only 20 characters,.

If you receive a message that indicates that another user account already exists with the same name, change your user logon name so that it is unique by adding **_6425** to the end.

26. In **Password**, type **Pa\$\$w0rd**.
27. In **Confirm password**, type **Pa\$\$w0rd**.
28. Click **Next**.
29. Click **Finish**.
30. Close Active Directory Users and Computers.

Exercise 2: View Delegated Permissions

► Task 1: View permissions in the Access Control List Editor interfaces

1. Run **Active Directory Users and Computers** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
2. In the console tree, expand the **contoso.com** domain, and then click the **User Accounts** OU.
3. Right-click the **User Accounts** OU, and then click **Properties**.
The User Accounts Properties dialog box appears.
4. Click the **Security** tab.
If you do not see the Security tab, close the dialog box. Click the View menu of the MMC console, and ensure that Advanced Features is selected. Then open the properties of the object again.
5. Click the **Advanced** button.
The Advanced Security Settings for User Accounts dialog box appears.
6. Click the **Name** column heading, so that the **Name** column is sorted alphabetically.

Question: How many permission entries were created for the AD_User Accounts_Support group by the Delegation of Control Wizard? Is it easy to tell what permissions were assigned in the Permission Entries list? List the permissions assigned to AD_User Accounts_Support.

Answer: Two permission entries appear in the list. It is not easy to tell exactly what permissions were assigned in the list: one entry reports "Special" and the other entry reports nothing in the Permission column. Clicking Edit for the "Special" permission shows that it is Reset Password. Clicking Edit for the other permission shows that it is Read pwdLastSet and Write pwdLastSet.

7. Click **Cancel** to close all open dialog boxes.

► **Task 2: Report permissions using DSACLs**

1. Click **Start**, and then click **Command Prompt**.
2. Type the command **dscls "ou=User Accounts,dc=contoso,dc=com"** and then press ENTER.

Question: What permissions are reported for AD_User Accounts_Support by the DSACLs command?

Answer: DSACLs reports the following permissions for AD_User Accounts_Support:
SPECIAL ACCESS for pwdLastSet: WRITE PROPERTY and READ PROPERTY
Reset Password

► **Task 3: Evaluate effective permissions**

1. In the Active Directory Users and Computers console tree, expand the **contoso.com** domain and the **User Accounts** OU.
2. Right-click the **User Accounts** OU, and then click **Properties**.
The User Accounts Properties dialog box appears.
3. Click the **Security** tab.
4. Click the **Advanced** button.
The Advanced Security Settings for User Accounts dialog box appears.
5. Click the **Effective Permissions** tab.
6. Click the **Select** button.
The Select User, Computer, or Group dialog box appears.
7. Type **April.Meyer_Admin**, and then press ENTER.
8. Locate the permissions **Create User objects** and **Delete User objects**, approximately halfway down the **Effective permissions** list.

Question: Do you see the Reset Password permission in this list?

Answer: No. A Lab Review question at the end of this lab will address why the permission does not appear.

9. Click **Cancel** to close all open dialog boxes.
10. In the console tree, expand the **contoso.com** domain and the **User Accounts** OU, and then click the **Employees** OU.
11. In the details pane, right-click **Aaron Lee**, and then click **Properties**.
The Aaron Lee Properties dialog box appears.
12. Click the **Security** tab.
13. Click the **Advanced** button.
The Advanced Security Settings for Aaron Lee dialog box appears.
14. Click the **Effective Permissions** tab.
15. Click the **Select** button
The Select User, Computer, or Group dialog box appears.
16. Type **Aaron.Painter_Admin**, and then press ENTER.
17. Locate the **Reset Password** permission in the **Effective Permissions** list.
18. Click **Cancel** to close all open dialog boxes.

Exercise 3: Remove and Reset Permissions

► **Task 1: Remove permissions assigned to AD_User Accounts_Support**

1. In the console tree, expand the **contoso.com** domain, and then click the **User Accounts** OU.
2. Right-click the **User Accounts** OU, and then click **Properties**.
The User Accounts Properties dialog box appears.
3. Click the **Security** tab.
4. Click the **Advanced** button.
The Advanced Security Settings for User Accounts dialog box appears.
5. Click the **Name** column heading so that the **Name** column is sorted alphabetically.
6. Select the first permission assigned to **AD_User Accounts_Support**, and then click **Remove**.
7. Select the remaining permission assigned to **AD_User Accounts_Support**, and then click **Remove**.
8. Click **OK** to close the remaining open dialog boxes.

► **Task 2: Reset the User Accounts OU to its default permissions**

1. In the console tree, expand the **contoso.com** domain, and then click the **User Accounts** OU.
2. Right-click the **User Accounts** OU, and then click **Properties**.
The User Accounts Properties dialog box appears.
3. Click the **Security** tab.
4. Click the **Advanced** button.
The Advanced Security Settings for User Accounts dialog box appears.
5. Click **Restore defaults**, and then click **Apply**.



Note: Do not shut down the virtual machine once you are finished with this lab as the settings you have configured here will be used in the subsequent lab.

Question: What do you achieve by clicking Restore defaults? What permissions remain?

Answer: All custom, explicit permissions are removed. What remain are the default permissions explicitly assigned to any new OU object, as defined by the Active Directory Schema. In addition, permissions inherited from parent objects apply.

Lab B: Audit Active Directory Changes

► Log on to a virtual machine

Unless otherwise instructed, use the following steps to log on to a virtual machine.

1. Press ALT+DELETE.

This sends the secure key sequence (CTRL+ALT+DELETE) to the virtual machine. If you press CTRL+ALT+DELETE, you send the secure key sequence to the host operating system.
2. Click **Switch User**.
3. Click **Other User**.
4. In **User name**, type the username.
5. In **Password**, type the password.
6. Press ENTER or click the log on arrow.

The Windows desktop appears.

► Run an application with administrative credentials

1. Right-click the application, and then click **Run as administrator**.
A User Account Control (UAC) dialog box appears.
2. The **UAC** dialog box will display one of three options. Do the steps based on the option you see:

If the UAC dialog box prompts you to continue or cancel:

- Click **Continue**.

If the UAC dialog box gives you the option to *Use another account*:

1. Click **Use Another Account**.
2. In **User Name**, type the username.
3. In **Password**, type the password.
4. Press ENTER or click **OK**.

If the UAC dialog box does not give you the option to use another account, and prompts you for a username and password:

1. In **User Name**, type the username.
2. In **Password**, type the password.
3. Press ENTER or click **OK**.

Exercise 1: Audit Changes to Active Directory by Using Default Audit Policy

► Task 1: Prepare for the lab

The virtual Machines should already be started and available after completing Lab A. However, if they are not, you should complete the below steps then step through Exercises 1 to 3 in Lab A before continuing.

1. Start 6425B-HQDC01-A.
2. Log on to HQDC01 as **Pat.Coleman** with the password **Pa\$\$w0rd**.

► Task 2: Confirm that the Domain Admins group is configured to audit changes to its membership

1. Run **Active Directory Users and Computers** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
2. In the console tree, expand the **contoso.com** domain, and then click the **Users** container.
3. Right-click the **Domain Admins** group, and then click **Properties**.
The Domain Admins Properties dialog box appears.
4. Click the **Security** tab.
If you do not see the Security tab, close the dialog box. Click the View menu of the MMC console, and ensure that Advanced Features is selected. Then open the properties of the object again.
5. Click the **Advanced** button.
The Advanced Security Settings for Domain Admins dialog box appears.
6. Click the **Auditing** tab.
7. Select the first audit entry, for which the **Access** column is **Special**, and then click **Edit**.
The Auditing Entry for Domain Admins dialog box appears.
8. Locate the entry that specifies for auditing of successful attempts to modify properties of the group such as membership.

Question: What is the Auditing Entry that achieves this goal?

Answer: Successful attempts to Write all properties by the Everyone group.

9. Click **Cancel** to close each open dialog box.

► **Task 3: Make a change to the membership of Domain Admins**

1. Right-click the **Domain Admins** group, and then click **Properties**.
The Domain Admins Properties dialog box appears.
2. Click the **Members** tab.
3. Click **Add**.
4. Type **Stuart.Munson**, and press ENTER.
5. Click **Apply** to apply your change.
6. Select **Stuart Munson**.
7. Click **Remove**.
A message appears asking you to confirm the removal.
8. Click **Yes**.
9. Click **OK** to close the **Domain Admins Properties** dialog box.
10. Make a note of the time when you made the changes. That will make it easier to locate the audit entries in the event logs.

► **Task 4: Examine the events that were generated**

1. Run **Event Viewer** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
2. In the console tree, expand **Windows Logs**, and then click **Security**.
3. Scroll down to the events that took place at approximately the time that you made the changes to **Domain Admins**. You should see events that are *not* logon, logoff, or Kerberos (authentication) related.

Question: What is the Event ID of the event logged when you made your changes? What is the Task Category?

Answer: 4662. Directory Service Access.

Question: Examine the information provided on the General tab. Can you identify the following in the event log entry?

Who made the change?

When the change was made?

What object was changed?

What type of access was performed?

What attribute was changed? How is the changed attribute identified?

What change was made to that attribute?

Answer: You will be able to identify that a user (Pat.Coleman_Admin) accessed an object (Domain Admins) and used a Write Property access. The time of the change is shown. The property itself is displayed as a globally unique identifier (GUID)—you cannot readily identify that the Members property was changed. The event also does not detail the exact change that was made to the property.

Exercise 2: Audit Changes to Active Directory by Using Directory Service Changes Auditing

► Task 1: Enable Directory Services Changes auditing

1. Run Command Prompt with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
2. Type the following command, and then press ENTER:

```
auditpol /set /subcategory:"directory service changes"  
/success:enable
```

► Task 2: Make a change to the membership of Domain Admins

1. Switch to Active Directory Users and Computers.
2. In the console tree, expand the **contoso.com** domain, and then click the **Users** container.
3. Right-click the **Domain Admins** group, and then click **Properties**.
The Domain Admins Properties dialog box appears.
4. Click the **Members** tab.
5. Click **Add**.
6. Type **Stuart.Munson** and press ENTER.
7. Click **Apply** to apply your change.
8. Select **Stuart Munson**.
9. Click **Remove**.

A message appears asking you to confirm the removal.

10. Click **Yes**.
11. Click **OK** to close the **Domain Admins Properties** dialog box.
12. Make a note of the time when you made the changes. That will make it easier to locate the audit entries in the event logs.

► **Task 3: Examine the events that were generated**

1. Switch to Event Viewer.
2. In the console tree, expand **Windows Logs**, and then click **Security**.
3. Right-click **Security**, and then click **Refresh**.
4. Scroll down to the events that took place at approximately the time that you made the changes to Domain Admins. You should see events that are different than those you saw in the previous task.



Note: After completing this exercise, turn off all virtual machines and discard undo disks.

Question: What are the Event IDs of the event logged when you made your changes? What is the Task Category?

Answer: Adding a member is event 4728. Removing a member is event 4729. Both events are in the Security Group Management Task Category.

Question: Examine the information provided on the General tab. Can you identify the following in the event log entry?

What type of change was made?

Who made the change?

What member was added or removed?

What group was affected?

When the change was made?

Answer: You can identify that a member was added or removed, that Pat.Coleman_Admin made the change, that Stuart Munson was the member that was added or removed, and the change was made to the Domain Admins group. The event metadata also shows when the change occurred.

Module 9: Improve the Security of Authentication in an Active Directory Domain Services (AD DS) Domain

Lab A: Configure Password and Account Lockout Policies

► Log on to a virtual machine

Unless otherwise instructed, use the following steps to log on to a virtual machine.

1. Press **ALT+DELETE**.

This sends the secure key sequence (CTRL+ALT+DELETE) to the virtual machine. If you press CTRL+ALT+DELETE, you send the secure key sequence to the host operating system.
2. Click **Switch User**.
3. Click **Other User**.
4. In **User name**, type the user name.
5. In **Password**, type the password.
6. Press **ENTER** or click the log on arrow.

The Windows desktop appears.

► Run an application with administrative credentials

1. Right-click the application, and then click **Run as administrator**.

A User Account Control (UAC) dialog box appears.
2. The **UAC** dialog box will display one of three options. Do the steps based on the option you see:

If the UAC dialog box prompts you to continue or cancel:
 - Click **Continue**.

If the UAC dialog box gives you the option to *Use another account*:

1. Click **Use Another Account**.
2. In **User Name**, type the user name.
3. In **Password**, type the password.
4. Press ENTER or click **OK**.

If the UAC dialog box does not give you the option to use another account, and prompts you for a user name and password:

1. In **User Name**, type the user name.
2. In **Password**, type the password.
3. Press ENTER or click **OK**.

Exercise 1: Configure the Domain's Password and Lockout Policies

► Task 1: Prepare for the lab

1. Start 6425B-HQDC01-A.
2. Log on to HQDC01 as **Pat.Coleman** with the password **Pa\$\$w0rd**.

► Task 2: Configure the domain account policies

1. Run **Group Policy Management** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
2. In the console tree, expand **Forest:contoso.com, Domains**, and **contoso.com**.
3. Right-click **Default Domain Policy** underneath the domain, contoso.com and click **Edit**.

You may be prompted with a reminder that you are changing the settings of a GPO. If so, click **OK**.

Group Policy Management Editor opens.

4. In the console tree, expand **Computer Configuration, Policies, Windows Settings, Security Settings**, and **Account Policies**, and then click **Password Policy**.
5. Double-click the following policy settings in the console details pane and configure the settings as indicated:
 - Maximum password age: **90** Days
 - Minimum password length: **10** characters
6. In the console tree, click **Account Lockout Policy**.
7. Double-click the **Account lockout threshold** policy setting and configure it for **5** Invalid Logon Attempts. Then click **OK**.

A Suggested Value Changes window appears.

8. Click **OK**.

The values for Account lockout duration and Reset account lockout counter after are automatically set to 30 minutes.

9. Close the Group Policy Management Editor window.
10. Close the Group Policy Management window.

Exercise 2: Configure Fine-Grained Password Policy

► Task 1: Create a PSO

1. Click **Start**, point to **Administrative Tools**, right-click **ADSI Edit**, and then click **Run as administrator**.
2. Click **Use another account**.
3. In the **User name** box, type **Pat.Coleman_Admin**.
4. In the **Password** box, type **Pa\$\$w0rd**, and then press ENTER. ADSI Edit opens.
5. Right-click **ADSI Edit**, and then click **Connect To**.
6. Accept all defaults. Click **OK**.
7. In the console tree, click **Default Naming Context**.
8. In the console tree, expand **Default Naming Context**, and then click **DC=contoso,DC=com**.
9. In the console tree, expand **DC=contoso,DC=com**, and then click **CN=System**.
10. In the console tree, expand **CN=System**, and then click **CN=Password Settings Container**.

All PSOs are created and stored in the Password Settings Container (PSC).

11. Right-click the **PSC**, point to **New**, and then click **Object**.

The Create Objects dialog box appears. It prompts you to select the type of object to create. There is only one choice: *msDS-PasswordSettings*—the technical name for the object class referred to as a PSO.

12. Click **Next**.

You are then prompted for the value for each attribute of a PSO. The attributes are similar to those found in the domain account policies.

13. Configure each attribute as indicated below. Click **Next** after each attribute.
 - **cn: My Domain Admins PSO**. This is the common name of the PSO.
 - **msDS-PasswordSettingsPrecedence: 1**. This PSO has the highest possible precedence.
 - **msDS-PasswordReversibleEncryptionEnabled: False**. The password is not stored using reversible encryption.

- *msDS-PasswordHistoryLength*: **30**. The user cannot reuse any of the last 30 passwords.
- *msDS-PasswordComplexityEnabled*: **True**. Password complexity rules are enforced.
- *msDS-MinimumPasswordLength*: **15**. Passwords must be at least 15 characters long.
- *msDS-MinimumPasswordAge*: **1:00:00:00**. A user cannot change his or her password within one day of a previous change. The format is d:hh:mm:ss (days, hours, minutes, seconds).
- *msDS-MaximumPasswordAge*: **45:00:00:00**. The password must be changed every 45 days.
- *msDS-LockoutThreshold*: **5**. Five invalid logons within the time frame specified by XXX (the next attribute) will result in account lockout.
- *msDS-LockoutObservationWindow*: **0:01:00:00**. Five invalid logons (specified by the previous attribute) within one hour will result in account lockout.
- *msDS-LockoutDuration*: **1:00:00:00**. An account, if locked out, will remain locked for one day, or until it is unlocked manually. A value of zero will result in the account remaining locked out until an administrator unlocks it.

14. Click **Finish**.

15. Close **ADSI Edit**.

► **Task 2: Link a PSO to a Group**

1. Run **Active Directory Users and Computers** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
2. In the console tree, expand the **System** container.
If you do not see the System container, then click the View menu of the MMC console, and ensure that Advanced Features is selected.
3. In the console tree, click the **Password Settings Container**.
4. Right-click **My Domain Admins PSO**, click **Properties** and then click the **Attribute Editor** tab.

5. In the **Attributes** list, select **msDS-PSOAppliesTo**, and then click **Edit**.
The Multi-valued Distinguished Name With Security Principal Editor dialog box appears.
6. Click **Add Windows Account**.
The Select Users, Computers, or Groups dialog box appears.
7. Type **Domain Admins**, and then press ENTER.
8. Click **OK** twice to close the open dialog boxes.

► **Task 3: Identify the Resultant PSO for a user**

1. In the console tree, expand the **contoso.com** domain and the **Admins** OU, and then click the **Admin Identities** OU.
2. Right-click **Pat Coleman (Administrator)** and click **Properties**.
3. Click the **Attribute Editor** tab.
4. Click the **Filter** button, and click the **Constructed** option, so that it is selected.
The attribute you will locate in the next step is a constructed attribute, meaning that the resultant PSO is not a hard-coded attribute of a user; rather it is calculated by examining the PSOs linked to a user in real-time.

Question: What is the resultant PSO for Pat Coleman (Administrator)?

Answer: Open the value of the msDS-ResultantPSO attribute. The My Domain Admins PSO is the resultant PSO. It is displayed using its distinguished name (DN), CN=My Domain Admins PSO,CN=Password Settings Container,CN=System,DC=contoso,DC=com.

► Task 4: Delete a PSO

1. Close any open dialog boxes in Active Directory Users and Computers.
2. In the console tree, expand the **contoso.com** domain and the **System** container, and then click **Password Settings Container**.
3. Right-click **My Domain Admins PSO**, and then click **Delete**.
A confirmation prompt appears.
4. Click **Yes**.



Note: Do not shut down the virtual machine once you are finished with this lab as the settings you have configured here will be used in subsequent labs in this module.

Lab Review Questions

Question: Where should you define the default password and account lockout policies for user accounts in the domain?

Answer: Configure the baseline password and account lockout policies in the Default Domain Policy GPO.

Question: What are the best practices for managing PSOs in a domain?

Answer: Each PSO must fully define the appropriate password and account lockout policies, because PSOs do not "merge." Link PSOs to global groups, and not to individual user accounts. Ensure that each PSO has a unique precedence value.

Question: How can you define a unique password policy for all of the service accounts in the Service Accounts OU?

Answer: PSOs cannot be linked to an OU. You must create a global group that contains the accounts that are in the Service Accounts OU. You can then link a PSO to that group.

Lab B: Audit Authentication

► Log on to a virtual machine

Unless otherwise instructed, use the following steps to log on to a virtual machine.

1. Press ALT+DELETE.
This sends the secure key sequence (CTRL+ALT+DELETE) to the virtual machine. If you press CTRL+ALT+DELETE, you send the secure key sequence to the host operating system.
2. Click **Switch User**.
3. Click **Other User**.
4. In **User name**, type the user name.
5. In **Password**, type the password.
6. Press ENTER or click the log on arrow.

The Windows desktop appears.

► Run an application with administrative credentials

1. Right-click the application, and then click **Run as administrator**.
A User Account Control (UAC) dialog box appears.
2. The **UAC** dialog box will display one of three options. Do the steps based on the option you see:

If the UAC dialog box prompts you to continue or cancel:

- Click **Continue**.

If the UAC dialog box gives you the option to *Use another account*:

1. Click **Use Another Account**.
2. In **User Name**, type the user name.
3. In **Password**, type the password.
4. Press ENTER or click **OK**.

If the UAC dialog box does not give you the option to use another account, and prompts you for a user name and password:

1. In **User Name**, type the user name.
2. In **Password**, type the password.
3. Press ENTER or click **OK**.

Exercise 1: Audit Authentication

► Task 1: Prepare for the lab

The virtual Machine required to start this lab should already be started and available after completing Lab A. However, if it are not, you should complete the below steps and complete exercises 1 and 2 in Lab A.

1. Start 6425B-HQDC01-A.
2. Log on to HQDC01 as **Pat.Coleman** with the password **Pa\$\$w0rd**.
3. Open **D:\Labfiles\Lab09b**.
4. Run **Lab09b_Setup.bat** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
5. The lab setup script runs. When it is complete, press any key to continue.
6. Close the Windows Explorer window, **Lab09b**.

► Task 2: Configure auditing of account logon events

1. Run **Group Policy Management** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
2. In the console tree, expand **Forest:contos.com**, **Domains**, **contoso.com**, and the **Domain Controllers** OU.
3. Right-click **Default Domain Controllers Policy**, and then click **Edit**.
The Group Policy Management Editor appears.
4. In the console tree, expand **Computer Configuration**, **Policies**, **Windows Settings**, **Security Settings**, and **Local Policies**, and then click **Audit Policy**.
5. Double-click **Audit account logon events**.
6. Select the **Define these policy settings** check box.
7. Select both the **Success** and **Failure** check boxes. Click **OK**.
8. Close the **Group Policy Management Editor**.

► **Task 3: Configure auditing of logon events**

1. In the **Group Policy Management** console tree, expand **Forest, Domains, contoso.com**, and the **Servers** OU, and then click the **Important Project** OU.
2. Right-click the **Important Project** OU and click **Create a GPO in this domain, and Link it here**.
3. In the **Name** box, type **Server Lockdown Policy**, and then click **OK**.
4. In the console tree, expand the **Important Project** OU.
5. In the console tree, right-click the link to the **Server Lockdown Policy** GPO, and then click **Edit**.

The Group Policy Management Editor appears.

5. In the console tree expand **Computer Configuration, Policies, Windows Settings, Security Settings**, and **Local Policies**, and then click **Audit Policy**.
6. Double-click **Audit logon events**.
7. Select the **Define these policy settings** check box.
8. Select both the **Success** and **Failure** check boxes. Click **OK**.
9. Close the **Group Policy Management Editor**.
10. Close **Group Policy Management**.

► **Task 4: Force a refresh Group Policy**

1. Start 6425B-SERVER01-A.

As the computer starts, it will apply the changes you made to Group Policy.

2. Switch to HQDC01.
3. Run Command Prompt with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
3. Type **gpupdate.exe /force**.

This command causes HQDC01 to update its policies, at which time the new auditing settings take effect.

4. Close the Command Prompt window.

► **Task 5: Generate account logon events**

1. Switch to SERVER01.
2. Press ALT+DELETE, which sends the secure key sequence (CTRL+ALT+DELETE) to the virtual machine guest.
3. Click **Switch User**, and then click **Other User**.
4. In the **User name** box, type **Pat.Coleman**.
5. In the **Password** box, type **NotMyPassword**, and then press ENTER.
A message appears: *The user name or password is incorrect.*
6. Click **OK**.
7. In the **Password** box, type **Pa\$\$w0rd**, and then press ENTER.

► **Task 6: Examine account logon events**

1. Switch to HQDC01.
2. Run **Event Viewer** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
3. In the console tree, expand **Windows Logs**, and then click **Security**.
4. Look in the first column to identify failure events, then in the second column to see the date and time of the events. You should see only one Failure event at the time you logged on incorrectly.

Question: What Event ID is associated with the account logon failure events? (Tip: Look for the earliest of a series of failure events at the time you logged on incorrectly to SERVER01.)

Answer: 4771: Kerberos pre-authentication failed.

5. Look for the Kerberos Authentication event that happened after the incorrect logon. This should be a successful event generated when you logged on successfully.

Question: What Event ID is associated with the successful account logon? (Tip: Look for the earliest of a series of events at the time you logged on successfully to SERVER01.)

Answer: 4768: A Kerberos Authentication Ticket was requested.

► **Task 7: Examine logon events**

1. Switch to SERVER01.
2. Run **Event Viewer** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
3. In the console tree, expand **Windows Logs**, and then click **Security**.
4. Look in the first column to identify failure events, then in the second column to see the date and time of the events. You should see only one Failure event at the time you logged on incorrectly.

Question: What Event ID is associated with the logon failure events? (Tip: Look for the earliest of a series of failure events at the time you logged on incorrectly to SERVER01.)

Answer: 4625: An account failed to log on.

5. Look for the Logon event that happened after the incorrect logon. This should be a successful event generated when you logged on successfully.

Question: What Event ID is associated with the successful logon? (Tip: Look for the earliest of a series of events at the time you logged on successfully to SERVER01.)

Answer: 4624: An account was successfully logged on. Event 4648 is also registered. The information in the event indicates, "A logon was attempted using explicit credentials." This event shows the initiation of a logon, but it is Event 4624 that shows the logon actually succeeded.



Note: Do not shut down the virtual machines once you are finished with this lab as the settings you have configured here will be used in subsequent labs in this module.

Lab Review Questions

Question: What would be the disadvantage of auditing all successful and failed logons on all machines in your domain?

Answer: Such an audit policy would generate a tremendous amount of audit entries across every machine in your domain. Managing the security event logs and locating the events that indicate potential problems would be very difficult. It is best to align your audit policy with specific, narrowly-targeted auditing goals and requirements of your organization.

Question: You have been asked to audit attempts to log on to desktops and laptops in the Finance division using local accounts such as Administrator. What type of audit policy do you set, and in what GPO(s)?

Answer: You will need to enable auditing for successful and failed account logon events. But because the accounts you are interested in are local accounts, which are authenticated by the local security authority on each desktop and laptop, you will need to do so in a GPO that is scoped to apply to the desktops and laptops in the Finance division. The settings do not need to be scoped to domain controllers.

Lab C: Configure Read-Only Domain Controllers

► Log on to a virtual machine

Unless otherwise instructed, use the following steps to log on to a virtual machine.

1. Press ALT+DELETE.

This sends the secure key sequence (CTRL+ALT+DELETE) to the virtual machine. If you press CTRL+ALT+DELETE, you send the secure key sequence to the host operating system.

2. Click **Switch User**.
3. Click **Other User**.
4. In **User name**, type the user name.
5. In **Password**, type the password.
6. Press ENTER or click the log on arrow.

The Windows desktop appears.

► Run an application with administrative credentials

1. Right-click the application, and then click **Run as administrator**.

A User Account Control (UAC) dialog box appears.

2. The **UAC** dialog box will display one of three options. Do the steps based on the option you see:

If the UAC dialog box prompts you to continue or cancel:

- Click **Continue**.

If the UAC dialog box gives you the option to *Use another account*:

1. Click **Use Another Account**.
2. In **User Name**, type the user name.
3. In **Password**, type the password.
4. Press ENTER or click **OK**.

If the UAC dialog box does not give you the option to use another account, and prompts you for a user name and password:

1. In **User Name**, type the user name.
2. In **Password**, type the password.
3. Press ENTER or click **OK**.

Exercise 1: Install an RODC

► Task 1: Prepare for the lab

The virtual Machine required to start this lab should already be started and available after completing Lab A. However, if it are not, you should complete the below.

1. Start 6425B-HQDC01-A.
2. Log on to HQDC01 as **Pat.Coleman** with the password **Pa\$\$w0rd**.
3. Open **D:\Labfiles\Lab09c**.
4. Run **Lab09c_Setup.bat** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
5. The lab setup script runs. When it is complete, press any key to continue.
6. Close the Windows Explorer window, **Lab09c**.

► Task 2: Stage a delegated installation of an RODC

1. Run **Active Directory Users and Computers** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
2. In the console tree, expand the **contoso.com** domain, and then click the **Domain Controlllers** OU.
3. Right-click **Domain Controlllers** and click **Pre-create Read-only Domain Controller Account**.

The Active Directory Domain Services Installation Wizard appears.

4. Click **Next**.
5. On the **Operating System Compatibility** page, click **Next**.
6. On the **Network Credentials** page, click **Next**.
7. On the **Specify the Computer Name** page, type **BRANCHDC01**, and then click **Next**.
8. On the **Select a Site** page, click **Next**.

9. On the **Additional Domain Controller Options** page, click **Next**.

Note that the option, Read-only domain controller, is selected and cannot be unselected. That is because, of course, you launched the wizard by choosing to pre-create a read-only domain controller account.

10. On the **Delegation of RODC Installation and Administration** page, click the **Set** button.

The Select User or Computer dialog box appears.

11. Type **Aaron.Painter_Admin**, and then press ENTER.

12. Click **Next**.

13. Review your selections on the **Summary** page, and then click **Next**.

14. On the **Completing the Active Directory Domain Services Installation Wizard** page, click **Finish**.

Note that in the DC Type column, the new server is listed as an Unoccupied DC Account (Read-only, GC).

► **Task 3: Run the Active Directory Domain Services Installation Wizard on a workgroup server**

1. Start 6425B-BRANCHDC01-A.
2. Log on to BRANCHDC01 as **Administrator** with the password **Pa\$\$w0rd**.
3. Click **Start**, and then click **Run**.
4. Type **dcpromo**, and then press ENTER.

A window appears that informs you that the Active Directory Domain Services binaries are being installed. When installation is completed, the Active Directory Domain Services Installation Wizard appears.

5. Click **Next**.
6. On the **Operating System Compatibility** page, click **Next**.
7. On the **Choose A Deployment Configuration** page, click the **Existing forest** option, then click **Add a domain controller to an existing domain**, and then click **Next**.
8. On the **Network Credentials** page, type **contoso.com**.

9. Click the **Set** button.

A Windows Security dialog box appears.

10. In the **User Name** box, type **Aaron.Painter_Admin**.
11. In the **Password** box, type **Pa\$\$w0rd**, and then press ENTER.
12. Click **Next**.
13. On the **Select a Domain** page, select **contoso.com**, and then click **Next**.

A message appears to inform you that your credentials do not belong to the Domain Admins or Enterprise Admins groups. Because you have pre-staged and delegated administration of the RODC, you are able to proceed with the delegated credentials.

14. Click **Yes**.

A message appears to inform you that the account for BRANCHDC01 has been pre-staged in Active Directory as an RODC.

15. Click **OK**.

A warning message appears that indicates the computer has a dynamically assigned IP address. BRANCHDC01 has a dynamically assigned IPv6 address. However, the server does have a fixed IPv4 address. IPv6 addresses are not being used in this course, so you can ignore this message.

16. Click **Yes, the computer will use a dynamically assigned IP address (not recommended)**.
17. On the **Location For Database, Log Files, And SYSVOL** page, click **Next**.
18. On the **Directory Services Restore Mode Administrator Password** page, type **Pa\$\$w0rd12345** in the **Password** and **Confirm Password** boxes, and then click **Next**.

In a production environment, you should assign a complex and secure password to the Directory Services Restore Mode Administrator account.

Also note that we altered the domain password policy in Lab A and the directory services restore mode password (Pa\$\$w0rd) is no longer long enough. Therefore we need to add additional characters to meet the minimum required length

19. On the **Summary** page, click **Next**.
20. In the progress window, select the **Reboot On Completion** check box. Active Directory Domain Services is installed on BRANCHDC01, the server reboots.

Exercise 2: Configure Password Replication Policy

► Task 1: Configure domain-wide password replication policy

1. Switch to HQDC01.
2. In the **Active Directory Users and Computers** console tree, click the **Users** container.
3. Double-click **Allowed RODC Password Replication Group**.
4. Click the **Members** tab.
5. Examine the default membership of **Allowed RODC Password Replication Group**.

Question: Who are the default members of Allowed RODC Password Replication Group?

Answer: There are no members by default.

6. Click **OK**.
7. Double-click **Denied RODC Password Replication Group**.
8. Click the **Members** tab.

Question: Who are the default members of Denied RODC Password Replication Group?

Answer: Security-sensitive groups, including Cert Publishers, Domain Admins, Domain Controllers, Enterprise Admins, Group Policy Creator Owners, krbtgt, Read-Only Domain Controllers, and Schema Admins

9. Click the **Add** button.

The Select Users, Contacts, Computers, or Groups dialog box appears.

10. Type **DNSAdmins**, and then press ENTER.
11. Click **OK**.
12. In the console tree, click the **Domain Controllers** OU.
13. Right-click **BRANCHDC01** and click **Properties**.
14. Click the **Password Replication Policy** tab.

Question: What is the password replication policy for the Allowed RODC Password Replication Group? For the Denied RODC Password Replication Group?

Answer: Allow and Deny, respectively.

15. Click **OK** to close the dialog box.

► **Task 2: Create a group to manage password replication to the branch office RODC**

1. In **Active Directory Users and Computers** console tree, expand **Groups**, and then click the **Role** OU.
2. Right-click **Role**, point to **New**, and then click **Group**.
3. In the **Group name:** field, type **Branch Office Users**, and then click **OK**.
4. Right-click **Branch Office Users**, and then click **Properties**.
5. Click the **Members** tab, and then click the **Add** button.
6. Type **Anav.Silverman; Chris.Gallagher; Christa.Geller; Daniel.Roth**, and then click **OK**.
7. Click **OK** to close the **Branch Office Users Properties** dialog box.

► **Task 3: Configure password replication policy for the branch office RODC**

1. In the console tree, click the **Domain Controllers** OU.
2. Right-click **BRANCHDC01** and click **Properties**.
3. Click the **Password Replication Policy** tab.
4. Click the **Add** button.
5. Click **Allow passwords for the account to replicate to this RODC**, and then click **OK**.

The **Select Users, Computers, or Groups** dialog box appears.

6. Type **Branch Office Users**, and then press **ENTER**.
7. Click **OK** to close the **BRANCHDC01 Properties** dialog box.

► **Task 4: Evaluate resultant password replication policy**

1. Right-click **BRANCHDC01** and click **Properties**.
2. Click the **Password Replication Policy** tab.
3. Click the **Advanced** button.

The Advanced Password Replication Policy for BRANCHDC01 dialog box appears.

4. Click the **Resultant Policy** tab, and then click the **Add** button.
The Select Users or Computers dialog box appears.
5. Type **Chris.Gallagher**, and then press ENTER.

Question: What is the resultant policy for Chris.Gallagher?

Answer: Allow.

6. Click **Close**.
7. Click **OK** to close the **BRANCHDC01 Properties** dialog box.

Exercise 3: Manage Credential Caching

► Task 1: Monitor credential caching

1. Switch to BRANCHDC01.
2. Log on to BRANCHDC01 as **Chris.Gallagher** with the password **Pa\$\$w0rd**.
3. Click **Start**, point to the arrow next to the **Lock** button, and then click **Log Off**.
4. Log on to BRANCHDC01 as **Mike.Danseglio** with the password **Pa\$\$w0rd**.
5. Click **Start**, point to the arrow next to the **Lock** button, and then click **Log Off**.
6. Switch to HQDC01.
7. In the **Active Directory Users and Computers** console tree, click the **Domain Controllers** OU.
8. In the details pane, right-click **BRANCHDC01**, and then click **Properties**.
9. Click the **Password Replication Policy** tab.
10. Click the **Advanced** button.

The Advanced Password Replication Policy for BRANCHDC01 dialog box appears.

The Policy Usage tab is displaying Accounts whose passwords are stored on this Read-Only Domain Controller.

Question: What users' passwords are currently cached on BRANCHDC01?

Answer: The only user whose password is stored on BRANCHDC01 is Chris Gallagher. Additionally, passwords for the computer account of BRANCHDC01 itself, and the Kerberos service account, `krbtgt_xyz`, are cached.

11. From the drop-down list, select **Accounts that have been authenticated to this Read-only Domain Controller**.

Question: What users have been authenticated by BRANCHDC01?

Answer: Mike Danseglio and Chris Gallagher.

12. Click **Close**, and then click **OK**.

► **Task 2: Pre-populate credential caching**

1. In the **Active Directory Users and Computers** console tree, click the **Domain Controllers** OU.
2. In the details pane, right-click BRANCHDC01, and then click **Properties**.
3. Click the **Password Replication Policy** tab.
4. Click the **Advanced** button.
The Advanced Password Replication Policy for BRANCHDC01 dialog box appears.
5. Click the **Prepopulate Passwords** button.
The Select Users or Computers dialog box appears.
6. Type **Christa Geller**, and then click **OK**.
7. Click **Yes** to confirm that you want to send the credentials to the RODC.
A message appears: *Passwords for all accounts were successfully prepopulated.*
8. On the **Policy Usage** tab, select **Accounts whose passwords are stored on this Read-only Domain Controller**.
9. Locate the entry for **Christa Geller**. Christa's credentials are now cached on the RODC.
10. Click **Close**.
11. Click **OK**.



Note: After completing this exercise, turn off all virtual machines and discard undo disks.

Lab Review Questions

Question: Why should you ensure that the PRP for a branch office RODC has, in its Allow list, the accounts for the *computers* in the branch office as well as the users?

Answer: Computers must authenticate to the domain as well as users, so the logic is the same as with users: you want to improve authentication performance over the WAN and ensure that authentication can continue even if the WAN link is unavailable.

Question: What would be the most manageable way to ensure that computers in a branch are in the Allow list of the RODC's PRP?

Answer: Create a group for computers, for example Branch Office Computers.

Question: What are the pro's and con's of prepopulating the credentials for all users and computers in a branch office to that branch's RODC?

Answer: There is no clear-cut answer to this question. Use it to review the strategic role of an RODC. By prepopulating the credentials of users (and computers) in the branch RODC cache, you ensure that authentication performance is maximized (on the first logon—after that, the credential would have been cached because the users are on the Allow list anyway); and you ensure that, if the WAN link is unavailable on the first logon, users can authenticate. The disadvantage is that, should there be a breach of physical security on the RODC, those credentials are exposed even if the users have not yet logged on in the branch.

Module 10: Configure Domain Name System (DNS)

Lab A: Install the DNS Service

► Log on to a virtual machine

Unless otherwise instructed, use the following steps to log on to a virtual machine.

1. Press ALT+DELETE.
This sends the secure key sequence (CTRL+ALT+DELETE) to the virtual machine. If you press CTRL+ALT+DELETE, you send the secure key sequence to the host operating system.
2. Click **Switch User**.
3. Click **Other User**.
4. In **User name**, type the user name.
5. In **Password**, type the password.
6. Press ENTER or click the log on arrow.
The Windows desktop appears.

► Run an application with administrative credentials

1. Right-click the application, and then click **Run as administrator**.
A User Account Control (UAC) dialog box appears.
2. The **UAC** dialog box will display one of three options. Do the steps based on the option you see:
If the UAC dialog box prompts you to continue or cancel:
 - Click **Continue**.
If the UAC dialog box gives you the option to *Use another account*:
 1. Click **Use Another Account**.
 2. In **User Name**, type the user name.
 3. In **Password**, type the password.
 4. Press ENTER or click **OK**.

If the UAC dialog box does not give you the option to use another account, and prompts you for a user name and password:

1. In **User Name**, type the user name.
2. In **Password**, type the password.
3. Press ENTER or click **OK**.

Exercise 1: Add the DNS Server Role

► Task 1: Prepare for the lab

1. Start 6425B-HQDC01-B.
2. Wait for startup to complete.
3. Start 6425B-HQDC02-B.
4. Log on to HQDC02 as **Pat.Coleman** with the password **Pa\$\$w0rd**.

► Task 2: Add the DNS server role

1. On HQDC02, click the **Server Manager** icon next to the **Start** button.
The User Account Control dialog box appears.
2. In **User name**, type **Pat.Coleman_Admin**.
3. In **Password**, type **Pa\$\$w0rd**, and then press ENTER.
Server Manager opens.
4. In the details pane, under **Roles Summary**, click **Add Roles**.
The Add Roles Wizard appears.
5. On the **Before You Begin** page, click **Next**.
6. In the **Roles** list, click **DNS Server**, and then click **Next**.
7. Read the information on the **DNS Server** page, and then click **Next**.
8. On the **Confirm Installation Selections** page, verify that the DNS Server role will be installed, and then click **Install**.
9. On the **Installation Results** page, click **Close**.
10. Close Server Manager.
11. Restart HQDC02.

This is not necessary in a production environment, but it speeds the process of restarting services and replicating the DNS records to HQDC02 for the purposes of this exercise.

12. Log on to HQDC02 as **Pat.Coleman** with the password **Pa\$\$w0rd**.

► **Task 3: Change the DNS server configuration of the DNS client**

1. Run Command Prompt with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
2. Type **netsh interface ipv4 set dnsserver "Local Area Connection" static 10.0.0.12 primary** and then press ENTER.
3. Type **netsh interface ipv4 add dnsserver "Local Area Connection" 10.0.0.11** and then press ENTER.

► **Task 4: Examine the domain forward lookup zone**

1. Run **DNS Manager** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.

DNS Manager is listed as DNS in the Administrative Tools folder.

DNS Manager opens.
2. In the console tree, expand **HQDC02** and **Forward Lookup Zones**, and then click **contoso.com**.
3. Examine the SOA, NS, and A records in the zone.

► **Task 5: Configure forwarders for Internet name resolution**

1. In the console tree, right-click **HQDC02**, and then click **Properties**.
The HQDC02 Properties dialog box appears.
2. Click the **Forwarders** tab.
3. Click the **Edit** button.
The **Edit Forwarders** dialog box appears.
4. Type **192.168.200.12** and press ENTER.
5. Type **192.168.200.13** and press ENTER.

6. Click **OK**.

Because these DNS servers do not actually exist, the Server FQDN will display either **<Attempting to resolve>** or **<Unable to resolve>**. In a production environment, you would configure forwarders to upstream DNS servers on the Internet, usually those provided by your Internet service provider (ISP).

7. Click **OK**.

Exercise 2: Configure Forward Lookup Zones and Resource Records

► Task 1: Create a forward lookup zone

1. In the console tree, right-click **Forward Lookup Zones**, and then click **New Zone**.
The New Zone Wizard appears.
2. Click **Next**.
3. On the **Zone Type** page, click **Primary zone** and ensure that the option **Store the zone in Active Directory** is selected, and then click **Next**.
4. On the **Active Directory Zone Replication Scope** page, click **To all domain controllers in this domain (for Windows 2000 compatibility): contoso.com**, and then click **Next**.
5. On the **Zone Name** page, type **development.contoso.com**, and then click **Next**.
6. On the **Dynamic Update** page, click **Do not allow dynamic updates**, and then click **Next**.
7. On the **Completing the New Zone Wizard** page, click **Finish**.

► Task 2: Create Host and CNAME records

1. In the console tree, expand **HQDC02, Forward Lookup Zones**, and then click **development.contoso.com**.
2. Right-click **development.contoso.com**, and then click **New Host (A or AAAA)**.
The New Host dialog box appears.
3. In **Name**, type **APPDEV01**.
4. In **IP address**, type **10.0.0.24**.
5. Click **Add Host**.
A message appears informing you that the host record was completed successfully.
6. Click **OK**.

7. Click **Done**.
8. Right-click **development.contoso.com**, and then click **New Alias (CNAME)**.
The New Resource Record dialog box appears.
9. In **Alias name**, type **www**.
10. In **Fully qualified domain name (FQDN) for target host**, type **appdev01.development.contoso.com**, and click **OK**.

► **Task 3: Test name resolution**

1. Switch to the command prompt.
2. Type **nslookup www.development.contoso.com**, and then press ENTER.
3. Examine the output of the command. What does the output tell you?

The first section of output tells you which DNS server you queried. The timeout and Server: Unknown lines are the result of the fact that there is not a reverse lookup zone. The nslookup command attempts to resolve the name of the server based on its IP address, 10.0.0.12, and fails. The second section of output is the result of the query. Aliases shows the name you queried. Name shows the host name to which the CNAME (Alias) record resolved. And Address is the IP address of the host.



Note: Do not shut down the virtual machines once you are finished with this lab as the settings you have configured here will be used in subsequent labs.

Lab Review Questions

Question: If you did not configure forwarders on HQDC02, what would be the result for clients that use HQDC02 as their primary DNS server?

Answer: They could not resolve names other than those in the contoso.com domain (zone).

Question: What would happen to clients' ability to resolve names in the development.contoso.com domain if you had chosen a stand-alone DNS zone, rather than an Active Directory–integrated zone? Why would this happen? What would you have to do to solve this problem?

Answer: Clients who query the other DNS server would be unable to resolve names in the zone, because the server would not receive a replica of the zone. This could be solved by making the zone Active Directory–integrated, by hosting a secondary zone on the other DNS server, or by creating a stub zone that refers queries to the server hosting the development.contoso.com zone.

Lab B: Advanced Configuration of DNS

► Log on to a virtual machine

Unless otherwise instructed, use the following steps to log on to a virtual machine.

1. Press ALT+DELETE.

This sends the secure key sequence (CTRL+ALT+DELETE) to the virtual machine. If you press CTRL+ALT+DELETE, you send the secure key sequence to the host operating system.

2. Click **Switch User**.
3. Click **Other User**.
4. In **User name**, type the user name.
5. In **Password**, type the password.
6. Press ENTER or click the log on arrow.

The Windows desktop appears.

► Run an application with administrative credentials

1. Right-click the application, and then click **Run as administrator**.

A User Account Control (UAC) dialog box appears.

2. The **UAC** dialog box will display one of three options. Do the steps based on the option you see:

If the UAC dialog box prompts you to continue or cancel:

- Click **Continue**.

If the UAC dialog box gives you the option to *Use another account*:

1. Click **Use Another Account**.
2. In **User Name**, type the user name.
3. In **Password**, type the password.
4. Press ENTER or click **OK**.

If the UAC dialog box does not give you the option to use another account, and prompts you for a user name and password:

1. In **User Name**, type the user name.
2. In **Password**, type the password.
3. Press ENTER or click **OK**.

Exercise 1: Enable Scavenging of DNS Zones

► Task 1: Prepare for the lab

Some of the virtual machines should already be started and available after completing Lab A. However, if they are not, you should step through Exercises 1 and 2 in Lab A before continuing as there are dependencies between Lab A and Lab B.

1. Start 6425B-HQDC01-B.
2. Log on to HQDC01 as **Pat.Coleman** with the password **Pa\$\$w0rd**.
3. Open **D:\Labfiles\Lab10b**.
4. Run **Lab10b_Setup.bat** with administrative credentials. Use the account **Administrator** with the password **Pa\$\$w0rd**.
5. The lab setup script runs. When it is complete, press any key to continue.
6. Close the Windows Explorer window, **Lab10b**.
7. Start 6425B-HQDC02-B.
8. Log on to HQDC02 as **Pat.Coleman** with the password **Pa\$\$w0rd**.
9. Start 6425B-TSTDC01-A.
10. Log on to TSTDC01 as **Sara.Davis** with the password **Pa\$\$w0rd**.
11. Start 6425B-BRANCHDC01-B.
12. Wait for BRANCHDC01 to complete startup before continuing.

► Task 2: Enable scavenging of a DNS zone

1. Switch to HQDC02.
2. Run **DNS Management** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
3. In the console tree, expand **HQDC02** and **Forward Lookup Zones**, and then click **contoso.com**.
4. Right-click **contoso.com**, and then click **Properties**.
5. On the **General** tab, click the **Aging** button.

The Zone Aging/Scavenging Properties dialog box appears.

6. Select the **Scavenge stale resource records** check box.
7. Click **OK**.
8. Click **OK** to close the **contoso.com Properties** dialog box.

► **Task 3: Configure default scavenging settings**

1. In the console tree, right-click **HQDC02**, and then click **Set Aging/Scavenging for All Zones**.

The Server Aging/Scavenging Properties dialog box appears.

2. Select the **Scavenge stale resource records** check box.
3. Click **OK**.

The Server Aging/Scavenging Confirmation dialog box appears.

4. Select the **Apply these settings to the exiting Active Directory-integrated zones** check box.
5. Click **OK**.

Exercise 2: Create Reverse Lookup Zones

► Task 1: Create a reverse lookup zone

1. In the console tree, click **Reverse Lookup Zones**.
2. Right-click **Reverse Lookup Zones**, and then click **New Zone**.
The New Zone Wizard appears.
3. Click **Next**.
4. On the **Zone Type** page, click **Next**.
5. On the **Active Directory Zone Replication Scope** page, click **To all domain controllers in this domain(for Windows 2000 compatability: contoso.com)**. Click **Next**.
6. On the **Reverse Lookup Zone Name** page, click **IPv4 Reverse Lookup Zone**. Click **Next**.
7. On the **Reverse Lookup Zone Name** page, in **Network ID**, type **10**. Leave the other two octets empty. Click **Next**.
8. On the **Dynamic Update** page, click **Allow only secure dynamic updates**. Click **Next**.
9. On the **Completing the New Zone Wizard** page, click **Finish**.

► Task 2: Explore and verify the functionality of a reverse lookup zone

1. Run Command Prompt with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
2. Type **nslookup www.development.contoso.com**, and then press ENTER.
3. Note that the first section of the command output, which identifies the DNS server that was queried, indicates the IP address of the server but, next to **Server**, reports that the server is **Unknown**. That is because the nslookup.exe command cannot resolve the IP address to a name.
4. Switch to **DNS Manager**.
5. In the console tree, click the **10.in-addr.arpa** zone under **Reverse Lookup Zones**.

6. Examine the records in the zone.
7. Switch to the command prompt.
8. Type **ipconfig /registerdns**, and then press ENTER.
9. Switch to DNS Manager.
10. Right-click the **10.in-addr.arpa** zone, and then click **Refresh**.
11. Examine the resource records that have appeared.
12. Switch to the command prompt.
13. Type **nslookup www.development.contoso.com**, and then press ENTER.
14. Note that the first section of the command is now able to identify the server by both address *and* name.
15. Note that the DNS server that was queried at 10.0.0.12 is now resolved to its name.

Exercise 3: Explore Domain Controller Location

► Task 1: Explore _tcp

1. Switch to **DNS Manager**.
2. In the console tree, expand **HQDC02**, **Forward Lookup Zones**, and **contoso.com**, and then click the **_tcp** node.

Question: What do the resource records in the details pane represent?

Answer: The services offered by every domain controller in the contoso.com domain

► Task 2: Explore _tcp.brancha._sites.contoso.com

1. Switch to **DNS Manager**.
2. In the console tree, expand **HQDC02**, **Forward Lookup Zones**, **contoso.com**, **_sites**, **BRANCHA**, and then click the **_tcp** node.

Question: What do the resource records in the details pane represent?

Answer: The services offered by every domain controller that is located in, or is covering, the BRANCHA site.

Exercise 4: Configure Name Resolution for External Domains

► Task 1: Configure a stub zone

1. In the console tree, expand **HQDC02**, and then click **Forward Lookup Zones**.
2. Right-click **Forward Lookup Zones**, and then click **New Zone**.
The Welcome to the New Zone Wizard page appears.
3. Click **Next**.
The Zone Type page appears.
4. Click **Stub Zone**, and then click **Next**.
The Active Directory Zone Replication Scope page appears.
5. Click **Next**.
The Zone Name page appears.
6. Type **tailspintoys.com**, and then click **Next**.
The Master DNS Servers page appears.
7. Type **10.0.0.31** and press TAB.
8. Select the **Use the above servers to create a local list of master servers** check box.
9. Click **Next**, and then click **Finish**.

► Task 2: Configure a conditional forwarder

1. Switch to TSTDC01.
2. Run **DNS Management** with administrative credentials. Use the account **Sara.Davis_Admin** with the password **Pa\$\$w0rd**.
3. In the console tree, expand **TSTDC01**, and then click **Conditional Forwarders**.
4. Right-click the **Conditional Forwarders** folder, and then click **New Conditional Forwarder**.
5. In the **DNS Domain** box, type **contoso.com**.

6. Click **Click here to add an IP Address or DNS Name**, and type **10.0.0.11**.
7. Select the **Store this conditional forwarder in Active Directory, and replicate it as follows** check box.
8. Click **OK**.

► **Task 3: Validate name resolution for external domains**

1. Click **Start**, and then click **Command Prompt**.
2. Type **nslookup www.development.contoso.com**, and then press ENTER.
The command should return the address **10.0.0.24**.
3. Switch to DNS Manager.
4. In the console tree, expand **TSTDC01, Forward Lookup Zones**, and then click the **tailspintoys.com** zone.
5. Right-click **tailspintoys.com**, and then click **New Host (A or AAAA)**.
The New Host dialog box appears.
6. In **Name**, type **www**.
7. In **IP address**, type **10.0.0.143**.
8. Click **Add Host**.
A message appears informing you that the record was added successfully.
9. Click **OK**.
10. Click **Done**.
11. Switch to HQDC02.
12. Click **Start**, and then click **Command Prompt**.
13. Type **nslookup www.tailspintoys.com**, and then press ENTER.
The command should return the address **10.0.0.143**.



Note: After completing this exercise, turn off all virtual machines and discard undo disks.

Lab Review Questions

Question: In this lab, you used a stub zone and a conditional forwarder to provide name resolution between two distinct domains. What other options might you have chosen to use?

Answer: You could create a secondary zone in each domain that hosts a copy of the zone from the other. If the domains have delegations in the top-level .com domain, you could use root hints and standard DNS recursive queries to get them to resolve names in each other's domains.

Module 11: Administer Active Directory® Domain Services (AD DS) Domain Controllers (DCs)

Lab A: Install Domain Controllers

► Log on to a virtual machine

Unless otherwise instructed, use the following steps to log on to a virtual machine.

1. Press ALT+DELETE.

This sends the secure key sequence (CTRL+ALT+DELETE) to the virtual machine. If you press CTRL+ALT+DELETE, you send the secure key sequence to the host operating system.

2. Click **Switch User**.
3. Click **Other User**.
4. In **User name**, type the user name.
5. In **Password**, type the password.
6. Press ENTER or click the log on arrow.

The Windows desktop appears.

► Run an application with administrative credentials

1. Right-click the application, and then click **Run as administrator**.

A User Account Control (UAC) dialog box appears.

2. The **UAC** dialog box will display one of three options. Do the steps based on the option you see:

If the UAC dialog box prompts you to continue or cancel:

- Click **Continue**.

If the UAC dialog box gives you the option to *Use another account*:

1. Click **Use Another Account**.
2. In **User Name**, type the user name.

3. In **Password**, type the password.
4. Press ENTER or click **OK**.

If the UAC dialog box does not give you the option to use another account, and prompts you for a user name and password:

1. In **User Name**, type the user name.
2. In **Password**, type the password.
3. Press ENTER or click **OK**.

Exercise 1: Create an Additional DC with the Active Directory Domain Services Installation Wizard

► Task 1: Prepare for the lab

1. Start 6425B-HQDC01-A.
2. Log on to HQDC01 as **Pat.Coleman** with the password **Pa\$\$w0rd**.
3. Start 6425B-HQDC02-A.
4. Log on to HQDC02 as **Administrator** with the password **Pa\$\$w0rd**.
The Windows desktop appears.

► Task 2: Promote a domain controller using the Active Directory Domain Services Installation Wizard

1. On HQDC02, click **Start**, then in the **Start Search** box, type **DCPromo.exe** and then press ENTER.

A message appears indicating that AD DS binaries are being installed. This takes several minutes.

The Active Directory Domain Services Installation Wizard appears.

2. On the **Welcome** page, click **Next**.
3. On the **Operating System Compatibility** page, review the warning about the default security settings for Windows Server 2008 domain controllers, and then click **Next**.
4. On the **Choose a Deployment Configuration** page, click **Existing forest**, then click **Add a domain controller to an existing domain**, and then click **Next**.
5. On the **Network Credentials** page, type **contoso.com** in the text box.
6. Click the **Set** button.
The Windows Security dialog box appears.
7. In the **User name** box, type **Pat.Coleman_Admin**.
8. In the **Password** box, type **Pa\$\$w0rd**, and then click **OK**.
9. Click **Next**.
10. On the **Select a Domain** page, select **contoso.com**, and then click **Next**.

11. On the **Select a Site** page, select **Default-First-Site-Name**, and then click **Next**.

The Additional Domain Controller Options page appears. DNS Server and Global Catalog are selected by default.

12. Click **Next**.

A Static IP assignment warning appears, informing you that the server has a dynamically assigned IP address.

HQDC02 has a fixed IPv4 address, and a dynamic IPv6 address. Because IPv6 is beyond the scope of this class, you can ignore this warning.

13. Click **Yes, the computer will use a dynamically assigned IP address (not recommended)**.

An Active Directory Domain Services Installation Wizard warning appears, informing you that a delegation could not be found.

The DNS configuration is correct in the sample contoso.com domain, so you can ignore this warning.

14. Click **Yes**.

15. On the **Location For Database, Log Files, And SYSVOL** page, accept the default locations for the database file, the directory service log files, and the SYSVOL files and click **Next**.

The best practice in a production environment is to store these files on three separate volumes that do not contain applications or other files not related to AD DS. This best practices design improves performance and increases the efficiency of backup and restore.

16. On the **Directory Services Restore Mode Administrator Password** page, type **Pa\$\$w0rd** in both the **Password** and **Confirm password** boxes. Click **Next**.

Do not forget the password you assigned to the Directory Services Restore Mode Administrator.

17. On the **Summary** page, review your selections.



Important: DO NOT CLICK NEXT.

If any settings are incorrect, click **Back** to make modifications.

18. Click **Export Settings**.
19. Click **Browse Folders**.

20. Click **Desktop**.
21. In the **File Name** box, type **AdditionalDC**, and then click **Save**.
A message appears, indicating that settings were saved successfully.
22. Click **OK**.
You will now cancel the domain controller installation and will, instead, promote the server to a domain controller in the next exercise.
23. On the **Active Directory Domain Services Installation Wizard Summary** page, click **Cancel**.
24. Click **Yes** to confirm that you are cancelling the installation of the DC.

Exercise 2: Add a Domain Controller from the Command Line

► Task 1: Create the DCPromo command

1. Open the **AdditionalDC.txt** file you created in Exercise 1.
2. Examine the answers in the file. Can you identify what some of the options mean?



Tip: Lines beginning with a semicolon are comments or inactive lines that have been commented out.

3. Click **Start**, and in the **Start Search** box, type **Notepad**. Then press ENTER. Notepad opens.
4. On the **Format** menu, click **Word Wrap**.
5. Position the blank Notepad window and the AdditionalDC.txt file so you can see both files.
6. In Notepad, type the dcpromo.exe command-line just as you would do in a command prompt. Determine the command-line to install the domain controller with the same options as those listed in the answer file. Options on the command-line take the form /option:value whereas, in the answer file, they take the form option=value. Configure both the **Password** and **SafeModeAdminPassword** values as **Pa\$\$w0rd**. Instruct DCPromo to reboot when complete.

Type on one line (with word wrap enabled):

```
dcpromo /unattend /ReplicaOrNewDomain:Replica
/ReplicaDomainDNSName:contoso.com
/SiteName:Default-First-Site-Name /InstallDNS:Yes /ConfirmGc:Yes
/CreatedNSDelegation:No /UserDomain:contoso.com
/UserName:contoso.com\Pat.Coleman_Admin /Password:Pa$$w0rd
/DatabasePath:"C:\Windows\NTDS" /LogPath:"C:\Windows\NTDS"
/SYSVOLPath:"C:\Windows\SYSVOL" /SafeModeAdminPassword:Pa$$w0rd
/RebootOnCompletion:Yes
```

As you will learn in Lab B, you can set the Password value to an asterisk (*) and you will be prompted to enter the password when you run the command.

7. Open `\\HQDC01\d$\Labfiles\Lab11a\Exercise2.txt`.
8. Compare the correct command in the **Exercise2.txt** file to the command you created in the previous step. Make any necessary corrections to your command.

► **Task 2: Execute the DCPromo command**

1. Click **Start**, and then click Command Prompt.
The Command Prompt opens.
2. Switch to the Notepad window containing your `dcpromo.exe` command.
3. Click the **Format** menu, and then clear the **Word Wrap** option.
If word wrap is on, the command will not copy and paste correctly into the command prompt: Each line that is wrapped will be interpreted as a separate command.
4. Press CTRL+A. Then click the **Edit** menu, and then click **Copy**.
5. Switch to the Command Prompt window.
6. Right-click in the Command Prompt window, and then click **Paste**.
7. Press ENTER to execute the command.



Tip: If you encounter errors, it is probably because of a typo in your command. Compare what you have typed to the correct command, contained in `\\HQDC01\d$\Labfiles\Lab11a\Exercise2.txt`. Alternately, copy and paste the command from the `Exercise2.txt` file instead of using the command you created.

HQDC02 is promoted to a domain controller. This takes a few minutes.

The computer restarts when configuration is complete.

Exercise 3: Remove a Domain Controller

► Task 1: Remove a domain controller

1. Wait for HQDC02 to complete startup.
2. Log on to HQDC02 as **Pat.Coleman** with the password **Pa\$\$w0rd**.
The Windows desktop appears.
3. Click the **Start** button, and then click **Run**.
4. Type **dcpromo.exe**, and then press ENTER.
The User Account Control dialog box appears.
5. In the **User name** box, type **Pat.Coleman_Admin**.
6. In the **Password** box, type **Pa\$\$w0rd**, and then press ENTER.
The Active Directory Domain Services Installation Wizard appears.
7. On the **Welcome** page, click **Next**.
A message appears, reminding you to make sure that this is not the last global catalog server in the forest.
8. Click **OK**.
9. On the **Delete the Domain** page, click **Next**.
10. On the **Administrator Password** page, type **Pa\$\$w0rd** in both the **Password** and **Confirm Password** boxes, and then click **Next**.
11. On the **Summary page**, click **Next**.
AD DS is removed from HQDC02.
12. Click **Finish**.
A message appears, prompting you to restart the server.
13. Click **Restart Now**.

Exercise 4: Create a Domain Controller from Installation Media

► Task 1: Create installation media

1. Switch to HQDC01.
2. Run Command Prompt with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
3. Type **ntdsutil**, and then press ENTER.
4. Type **activate instance ntds**, and then press ENTER.
5. Type **ifm**, and then press ENTER.
6. Type **?**, and then press ENTER to list the commands available in IFM mode.
7. Type **create sysvol full c:\IFM**, and then press ENTER.

The installation media files are copied to c:\IFM.

When the process is complete, a message appears: *IFM media created successfully in c:\IFM*.

8. Type **quit**, and then press ENTER.
9. Type **quit**, and then press ENTER.

► Task 2: Promote a domain controller using installation media

1. Log on to HQDC02 as **Pat.Coleman** with the password **Pa\$\$w0rd**.
The Windows desktop appears.
2. Click the **Start** button, and then click **Run**.
3. Type **\\HQDC01\c\$**, and then press ENTER.
The Connect to hqdc01.contoso.com dialog box appears.
4. In the **User name** box, type **CONTOSO\Pat.Coleman_Admin**.
5. In the **Password** box, type **Pa\$\$w0rd**, and then press ENTER.
A Windows Explorer window opens, showing the root of drive C on HQDC01.
6. Right-click the **IFM** folder and click **Copy**.
7. In the **Address** bar, type **C:**, and then press ENTER.

8. Right-click in an empty area of the details pane, and then click **Paste**.
The IFM folder is copied from HQDC01 to drive C.
9. Close the Windows Explorer window.
10. Click the **Start** button, and then click **Run**.
11. Type **dcpromo.exe**, and then press ENTER.
The User Account Control dialog box appears.
12. In the **User name** box, type **Pat.Coleman_Admin**.
13. In the **Password** box, type **Pa\$\$w0rd**, and then press ENTER.
The Active Directory Domain Services Installation Wizard appears.
14. On the **Welcome** page, select the **Use advanced mode installation** check box.
15. Click **Next**.
16. On the **Operating System Compatibility** page, review the warning about the default security settings for Windows Server® 2008 domain controllers, and then click **Next**.
17. On the **Choose a Deployment Configuration** page, click **Existing forest**, then click **Add a domain controller to an existing domain**, and then click **Next**.
18. On the **Network Credentials** page, type **contoso.com** in the text box.
19. Click **Next**.
20. On the **Select a Domain** page, select **contoso.com**, and then click **Next**.
21. On the **Select a Site** page, select **Default-First-Site-Name**, and then click **Next**.
The Additional Domain Controller Options page appears. DNS Server and Global Catalog are selected by default.
22. Click **Next**.
A Static IP assignment warning appears, informing you that the server has a dynamically assigned IP address.
HQDC01 has a fixed IPv4 address, and a dynamic IPv6 address. Because IPv6 is beyond the scope of this class, you can ignore this warning.

23. Click **Yes, the computer will use a dynamically assigned IP address (not recommended)**.

An Active Directory Domain Services Installation Wizard warning appears, informing you that a delegation could not be found.

The DNS configuration is correct in the sample contoso.com domain, so you can ignore this warning.

24. Click **Yes**.
25. On the **Install from Media** page, click **Replicate data from media at the following location**.
26. In the **Location** box, type **C:\IFM**, and then click **Next**.
27. On the **Source Domain Controller** page, click **Next**.

You will now cancel the domain controller installation.

28. Click **Cancel**.
29. Click **Yes** to confirm that you are cancelling the installation of the DC.
30. Shut down HQDC02. but do not shut down HQDC01 as it will be used in subsequent labs.



Note: Do not shut down the virtual machines once you are finished with this lab as the settings you have configured here will be used in Lab B.

Lab Review Questions

Question: Why would you choose to use an answer file, or a dcpromo.exe command-line to install a domain controller rather than the Active Directory Domain Services Installation Wizard?

Answer: Automation of installation. Consistency (always using the same options in a script versus hoping that an admin uses the correct options). Documentation (the script “documents” how the DC was installed). And, of course, in a Server Core installation.

Question: In what situations does it make sense to create a domain controller using installation media?

Answer: When the replication of Active Directory to the new domain controller will be problematic from a performance or network impact perspective.

Lab B: Install a Server Core DC

Exercise 1: Perform Post-Installation Configuration on Server Core

► Task 1: Prepare for the lab

The 6425B-HQDC01-A virtual machine should already be started and available after completing Lab A.

1. Start 6425B-HQDC01-A but do not log on.
2. Start 6425B-HQDC03-A but do not log on.

► Task 2: Perform post-installation configuration of Server Core

1. Log on to HQDC03 as **Administrator** with the password **Pa\$\$w0rd**.

The Command Prompt appears.

2. Type the following command, and then press ENTER:

```
netsh interface ipv4 set address name="Local Area Connection"  
source=static address=10.0.0.13 mask=255.255.255.0  
gateway=10.0.0.1
```

3. Type the following command, and then press ENTER:

```
netsh interface ipv4 set dns name="Local Area Connection"  
source=static address=10.0.0.11 primary
```

4. Type **ipconfig /all**, and then press ENTER.
5. Type the following command, and then press ENTER:

```
netdom renamecomputer %computername% /newname:HQDC03
```

You will be prompted to confirm the operation.

6. Press **Y** and then press ENTER.
7. Type **shutdown -r -t 0**, and then press ENTER.
The server restarts.
8. Wait for HQDC03 to restart.

9. Log on to HQDC03 as **Administrator** with the password **Pa\$\$w0rd**.
The Command Prompt appears.
10. Type the following command, and then press ENTER:

```
netdom join %computername% /domain:contoso.com  
/UserD:CONTOSO\Pat.Coleman_Admin /PasswordD:Pa$$w0rd  
/OU:"ou=servers,dc=contoso,dc=com"
```

11. Type **shutdown -r -t 0**, and then press ENTER.

Exercise 2: Create a Domain Controller with Server Core

► Task 1: Add the DNS Server role to Server Core

1. Wait for HQDC03 to restart.
2. Log on to HQDC03 as **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
3. Type **oclist**, and then press ENTER.

Question: What is the package identifier for the DNS server role?

Answer: DNS-Server-Core-Role.

Question: What is its status?

Answer: Not installed.

4. Type **ocsetup**, and then press ENTER.
The Windows Optional Component Setup dialog box appears.
Surprise! There is a minor amount of GUI in Server Core.
5. Click **OK**.
6. Type **ocsetup DNS-Server-Core-Role**, and then press ENTER.
Package identifiers are case sensitive.
7. Type **oclist**, and then press ENTER.
8. Confirm that DNS-Server-Core-Role shows a status of **Installed**.

► Task 2: Create a domain controller on Server Core with the **dcpromo.exe** command

1. Make sure you are still logged on to HQDC03 as **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**
2. Type **dcpromo.exe /?**, and then press ENTER.
3. Review the usage information.
4. Type **dcpromo.exe /?:Promotion**, and then press ENTER.

5. Review the usage information.
6. Type the following command to add and configure the AD DS role, and then press ENTER:

```
dcpromo /unattend /ReplicaOrNewDomain:replica  
/ReplicaDomainDNSName:contoso.com /ConfirmGC:Yes  
/UserName:CONTOSO\Pat.Coleman_Admin /Password:*  
/safeModeAdminPassword:Pa$$w0rd
```

7. When prompted to enter network credentials, type **Pa\$\$w0rd**, and then click **OK**.

The AD DS role is installed and configured, and the server reboots.



Note: You can shut down both virtual machines as different virtual machines are used in the next Lab.

Lab Review Questions

Question: Did you find the configuration of Server Core to be particularly difficult?

Answer: The correct answer will be based on your own experience and situation.

Question: What are the advantages of using Server Core for domain controllers?

Answer: Reduced system requirements, reduced attack surface (vulnerability) and therefore increased security.

Lab C: Transfer Operations Master Roles

Exercise 1: Identify Operations Masters

► Task 1: Prepare for the lab

1. Start 6425B-HQDC01-B.
2. Log on to HQDC01 as **Pat.Coleman** with the password **Pa\$\$w0rd**.
3. Open **D:\Labfiles\Lab11c**.
4. Run **Lab11c_Setup.bat** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
5. The lab setup script runs. When it is complete, press any key to continue.
6. Close the Windows Explorer window, **Lab11c**.
7. Start 6425B-HQDC02-B, but do not log on.
8. Wait for HQDC02 to complete startup before continuing.

► Task 2: Identify operations masters using the Active Directory administrative snap-ins

1. Run **Active Directory Users and Computers** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
2. In the console tree, right-click the **contoso.com** domain, and then click **Operations Masters**.

The Operations Masters dialog box appears.

The tabs identify the domain controllers currently performing the single master operations roles for the domain: PDC emulator, RID master, and Infrastructure master.

3. Click the tab for each operations master.

Question: Which DC holds those roles?

Answer: HQDC01.contoso.com holds all three roles.

4. Click **Close**.
5. Close Active Directory Users and Computers.

6. Run **Active Directory Domains and Trusts** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
7. In the console tree, right-click the root node of the snap-in, **Active Directory Domains and Trusts**, and then click **Operations Master**.
The Operations Master dialog box appears.

Question: Which DC holds the domain naming operations master role?

Answer: HQDC01.contoso.com.

8. Click **Close**.
9. Close Active Directory Domains and Trusts.
The Active Directory Schema snap-in does not have a console of its own and cannot be added to a custom console until you have registered the snap-in.
10. Run Command Prompt with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
11. Type **regsvr32 schmmgmt.dll**, and then press ENTER.
12. Click **OK** to close the message box that appears.
13. Click **Start** and, in the **Start Search** box, type **mmc.exe**, and then press ENTER.
The User Account Control dialog box appears.
14. Click **Use another account**.
15. In the **User name** box, type **Pat.Coleman_Admin**.
16. In the **Password** box, type **Pa\$\$w0rd**, and then press ENTER.
An empty MMC console appears.
17. Click the **File** menu, and then click **Add/Remove Snap-In**.
18. From the **Available snap-ins** list, select **Active Directory Schema**, click **Add**, and then click **OK**.
19. Click the root node of the snap-in, **Active Directory Schema**.
20. Right-click **Active Directory Schema**, and then click **Operations Master**.
The Change Schema Master dialog box appears.

Question: Which DC holds the schema master role?

Answer: HQDC01.contoso.com.

21. Click **Close**.
22. Close the console. You do not need to save any changes.

► **Task 3: Identify operations masters using NetDom**

1. Run Command Prompt with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
2. Type the command **netdom query fsmo**, and then press ENTER.
All operations master role holders are listed.

Exercise 2: Transfer Operations Master Roles

► Task 1: Transfer the PDC role using the Active Directory Users And Computers snap-in

1. Run **Active Directory Users and Computers** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
2. Right-click the **contoso.com** domain and click **Change Domain Controller**.
3. In the list of directory servers, select **HQDC02.contoso.com**, and then click **OK**.

Before transferring an operations master, you must connect to the domain controller to which the role will be transferred.

The root node of the snap-in indicates the domain controller to which you are connected: Active Directory Users and Computers [HQDC02.contoso.com].

4. Right-click the **contoso.com** domain and click **Operations Masters**.
5. Click the **PDC** tab.

The tab indicates that HQDC01.contoso.com currently holds the role token. HQDC02.contoso.com is listed in the second text box.

6. Click the **Change** button.

An Active Directory Domain Services dialog box prompts you to confirm the transfer of the operations master role.

7. Click **Yes**.

An Active Directory Domain Services dialog box confirms the role was successfully transferred.

8. Click **OK**, and then click **Close**.

At this point in a production environment, you would also transfer other FSMO roles held by HQDC01 to HQDC02 or other domain controllers. You would ensure that other roles performed by HQDC01 – DNS and global catalog, for example—were covered by other servers. Then you could take HQDC01 offline.

Remember that you cannot bring a domain controller back online if the RID, schema, or domain-naming roles have been seized. But you can bring it back online if a role was transferred.

► **Task 2: Consider other roles before taking a domain controller offline**

You are preparing to take HQDC01 offline. You have just transferred the PDC operations role to HQDC02.

Question: List other operations master roles that must be transferred prior to taking HQDC01 offline?

Answer: All other operations master roles held by HQDC01 should be transferred to HQDC02 or to other domain controllers prior to taking HQDC01 offline. Specifically, RID, Infrastructure, Domain Naming, and Schema master roles.

Question: List other server roles that must be transferred prior to taking HQDC01 offline?

Answer: You should consider other roles performed by HQDC01, such as DNS Server and global catalog. Ensure that these roles are covered by other servers or domain controllers prior to taking HQDC01 offline.

► **Task 3: Transfer the PDC role using NTDSUtil**

You have finished performing maintenance on **HQDC01**. You bring it back online.

1. Run Command Prompt with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
2. Type **ntdsutil**, and then press ENTER.
3. Type **roles**, and then press ENTER.
4. Type **connections**, and then press ENTER.
5. Type **connect to server HQDC01**, and then press ENTER.
6. Type **quit**, and then press ENTER.
7. Type **transfer PDC**, and then press ENTER.
The Role Transfer Confirmation dialog box appears.
8. Click **Yes**.



Note: You can shut down these virtual machines when finished with them as they will need to be restarted for the next lab.

Lab Review Questions

Question: If you transfer all roles before taking a domain controller offline, is it OK to bring the domain controller back online?

Answer: Yes

Question: If a domain controller fails and you seize roles to another domain controller, is it OK to bring the failed domain controller back online?

Answer: Only if the failed domain controller was the PDC emulator or infrastructure master. Schema, domain naming, and RID master role holders cannot be brought back online if the role was seized while the domain controller was offline. Instead, the failed domain controller must be demoted or, preferably, reinstalled entirely while offline. After the server is back online, it can be re-promoted to a domain controller and, at that time, the operations master role can be transferred gracefully to it.

Lab D: Configure DFS-R Replication of SYSVOL

Exercise 1: Observe the Replication of SYSVOL

► Task 1: Prepare for the lab

1. Shut down all VMs.
2. Start 6425B-HQDC01-B.
3. Log on to HQDC01 as **Pat.Coleman** with the password **Pa\$\$w0rd**.
4. Open **D:\Labfiles\Lab11d**.
5. Run **Lab11d_Setup.bat** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
6. The lab setup script runs. When it is complete, press any key to continue.
7. Close the Windows Explorer window, **Lab11d**.
8. Start 6425B-HQDC02-B.
9. Log on to HQDC02 as **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.

► Task 2: Observe SYSVOL replication

1. Switch to HQDC01.
2. Click **Start**, and in the **Start Search** box, type **%SystemRoot%\Sysvol\Sysvol\contoso.com\Scripts**. Then press ENTER.
3. Run **Notepad** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
4. Click **File**, and then click **Save**.
5. In the **File name** box, type **%SystemRoot%\Sysvol\Sysvol\contoso.com\Scripts\TestFRS.txt**, and then press ENTER.
6. Close Notepad.
7. Confirm that you see the file, **TestFRS.txt**, in the Scripts folder.
8. Switch to HQDC02.

9. Click **Start**, and in the **Start Search** box type **%SystemRoot%\Sysvol\Sysvol\contoso.com\Scripts**. Then press ENTER.
10. Confirm that you see the file, **TestFRS.txt**, to the HQDC02 Scripts folder.

If the file does not appear immediately, wait a few moments. It can take up to 15 minutes for replication to occur. You can, optionally, continue with Exercise 2. Before continuing even further with Exercise 3, check back to ensure that the file has replicated.
11. After you have observed the replication, close the Windows Explorer window showing the Scripts folder on both HQDC01 and HQDC02.

Exercise 2: Prepare to Migrate to DFS-R

► Task 1: Confirm that the current domain functional level is lower than Windows Server 2008

1. Still on HQDC02 Run **Active Directory Users and Computers** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd** if prompted otherwise click **continue** on the **User Account Control** dialogue box.
2. In the console tree, right-click the **contoso.com** domain, and then click **Raise Domain Functional Level**.
The Raise Domain Functional Level dialog box appears.
3. Confirm that the **Current domain functional level** is **Windows Server 2003**.
4. Click **Cancel**. Do not make any change to the domain functional level.

► Task 2: Confirm that DFS-R replication is not available at domain functional levels lower than Windows Server 2008

1. Run Command Prompt with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd** if prompted otherwise click **continue** on the **User Account Control** dialogue box.
2. Type **dfsrmig /getglobalstate**, and then press ENTER.
A message appears informing you that dfsrmig is supported only on domains at the Windows Server 2008 functional level.

► Task 3: Raise the domain functional level

1. Switch to **Active Directory Users and Computers**.
2. In the console tree, right-click the **contoso.com** domain, and then click **Raise Domain Functional Level**.
3. Confirm that the **Select an available domain functional level** list indicates **Windows Server 2008**.
4. Click **Raise**.

A message appears to remind you that the action cannot be reversed.

5. Click **OK** to confirm your change.

A message appears informing you that the functional level was raised successfully.

6. Click **OK**.
7. Close Active Directory Users and Computers.

► **Task 4: Confirm that DFS-R replication is available at Windows Server 2008 domain functional level**

1. Switch to the Command Prompt.
2. Type **dfsrmig /getglobalstate**, and then press ENTER.

A message appears informing you that DFS-R migration has not yet been initialized.

Exercise 3: Migrate SYSVOL Replication to DFS-R

► Task 1: Migrate SYSVOL replication to DFS-R

1. Switch to the Command Prompt
2. Type **dfsrmig /setglobalstate 0**, and then press ENTER.

The following message appears:

```
Current DFSR global state: 'Start'  
New DFSR global state: 'Start'  
Invalid state change requested.
```

The default global state is already 0, 'Start,' so your command is not valid. However, this does serve to initialize DFSR migration.

3. Type **dfsrmig /getglobalstate**, and then press ENTER.

The following message appears:

```
Current DFSR global state: 'Start'  
Succeeded.
```

4. Type **dfsrmig /getmigrationstate**, and then press ENTER.

The following message appears:

```
All Domain Controllers have migrated successfully to Global state  
( 'Start' ).  
Migration has reached a consistent state on all Domain  
Controllers.  
Succeeded.
```

5. Type **dfsrmig /setglobalstate 1**, and then press ENTER.

The following message appears:

```
Current DFSR global state: 'Start'
New DFSR global state: 'Prepared'

Migration will proceed to 'Prepared' state. DFSR service will
copy the contents of SYSVOL to SYSVOL_DFSR
folder.

If any DC is unable to start migration then try manual polling.
OR Run with option /CreateGlobalObjects.
Migration can start anytime between 15 min to 1 hour.
Succeeded.
```

6. Type **dfsrmig /getmigrationstate**, and then press ENTER.
A message appears that reflects the migration state of each domain controller. Migration can take up to 15 minutes.
7. Repeat this step until you receive the following message that indicates migration has progressed to the 'Prepared' state and is successful:

```
All Domain Controllers have migrated successfully to Global state
('Prepared').
Migration has reached a consistent state on all Domain
Controllers.
Succeeded.
```

When you receive the message just shown, continue to the next step.

During migration to the 'Prepared' state, you might see one of these messages:

```
The following Domain Controllers are not in sync with Global state
('Prepared'):
```

```
Domain Controller (Local Migration State) - DC Type
=====
```

```
HQDC01 ('Start') - Primary DC
HQDC02 ('Start') - Writable DC
```

```
Migration has not yet reached a consistent state on all Domain
Controllers.
State information might be stale due to AD latency.
```

or

The following Domain Controllers are not in sync with Global state ('Prepared'):

Domain Controller (Local Migration State) - DC Type
=====

HQDC01 ('Start') - Primary DC
HQDC02 ('Waiting For Initial Sync') - Writable DC

Migration has not yet reached a consistent state on all Domain Controllers.
State information might be stale due to AD latency.

or

The following Domain Controllers are not in sync with Global state ('Prepared'):

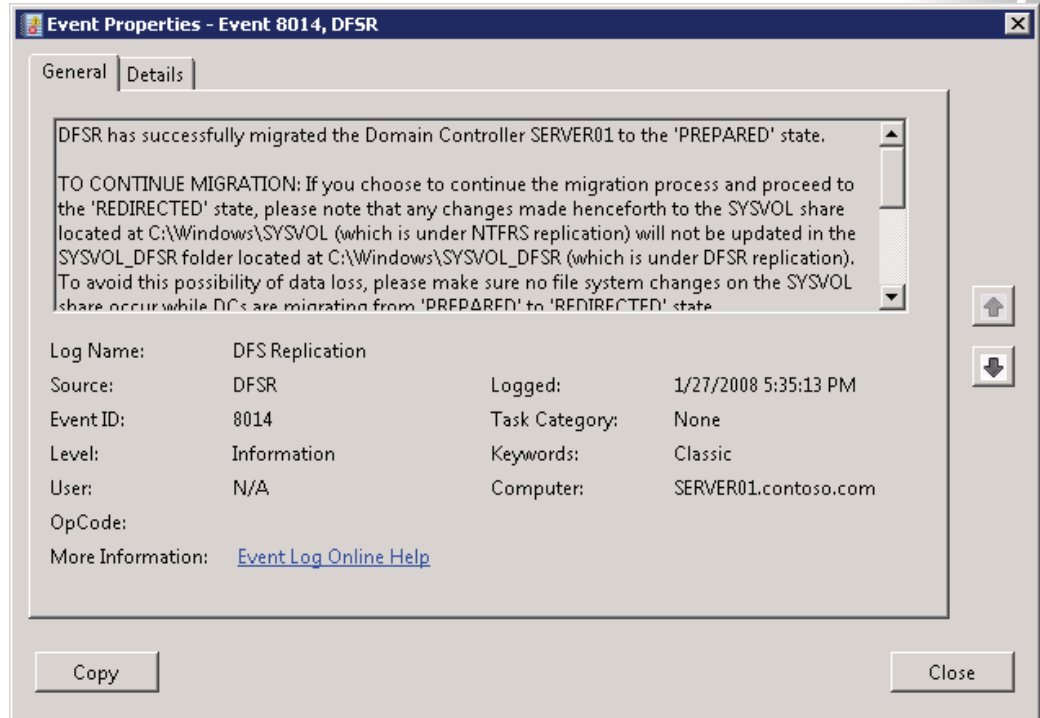
Domain Controller (Local Migration State) - DC Type
=====

HQDC02 ('Waiting For Initial Sync') - Writable DC

Migration has not yet reached a consistent state on all Domain Controllers.
State information might be stale due to AD latency.

8. Run **Event Viewer** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd** if prompted otherwise click **continue** on the **User Account Control** dialog box.
9. In the console tree, expand **Applications and Services Logs**, and then click **DFS Replication**.

10. Locate the event with **Event ID 8014** and open its properties.
You should see the details shown in the following screen shot.



11. Close **Event Viewer**.
12. Switch to the Command Prompt.

13. Type **dfsrmig /setglobalstate 2**, and then press ENTER.

The following message appears:

```
Current DFSR global state: 'Prepared'
New DFSR global state: 'Redirected'

Migration will proceed to 'Redirected' state. The SYSVOL share
will be
changed to SYSVOL_DFSR folder.

If any changes have been made to the SYSVOL share during the state
transition from 'Prepared' to 'Redirected', please robocopy the
changes
from SYSVOL to SYSVOL_DFSR on any replicated RWDC.
Succeeded.
```

14. Type **dfsrmig /getmigrationstate**, and then press ENTER.

A message appears that reflects the migration state of each domain controller. Migration can take up to 15 minutes.

15. Repeat step 14 until you receive the following message that indicates migration has progressed to the 'Prepared' state and is successful:

```
All Domain Controllers have migrated successfully to Global state
('Redirected').
Migration has reached a consistent state on all Domain
Controllers.
Succeeded.
```

When you receive the message just shown, continue to the next task.

During migration, you might receive messages like the following:

```
The following Domain Controllers are not in sync with Global state
('Redirected'):

Domain Controller (Local Migration State) - DC Type
=====

HQDC02 ('Prepared') - Writable DC

Migration has not yet reached a consistent state on all Domain
Controllers.
State information might be stale due to AD latency.
```

Exercise 4: Verify DFS-R Replication of SYSVOL

► Task 1: Confirm the new location of SYSVOL

1. Still on HQDC02, switch to the Command Prompt.
2. Type **net share**, and then press ENTER.
3. Confirm that the NETLOGON share refers to the %SystemRoot%\SYSVOL_DFSR\Sysvol\contoso.com\Scripts folder.
4. Confirm that the SYSVOL share refers to the %SystemRoot%\SYSVOL_DFSR\Sysvol folder.

► Task 2: Observe SYSVOL replication

1. Switch to HQDC01.
2. Click **Start**, and in the **Start Search** box, type %SystemRoot%\SYSVOL_DFSR\Sysvol\contoso.com\Scripts. Then press ENTER.

Note that the TestFRS.txt file created earlier is already in the Scripts folder. While the domain controllers were at the Prepared state, files were replicated between the legacy FRS SYSVOL folder and the new DFS-R SYSVOL folder.
3. Run **Notepad** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$sw0rd** if prompted otherwise click **continue** on the **User Account Control** dialogue box.
4. Click **File**, and then click **Save**.
5. In the **File name** box, type %SystemRoot%\SYSVOL_DFSR\Sysvol\contoso.com\Scripts\TestDFSR, and then press ENTER.
6. Close Notepad.
7. Confirm that you see the file, TestDFSR.txt, in the Scripts folder.
8. Switch to HQDC02.

9. Click **Start**, and in the **Start Search** box, type `%SystemRoot%\SYSVOL_DFSR\Sysvol\contoso.com\Scripts`. Then press ENTER.
10. Confirm that you see the file, TestDFSR.txt, in the Scripts folder.
If the file does not appear immediately, wait a few moments.



Note: After completing this exercise, turn off all virtual machines and discard undo disks.

Lab Review Questions

Question: What would you expect to be different between two enterprises, one which created its domain initially with Windows 2008 domain controllers, and one that migrated to Windows Server 2008 from Windows Server 2003?

Answer: In a domain that was created with Windows 2008 in the first place, the SYSVOL share will refer to a folder named SYSVOL that is replicated with DFS-R. In a domain that was created with domain controllers prior to Windows 2008, SYSVOL will be replicated with FRS, until it has been migrated. After that point, the SYSVOL share will refer to a folder named SYSVOL_DFSR.

Question: What must you be aware of while migrating from the Prepared to the Redirected state?

Answer: While migrating from the Prepared to the Redirected state, any changes made to SYSVOL must be manually duplicated in SYSVOL_DFSR.

Module 12: Manage Sites and Active Directory® Replication

Lab A: Configure Sites and Subnets

► Log on to a virtual machine

Unless otherwise instructed, use the following steps to log on to a virtual machine.

1. Press ALT+DELETE.
This sends the secure key sequence (CTRL+ALT+DELETE) to the virtual machine. If you press CTRL+ALT+DELETE, you send the secure key sequence to the host operating system.
2. Click **Switch User**.
3. Click **Other User**.
4. In **User name**, type the user name.
5. In **Password**, type the password.
6. Press ENTER or click the log on arrow.
The Windows desktop appears.

► Run an application with administrative credentials

1. Right-click the application, and then click **Run as administrator**.
A User Account Control (UAC) dialog box appears.
2. The **UAC** dialog box will display one of three options. Do the steps based on the option you see:
If the UAC dialog box prompts you to continue or cancel:
 - Click **Continue**.
If the UAC dialog box gives you the option to *Use another account*:
 1. Click **Use Another Account**.
 2. In **User Name**, type the user name.
 3. In **Password**, type the password.
 4. Press ENTER or click **OK**.

If the UAC dialog box does not give you the option to use another account, and prompts you for a user name and password:

1. In **User Name**, type the user name.
2. In **Password**, type the password.
3. Press ENTER or click **OK**.

Exercise 1: Configure the Default Site

► Task 1: Prepare for the lab

1. Start 6425B-HQDC01-B. This virtual machine may take several minutes to start.
2. Log on to HQDC01 as **Pat.Coleman** with the password **Pa\$\$w0rd**.
3. Start 6425B-HQDC02-B but do not log on.
4. After HQDC02 has completed startup, start 6425B-HQDC03-B but do not log on.
5. After HQDC03 has completed startup, start 6425B-BRANCHDC01-B, but do not log on.
6. Wait for BRANCHDC01 to finish startup before continuing to the next task.

► Task 2: Rename Default-First-Site-Name

1. On HQDC01, run **Active Directory Sites and Services** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
2. In the console tree, expand **Sites**, and then click **Default-First-Site-Name**.
3. Right-click **Default-First-Site-Name** and click **Rename**.
4. Type **HEADQUARTERS**, and then press ENTER.

Because site names are registered in DNS, you should use DNS-compliant names that avoid special characters and spaces.

► Task 3: Create a subnet and associate it with a site

1. In the console tree, click **Subnets**.
2. Right-click **Subnets** and click **New Subnet**.
3. In the **Prefix** box, type **10.0.0.0/24**.
4. In the **Select a site object for this prefix** list, select **HEADQUARTERS**.
5. Click **OK**.
6. Right-click **10.0.0.0/24**, and then click **Properties**.

7. In the **Description** box, type **Server and back-end subnet**, and then click **OK**.
8. In the console tree, right-click **Subnets**, and then click **New Subnet**.
9. In the **Prefix** box, type **10.0.1.0/24**.
10. In the **Select a site object for this prefix** list, select **HEADQUARTERS**.
11. Click **OK**.
12. Right-click **10.0.1.0/24**, and then click **Properties**.
13. In the **Description** box, type **Client subnet**, and then click **OK**.

Exercise 2: Create Additional Sites

► Task 1: Create additional sites

1. In the console tree, right-click **Sites**, and then click **New Site**.
2. In the **Name** box, type **HQ-BUILDING-2**.
3. Select **DEFAULTIPSITELINK**.
4. Click **OK**.

An Active Directory Domain Services dialog box appears, explaining the steps required to complete the configuration of the site.

5. Click **OK**.
6. In the console tree, right-click **Sites**, and then click **New Site**.
7. In the **Name** box, type **BRANCHA**.
8. Select **DEFAULTIPSITELINK**.
9. Click **OK**.

► Task 2: Create subnets and associate them with sites

1. In the console tree, right-click **Subnets** and click **New Subnet**.
2. In the **Prefix** box, type **10.1.0.0/24**.
3. In the **Select a site object for this prefix** list, select **HQ-BUILDING-2**.
4. Click **OK**.
5. Right-click **10.1.0.0/24** and then click **Properties**.
6. In the **Description** box, type **Headquarters Building 2**.
7. In the **Site** drop-down list, select **HQ-BUILDING-2**.
8. Click **OK**.
9. In the console tree, right-click **Subnets** and click **New Subnet**.
10. In the **Prefix** box, type **10.2.0.0/24**.
11. In the **Select a site object for this prefix** list, select **BRANCHA**.

12. Click **OK**.
13. Right-click **10.2.0.0/24** and then click **Properties**.
14. In the **Description** box, type **Branch Office A**.
15. In the **Site** drop-down list, select **BRANCHA**.
16. Click **OK**.

Exercise 3: Move Domain Controllers into Sites

► Task 1: Move domain controllers to new sites

1. In the console tree, expand **HEADQUARTERS**, and then click the **Servers** node.
2. In the details pane, right-click **HQDC03** and click **Move**.
The Move Server dialog box appears.
3. Click **HQ-BUILDING-2**, and then click **OK**.
4. In the details pane, right-click **BRANCHDC01** and click **Move**.
The Move Server dialog box appears.
5. Click **BRANCHA**, and then click **OK**.



Note: Do not shut down the virtual machines once you are finished with this lab as the settings you have configured here will be used in subsequent labs.

Lab Review Questions

Question: You have a site with 50 subnets, each with a subnet address of 10.0.x.0/24, and you have no other 10.0.x.0 subnets, what could you do to make it easier to identify the 50 subnets and associate them with a site?

Answer: Define a single subnet, 10.0.0.0/16.

Question: Why is it important that all subnets are identified and associated with a site in a multisite enterprise?

Answer: Domain controller (and other service) location is made efficient by referring clients to the correct site, based on the client's IP address and the definition of subnets. If a client has an IP address that does not belong to a site, the client will query for all DCs in the domain, and that is not at all efficient. In fact, a single client can be performing actions against domain controllers in different sites, which (if those changes have not replicated yet) can lead to very strange results. It's very important that each client knows what site it's in, and that's achieved by ensuring that DCs can identify what site a client is in.

Lab B: Configure the Global Catalog and Application Partitions

► Log on to a virtual machine

Unless otherwise instructed, use the following steps to log on to a virtual machine.

1. Press ALT+DELETE.

This sends the secure key sequence (CTRL+ALT+DELETE) to the virtual machine. If you press CTRL+ALT+DELETE, you send the secure key sequence to the host operating system.

2. Click **Switch User**.
3. Click **Other User**.
4. In **User name**, type the user name.
5. In **Password**, type the password.
6. Press ENTER or click the log on arrow.

The Windows desktop appears.

► Run an application with administrative credentials

1. Right-click the application, and then click **Run as administrator**.

A User Account Control (UAC) dialog box appears.

2. The **UAC** dialog box will display one of three options. Do the steps based on the option you see:

If the UAC dialog box prompts you to continue or cancel:

- Click **Continue**.

If the UAC dialog box gives you the option to *Use another account*:

1. Click **Use Another Account**.
2. In **User Name**, type the user name.
3. In **Password**, type the password.
4. Press ENTER or click **OK**.

If the UAC dialog box does not give you the option to use another account, and prompts you for a user name and password:

1. In **User Name**, type the user name.
2. In **Password**, type the password.
3. Press ENTER or click **OK**.

Exercise 1: Configure a Global Catalog

► Task 1: Prepare for the lab

The virtual Machines should already be started and available after completing Lab A. However, if they are not, you should complete the below steps then step through Exercises 1 to 3 in Lab A before continuing.

1. Start 6425B-HQDC01-B. This virtual machine may take several minutes to start.
2. Log on to HQDC01 as **Pat.Coleman** with the password **Pa\$\$w0rd**.
3. Start 6425B-HQDC02-B but do not log on.
4. After HQDC02 has completed startup, start 6425B-HQDC03-B but do not log on.
5. After HQDC03 has completed startup, start 6425B-BRANCHDC01-B, but do not log on.
6. Wait for BRANCHDC01 to finish startup before continuing to the next task.

► Task 2: Configure a global catalog server

1. On HQDC01, run **Active Directory Sites and Services** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
2. In the console tree, expand **HEADQUARTERS**, **Servers**, and HQDC02, and then click the **NTDS Settings** node below HQDC02.
3. Right-click the **NTDS Settings** node below HQDC02, and then click **Properties**.
4. Select the **Global catalog** check box, and then click **OK**.
5. Repeat steps 2 and 3 to confirm that BRANCHDC01 in the **BRANCHA** site is a global catalog server.

Exercise 2: Configure Universal Group Membership Caching

► Task 1: Configure universal group membership caching

1. In the console tree, click **BRANCHA**.
2. In the details pane, right-click **NTDS Site Settings** and click **Properties**.
3. Click the **Site Settings** tab.
4. Select the **Enable universal group membership caching** check box.
5. Click **OK**.

Exercise 3: Examine DNS and Application Directory Partitions

► Task 1: Examine DNS records related to replication

1. Run **DNS Manager** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
2. In the console tree, expand **HQDC01**, **Forward Lookup Zones**, **contoso.com**, **_sites**, and **HEADQUARTERS**, and then click **_tcp** under **HEADQUARTERS**.
3. Examine the service locator records.
4. In the console tree, expand **BRANCHA**, and then click **_tcp** under **BRANCHA**.
5. Examine the service locator records.

► Task 2: Examine the DNS application directory partition

1. Click **Start >Administrative Tools >ADSI Edit** and enter administrative credentials when prompted. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
2. In the console tree, right-click **ADSI Edit**, and then click **Connect To**.
3. In the **Select a well known naming context** drop-down list, select **Configuration**.
4. Accept all other defaults. Click **OK**.
5. In the console tree, click **Configuration**, and then expand it.
6. In the console tree, click **CN=Configuration, DC=contoso, DC=com**, and then expand it.
7. In the console tree, click **CN=Partitions**.
8. Right-click **ADSI Edit**, and then click **Connect To**.
9. Click **Select or type a distinguished name or naming context**.
10. In the combo box, type **DC=DomainDnsZones,DC=contoso,DC=com**. Click **OK**.
11. In the console tree, click **Default Naming Context**, and then expand it.
12. Click on **DC=DomainDnsZones,DC=contoso,DC=com**, and then expand it.
13. Click on **CN=MicrosoftDNS**, and then expand it.

14. Click **DC=contoso.com**.
15. Examine the objects in this container. Compare the records to the DNS records you examined in the previous exercise.



Note: Do not shut down the virtual machines once you are finished with this lab as the settings you have configured here will be used in subsequent labs.

Lab Review Questions

Question: Describe the relationship between the records you viewed in ADSI Edit and the records you viewed in DNS Manager.

Answer: Every record seen in DNS Manager's forward lookup zones has a corresponding record in the application directory partitions for DNS. However, the records as viewed in the application directory partition are flat. DNS Manager presents the records in a hierarchy.

Question: When you examined the DNS records in `_tcp.BRANCHA._sites.contoso.com`, what domain controller was registering service locator records in the site? Explain why it did so.

Answer: Answers will vary as to which DC covered BRANCHA. The site had no domain controllers, so a domain controller covers clients in the site by advertising itself using SRV records in the site.

Lab C: Configure Replication

► Log on to a virtual machine

Unless otherwise instructed, use the following steps to log on to a virtual machine.

1. Press ALT+DELETE.

This sends the secure key sequence (CTRL+ALT+DELETE) to the virtual machine. If you press CTRL+ALT+DELETE, you send the secure key sequence to the host operating system.

2. Click **Switch User**.
3. Click **Other User**.
4. In **User name**, type the user name.
5. In **Password**, type the password.
6. Press ENTER or click the log on arrow.

The Windows desktop appears.

► Run an application with administrative credentials

1. Right-click the application, and then click **Run as administrator**.

A User Account Control (UAC) dialog box appears.

2. The **UAC** dialog box will display one of three options. Do the steps based on the option you see:

If the UAC dialog box prompts you to continue or cancel:

- Click **Continue**.

If the UAC dialog box gives you the option to *Use another account*:

1. Click **Use Another Account**.
2. In **User Name**, type the user name.
3. In **Password**, type the password.
4. Press ENTER or click **OK**.

If the UAC dialog box does not give you the option to use another account, and prompts you for a user name and password:

1. In **User Name**, type the user name.
2. In **Password**, type the password.
3. Press ENTER or click **OK**.

Exercise 1: Create a Connection Object

► Task 1: Prepare for the lab

The virtual Machines should already be started and available after completing Labs A and B. However, if they are not, you should complete the below steps then step through Exercises 1 to 3 in Labs A and B before continuing.

1. Start 6425B-HQDC01-B.
2. Log on to HQDC01 as **Pat.Coleman** with the password **Pa\$\$w0rd**.
3. After logging on to HQDC01, start 6425B-HQDC02-B but do not log on.
4. After HQDC02 has completed startup, start 6425B-HQDC03-B but do not log on.
5. After HQDC03 has completed startup, start 6425B-BRANCHDC01-B but do not log on.
6. Wait for BRANCHDC01 to finish startup before continuing to the next task.

► Task 2: Create a connection object

1. Run **Active Directory Sites and Services** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
2. In the console tree, expand **HEADQUARTERS, Servers** and **HQDC02**, and then click the **NTDS Settings** node below HQDC02.
3. Right-click **NTDS Settings** and click **New Active Directory Domain Services Connection**.
4. In the **Find Active Directory Domain Controllers** dialog box, select HQDC01, and then click **OK**.

A warning appears asking if you want to create another connection.

Because the Knowledge Consistency Checker (KCC) has already created a connection from HQDC01 to HQDC02, you are asked if you want to create a duplicate connection. The direct connection that you create will be persistent, whereas connections that are automatically generated by the KCC may be changed. You want to ensure the connection is always maintained.

5. Click **Yes**.

6. In the **New Object – Connection** dialog box, type the name **HQDC01 - OPERATIONS MASTER**, and click **OK**.
7. Right-click the **HQDC01 - OPERATIONS MASTER** connection object under the NTDS settings object in the details pane, and then click **Properties**.

Question: Examine the properties of the connection object. Do not make any changes. What partitions are replicated from HQDC01? Is HQDC02 a GC server? How can you tell?

Answer: HQDC02 replicates the domain (contoso.com), Schema, and Configuration from HQDC01. It is also a global catalog server. The Partially Replicated Naming Context(s) property shows *All other domains*. This is another way of describing the forest's partial attribute set.

8. Click **OK** to close the **Properties** dialog box.

Exercise 2: Create Site Links

► Task 1: Create site links

1. In the **Active Directory Sites and Services** console tree, expand **Inter-Site Transports**, and then click **IP**.
2. In the details pane, right-click **DEFAULTIPSITELINK**, and then click **Rename**.
3. Type **HQ-HQB2**, and then press **ENTER**.
4. Double-click **HQ-HQB2**.
5. On the **General** tab, In the **Sites in this site link** list, click **BRANCHA**, and then click **Remove**. Click **OK**.
6. In the console tree, right-click **IP**, and then click **New Site Link**.
7. In the **Name** box, type **HQ-BRANCHA**.
8. In the **Sites not in this site link** list, click **HEADQUARTERS**, and then click **Add**.
9. In the **Sites not in this site link** list, click **BRANCHA**, and then click **Add**.
10. Click **OK**.

Exercise 3: Move Domain Controllers into Sites

► Task 1: Move domain controllers to new sites

1. In the console tree, expand **HEADQUARTERS**, and then click the **Servers** node.
2. In the details pane, right-click **BRANCHDC01** and click **Move**.
The Move Server dialog box appears.
3. Click **BRANCHA**, and then click **OK**.

Exercise 4: Designate a Preferred Bridgehead Server

► Task 1: Designate a preferred bridgehead server

1. In the console tree, expand **HEADQUARTERS, Servers**, and then click the **HQDC02** node.
2. Right-click **HQDC02** and click **Properties**.
3. In the **Transports available for inter-site data transfer** list, click **IP**.
4. Click **Add**, and then click **OK**.
A lengthy warning message appears.
5. Read the message. You will discuss it at the end of the lab.
6. Click **OK**.

Exercise 5: Configure Intersite Replication

► Task 1: Configure Intersite Replication

1. In the console tree, expand **Inter-Site Transports**, and then click the **IP** node.
2. In the details pane, double-click the **HQ-HQB2** site link.
3. In the **Replicate every** spin-box, type **15**, and then click **OK**.
4. In the details pane, double-click the **HQ-BRANCHA** site link.
5. In the **Replicate every** spin-box, type **15**.
6. Click the **Change Schedule** button.
7. Examine the **Schedule For HQ-BRANCHA** dialog box. Experiment with configuring the schedule but click **Cancel** when you are finished.
8. In the **Cost** spin-box, type **200**.
9. Click **OK**.



Note: After completing this exercise, turn off all virtual machines and discard undo disks.

Lab Review Questions

Question: Explain the warning message that appeared when you designated HQDC02 as a preferred bridgehead server.

Answer: A bridgehead server acts as the bridgehead only for Active Directory partitions that it contains. Because HQDC02 is not a DNS server, it does not host the ForestDnsZones or DomainDnsZones application partitions. The ISTG will continue to automatically designate another DC in the site as the bridgehead server for those two partitions. The warning message explained that the best practice is to designate bridgeheads for each partition. Ideally, the bridgehead server should host all partitions—in this case, including the DNS application partitions.

Question: What are the advantages of reducing the intersite replication interval? What are the disadvantages?

Answer: Convergence is improved. Changes made in one site are replicated more quickly to other sites. There are actually few, if any, disadvantages. If you consider that the same changes must replicate whether they wait 15 minutes or 3 hours to replicate, it's really a matter of timing of replication rather than quantity of replication. However, in some extreme situations, it's possible that allowing a smaller number of changes to happen more frequently might be less preferable than allowing a large number of changes to replicate less frequently.

Question: Is the procedure you performed in Exercise 2 enough to create a "hub and spoke" replication topology, which ensures that all changes from branches are replicated to the headquarters before being replicated to other branches? If not, what must still be done?

Answer: You must disable "Bridge all site links."

MCT USE ONLY. STUDENT USE PROHIBITED

Module 13: Directory Service Continuity

Lab A: Monitor Active Directory Events and Performance

► Log on to a virtual machine

Unless otherwise instructed, use the following steps to log on to a virtual machine.

1. Press ALT+DELETE.

This sends the secure key sequence (CTRL+ALT+DELETE) to the virtual machine. If you press CTRL+ALT+DELETE, you send the secure key sequence to the host operating system.

2. Click **Switch User**.
3. Click **Other User**.
4. In **User name**, type the user name.
5. In **Password**, type the password.
6. Press ENTER or click the log on arrow.

The Windows desktop appears.

► Run an application with administrative credentials

1. Right-click the application, and then click **Run as administrator**.

A User Account Control (UAC) dialog box appears.

2. The **UAC** dialog box will display one of three options. Do the steps based on the option you see:

If the UAC dialog box prompts you to continue or cancel:

- Click **Continue**.

If the UAC dialog box gives you the option to *Use another account*:

1. Click **Use Another Account**.
2. In **User Name**, type the user name.
3. In **Password**, type the password.
4. Press ENTER or click **OK**.

If the UAC dialog box does not give you the option to use another account, and prompts you for a user name and password:

1. In **User Name**, type the user name.
2. In **Password**, type the password.
3. Press ENTER or click **OK**.

Exercise 1: Monitor Real-Time Performance Using Task Manager and Resource Monitor

► Task 1: Prepare for the lab

1. Start 6425B-HQDC01-B.
2. Log on to HQDC01 as **Pat.Coleman** with the password **Pa\$\$w0rd**.
3. Open **D:\Labfiles\Lab13a**.
4. Run **Lab13a_Setup.bat** with administrative credentials. Use the account **Administrator** with the password **Pa\$\$w0rd**.
5. The lab setup script runs. When it is complete, press any key to continue.
6. Close the Windows Explorer window, **Lab13a**.
7. Start 6425B-HQDC02-B.
8. Log on to HQDC02 as **Pat.Coleman** with the password **Pa\$\$w0rd**.

► Task 2: Monitor real-time performance with Task Manager

1. Switch to HQDC01.
2. Press CTRL+SHIFT+ESC to launch Task Manager.
3. Click the **Processes** tab.
4. Right-click **taskmgr.exe** and examine the available commands. Then click **Properties**.

The Properties dialog box for the executable opens.

5. Close the **Properties** dialog box.
6. Click **Show processes from all users**.
7. Click **Use Another Account**.
8. In **User name**, type **Pat.Coleman_Admin**.

9. In **Password**, type **Pa\$\$w0rd**, and then press ENTER.

Task Manager re-opens with all processes displayed and with all administrative features enabled.

10. If you do not see Task Manager, it may be minimized or behind other windows. Click its icon in the task bar to make it visible.
11. Click the **Processes** tab.
12. Examine the full list of processes running on the system.
13. Click the **Services** tab.
14. Right-click **Dnscache**, and then click **Stop Service**.
15. Right-click **Dnscache**, and then click **Start Service**.
16. Right-click **Dnscache**, and then click **Go to Process**.

Question: What process is hosting the DNS Client service?

Answer: svchost.exe

17. Right-click the process, and then click **Go to Service(s)**.

Question: The Services tab exposes a subset of the most-used functionality of which administrative snap-in?

Answer: The Services snap-in

18. Click the **Services** button.
The Services console appears.
19. Close the **Services** console.

20. Click the **Users** tab.

This tab displays users who have either local (Console) or remote desktop connections to the server.

21. Click the **Networking** tab.

This tab provides an overview of performance for each available network adapter.

22. Click the **Performance** tab.

This tab provides an overview of performance for CPU utilization and Memory.

Question: Which major system component is *not* shown by task manager?

Answer: Disk

► **Task 3: Monitor real-time performance with Resource Monitor**

1. In Task Manager, on the **Performance** tab, click the **Resource Monitor** button.
If you are prompted for administrative credentials, use the account Pat.Coleman_Admin with the password Pa\$\$w0rd.
2. Resource Monitor appears. Maximize the Resource Monitor window and close Task Manager.
3. Click the **CPU** graph. The CPU section expands.

Question: How much CPU utilization is being generated by Reliability and Performance Monitor itself?

Answer: Answers will vary. Utilization will be higher at first, when the tool is opened, and will rise when views are changed. If a view is left alone, utilization drops.

5. Click the **CPU** graph. The **CPU** section collapses.
6. Click the **Disk** graph. The **Disk** section expands.

Questions: What file is experiencing the most Read activity? Which process is causing the Read activity for that file? Which file is experiencing the most Write activity? Which process is causing the Write activity for that file?

Answer: Answers will vary.

7. To view the activity of the page file, click the **File** column label.
8. If C:\pagefile.sys is not listed, open an application such as Server Manager with administrative credentials. Use the account **Pat.Coleman_admin** with the password **Pa\$\$w0rd**. This should generate some paging activity.

Questions: How many processes are reading from or writing to pagefile.sys?

Answer: Answers will vary.

Question: If the pagefile Read and Write activity is consistently high, what system component should be augmented?

Answer: Memory. Excessive paging causes disk activity, but paging itself is caused by insufficient RAM.

9. Close Resource Manager.
10. Click the **Start** button.
11. In the **Start Search** box, type **perfmon**, and then press ENTER.
The User Account Control dialog box appears.
12. Click **Use Another Account**.
13. In **User name**, type **Pat.Coleman_Admin**.
14. In **Password**, type **Pa\$\$w0rd**, and then press ENTER.

Users, members of the Performance Monitor Users group, members of the Performance Log Users group, and members of the local Administrators group, are able to access increasing levels of functionality from Windows Reliability and Performance Monitor (WRPM).

Reliability and Performance Monitor opens.

The home view for the console is the Resource Overview, equivalent to Resource Monitor.

Note that the console tree contains each of the WRPM snap-ins.

15. Close **Reliability and Performance Monitor**.
16. Click the **Start** button.
17. In the **Start Search** box, type **perfmon /res**, and then press ENTER.
The User Account Control dialog box appears.
18. In **User name**, type **Pat.Coleman_Admin**.

19. In **Password**, type **Pa\$\$w0rd**, and then press ENTER. The **Resource Monitor** opens.

This is an alternate way to open Resource Monitor, which you have opened from Task Manager, and which is the home view of the Reliability and Performance Monitor console.

20. Close **Resource Monitor**.

Exercise 2: Use Reliability Monitor and Event Viewer to Identify Performance-Related Events

► Task 1: Monitor stability-related events with Reliability Monitor

1. Click the **Server Manager** icon next to the **Start** button.
The User Account Control dialog box appears.
2. In **User name**, type **Pat.Coleman_Admin**.
3. In **Password**, type **Pa\$\$w0rd**, and then press ENTER.
Server Manager opens.
4. In the console tree, expand **Diagnostics, Reliability and Performance, Monitoring Tools**, and then click **Reliability Monitor**.
5. In the **System Stability Chart**, scroll to the left and right.
6. Click the **Information** icon in the **Software (Un) Installs** row on Sept 9, 2009.
7. Examine the events that affected system stability on Sept 9, 2009.

► Task 2: Identify role-related events with Server Manager

1. In the Server Manager console tree, click the root node, **Server Manager**.
2. In the details pane, scroll to the **Roles Summary** section.

Question: What icons appear next to the ADDS and DNS Server roles?

Answer: Answers will vary.

3. Click the link to the **Active Directory Domain Services** role in the **Roles Summary** section.
4. In the **Summary** section, examine the information shown in the **Events** section.
5. Click the **Filter Events** link in the **Events** section.
The Filter Events dialog box appears.

6. Clear the **Information** check box, and then click **OK**.
7. Double-click an event to open its details, examine the event, and then close the event.
8. Note the information shown in the **System Services** section.

► **Task 3: Examine the event logs**

1. In the Server Manager console tree, expand **Diagnostics** and **Event Viewer**, and then click **Event Viewer**.
The Event Viewer Overview and Summary view appears in the details pane.
2. In the **Summary of Administrative Events** section, click the plus sign (+) icon next to **Error** to expand the **Error** events summary.
3. Double-click a summary row with **ActiveDirectory** as the source.
If you do not see a row in the summary with ActiveDirectory as the source, double-click another row in the **Error** events summary.
The Summary page events view opens in the details pane.
This view "drills down" to show the events that were summarized on the row of the Error events summary.
4. In the console tree, expand **Windows Logs** and **Applications and Services Logs**.
5. Examine the logs contained in those nodes, and the types of events they display.
6. In the console tree, click the **Administrative Events** node underneath **Custom Views**.
7. Examine the events in the view.
8. Right-click **Administrative Events**, and then click **Properties**.
9. Note that the **Description** indicates that the view shows **Critical**, **Error** and **Warning** events from all administrative logs.
10. Click the **Edit Filter** button.
The Custom View Properties (Read Only) dialog box appears.
11. Note that this custom view cannot be modified—it is **Read Only**.

12. Note that it is difficult to know exactly which logs are being included in the **Event Logs** list. The information is truncated.
13. Click the **XML** tab.

Question: Can you identify which logs are included using the information on the XML tab?

Answer: Application, Security, System, DFS Replication, Directory Service, DNS Server, Hardware Events, Internet Explorer, Key Management Service, and Microsoft-Windows-TerminalServices-PnPDevices/Admin logs are included.

Question: In each XML Select element, what do you think Level refers to?

Answer: The Level refers to the event level: Warning, Error, or Critical events.

14. Click **Cancel** twice to close the open dialog boxes.

► **Task 4: Create a custom view**

1. In the console tree, click **Custom Views**.
2. Right-click **Custom Views**, and then click **Create Custom View**.
The **Create Custom View** dialog box appears.
3. In the **Event level** options, select **Critical**, **Warning**, and **Error**.
4. In the **Event logs** list, expand **Applications and Services Logs**, and then select **DFS Replication**, **Directory Service**, and **DNS Server**.
5. Click **OK**.
The **Save Filter to Custom View** dialog box appears.
6. In **Name**, type **Custom Directory Service Event View**, and then click **OK**.
7. In the console tree, right-click **Custom Directory Service Event View** and then examine the commands that are available for the view.

► **Task 5: Export a custom view**

1. In the console tree, right-click **Custom Directory Service Event View**, and then click **Export Custom View**.

The Save As dialog box appears.

2. In **File name**, type **D:\Data\DSEventView**, and then press ENTER.

► **Task 6: Import a custom view**

1. Switch to HQDC02.
2. Click the **Server Manager** icon next to the **Start** button.

The User Account Control dialog box appears.

3. In **User name**, type **Pat.Coleman_Admin**.
4. In **Password**, type **Pa\$\$w0rd**, and then press ENTER.
5. In the console tree, expand **Diagnostics**, **Event Viewer**, and **Custom Views**, and then click **Custom Views**.
6. Right-click **Custom Views**, and then click **Import Custom View**.

The Import Custom View dialog box opens.

7. In **File Name**, type **\\HQDC01\Data\DSEventView.xml** and then press ENTER.

The Import Custom View File dialog box appears.

8. In **Name**, type **Custom Directory Service Event View**, and then click **OK**.
A Query Error message appears, because HQDC02 is not a Domain Name System (DNS) server and therefore has no DNS Server log.
9. Click **OK**.

Exercise 3: Monitor Events on Remote Computers with Event Subscriptions

► Task 1: Configure computers to forward and collect events

1. Switch to HQDC01 (the collector computer).
2. Run Command Prompt with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
3. Type **wecutil qc** then press ENTER.
You are prompted to confirm the change.
4. Type **Y** and then press ENTER.
5. Switch to HQDC02 (the source computer).
6. Run Command Prompt with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
7. Type **winrm quickconfig** and then press ENTER.
You are prompted to confirm the change.
8. Type **Y** and then press ENTER.

► Task 2: Create a subscription to collect events

1. Switch to HQDC01.
2. Switch to Server Manager.
3. In the console tree, under **Event Viewer**, click **Subscriptions**.
4. Right-click **Subscriptions** and click **Create Subscription**.
The Subscription Properties dialog box appears.
5. In **Subscription name**, type **DC Services**.
6. Ensure that **Collector initiated** is selected.
7. Click the **Select Computers** button.
The Computers dialog box appears.
8. Click the **Add Domain Computers** button.
The Select Computer dialog box appears.

9. Type **HQDC02**, and then click **OK**.
10. Click the **Test** button.

An Event Viewer message appears, indicating that the connectivity test succeeded.
11. Click **OK**.
12. Click **OK** to close the **Computers** dialog box.
13. Click the **Select Events** button.

The Query Filter dialog box opens.
14. Click the **Information** checkbox in the **Event Level:** section.
15. Click the **Event Logs** drop-down arrow.
16. Expand **Windows Logs**, and then select the **System** log.
17. Click in the **Includes/Excludes Event IDs** box.
18. Type **7036**, the Event ID associated with starting and stopping a service.
19. Click **OK**.
20. Click the **Advanced** button.

The Advanced Subscription Settings dialog box appears.
21. Click **Specific User**.
22. Click the **User and Password** button.

The Credentials for Subscription Source dialog box appears.
23. In **User name**, type **CONTOSO\Pat.Coleman_admin**.

We are using an account who is a member of the Domain Admins group for Lab purposes, but you should create a dedicated account to carry out this monitoring in a real world environment.
24. In **Password**, type **Pa\$\$w0rd**, and then press ENTER.
25. Click the **Minimize Latency** option, and then click **OK**.
26. Click **OK** to close the **Subscription Properties** dialog box.
27. If **Event Viewer** messages appear, click **Yes**.
28. Ensure that the **Status** column for the subscription indicates **Active**.

► **Task 3: Generate events**

1. Switch to HQDC02.
2. In the command prompt (running as an administrator), type **net stop dfsr**, and then press ENTER.
3. Type **net start dfsr**, and then press ENTER.

► **Task 4: View forwarded events**

1. Switch to HQDC01.
2. In the Server Manager console tree, under **Event Viewer\Windows Logs**, click **Forwarded Events**.

Forwarded events may take several minutes to appear. If the events do not appear right away, wait a few minutes, start and stop the Distributed File System Replication (DFSR) service on HQDC02 again, then wait a few more minutes.

Exercise 4: Attach Tasks to Event Logs and Events

► Task 1: Attach a task to an event log and to an event

1. Switch to HQDC01.
2. In the Server Manager console tree, under **Event Viewer\Windows Logs**, click **Forwarded Events**.
3. Right-click **Forwarded Events**, and then click **Attach a Task to this Log**, and then click **Next**.
4. On the **When a Specific Event is Logged** page, click **Next**.

You can invoke a task when an event matching specific criteria is logged, or when any event is added to a log. For each trigger, you can send an e-mail message, start a program, or display a message on the desktop. In a production environment, sending an e-mail message or starting a program that responds to the event are the most common tasks to invoke. In this lab, however, you will use the "display a message" task to demonstrate that, in fact, tasks are triggered.

5. On the **Action** page, click **Display a message**, and then click **Next**.
6. On the **Display a Message** page, in **Title**, type **Forwarded Event Received**.
7. In **Message**, type **A forwarded event was received**.
8. Click **Next**, and then click **Finish**.
9. Click **OK** to acknowledge the Event Viewer message.
10. In the details pane, right-click **one of the 7036** events, and then click **Attach Task to this Event**, and then click **Next**.
11. On the **When a Specific Event is Logged** page, click **Next**.
12. On the **Action** page, click **Display a message**, and then click **Next**.
13. On the **Display a Message** page, in **Title**, type **DC Service Event**.
14. In **Message**, type **A service was started or stopped**.
15. Click **Next**, and then click **Finish**.
16. Click **OK** to acknowledge the Event Viewer message.

17. In the console tree, expand **Configuration, Task Scheduler**, and then click **Event Viewer Tasks**.
18. Double-click the first event viewer task.
19. Explore the properties of the task that you created.

► **Task 2: Prepare to view event viewer task messages**

When you choose to display a message in a task, because messages are displayed on the desktop of the user whose account is used to create the event viewer task (Pat.Coleman_Admin), you will need to log on interactively as Pat.Coleman_Admin to fully experience this simulation.

1. Click the **Start** button, then click the arrow next to the **Lock** button, and then click **Log Off**.

The logon prompt appears.

2. Press ALT+DEL, which sends the secure key sequence (CTRL+ALT+DELETE) to the virtual machine guest.
3. Click **Switch User**.
4. Click **Other User**.
5. In **User name**, type **Pat.Coleman_Admin**.
6. In **Password**, type **Pa\$\$w0rd**, then press ENTER or click the log on arrow.

The Windows desktop appears.

► **Task 3: Confirm that event viewer tasks are functioning**

1. Switch to HQDC02.
2. In the command prompt (running as an administrator), type **net stop dfsr**, and then press ENTER.
3. Type **net start dfsr**, and then press ENTER.
4. Switch to HQDC01.
5. Wait for the event viewer task messages to appear.

Exercise 5: Monitor Active Directory Domain Services (AD DS) with Performance Monitor

► Task 1: Configure Performance Monitor to monitor AD DS

1. Switch to HQDC02.
2. In Server Manager's console tree, expand **Diagnostics, Reliability and Performance**, and **Monitoring Tools**, and then click **Performance Monitor**.
3. Click the **Add** button (the green plus sign) on the toolbar to add objects and counters.

The Add Counters dialog box appears.
4. In the **Available Counters** list, expand the **DirectoryServices** object.
5. Click the **DRA Inbound Bytes Total/sec** counter, and then click the **Add** button.
6. Repeat the previous step to add the following counters:
 - **DRA Outbound Bytes Total/sec**
 - **DS Threads In Use**
 - **DS Directory Reads/sec**
 - **DS Directory Writes/sec**
 - **DS Directory Searches/sec**
7. In the **Available Counters** list, expand the **Security System-Wide Statistics** object.
8. Select the **Kerberos Authentications** counter, and then click the **Add** button.
9. In the **Available Counters** list, expand the **DNS** object.
10. Select the **UDP Query Received/sec** counter, and then click the **Add** button.
11. Click **OK**.
12. Watch performance for a few moments.
13. In the counter list below the graph, select **UDP Query Received/sec**.

14. Click the **Highlight** button in the toolbar.

The selected counter is highlighted, making it easier to see that counter's performance.

15. Click the **Highlight** button in the toolbar again to turn off the highlight.
16. Spend a few moments exploring the functionality of Performance Monitor. Do not add or remove counters, however.

► **Task 2: Create a Data Collector Set from Performance Monitor counters**

1. In the console tree, right-click **Performance Monitor**, then point to **New**, and then click **Data Collector Set**.

The Create new Data Collector Set dialog box appears.

2. In **Name**, type **Custom ADDS Performance Counters**, and then click **Next**.
3. Make a note of the default root directory in which the data collector set will be saved, and then click **Next**.
4. Click **Finish**.

► **Task 3: Start a Data Collector Set**

1. In the console tree, expand **Data Collector Sets** and **User Defined**, and then click **User Defined**.

2. Right-click **Custom ADDS Performance Counters**, and then click **Start**.

The Custom ADDS Performance Counters node is automatically selected.

You can identify the individual data collectors in the Data Collector Set. In this case, only one data collector (the System Monitor Log performance counters) is contained in the data collector set.

You can also identify where the output from the data collector is being saved.

3. In the console tree, right-click the **Custom ADDS Performance Counters** data collector set, and then click **Stop**.

► **Task 4: View a Data Collector Set report**

- In the console tree, expand **Reports, User Defined, Custom ADDS Performance Counters**, and then click **System Monitor Log.blg**.

The graph of the log's performance counters is displayed.

Exercise 6: Work with Data Collector Sets

► Task 1: Examine a predefined Data Collector Set

1. Still on HQDC02 logged on as **contoso\Pat.Coleman** with password **Pa\$\$w0rd**.
2. In Server Manager's console tree, expand **Diagnostics, Reliability and Performance, Data Collector Sets, System**, and then click **Active Directory Diagnostics**.

Question: What data collectors are part of the Data Collector Set?

Answer: Event traces for NT Kernel and Active Directory, Configuration for AD Registry, and Performance Counters

3. Right-click **Active Directory Diagnostics**, and then click **Start**.
4. In the console tree, expand **Reports, System** and **Active Directory Diagnostics**, and then click the report, which will be named **yyyymmdd-xxxx** where **yyyy** is the current year, **mm** is the current date, **dd** is the current day, and **xxxx** is a four-digit incrementing serial number.

The Report Status indicates that data is being collected for 300 seconds (5 minutes).

5. Wait five minutes or at least one minute then right-click **Active Directory Diagnostics** under **Data Collector Sets\System**, and then click **Stop**.

The Report Status indicates that the report is being generated.

The report appears.

6. Spend a few moments examining the sections of the report.
7. Right-click the report, then point to **View**, and then click **Performance Monitor**.
8. Right-click the report, then point to **View**, and then click **Report**.
9. Right-click the report, then point to **View**, and then click **Folder**.
10. In the details pane, double-click **Performance Counter**.

The log is opened in a new instance of Reliability and Performance Monitor.

11. If the new instance of WRPM is minimized, open it by clicking its button on the taskbar.
12. Close the new instance of WRPM.
13. In the Server Manager console tree, expand **Monitoring Tools**, and then click **Performance Monitor**.
14. Click the **View Log Data** button in the toolbar, which is the second button from the leftmost edge of the toolbar.

The Performance Monitor Properties dialog box opens.

15. Click the **Log files** option.
16. Click the **Add** button.

The Select Log File dialog box opens, focused on C:\PerfLogs.

17. Double-click **ADDS**.
18. Double-click the folder with the same name as the report you generated.
19. Click **Performance Counter**, and then click **Open**.
20. Click **OK**.
21. Note that no counters are immediately visible.
22. Click the green plus sign—the **Add** button—on the toolbar.
23. In the **Available counters** list, expand the **DirectoryServices** object.
24. Select **DS Directory Reads/sec**, **DS Directory Searches/sec** and **DS DirectoryWrites/sec**, and then click **Add**.
25. Click **OK**.

► Task 2: Create a Data Collector Set

1. In the Server Manager console tree, expand **Diagnostics, Reliability and Performance**, and **Data Collector Sets**, and then click **User Defined**.
2. Right-click **User Defined**, point to **New**, and then click **Data Collector Set**.
3. On the **Create new Data Collector Set** page, in the **Name** box, type **Custom ADDS Diagnostics**.
4. Click the **Create from a template (Recommended)** option.
5. Click **Next**.

6. On the **Which template would you like to use?** page, select **Active Directory Diagnostics**, and then click **Next**.
7. On the **Where would you like the data to be saved?** page, in **Root directory**, create a folder **C:\ADDS Data Collector Sets**, and then click **Next**.
8. On the **Create the data collector set?** page, click the **Change** button.
A Reliability and Performance Monitor credentials dialog box appears.
9. In **User name**, type **CONTOSO\Pat.Coleman_Admin**.
10. In **Password**, type **Pa\$\$w0rd**, then click **OK**.

In a production environment, the account you use should be a unique domain account. It must be a member of the Performance Log Users group and must have the Log On As A Batch Job User logon right. By default, the Performance Log Users group has this right, so you can simply create a domain account and make it a member of the group.
11. Click **Finish**.

► **Task 3: Configure start conditions for a Data Collector Set**

1. In the console tree, right-click **Custom ADDS Diagnostics**, and then click **Properties**.
The Custom ADDS Diagnostics Properties dialog box appears.
2. Click the **Schedule** tab.
3. Click the **Add** button.
The Folder Action dialog box appears.
4. Confirm that **Beginning date** is today's date.
5. Select the **Expiration date** check box.
6. In the **Expiration date** drop-down list, select the date one week from today.
7. Configure the start time to the current time plus five minutes. Make a note of the start time you configure.

Note that the Expiration date property specifies when new instances of data collection will no longer be started. It does *not* stop existing sessions. You must configure the Stop Condition to specify when data collection is stopped.
8. Click **OK**.

9. In the **Custom ADDS Diagnostics Properties** dialog box, click **Apply**.
A Reliability and Performance Monitor credentials dialog box appears.
10. In **User name**, type **CONTOSO\Pat.Coleman_Admin**.
11. In **Password**, type **Pa\$\$w0rd**, then click **OK**.

► **Task 4: Configure stop conditions for a Data Collector Set**

1. Click the **Stop Condition** tab.
2. Select the **Overall Duration** check box.
3. Configure the duration to **2 Minutes**.
In a production environment, you would likely run a data collector for a longer period of time.
4. Select the check box, **Stop when all data collectors have finished**.
This option allows data collectors that are running when the Overall Duration is reached to finish recording the most recent values.
5. Click **OK**.

► **Task 5: Configure data management for a data collector**

1. Right-click **Custom ADDS Diagnostics**, and then click **Data Manager**.
2. On the **Data Manager** tab, click the **Resource policy** list, and then select **Delete oldest**.
3. Click the **Actions** tab.
4. Click **1 Day(s)**.
5. Click the **Edit** button.
The Folder Action dialog box appears.
6. In the **Action** section, select the check box **Copy cab file to this directory**.
7. In the **Copy cab file to this directory** box, type
\\hqdc01\ADDS_Diag_Reports.
8. Confirm that the **Create cab file** and **Delete data file** check boxes are selected.
9. Click **OK**.

10. Click **OK**.

A Reliability and Performance Monitor credentials dialog box appears.

11. In **User name**, type **Contoso\Pat.Coleman_Admin**.
12. In **Password**, type **Pa\$\$w0rd**, then click **OK**.

► **Task 6: View the results of data collection**

1. Wait until the time that you configured as the start time for the Data Collector Set passes.
2. Select the report under **Reports\User Defined\Custom ADDS Diagnostics**.

The Report Status indicates that data is being collected for 120 seconds (two minutes).

After data collection has completed, the Report Status indicates that the report is being generated.

3. Spend a few moments examining the report.
4. Right-click the report in the console tree, then point to **View**, and then click **Folder**.
5. Double-click **Performance Counter** in the details pane.

A new instance of Reliability and Performance Monitor opens, with Performance Monitor displaying the logged data in the Performance Counter log.

6. Spend a few moments examining the performance graph, and then close the window.



Note: Do not shut down the virtual machines once you are finished with this lab as the settings you have configured here will be used in subsequent labs in this module.

Lab Review Questions

Question: In what situations do you currently use, or can you envision using, event subscriptions as a monitoring tool?

Answer: Answers may vary depending on the situation.

Question: To what events or performance counters would you consider attaching e-mail notifications or actions? Do you use notifications or actions currently in your enterprise monitoring?

Answer: Answers may vary depending on the situation.

Lab B: Manage the Active Directory Database

► Log on to a virtual machine

Unless otherwise instructed, use the following steps to log on to a virtual machine.

1. Press ALT+DELETE.

This sends the secure key sequence (CTRL+ALT+DELETE) to the virtual machine. If you press CTRL+ALT+DELETE, you send the secure key sequence to the host operating system.

2. Click **Switch User**.
3. Click **Other User**.
4. In **User name**, type the user name.
5. In **Password**, type the password.
6. Press ENTER or click the log on arrow.

The Windows desktop appears.

► Run an application with administrative credentials

1. Right-click the application, and then click **Run as administrator**.

A User Account Control (UAC) dialog box appears.

2. The **UAC** dialog box will display one of three options. Do the steps based on the option you see:

If the UAC dialog box prompts you to continue or cancel:

- Click **Continue**.

If the UAC dialog box gives you the option to *Use another account*:

1. Click **Use Another Account**.
2. In **User Name**, type the user name.
3. In **Password**, type the password.
4. Press ENTER or click **OK**.

If the UAC dialog box does not give you the option to use another account, and prompts you for a user name and password:

1. In **User Name**, type the user name.
2. In **Password**, type the password.
3. Press ENTER or click **OK**.

Exercise 1: Perform Database Maintenance

► Task 1: Prepare for the lab

The virtual machines should already be started and available after completing Lab A. However, if they are not, you should complete the below steps.

1. Start 6425B-HQDC01-B.
2. Log on to HQDC01 as **Pat.Coleman** with the password **Pa\$\$w0rd**.
3. Start 6425B-HQDC02-B, but do not log on.

► Task 2: Prepare to compact the Active Directory database

1. Run Command Prompt with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
2. Type **md D:\NTDSCompact**.
3. Type **md D:\NTDSOriginal**.

► Task 3: Stop the AD DS service

1. Click **Start**, then point to **Administrative Tools**, then right-click **Services**, and then click **Run as administrator**.
2. Click **Use another account**.
3. In **User name**, type **Pat.Coleman_Admin**.
4. In **Password**, type **Pa\$\$w0rd**, and then press ENTER.
The Services console opens.
5. Click **Active Directory Domain Services**.
6. Click the **Stop** button on the toolbar.
The Stop Other Services dialog box appears, informing you of dependent services that will also be stopped.
7. Click **Yes**.

► **Task 4: Compact the Active Directory database**

1. Switch to the command prompt.
2. Type **ntdsutil**, and then press ENTER.
3. Type **activate instance ntds**, and then press ENTER.
4. Type **files**, and then press ENTER.
5. Type **compact to D:\NTDSCompact**, and then press ENTER.
NTDSUtil compacts the database to a new copy of NTDS.dit in the D:\NTDSCompact folder.
6. Wait for the operation to complete.

You are reminded that you need to copy the compacted file over the current version of ntds.dit, and to delete the log files. In the next task, you will perform more effective procedures that also back up Active Directory.

7. Type **quit**, and then press ENTER.
8. Type **quit**, and then press ENTER.

► **Task 5: Replace the Active Directory database with the compacted copy**

1. Type **cd %systemroot%\ntds**, and then press ENTER.
2. Type **move ntds.dit D:\NTDSOriginal**, and then press ENTER.
3. Type **move *.log D:\NTDSOriginal**, and then press ENTER.
4. Type **copy D:\NTDSCompact\ntds.dit**, and then press ENTER.

► **Task 6: Verify the integrity of the compacted database**

1. Type **ntdsutil**, and then press ENTER.
2. Type **activate instance NTDS**, and then press ENTER.
3. Type **files**, and then press ENTER.
4. Type **integrity**, and then press ENTER.
5. Type **quit**, and then press ENTER.
6. Type **semantic database analysis**, and then press ENTER.

7. Type **go fixup**, and then press ENTER.
8. Type **quit**, and then press ENTER.
9. Type **quit**, and then press ENTER.

► **Task 7: Start the AD DS service**

1. Switch to the **Services** console.
2. Click **Active Directory Domain Services**.
3. Click the **Start** button on the toolbar.
4. Close the **Services** console.

Exercise 2: Work with Snapshots and Recover a Deleted User

► Task 1: Create a snapshot of Active Directory

1. Switch to the command prompt.
2. Type **ntdsutil**, and then press ENTER.
3. Type **snapshot**, and then press ENTER.
4. Type **activate instance ntds**, and then press ENTER.
5. Type **create**, and then press ENTER.

The command returns a message indicating that the snapshot set was generated successfully. The GUID that is displayed is important for commands in later tasks. Make a note of the GUID or, alternately, copy it to the Clipboard.

6. Type **quit**, and then press ENTER.
7. Type **quit**, and then press ENTER.

► Task 2: Make a change to Active Directory

1. Run **Active Directory Users and Computers** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
2. In the console tree, expand the **contoso.com** domain, and the **User Accounts** OU, and then click the **Employees** OU.
3. Right-click the user account for **Adriana Giorgi**, and then click **Delete**.
A confirmation prompt appears.
4. Click **Yes**.

► Task 3: Mount an Active Directory snapshot and create a new instance

1. Switch to the command prompt.
2. Type **ntdsutil**, and then press ENTER.
3. Type **activate instance ntds**, and then press ENTER.
4. Type **snapshot**, and then press ENTER.

5. Type **list all**, and then press ENTER.

The command returns a list of all snapshots.

6. Type **mount guid**, where **guid** is the GUID returned by the create snapshot command, and then press ENTER.

i.e. `mount xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxxxx`

You should receive a message saying the ".....xxxxxxx was mounted"

7. Type **quit**, and then press ENTER.

8. Type **quit**, and then press ENTER.

9. Type **dsamain -dbpath**

c:\\$snap_datetime_volume c\$\windows\ntds\ntds.dit -ldapport 50000, and then press ENTER.

Note that datetime will be a value that is unique for you. There should only be one folder on your drive C with a name that begins with *\$snap*.

A message indicates that Active Directory Domain Services startup is complete. Leave Dsamain.exe running. Do not close the command prompt.

► Task 4: Explore a snapshot with Active Directory Users and Computers

1. Switch to **Active Directory Users and Computers**.
2. Right-click the root node, and then click **Change Domain Controller**.
The Change Directory Server dialog box appears.
3. Click **<Type a Directory Server name[:port] here>**.
4. Type **HQDC01:50000**, and then press ENTER.
5. Click **OK**.
6. In the console tree, expand the **contoso.com** domain, and the **User Accounts** OU, and then click the **Employees** OU.
7. Note that Adriana Giorgi's object is displayed because the snapshot was taken prior to deleting it.
8. Close Active Directory Users and Computers.

► **Task 5 (Optional): Use LDP to restore a deleted object**

Restoring a deleted user account is a task that is not directly related to snapshots. You use the Ldp.exe command to reanimate objects from the Deleted Objects container of Active Directory. A deleted object is stripped of most of its attributes, so a snapshot can be helpful to examine attributes of the object prior to its deletion.

1. Click the **Start** button. In the **Start Search** box, type **LDP.exe** and press CTRL+SHIFT+ENTER, which executes the command as an administrator.
The User Account Control dialog box appears.
2. Click **Use another account**.
3. In **User name**, type **Pat.Coleman_Admin**.
4. In **Password**, type **Pa\$\$w0rd**, and then press ENTER.
LDP opens.
5. Click the **Connection** menu, then click **Connect**, and then click **OK**.
6. Click the **Connection** menu, then click **Bind**, and then click **OK**.
7. Click the **Options** menu, and then click **Controls**.
8. In the **Load Predefined** list, click **Return Deleted Objects**, and then click **OK**.
9. Click the **View** menu, then click **Tree**, and then click **OK**.
10. In the console tree, expand **DC=contoso,DC=com**, and then double-click **CN=Deleted Objects,DC=contoso,DC=com**.
11. Right-click **CN=Adriana Giorgi**, and then click **Modify**.
12. In the **Attribute** box, type **isDeleted**.
13. In the **Operation** section, click **Delete**.
14. Click the **Enter** button.
15. In the **Attribute** box, type **distinguishedName**.
16. In the **Values** box, type **CN=Adriana Giorgi,OU=Employees,OU=User Accounts,DC=contoso,DC=com**.
17. In the **Operation** section, click **Replace**.
18. Click the ENTER button.
19. Select the **Extended** check box.

20. Click the **Run** button.
21. Click the **Close** button.
22. Close LDP.
23. Run **Active Directory Users and Computers** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
24. In the console tree, expand the **contoso.com** domain, and the **User Accounts** OU, and then click the **Employees** OU.
25. Note that Adriana Giorgi's account is restored; however, all attributes are missing, including the description and the password. Because the password is missing, the account has been disabled.
26. Switch to the instance of Active Directory Users and Computers that is displaying the snapshot data.
27. Note that you can use the attributes contained in the snapshot to manually re-populate attributes in Active Directory.
28. Close both instances of Active Directory Users and Computers.

► **Task 6: Unmount an Active Directory snapshot**

1. Switch to the command prompt.
2. Press CTRL+C to stop DSAMain.exe.
3. Type **ntdsutil**, and then press ENTER.
4. Type **activate instance ntds**, and then press ENTER.
5. Type **snapshot**, and then press ENTER.
6. Type **unmount guid**, where **guid** is the GUID of the snapshot, and then press ENTER.
7. Type **quit**, and then press ENTER.
8. Type **quit**, and then press ENTER.



Note: Do not shut down the virtual machines once you are finished with this lab as the settings you have configured here will be used in subsequent labs in this module.

Lab Review Questions

Question: In what other situations might it be useful to mount a snapshot of Active Directory?

Answer: If you discover a problem with Active Directory that will require restoring a backup, you might want to look at snapshots to determine just how far back you need to go to restore. Once you've found the snapshot in which the correct data resides, you can then restore the backup taken on the same date.

Question: What are the disadvantages of restoring a deleted object with a tool such as LDP?

Answer: You must repopulate all attributes.

Lab C: Backup and Restore Active Directory

► Log on to a virtual machine

Unless otherwise instructed, use the following steps to log on to a virtual machine.

1. Press ALT+DELETE.

This sends the secure key sequence (CTRL+ALT+DELETE) to the virtual machine. If you press CTRL+ALT+DELETE, you send the secure key sequence to the host operating system.

2. Click **Switch User**.
3. Click **Other User**.
4. In **User name**, type the user name.
5. In **Password**, type the password.
6. Press ENTER or click the log on arrow.

The Windows desktop appears.

► Run an application with administrative credentials

1. Right-click the application, and then click **Run as administrator**.

A User Account Control (UAC) dialog box appears.

2. The **UAC** dialog box will display one of three options. Do the steps based on the option you see:

If the UAC dialog box prompts you to continue or cancel:

- Click **Continue**.

If the UAC dialog box gives you the option to *Use another account*:

1. Click **Use Another Account**.
2. In **User Name**, type the user name.
3. In **Password**, type the password.
4. Press ENTER or click **OK**.

If the UAC dialog box does not give you the option to use another account, and prompts you for a user name and password:

1. In **User Name**, type the user name.
2. In **Password**, type the password.
3. Press ENTER or click **OK**.

Exercise 1: Back up Active Directory

► Task 1: Prepare for the lab

The virtual machines should already be started and available after completing Labs A and B. However, if they are not, you should complete the below steps.

1. Start 6425B-HQDC01-B.
2. Log on to HQDC01 as **Pat.Coleman** with the password **Pa\$\$w0rd**.
3. Start 6425B-HQDC02-B.
4. Log on to HQDC02 as **Pat.Coleman** with the password **Pa\$\$w0rd**.

► Task 2: Install the Windows Server Backup feature

1. Switch to HQDC01.
2. Click the **Server Manager** icon next to the **Start** button.
The User Account Control dialog box appears.
3. In **User name**, type **Pat.Coleman_Admin**.
4. In **Password**, type **Pa\$\$w0rd**, and then press ENTER.
5. Server Manager opens.
6. In the console tree, click **Features**.
7. In the details pane, click the **Add Features** link.
8. On the **Select Features** page, expand **Windows Server Backup Features**, and then select the **Windows Server Backup** and **Command-line Tools** check boxes.

When you select Command-line Tools, the Add Features Wizard prompts you to install Windows PowerShell™, a required feature.

9. Click **Add Required Features**.
10. Click **Next**.
11. Click **Install**.
12. When the installation finishes, click **Close**.

► **Task 3: Create a scheduled backup**

1. Go to **Start>Administrative Tools>** and run **Windows Server Backup** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
2. In the Actions pane, click the **Backup Schedule** link.
The Backup Schedule Wizard appears.
3. On the **Getting Started** page, click **Next**.
4. On the **Select backup configuration** page, click **Custom**, and then click **Next**.
5. On the **Select backup items** page, clear the **6425B (D:) drive** check box, and then click **Next**.
6. On the **Specify backup time** page, click **Once a day**.
7. In the **Select time of day** list, select **12:00 am**.
8. Click **Next**.
9. On the **Select destination disk** page, click **Show All Available Disks**.
The Show All Available Disks dialog box appears.
10. Select the **Disk 1** check box, and then click **OK**.
11. On the **Select destination disk** page, select the **Disk 1** check box, and then click **Next**.
The Windows Server Backup dialog box appears, informing you that all data on the disk will be deleted.
12. Click **Yes** to continue.
13. On the **Label destination disk** page, click **Next**.
14. On the **Confirmation** page, click **Cancel** to avoid formatting D drive D.

► **Task 4: Perform an interactive backup**

1. In the Windows Server Backup console's **Actions** pane, click the **Backup Once** link.
The Backup Once Wizard appears.
2. On the **Backup options** page, ensure that **Different options** is selected, and then click **Next**.

3. On the **Select backup configuration** page, click **Custom**, and then click **Next**.
4. On the **Select backup items** page, ensure that the **Enable system recovery** check box is selected, and then click **Next**.
5. On the **Specify destination type** page, click **Next**.
6. On the **Select backup destination** page, click **Next**.
7. On the **Specify advanced option** page, click **VSS full backup**, and then click **Next**.
8. On the **Confirmation** page, click **Backup**.

The backup will take about 10-15 minutes to complete. When the backup is complete, close Windows Server Backup.

Exercise 2: Restore Active Directory and a Deleted OU

► Task 1: Delete the Employees OU

1. Still on HQDC01, run **Active Directory Users and Computers** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
2. In the console tree, expand **contoso.com**, and then click the **User Accounts** OU.
3. In the details pane, right-click **Contractors**, and then click **Delete**.
A confirmation message appears.
4. Click **Yes**.
A warning message appears.
5. Click **Yes**.
6. Wait for the deletion to complete.
7. Switch to HQDC02.
8. Run **Active Directory Users and Computers** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
9. In the console tree, expand **contoso.com**, and then click the **User Accounts** OU.
10. Verify that the **Contractors** OU is deleted.

► Task 2: Restart in Directory Services Restore Mode (DSRM)

1. Switch to HQDC01.
2. Run **Command Prompt** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
3. Type **bcdedit /set safeboot dsrepair**, and then press ENTER.
4. Type **shutdown -t 0 -r** and then press ENTER.

► **Task 3: Restore System State data**

1. Log on to HQDC01 as **Administrator** with the password **Pa\$\$w0rd**.
2. Click **Start**, then right-click **Command Prompt**, and then click **Run as administrator**.
The command prompt opens.
3. Type **wbadmin get versions -backuptarget:D: -machine:HQDC01**, and then press ENTER.
4. Note the version information that is returned.
5. Type **wbadmin start systemstaterecovery -version:version -backuptarget:D: -machine:HQDC01**, where version is the number that you recorded in the previous step, and then press ENTER.
i.e. **wbadmin start systemstaterecovery -version:10/14/2009-01:11 -backuptarget:D: -machine:HQDC01**
6. Type **Y**, and then press ENTER.
The restore will take about 30-35 minutes. Depending on the host machine it could take up to an hour.

► **Task 4: Mark the restored information as authoritative and restart the server**

1. At the command prompt, type **ntdsutil**, and then press ENTER.
2. Type **activate instance ntds**, and then press ENTER.
3. Type **authoritative restore**, and then press ENTER.
4. Type **restore subtree "ou=Contractors,ou=User Accounts,dc=contoso,dc=com"**, and then press ENTER.
5. Click **Yes** in the confirmation dialogue message box that appears.
6. Type **quit**, and then press ENTER.
7. Type **quit**, and then press ENTER.
8. Type **bcdedit /deletevalue safeboot**, and then press ENTER.
9. Type **shutdown -t 0 -r**, and then press ENTER.

► **Task 5: Verify that the deleted data has been restored**

1. Wait for HQDC01 to restart.
2. Log on to HQDC01 as **Pat.Coleman** with the password **Pa\$\$w0rd**.
3. Run **Active Directory Users and Computers** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
4. In the console tree, expand **contoso.com**, and then click the **User Accounts** OU.
5. Verify that the **Contractors** OU is restored.
6. Switch to HQDC02.
7. In the **Active Directory Users and Computers** console tree, click the **User Accounts** OU.
8. Press F5 (Refresh).
9. Verify that the **Contractors** OU is restored.

Lab Review Questions

Question: What type of domain controller and directory service backup plan do you have in place? What do you expect to put in place after having completed this lesson and this Lab?

Answer: Answers will vary.

Question: When you restore a deleted user (or an OU with user objects) using authoritative restore, will the objects be exactly the same as before? What attributes might not be the same?

Answer: Answers may vary somewhat, but the question is designed to frame a discussion of group membership. A user's group membership is not an attribute of the user object but rather of the group object. When you authoritatively restore a user, you are not restoring users' membership in groups. The user was removed from the member attribute of groups when it was deleted. So the restored user will not be a member of any groups other than its primary group. In order to restore group memberships, you would have to consider authoritatively restoring groups as well. This may or may not always be desirable, because when you authoritatively restore the groups you return their membership to the day on which the backup was made.

Module 14: Manage Multiple Domains and Forests

Lab A: Raise Domain and Forest Functional Levels

► Log on to a virtual machine

Unless otherwise instructed, use the following steps to log on to a virtual machine.

1. Press ALT+DELETE.

This sends the secure key sequence (CTRL+ALT+DELETE) to the virtual machine. If you press CTRL+ALT+DELETE, you send the secure key sequence to the host operating system.

2. Click **Switch User**.
3. Click **Other User**.
4. In **User name**, type the user name.
5. In **Password**, type the password.
6. Press ENTER or click the log on arrow.

The Windows desktop appears.

► Run an application with administrative credentials

1. Right-click the application, and then click **Run as administrator**.

A User Account Control (UAC) dialog box appears.

2. The **UAC** dialog box will display one of three options. Do the steps based on the option you see:

If the UAC dialog box prompts you to continue or cancel:

- Click **Continue**.

If the UAC dialog box gives you the option to *Use another account*:

1. Click **Use Another Account**.
2. In **User Name**, type the user name.
3. In **Password**, type the password.
4. Press ENTER or click **OK**.

If the UAC dialog box does not give you the option to use another account, and prompts you for a user name and password:

1. In **User Name**, type the user name.
2. In **Password**, type the password.
3. Press ENTER or click **OK**.

Exercise 1: Raise the Domain Functional Level to Windows Server® 2003

► Task 1: Prepare for the lab

1. Start 6425B-TSTDC01-A.
2. Log on to TSTDC01 as **Sara.Davis** with the password **Pa\$\$w0rd**.

► Task 2: Confirm that the current domain functional level is Windows 2000 Native

1. Run **Active Directory Domains and Trusts** with administrative credentials. Use the account **Sara.Davis_Admin** with the password **Pa\$\$w0rd**.
2. In the console tree, right-click the **tailspintoys.com** domain, and then click **Raise Domain Functional Level**.
The Raise Domain Functional Level dialog box appears.
3. Confirm that the **Current domain functional level** is **Windows 2000 Native**.
4. Click **Cancel**. Do not make any change to the domain functional level.

► Task 3: Experience functionality not supported by the Windows 2000 Native domain functional level

1. Run the Command Prompt with administrative credentials. Use the account **Sara.Davis_Admin** with the password **Pa\$\$w0rd**.
2. Type **redircmp.exe "ou=Client Computers,dc=tailspintoys,dc=com"** and press ENTER.

A message appears indicating that redirection was not successful.

This is because the domain functional level is not at least Windows Server 2003.

3. Type **redirusr.exe "ou=User Accounts,dc=tailspintoys,dc=com"** and press ENTER.

A message appears indicating that redirection was not successful.

This is because the domain functional level is not at least Windows Server 2003.

► **Task 4: Raise the domain functional level to Windows Server 2003**

1. Switch to Active Directory Domains and Trusts.
2. In the console tree, right-click the **tailspintoys.com** domain, and then click **Raise Domain Functional Level**.
3. In the **Select an available domain functional level** list, select **Windows Server 2003**.
4. Click **Raise**.
A message appears to remind you that the action cannot be reversed.
5. Click **OK** to confirm your change.
A message appears informing you that the functional level was raised successfully.
6. Click **OK**.

► **Task 5: Verify functionality supported by the Windows Server 2003 domain functional level**

1. Switch to the Command Prompt.
2. Type **redircmp.exe "ou=Client Computers,dc=tailspintoys,dc=com"** and press ENTER.
A message appears indicating that redirection was successful.
3. Type **redirusr.exe "ou=User Accounts,dc=tailspintoys,dc=com"** and press ENTER.
A message appears indicating that redirection was successful.

Exercise 2: Raise the Forest Functional Level to Windows Server 2003

► Task 1: Confirm that the current forest functional level is Windows 2000 Native

1. Switch to Active Directory Domains and Trusts.
2. In the console tree, right-click the root node, **Active Directory Domains and Trusts**, and then click **Raise Forest Functional Level**.
The Raise Forest Functional Level dialog box appears.
3. Confirm that the **Current forest functional level** is **Windows 2000 Native**.
4. Click **Cancel**. Do not make any change to the forest functional level.

► Task 2: Experience functionality not supported by the Windows 2000 Native forest functional level

1. Run **Active Directory Users and Computers** with administrative credentials. Use the account **Sara.Davis_Admin** with the password **Pa\$\$w0rd**.
2. In the console tree, expand the **Tailspintoys.com** domain, and then click the **Domain Controllers** OU.
3. Right-click the **Domain Controllers** OU, and then click **Pre-create Read-only Domain Controller account**.

The Active Directory Domain Services Installation Wizard appears.

4. Click **Next**.
5. On the **Operating System Compatibility** page, click **Next**.
6. On the **Network Credentials** page, click **Next**.

A message appears informing you that the forest functional level must be Windows Server 2003 or higher.

7. Click **OK**.
8. Click **Cancel** to close the Active Directory Domain Services Installation Wizard.

A confirmation message appears, asking you if you want to quit the wizard.

9. Click **Yes**.

► **Task 3: Raise the forest functional level to Windows Server 2003**

1. Switch to Active Directory Domains and Trusts.
2. In the console tree, right-click the root node, **Active Directory Domains and Trusts**, and then click **Raise Forest Functional Level**.
3. In the **Select an available forest functional level** list, select **Windows Server 2003**.
4. Click **Raise**.
A message appears to remind you that the action cannot be reversed.
5. Click **OK** to confirm your change.
A message appears informing you that the functional level was raised successfully.
6. Click **OK**.

► **Task 4: Verify functionality supported by the Windows Server 2003 forest functional level**

1. Switch to Active Directory Users and Computers.
2. Right-click the **Domain Controllers** OU, and then click **Pre-create Read-only Domain Controller account**.
The Active Directory Domain Services Installation Wizard appears.
3. Click **Next**.
4. On the **Operating System Compatibility** page, click **Next**.
5. On the **Network Credentials** page, click **Next**.
6. On the **Specify the Computer Name** page, type **TSTDC03**, and then click **Next**.
7. On the **Select a Site** page, click **Next**.
8. On the **Additional Domain Controller Options** page, click **Next**.

9. On the **Delegation of RODC Installation and Administration** page, click **Next**.
10. On the **Summary** page, click **Next**.
11. Click **Finish**.

A staged RODC object named **TSTDC03** is created in the **Domain Controllers** OU.

Exercise 3: Raise the Domain Functional Level to Windows Server 2008

► **Task 1: Confirm that the current domain functional level is lower than Windows Server 2008.**

1. Switch to Active Directory Domains and Trusts.
2. In the console tree, right-click the **tailspintoys.com** domain, and then click **Raise Domain Functional Level**.
The Raise Domain Functional Level dialog box appears.
3. Confirm that the **Current domain functional level** is **Windows Server 2003**.
4. Click **Cancel**. Do not make any change to the domain functional level.

► **Task 2: Confirm that DFS-R replication is not available at domain functional levels lower than Windows Server 2008**

1. Run the Command Prompt with administrative credentials. Use the account **Sara.Davis_Admin** with the password **Pa\$\$w0rd**.
2. Type **dfsrmig /getglobalstate** and then press ENTER.
A message appears informing you that dfsrmig is supported only on domains at the Windows Server 2008 functional level.

► **Task 3: Raise the domain functional level**

1. Switch to Active Directory Domains and Trusts.
2. In the console tree, right-click the **tailspintoys.com** domain, and then click **Raise Domain Functional Level**.
3. Confirm that the **Select an available domain functional level** list indicates **Windows Server 2008**.
4. Click **Raise**.

A message appears to remind you that the action cannot be reversed.

5. Click **OK** to confirm your change.

A message appears informing you that the functional level was raised successfully.

6. Click **OK**.
7. Close Active Directory Domains and Trusts.

► **Task 4: Confirm that DFS-R replication is available at the Windows Server 2008 domain functional level**

1. Switch to the command prompt.
2. Type **dfsrmig /getglobalstate** and then press ENTER.

A message appears informing you that DFS-R migration has not yet been initialized. This indicates that the feature is now available, but has not yet been initialized.



Note: Do not shut down the virtual machines once you are finished with this lab as the settings you have configured here will be used in subsequent labs.

Lab Review Questions

Question: Can you raise the domain functional level to Windows Server 2008 when your Microsoft Exchange server is still running Windows Server 2003?

Answer: Yes. As long as the Exchange server is not a domain controller. All that matters when determining the domain functional level is the operating system of the domain controller.

Question: Can you raise the domain functional level of a domain to Windows Server 2008 when other domains contain domain controllers running Windows Server 2003?

Answer: Yes. Domain functional levels within a forest can be different.

Lab B: Administer a Trust Relationship

► Log on to a virtual machine

Unless otherwise instructed, use the following steps to log on to a virtual machine.

1. Press ALT+DELETE.

This sends the secure key sequence (CTRL+ALT+DELETE) to the virtual machine. If you press CTRL+ALT+DELETE, you send the secure key sequence to the host operating system.

2. Click **Switch User**.
3. Click **Other User**.
4. In **User name**, type the user name.
5. In **Password**, type the password.
6. Press ENTER or click the log on arrow.

The Windows desktop appears.

► Run an application with administrative credentials

1. Right-click the application, and then click **Run as administrator**.

A User Account Control (UAC) dialog box appears.

2. The **UAC** dialog box will display one of three options. Do the steps based on the option you see:

If the UAC dialog box prompts you to continue or cancel:

- Click **Continue**.

If the UAC dialog box gives you the option to *Use another account*:

1. Click **Use Another Account**.
2. In **User Name**, type the user name.
3. In **Password**, type the password.
4. Press ENTER or click **OK**.

If the UAC dialog box does not give you the option to use another account, and prompts you for a user name and password:

1. In **User Name**, type the user name.
2. In **Password**, type the password.
3. Press ENTER or click **OK**.

Exercise 1: Configure DNS

► Task 1: Prepare for the lab

1. Start 6425B-HQDC01-A.
2. Log on to HQDC01 as **Pat.Coleman** with the password **Pa\$\$w0rd**.
3. Start 6425B-TSTDC01-A.
4. Log on to TSTDC01 as **Sara.Davis** with the password **Pa\$\$w0rd**.

► Task 2: Configure DNS in contoso.com

1. Switch to HQDC01.
2. Run DNS Management with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
3. In the console tree, expand **HQDC01**, and then click **Forward Lookup Zones**.
4. Right-click **Forward Lookup Zones**, and then click **New Zone**.
The Welcome to the New Zone Wizard page appears.
5. Click **Next**.
The Zone Type page appears.
6. Click **Stub Zone**, and then click **Next**.
The Active Directory Zone Replication Scope page appears.
7. Click **Next**.
The Zone Name page appears.
8. Type **tailspintoys.com**, and then click **Next**.
The Master DNS Servers page appears.
9. Type **10.0.0.31** and press **Tab**.
10. Select the **Use the above servers to create a local list of master servers** check box.
11. Click **Next**, and then click **Finish**.

► **Task 3: Configure DNS in tailspintoys.com**

1. Switch to TSTDC01.
2. Run **DNS Management** with administrative credentials. Use the account **Sara.Davis_Admin** with the password **Pa\$\$w0rd**.
3. In the console tree, expand **TSTDC01**, and then click **Conditional Forwarders**.
4. Right-click the **Conditional Forwarders** folder, and then click **New Conditional Forwarder**.
5. In the **DNS Domain** box, type **contoso.com**.
6. Click **Click here to add an IP** and type **10.0.0.11**.
7. Select the **Store this conditional forwarder in Active Directory, and replicate it as follows** check box.
8. Click **OK**.

Exercise 2: Create a Trust Relationship

► Task 1: Identify the trusted and trusting domains

Users in tailspintoys.com require access to a shared folder in contoso.com. Answer the following questions:

Questions:

- Which domain is the trusting domain, and which is the trusted domain?
- Which domain has an outgoing trust, and which has an incoming trust?

Answer:

- The contoso.com domain is the trusting domain with an outgoing trust to the tailspintoys.com domain, which is the trusted domain with an incoming trust.

► Task 2: Initiate the trust in the trusted domain

1. Switch to HQDC01.
2. Run **Active Directory Domains and Trusts** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
3. In the console tree, right-click the **contoso.com** domain, and then click **Properties**.
4. Click the **Trusts** tab.
5. Click **New Trust**.
The Welcome to the New Trust Wizard page appears.
6. Click **Next**.
The Trust Name page appears.
7. In the **Name** box, type **tailspintoys.com**, and then click **Next**.
The Trust Type page appears.
8. Click **External Trust**. Click **Next**.
The Direction of Trust page appears.
9. Click **One-way: Outgoing**. Click **Next**.
The Sides of Trust page appears.

10. Click **This Domain Only**. Click **Next**.

The Outgoing Trust Authentication Level page appears.

11. Click **Domain-wide authentication**. Click **Next**.

The Trust Password page appears.

12. Type **Pa\$\$w0rd** in both the **Trust password** and **Confirm trust password** boxes.

In a production environment, you should use a complex password that is unique. It should not be the password of a user account.

13. Click **Next**.

The Trust Selections Complete page appears.

14. Review the settings. Click **Next**.

The Trust Creation Complete page appears.

15. Review the status of changes. Click **Next**.

The Confirm Outgoing Trust page appears. You should not confirm the trust until both sides of the trust have been created.

16. Click **Next**.

The Completing the New Trust Wizard page appears.

17. Click **Finish**.

A dialog box appears to remind you that SID filtering is enabled by default.

18. Click **OK**.

19. Click **OK** to close the **contoso.com Properties** dialog box.

► Task 3: Complete the trust in the trusting domain

1. Switch to TSTDC01.
2. Run **Active Directory Domains and Trusts** with administrative credentials. Use the account **Sara.Davis_Admin** with the password **Pa\$\$w0rd**.
3. In the console tree, right-click the **tailspintoys.com** domain, and then click **Properties**.
4. Click the **Trusts** tab.

5. Click **New Trusts**.
The Welcome to the New Trust Wizard page appears.
6. Click **Next**.
The Trust Name page appears.
7. In the **Name** box, type **contoso.com**. Click **Next**.
The Trust Type page appears.
8. Click **External Trust**. Click **Next**.
The Direction of Trust page appears.
9. Click **One-way: Incoming**. Click **Next**.
The Sides of Trust page appears.
10. Click **This Domain Only**. Click **Next**.
The Trust Password page appears.
11. Type **Pa\$\$w0rd** in the **Trust Password** and **Confirm Trust Password** boxes.
Click **Next**.
The Trust Selections Complete page appears.
12. Click **Next**.
The Trust Creation Complete page appears.
13. Review the status of changes. Click **Next**.
The Confirm Incoming Trust page appears.
You will validate the trust in the next exercise.
14. Click **Next**.
The Completing The New Trust Wizard page appears.
15. Click **Finish**.
16. Click **OK** to close the **tailspintoys.com Properties** dialog box.

Exercise 3: Validate a Trust Relationship

► Task 1: Validate a trust relationship

1. Switch to HQDC01.
2. In the console tree of **Active Directory Domains and Trusts**, right-click the **contoso.com** domain, and then click **Properties**.
3. Click the **Trusts** tab.
4. Click **tailspintoys.com**, and then click **Properties**.
5. Click **Validate**.

A message appears indicating that the trust has been validated and that it is in place and active.

6. Click **OK**.
7. Click **OK** twice to close the **Properties** dialog boxes.

Exercise 4: Assign Permissions to Trusted Identities

► Task 1: Assign permissions to trusted groups

1. Switch to TSTDC01.
2. Run **Active Directory Users and Computers** with administrative credentials. Use the account **Sara.Davis_Admin** with the password **Pa\$\$w0rd**.
3. In the console tree, expand the **tailspintoys.com** domain, and then click the **User Accounts** OU.
4. Right-click **User Accounts**, then point to **New**, and then click **User**.
5. In **First Name**, type **Pat**.
6. In **Last Name**, type **Coleman**.
7. In **User logon name**, type **Pat.Coleman**.
8. Click **Next**.
9. In **Password** and **Confirm password**, type **Pa\$\$w0rd**.
10. Clear the **User must change password at next logon** check box.
11. Click **Next**.
12. Click **Finish**.
13. In the console tree, right-click the **tailspintoys.com** domain, then point to **New**, and then click **Organizational Unit**.
The New Object - Organizational Unit dialog box appears.
14. In the **Name** box, type **Groups**.
15. Click **OK**.
16. In the console tree, right-click the **Groups** OU, then point to **New**, and then click **Group**.
The New Object - Group dialog box appears.
17. In **Group name**, type **Product Team**.
18. Click **OK**.
19. Switch to HQDC01.
20. Run **Active Directory Users and Computers** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.

21. In the console tree, expand the **contoso.com** domain, and the **Groups** OU, and then click the **Role** OU.
22. Right-click the **Role** OU, then point to **New**, and then click **Group**.
The New Object - Group dialog box appears.
23. In **Group name**, type **Product Developers**.
24. Click **OK**.
25. In the console tree, click the **Access** OU.
26. Right-click the **Access** OU, then point to **New**, and then click **Group**.
The New Object - Group dialog box appears.
27. In **Group name**, type **ACL_Product Information_Modify**.
28. In the **Group scope** section, click **Domain local**.
29. Click **OK**.
30. Open drive C.
31. Create a new folder named **Product Information** on drive C.
32. Right-click the **Product Information** folder, and then click **Properties**.
The Product Information Properties dialog box appears.
33. Click the **Security** tab.
34. Click **Edit**.
35. Click **Add**.
36. Type **ACL_Product Information_Modify**, and then press ENTER.
37. Select the check box below **Allow** and next to **Modify**.
38. Click **OK** twice to close the dialog boxes.
39. Switch to Active Directory Users and Computers.
40. In the details pane, double-click **ACL_Product Information_Modify**.
41. Click the **Members** tab.
42. Click **Add**.
43. Type **Product Developers**, and then press ENTER.
44. Click **Add**.

45. Type **TAILSPINTOYS\Product Team**, and then press ENTER.

A Windows Security dialog box appears.

Your account that is an administrator of contoso.com (Pat.Coleman_Admin) does not have permissions to read the directory of the tailspintoys.com domain.

You must have an account in tailspintoys.com to read its directory. If the trust were a two-way trust, this message would not have appeared.

Your standard user account in the tailspintoys.com domain will be used to provide you Read Access to the directory service.

46. In the **User Name** box, type **TAILSPINTOYS\Pat.Coleman**.

47. In the **Password** box, type **Pa\$\$w0rd**, and then click **OK**.

Note that the two global groups from the two domains are now members of the domain local group in the contoso.com domain that has access to the Product Information folder.

48. Click **OK** to close the group properties dialog box.

Exercise 5: Implement Selective Authentication

► Task 1: Implement selective authentication

1. On HQDC01, switch to **Active Directory Domains and Trusts**.
2. Right-click the **contoso.com** domain, and then click **Properties**.
3. Click the **Trusts** tab.
4. Click **tailspintoys.com**, and then click **Properties**.
5. Click the **Authentication** tab.
6. Click the **Selective Authentication** option, and then click **OK** twice.

With selective authentication enabled, users from a trusted domain cannot authenticate against computers in the trusting domain, even if they've been given permissions to a folder. Trusted users must also be given the Allowed To Authenticate permission on the computer itself.

7. Switch to **Active Directory Users and Computers**.
8. Click the **View** menu and ensure that **Advanced Features** is selected.
9. In the console tree, click the **Domain Controllers** OU.
10. In the details pane, right-click **HQDC01**, and then click **Properties**.
11. Click the **Security** tab.
12. Click **Add**.
13. Type **TAILSPINTOYS\Product Team** and click **OK**.

A Windows Security dialog box appears.

Your account that is an administrator of contoso.com (Pat.Coleman_Admin) does not have permissions to read the directory of the tailspintoys.com domain.

You must have an account in tailspintoys.com to read its directory. If the trust were a two-way trust, this message would not have appeared.

Your standard user account in the tailspintoys.com domain will be used to provide you Read Access to the directory service.

14. In the **User Name** box, type **TAILSPINTOYS\Pat.Coleman**.
15. In the **Password** box, type **Pa\$\$w0rd**, and then click **OK**.

16. Select the check box below **Allow** next to **Allowed to authenticate**.

Now, the Product Team from Tailspintoys.com can authenticate to HQDC01 and has been given permission to the Product Information folder through its membership in the ACL_Product Information_Modify group.

17. Click **OK**.



Note: After completing this exercise, turn off all virtual machines and discard undo disks.

Lab Review Questions

Question: You have given the Research and Development group from Tailspin Toys Modify permission to the Product Information folder on HQDC01. However, of the ten users in the group, only one user (who happens to also be a member of the Product Team group) has access. The others cannot access the folder. What must be done?

Answer: Because selective authentication is enabled, the users in the Research and Development group must be given Allowed to Authenticate permission to HQDC01. The Product Team group already had that permission, which is why one user was able to authenticate and then to access the folder.

Question: A user from Contoso attempts to access a shared folder in the Tailspin Toys domain, and receives an Access Denied error. What must be done to provide access to the user?

Answer: A trust relationship must be established in which Tailspin Toys trusts Contoso, then the user (or a group to which the user belongs) must be given permission to the shared folder in the Tailspin Toys domain.