

OFFICIAL MICROSOFT LEARNING PRODUCT

# 20742A

## Identity with Windows Server 2016

Information in this document, including URLs and other Internet website references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, domain names, email addresses, logos, people, places, and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, email 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.

©2016 Microsoft Corporation. All rights reserved.

Microsoft and the trademarks listed at <http://www.microsoft.com/about/legal/en/us/IntellectualProperty/Trademarks/EN-US.aspx> are trademarks of the Microsoft group of companies. All other trademarks are property of their respective owners.

Product Number: 20742A

Part Number: X21-15013

Released: 08/2016

## **MICROSOFT LICENSE TERMS MICROSOFT INSTRUCTOR-LED COURSEWARE**

---

These license terms are an agreement between Microsoft Corporation (or based on where you live, one of its affiliates) and you. Please read them. They apply to your use of the content accompanying this agreement which includes the media on which you received it, if any. These license terms also apply to Trainer Content and any updates and supplements for the Licensed Content unless other terms accompany those items. If so, those terms apply.

**BY ACCESSING, DOWNLOADING OR USING THE LICENSED CONTENT, YOU ACCEPT THESE TERMS.  
IF YOU DO NOT ACCEPT THEM, DO NOT ACCESS, DOWNLOAD OR USE THE LICENSED CONTENT.**

---

**If you comply with these license terms, you have the rights below for each license you acquire.**

### **1. DEFINITIONS.**

- a. "Authorized Learning Center" means a Microsoft IT Academy Program Member, Microsoft Learning Competency Member, or such other entity as Microsoft may designate from time to time.
- b. "Authorized Training Session" means the instructor-led training class using Microsoft Instructor-Led Courseware conducted by a Trainer at or through an Authorized Learning Center.
- c. "Classroom Device" means one (1) dedicated, secure computer that an Authorized Learning Center owns or controls that is located at an Authorized Learning Center's training facilities that meets or exceeds the hardware level specified for the particular Microsoft Instructor-Led Courseware.
- d. "End User" means an individual who is (i) duly enrolled in and attending an Authorized Training Session or Private Training Session, (ii) an employee of a MPN Member, or (iii) a Microsoft full-time employee.
- e. "Licensed Content" means the content accompanying this agreement which may include the Microsoft Instructor-Led Courseware or Trainer Content.
- f. "Microsoft Certified Trainer" or "MCT" means an individual who is (i) engaged to teach a training session to End Users on behalf of an Authorized Learning Center or MPN Member, and (ii) currently certified as a Microsoft Certified Trainer under the Microsoft Certification Program.
- g. "Microsoft Instructor-Led Courseware" means the Microsoft-branded instructor-led training course that educates IT professionals and developers on Microsoft technologies. A Microsoft Instructor-Led Courseware title may be branded as MOC, Microsoft Dynamics or Microsoft Business Group courseware.
- h. "Microsoft IT Academy Program Member" means an active member of the Microsoft IT Academy Program.
- i. "Microsoft Learning Competency Member" means an active member of the Microsoft Partner Network program in good standing that currently holds the Learning Competency status.
- j. "MOC" means the "Official Microsoft Learning Product" instructor-led courseware known as Microsoft Official Course that educates IT professionals and developers on Microsoft technologies.
- k. "MPN Member" means an active Microsoft Partner Network program member in good standing.

- l. "Personal Device" means one (1) personal computer, device, workstation or other digital electronic device that you personally own or control that meets or exceeds the hardware level specified for the particular Microsoft Instructor-Led Courseware.
- m. "Private Training Session" means the instructor-led training classes provided by MPN Members for corporate customers to teach a predefined learning objective using Microsoft Instructor-Led Courseware. These classes are not advertised or promoted to the general public and class attendance is restricted to individuals employed by or contracted by the corporate customer.
- n. "Trainer" means (i) an academically accredited educator engaged by a Microsoft IT Academy Program Member to teach an Authorized Training Session, and/or (ii) a MCT.
- o. "Trainer Content" means the trainer version of the Microsoft Instructor-Led Courseware and additional supplemental content designated solely for Trainers' use to teach a training session using the Microsoft Instructor-Led Courseware. Trainer Content may include Microsoft PowerPoint presentations, trainer preparation guide, train the trainer materials, Microsoft One Note packs, classroom setup guide and Pre-release course feedback form. To clarify, Trainer Content does not include any software, virtual hard disks or virtual machines.

**2. USE RIGHTS.** The Licensed Content is licensed not sold. The Licensed Content is licensed on a **one copy per user basis**, such that you must acquire a license for each individual that accesses or uses the Licensed Content.

2.1 Below are five separate sets of use rights. Only one set of rights apply to you.

**a. If you are a Microsoft IT Academy Program Member:**

- i. Each license acquired on behalf of yourself may only be used to review one (1) copy of the Microsoft Instructor-Led Courseware in the form provided to you. If the Microsoft Instructor-Led Courseware is in digital format, you may install one (1) copy on up to three (3) Personal Devices. You may not install the Microsoft Instructor-Led Courseware on a device you do not own or control.
- ii. For each license you acquire on behalf of an End User or Trainer, you may either:
  - 1. distribute one (1) hard copy version of the Microsoft Instructor-Led Courseware to one (1) End User who is enrolled in the Authorized Training Session, and only immediately prior to the commencement of the Authorized Training Session that is the subject matter of the Microsoft Instructor-Led Courseware being provided, **or**
  - 2. provide one (1) End User with the unique redemption code and instructions on how they can access one (1) digital version of the Microsoft Instructor-Led Courseware, **or**
  - 3. provide one (1) Trainer with the unique redemption code and instructions on how they can access one (1) Trainer Content,

**provided you comply with the following:**
- iii. you will only provide access to the Licensed Content to those individuals who have acquired a valid license to the Licensed Content,
- iv. you will ensure each End User attending an Authorized Training Session has their own valid licensed copy of the Microsoft Instructor-Led Courseware that is the subject of the Authorized Training Session,
- v. you will ensure that each End User provided with the hard-copy version of the Microsoft Instructor-Led Courseware will be presented with a copy of this agreement and each End User will agree that their use of the Microsoft Instructor-Led Courseware will be subject to the terms in this agreement prior to providing them with the Microsoft Instructor-Led Courseware. Each individual will be required to denote their acceptance of this agreement in a manner that is enforceable under local law prior to their accessing the Microsoft Instructor-Led Courseware,
- vi. you will ensure that each Trainer teaching an Authorized Training Session has their own valid licensed copy of the Trainer Content that is the subject of the Authorized Training Session,

- vii. you will only use qualified Trainers who have in-depth knowledge of and experience with the Microsoft technology that is the subject of the Microsoft Instructor-Led Courseware being taught for all your Authorized Training Sessions,
- viii. you will only deliver a maximum of 15 hours of training per week for each Authorized Training Session that uses a MOC title, and
- ix. you acknowledge that Trainers that are not MCTs will not have access to all of the trainer resources for the Microsoft Instructor-Led Courseware.

**b. If you are a Microsoft Learning Competency Member:**

- i. Each license acquired on behalf of yourself may only be used to review one (1) copy of the Microsoft Instructor-Led Courseware in the form provided to you. If the Microsoft Instructor-Led Courseware is in digital format, you may install one (1) copy on up to three (3) Personal Devices. You may not install the Microsoft Instructor-Led Courseware on a device you do not own or control.
- ii. For each license you acquire on behalf of an End User or Trainer, you may either:
  - 1. distribute one (1) hard copy version of the Microsoft Instructor-Led Courseware to one (1) End User attending the Authorized Training Session and only immediately prior to the commencement of the Authorized Training Session that is the subject matter of the Microsoft Instructor-Led Courseware provided, **or**
  - 2. provide one (1) End User attending the Authorized Training Session with the unique redemption code and instructions on how they can access one (1) digital version of the Microsoft Instructor-Led Courseware, **or**
  - 3. you will provide one (1) Trainer with the unique redemption code and instructions on how they can access one (1) Trainer Content,  
**provided you comply with the following:**
- iii. you will only provide access to the Licensed Content to those individuals who have acquired a valid license to the Licensed Content,
- iv. you will ensure that each End User attending an Authorized Training Session has their own valid licensed copy of the Microsoft Instructor-Led Courseware that is the subject of the Authorized Training Session,
- v. you will ensure that each End User provided with a hard-copy version of the Microsoft Instructor-Led Courseware will be presented with a copy of this agreement and each End User will agree that their use of the Microsoft Instructor-Led Courseware will be subject to the terms in this agreement prior to providing them with the Microsoft Instructor-Led Courseware. Each individual will be required to denote their acceptance of this agreement in a manner that is enforceable under local law prior to their accessing the Microsoft Instructor-Led Courseware,
- vi. you will ensure that each Trainer teaching an Authorized Training Session has their own valid licensed copy of the Trainer Content that is the subject of the Authorized Training Session,
- vii. you will only use qualified Trainers who hold the applicable Microsoft Certification credential that is the subject of the Microsoft Instructor-Led Courseware being taught for your Authorized Training Sessions,
- viii. you will only use qualified MCTs who also hold the applicable Microsoft Certification credential that is the subject of the MOC title being taught for all your Authorized Training Sessions using MOC,
- ix. you will only provide access to the Microsoft Instructor-Led Courseware to End Users, and
- x. you will only provide access to the Trainer Content to Trainers.

**c. If you are a MPN Member:**

- i. Each license acquired on behalf of yourself may only be used to review one (1) copy of the Microsoft Instructor-Led Courseware in the form provided to you. If the Microsoft Instructor-Led Courseware is in digital format, you may install one (1) copy on up to three (3) Personal Devices. You may not install the Microsoft Instructor-Led Courseware on a device you do not own or control.
- ii. For each license you acquire on behalf of an End User or Trainer, you may either:
  1. distribute one (1) hard copy version of the Microsoft Instructor-Led Courseware to one (1) End User attending the Private Training Session, and only immediately prior to the commencement of the Private Training Session that is the subject matter of the Microsoft Instructor-Led Courseware being provided, **or**
  2. provide one (1) End User who is attending the Private Training Session with the unique redemption code and instructions on how they can access one (1) digital version of the Microsoft Instructor-Led Courseware, **or**
  3. you will provide one (1) Trainer who is teaching the Private Training Session with the unique redemption code and instructions on how they can access one (1) Trainer Content,  
**provided you comply with the following:**
- iii. you will only provide access to the Licensed Content to those individuals who have acquired a valid license to the Licensed Content,
- iv. you will ensure that each End User attending an Private Training Session has their own valid licensed copy of the Microsoft Instructor-Led Courseware that is the subject of the Private Training Session,
- v. you will ensure that each End User provided with a hard copy version of the Microsoft Instructor-Led Courseware will be presented with a copy of this agreement and each End User will agree that their use of the Microsoft Instructor-Led Courseware will be subject to the terms in this agreement prior to providing them with the Microsoft Instructor-Led Courseware. Each individual will be required to denote their acceptance of this agreement in a manner that is enforceable under local law prior to their accessing the Microsoft Instructor-Led Courseware,
- vi. you will ensure that each Trainer teaching an Private Training Session has their own valid licensed copy of the Trainer Content that is the subject of the Private Training Session,
- vii. you will only use qualified Trainers who hold the applicable Microsoft Certification credential that is the subject of the Microsoft Instructor-Led Courseware being taught for all your Private Training Sessions,
- viii. you will only use qualified MCTs who hold the applicable Microsoft Certification credential that is the subject of the MOC title being taught for all your Private Training Sessions using MOC,
- ix. you will only provide access to the Microsoft Instructor-Led Courseware to End Users, and
- x. you will only provide access to the Trainer Content to Trainers.

**d. If you are an End User:**

For each license you acquire, you may use the Microsoft Instructor-Led Courseware solely for your personal training use. If the Microsoft Instructor-Led Courseware is in digital format, you may access the Microsoft Instructor-Led Courseware online using the unique redemption code provided to you by the training provider and install and use one (1) copy of the Microsoft Instructor-Led Courseware on up to three (3) Personal Devices. You may also print one (1) copy of the Microsoft Instructor-Led Courseware. You may not install the Microsoft Instructor-Led Courseware on a device you do not own or control.

**e. If you are a Trainer.**

- i. For each license you acquire, you may install and use one (1) copy of the Trainer Content in the form provided to you on one (1) Personal Device solely to prepare and deliver an Authorized Training Session or Private Training Session, and install one (1) additional copy on another Personal Device as a backup copy, which may be used only to reinstall the Trainer Content. You may not install or use a copy of the Trainer Content on a device you do not own or control. You may also print one (1) copy of the Trainer Content solely to prepare for and deliver an Authorized Training Session or Private Training Session.

- ii. You may customize the written portions of the Trainer Content that are logically associated with instruction of a training session in accordance with the most recent version of the MCT agreement. If you elect to exercise the foregoing rights, you agree to comply with the following: (i) customizations may only be used for teaching Authorized Training Sessions and Private Training Sessions, and (ii) all customizations will comply with this agreement. For clarity, any use of “*customize*” refers only to changing the order of slides and content, and/or not using all the slides or content, it does not mean changing or modifying any slide or content.

2.2 **Separation of Components.** The Licensed Content is licensed as a single unit and you may not separate their components and install them on different devices.

2.3 **Redistribution of Licensed Content.** Except as expressly provided in the use rights above, you may not distribute any Licensed Content or any portion thereof (including any permitted modifications) to any third parties without the express written permission of Microsoft.

2.4 **Third Party Notices.** The Licensed Content may include third party code that Microsoft, not the third party, licenses to you under this agreement. Notices, if any, for the third party code are included for your information only.

2.5 **Additional Terms.** Some Licensed Content may contain components with additional terms, conditions, and licenses regarding its use. Any non-conflicting terms in those conditions and licenses also apply to your use of that respective component and supplements the terms described in this agreement.

3. **LICENSED CONTENT BASED ON PRE-RELEASE TECHNOLOGY.** If the Licensed Content’s subject matter is based on a pre-release version of Microsoft technology (“**Pre-release**”), then in addition to the other provisions in this agreement, these terms also apply:

- a. **Pre-Release Licensed Content.** This Licensed Content subject matter is on the Pre-release version of the Microsoft technology. The technology may not work the way a final version of the technology will and we may change the technology for the final version. We also may not release a final version. Licensed Content based on the final version of the technology may not contain the same information as the Licensed Content based on the Pre-release version. Microsoft is under no obligation to provide you with any further content, including any Licensed Content based on the final version of the technology.
- b. **Feedback.** If you agree to give feedback about the Licensed Content to Microsoft, either directly or through its third party designee, 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 technology, Microsoft product, or service that includes the feedback. You will not give feedback that is subject to a license that requires Microsoft to license its technology, technologies, or products to third parties because we include your feedback in them. These rights survive this agreement.
- c. **Pre-release Term.** If you are an Microsoft IT Academy Program Member, Microsoft Learning Competency Member, MPN Member or Trainer, you will cease using all copies of the Licensed Content on the Pre-release technology upon (i) the date which Microsoft informs you is the end date for using the Licensed Content on the Pre-release technology, or (ii) sixty (60) days after the commercial release of the technology that is the subject of the Licensed Content, whichever is earliest (“**Pre-release term**”). Upon expiration or termination of the Pre-release term, you will irretrievably delete and destroy all copies of the Licensed Content in your possession or under your control.

- 4. 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 allows you to use it in certain ways. Except as expressly permitted in this agreement, you may not:
- access or allow any individual to access the Licensed Content if they have not acquired a valid license for the Licensed Content,
  - alter, remove or obscure any copyright or other protective notices (including watermarks), branding or identifications contained in the Licensed Content,
  - modify or create a derivative work of any Licensed Content,
  - publicly display, or make the Licensed Content available for others to access or use,
  - copy, print, install, sell, publish, transmit, lend, adapt, reuse, link to or post, make available or distribute the Licensed Content to any third party,
  - work around any technical limitations in the Licensed Content, or
  - reverse engineer, decompile, remove or otherwise thwart any protections or disassemble the Licensed Content except and only to the extent that applicable law expressly permits, despite this limitation.
- 5. RESERVATION OF RIGHTS AND OWNERSHIP.** Microsoft reserves all rights not expressly granted to you in this agreement. The Licensed Content is protected by copyright and other intellectual property laws and treaties. Microsoft or its suppliers own the title, copyright, and other intellectual property rights in the Licensed Content.
- 6. 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](http://www.microsoft.com/exporting).
- 7. SUPPORT SERVICES.** Because the Licensed Content is “as is”, we may not provide support services for it.
- 8. TERMINATION.** Without prejudice to any other rights, Microsoft may terminate this agreement if you fail to comply with the terms and conditions of this agreement. Upon termination of this agreement for any reason, you will immediately stop all use of and delete and destroy all copies of the Licensed Content in your possession or under your control.
- 9. LINKS TO THIRD PARTY SITES.** You may link to third party sites through the use of the Licensed Content. The third party sites are not under the control of Microsoft, and Microsoft is not responsible for the contents of any third party sites, any links contained in third party sites, or any changes or updates to third party sites. Microsoft is not responsible for webcasting or any other form of transmission received from any third party sites. Microsoft is providing these links to third party sites to you only as a convenience, and the inclusion of any link does not imply an endorsement by Microsoft of the third party site.
- 10. ENTIRE AGREEMENT.** This agreement, and any additional terms for the Trainer Content, updates and supplements are the entire agreement for the Licensed Content, updates and supplements.
- 11. 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.

- 12. 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.
- 13. DISCLAIMER OF WARRANTY. THE LICENSED CONTENT IS LICENSED "AS-IS" AND "AS AVAILABLE." YOU BEAR THE RISK OF USING IT. MICROSOFT AND ITS RESPECTIVE AFFILIATES 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 AND ITS RESPECTIVE AFFILIATES EXCLUDES ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT.**
- 14. LIMITATION ON AND EXCLUSION OF REMEDIES AND DAMAGES. YOU CAN RECOVER FROM MICROSOFT, ITS RESPECTIVE AFFILIATES AND ITS SUPPLIERS ONLY DIRECT DAMAGES UP TO US\$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, 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.

Revised July 2013

# 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 performance<sup>1</sup>. 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](http://www.microsoft.com/learning)

**Microsoft** | Learning

<sup>1</sup> IDC, Value of Certification: Team Certification and Organizational Performance, November 2006

## Acknowledgments

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

### **Jason Hershey - Content Developer**

Jason Hershey is the owner of Tellus Consulting and Tellus Project Management, located in Western Washington. He is a Microsoft Certified Professional (MCP), Project Management Professional (PMP), and Certified Scrum Master. He also holds an MBA in finance. Prior to starting his own company, Jason worked for almost 20 years at Microsoft in nearly every product team, including Microsoft Official Curriculum (MOC), Windows client and Windows Server, SQL Server, and the Office product team. With these teams, Jason worked at designing, developing, and deploying solutions using Microsoft SharePoint, from SharePoint 2007 to SharePoint 2013, and the full stack of Microsoft technologies.

### **Gary Dunlop - Content Developer**

Gary Dunlop is based in Winnipeg, Canada, and is a technical consultant and trainer for Broadview Networks. He has authored a number of Microsoft Learning titles and has been a Microsoft Certified Trainer (MCT) since 1997.

### **Jamie Nelson - Content Developer**

Jamie Nelson is a Subject Matter Expert with more than 15 years of experience in various IT engineering and leadership roles. Jamie has extensive experience consulting on Active Directory, Group Policy, Exchange Server, System Center Configuration Manager, identity management, and virtualization. However, his passion lies in harnessing the capabilities of Windows PowerShell for enterprise automation, and for sharing his enthusiasm on the subject with others whenever and wherever the opportunity presents itself. Jamie's clients include public- and private-sector organizations in the energy and healthcare industries, and the United States Air Force. Jamie has served as adjunct faculty, teaching Windows Server and networking courses, and he holds several industry certifications, in addition to a Master's degree in Business Administration.

### **Jason Kellington - Content Developer**

Jason Kellington (MCT, MCSE, and MCITP) is a consultant, trainer, and author. He has experience working with a wide range of Microsoft technologies, focusing on enterprise network infrastructure. Jason works in several capacities with Microsoft. He is a content developer for Microsoft Learning courseware titles, a senior technical writer for Microsoft IT Showcase, and an author for Microsoft Press.

### **Claus Jacob Wordenskjold - Content Developer**

Claus Jacob Wordenskjold is an independent consultant and trainer based in Denmark. He founded his company, Chinchilla Data, in 1995, and he has more than 25 years of experience in IT. Claus has been an MCT since 2002, and he has delivered training throughout Europe. He specializes in Windows Client and Windows Server courses, but conducts occasional training in Microsoft SharePoint. Claus holds certifications in every Windows operating system since Windows 2000, and provides consulting services on Windows Server, Active Directory Domain Services (AD DS), and Group Policy. Claus has been a speaker at local Danish Microsoft events, and has authored several Windows-related courses.

**Damir Dizdarevic - Content Developer**

Damir Dizdarevic is an MCSE, MCTS, MCITP and MCT. He is the Executive Director for Services at Logosoft d.o.o., in Sarajevo, Bosnia, Herzegovina. Occasionally, he also works as a consultant for enterprise clients. Damir has more than 20 years of experience on Microsoft platforms, and he specializes in Windows Server, Exchange Server, and cloud and mobility solutions. He has worked as a designer, Subject Matter Expert, and technical reviewer on many Microsoft Official Courses on Windows Server, Exchange Server, Office 365 and Microsoft Azure topics, and has published more than 400 articles in various IT magazines, such as Windows ITPro and INFO Magazine. He is also a frequent and highly rated speaker at most Microsoft conferences in Eastern Europe. Additionally, Damir has been a Microsoft MVP for Cloud and Datacenter Management for nine years in a row. His technical blog is available at: <http://dizdarevic.ba/ddamirblog>.

**Clifton Leonard - Content Developer**

Clifton Leonard is a content developer and Subject Matter Expert with more than 25 years of experience in the IT industry as an engineer, architect, consultant, trainer, and author. Clifton has extensive experience consulting on Active Directory, Exchange Server, Lync Server, identity management, and Office 365. His clients include large energy corporations, K-12 schools, universities, technology manufacturers, financial institutions, the United States Air Force, and the United States Department of Defense. Clifton has been a Subject Matter Expert for multiple courses on Windows Desktop, Windows Server, Exchange Server, Microsoft SharePoint Server, Hyper-V, identity management, and Office 365.

**Andrew Warren - Technical Reviewer**

Andrew Warren has more than 25 years of experience in the IT industry, many of which he has spent teaching and writing. He has been involved as a Subject Matter Expert for many of the Windows Server 2012 courses, and as the technical lead on many Windows 8 courses. He also has been involved in developing TechNet sessions on Microsoft Exchange Server. Based in the United Kingdom, Andrew runs his own IT training and education consultancy.

# Contents

<b>Module 1: Implementing and configuring domain controllers</b>	
Module Overview	1-1
Lesson 1: Overview of AD DS	1-2
Lesson 2: Overview of AD DS domain controllers	1-14
Lesson 3: Deploying a domain controller	1-23
Lab: Deploying and administering AD DS	1-34
Module Review and Takeaways	1-39
<b>Module 2: Managing objects in AD DS</b>	
Module Overview	2-1
Lesson 1: Managing user accounts	2-2
Lesson 2: Managing groups in AD DS	2-11
Lesson 3: Managing computer objects in AD DS	2-21
Lab A: Managing AD DS objects	2-28
Lesson 4: Using Windows PowerShell for AD DS administration	2-33
Lesson 5: Implementing and managing OUs	2-48
Lab B: Administering AD DS	2-56
Module Review and Takeaways	2-61
<b>Module 3: Advanced AD DS infrastructure management</b>	
Module Overview	3-1
Lesson 1: Overview of advanced AD DS deployments	3-2
Lesson 2: Deploying a distributed AD DS environment	3-10
Lesson 3: Configuring AD DS trusts	3-24
Lab: Domain and trust management in AD DS	3-30
Module Review and Takeaways	3-34
<b>Module 4: Implementing and administering AD DS sites and replication</b>	
Module Overview	4-1
Lesson 1: Overview of AD DS replication	4-2
Lesson 2: Configuring AD DS sites	4-10
Lesson 3: Configuring and monitoring AD DS replication	4-18
Lab: Implementing AD DS sites and replication	4-25
Module Review and Takeaways	4-31

<b>Module 5: Implementing Group Policy</b>	
Module Overview	5-1
<b>Lesson 1:</b> Introducing Group Policy	5-2
<b>Lesson 2:</b> Implementing and administering GPOs	5-13
<b>Lesson 3:</b> Group Policy scope and Group Policy processing	5-21
<b>Lab A:</b> Implementing a Group Policy infrastructure	5-36
<b>Lesson 4:</b> Troubleshooting the application of GPOs	5-40
<b>Lab B:</b> Troubleshooting Group Policy infrastructure	5-48
Module Review and Takeaways	5-53
<b>Module 6: Managing user settings with Group Policy</b>	
Module Overview	6-1
<b>Lesson 1:</b> Implementing administrative templates	6-2
<b>Lesson 2:</b> Configuring Folder Redirection, Software Installation, and Scripts	6-12
<b>Lesson 3:</b> Configuring Group Policy preferences	6-22
<b>Lab:</b> Managing user settings with Group Policy	6-29
Module Review and Takeaways	6-38
<b>Module 7: Securing Active Directory Domain Services</b>	
Module Overview	7-1
<b>Lesson 1:</b> Securing domain controllers	7-2
<b>Lesson 2:</b> Implementing account security	7-15
<b>Lesson 3:</b> Implementing audit authentication	7-34
<b>Lesson 4:</b> Configuring managed service accounts	7-38
<b>Lab:</b> Securing AD DS	7-45
Module Review and Takeaways	7-55
<b>Module 8: Deploying and managing AD CS</b>	
Module Overview	8-1
<b>Lesson 1:</b> Deploying CAs	8-2
<b>Lesson 2:</b> Administering CAs	8-11
<b>Lesson 3:</b> Troubleshooting and maintaining CAs	8-21
<b>Lab:</b> Deploying and configuring a two-tier CA hierarchy	8-28
Module Review and Takeaways	8-32

<b>Module 9: Deploying and managing certificates</b>	
Module Overview	9-1
Lesson 1: Deploying and managing certificate templates	9-2
Lesson 2: Managing certificate deployment, revocation, and recovery	9-8
Lesson 3: Using certificates in a business environment	9-18
Lesson 4: Implementing and managing smart cards	9-27
Lab: Deploying and using certificates	9-33
Module Review and Takeaways	9-40
<b>Module 10: Deploying and administering AD FS</b>	
Module Overview	10-1
Lesson 1: Overview of AD FS	10-2
Lesson 2: AD FS requirements and planning	10-11
Lesson 3: Deploying and configuring AD FS	10-23
Lesson 4: Web Application Proxy overview	10-38
Lab: Implementing AD FS	10-49
Module Review and Takeaways	10-60
<b>Module 11: Implementing and administering AD RMS</b>	
Module Overview	11-1
Lesson 1: Overview of AD RMS	11-2
Lesson 2: Deploying and managing an AD RMS infrastructure	11-10
Lesson 3: Configuring AD RMS content protection	11-18
Lab: Implementing an AD RMS infrastructure	11-23
Module Review and Takeaways	11-28
<b>Module 12: Implementing AD DS synchronization with Microsoft Azure AD</b>	
Module Overview	12-1
Lesson 1: Planning and preparing for directory synchronization	12-2
Lesson 2: Implementing directory synchronization by using Azure AD Connect	12-13
Lesson 3: Managing identities with directory synchronization	12-23
Lab: Configuring directory synchronization	12-37
Module Review and Takeaways	12-43



<b>Module 13: Monitoring, managing, and recovering AD DS</b>	
Module Overview	13-1
<b>Lesson 1:</b> Monitoring AD DS	13-2
<b>Lesson 2:</b> Managing the Active Directory database	13-11
<b>Lesson 3:</b> Active Directory backup and recovery options for AD DS and other identity and access solutions	13-18
<b>Lab:</b> Recovering Objects in AD DS	13-27
Module Review and Takeaways	13-32
<b>Lab Answer Keys</b>	
<b>Module 1 Lab:</b> Deploying and administering AD DS	L1-1
<b>Module 2 Lab A:</b> Managing AD DS objects	L2-7
<b>Module 2 Lab B:</b> Administering AD DS	L2-11
<b>Module 3 Lab:</b> Domain and trust management in AD DS	L3-17
<b>Module 4 Lab:</b> Implementing AD DS sites and replication	L4-23
<b>Module 5 Lab A:</b> Implementing a Group Policy infrastructure	L5-31
<b>Module 5 Lab B:</b> Troubleshooting Group Policy infrastructure	L5-35
<b>Module 6 Lab:</b> Managing user settings with Group Policy	L6-41
<b>Module 7 Lab:</b> Securing AD DS	L7-51
<b>Module 8 Lab:</b> Deploying and configuring a two-tier CA hierarchy	L8-65
<b>Module 9 Lab:</b> Deploying and using certificates	L9-71
<b>Module 10 Lab:</b> Implementing AD FS	L10-79
<b>Module 11 Lab:</b> Implementing an AD RMS infrastructure	L11-91
<b>Module 12 Lab:</b> Configuring directory synchronization	L12-99
<b>Module 13 Lab:</b> Recovering objects in AD DS	L13-105

**MCT USE ONLY. STUDENT USE PROHIBITED**

## About This Course

This section provides a brief description of the course, audience, suggested prerequisites, and course objectives.

### Course Description



**Note:** This first release ('A') MOC version of course 20742A has been developed Windows Server 2016 Technical Preview 5. Microsoft Learning will release a 'B' version of this course with enhanced PowerPoint slides, and Course Companion content on Microsoft Learning site.

This five-day instructor-led course teaches IT professionals how to deploy and configure Active Directory Domain Services (AD DS) in a distributed environment, how to implement Group Policy, how to perform backup and restore, and how to monitor and troubleshoot Active Directory–related issues with Windows Server 2016. Additionally, this course teaches students how to deploy other Active Directory server roles, such as Active Directory Federation Services (AD FS) and Active Directory Certificate Services (AD CS).

### Audience

This course is primarily intended for working IT professionals who have some AD DS knowledge and experience, and who aim to develop knowledge about identity and access technologies in Windows Server 2016. This audience would typically include:

- AD DS administrators who want to train in identity and access technologies with Windows Server 2016.
- System or infrastructure administrators with general AD DS experience and knowledge who want to cross train in core and advanced identity and access technologies in Windows Server 2016.

The secondary audience for this course includes IT professionals who want to consolidate their knowledge about AD DS and related technologies, in addition to IT professionals who want to prepare for the 70-742 exam.

### Student Prerequisites

This course requires that you meet the following prerequisites:

- Some exposure to and experience with AD DS concepts and technologies in Windows Server 2012 or Windows Server 2016.
- Experience working with and configuring Windows Server 2012 or Windows Server 2016.
- Experience and an understanding of core networking technologies such as IP addressing, name resolution, and Dynamic Host Configuration Protocol (DHCP).
- Experience working with, and an understanding of Microsoft Hyper-V and basic server virtualization concepts.
- An awareness of basic security best practices.
- Hands-on working experience with Windows client operating systems such as Windows 7, Windows 8, Windows 8.1, or Windows 10.
- Basic experience with the Windows PowerShell command-line interface.

## Course Objectives

After completing this course, students will be able to:

- Install and configure domain controllers.
- Manage objects in AD DS by using graphical tools and Windows PowerShell.
- Implement AD DS in complex environments.
- Implement AD DS sites, and configure and manage replication.
- Implement and manage Group Policy Objects (GPOs).
- Manage user settings by using GPOs.
- Secure AD DS and user accounts.
- Implement and manage a certificate authority (CA) hierarchy with AD CS.
- Deploy and manage certificates.
- Implement and administer AD FS.
- Implement and administer Active Directory Rights Management Services (AD RMS).
- Implement synchronization between AD DS and Azure AD.
- Monitor, troubleshoot, and establish business continuity for AD DS services.

## Course Outline

The course outline is as follows:

**Module 1**, "Installing and configuring domain controllers," describes features of AD DS and how to install domain controllers (DCs). It also covers the considerations for deploying DCs.

**Module 2**, "Managing objects in AD DS," describes how to use various techniques to manage objects in AD DS. This includes creating and configuring users, groups, and computer objects.

**Module 3**, "Advanced AD DS infrastructure management," describes how to plan and implement an AD DS deployment that includes multiple domains and forests. The module provides an overview of the components in an advanced AD DS deployment, the process of implementing a distributed AD DS environment, and the procedure for configuring AD DS trusts.

**Module 4**, "Implementing and administering AD DS sites and replication," describes how to plan and implement an AD DS deployment that includes multiple locations. The module explains how replication works in a Windows Server 2016 AD DS environment.

**Module 5**, "Implementing Group Policy," describes how to implement a GPO infrastructure. The module provides an overview of the components and technologies that constitute the Group Policy framework.

**Module 6**, "Managing user settings with Group Policy," describes how to configure Group Policy settings and Group Policy preferences. This includes implementing administrative templates, configuring folder redirection and scripts, and configuring Group Policy preferences.

**Module 7**, "Securing Active Directory Domain Services," describes how to configure domain controller security, account security, password security, and Group Managed Service Accounts.

**Module 8**, "Deploying and managing AD CS," describes how to implement an AD CS deployment. This includes deploying, administering, and troubleshooting CAs.

**Module 9**, "Deploying and managing certificates," describes how to deploy and manage certificates in an AD DS environment. This involves deploying and managing certificate templates, managing certificate revocation and recovery, using certificates in a business environment, and implementing smart cards.

**Module 10**, “Deploying and administering AD FS,” describes AD FS and how to configure AD FS in a single-organization scenario and in a partner-organization scenario.

**Module 11**, “Implementing and administering AD RMS,” describes how to implement an AD RMS deployment. The module provides an overview of AD RMS, explains how to deploy and manage an AD RMS infrastructure, and explains how to configure AD RMS content protection.

**Module 12**, “Implementing AD DS synchronization with Microsoft Azure AD,” describes how to plan and configure directory syncing between Microsoft Azure Active Directory (Azure AD) and on-premises AD DS. The module describes various sync scenarios, such as Azure AD sync, AD FS and Azure AD, and Azure AD Connect.

**Module 13**, “Monitoring, managing, and recovering AD DS,” describes how to monitor, manage, and maintain AD DS to help achieve high availability of AD DS.

## Course Materials

The following materials are included with your kit:

- **Course Handbook:** a succinct classroom learning guide that provides the critical technical information in a crisp, tightly-focused format, which is essential for an effective in-class learning experience.
  - **Lessons:** guide you through the learning objectives and provide the key points that are critical to the success of the in-class learning experience.
  - **Labs:** provide a real-world, hands-on platform for you to apply the knowledge and skills learned in the module.
  - **Module Reviews and Takeaways:** provide on-the-job reference material to boost knowledge and skills retention.
  - **Lab Answer Keys:** provide step-by-step lab solution guidance.



**Additional Reading: Course Companion Content on the <http://www.microsoft.com/learning/en/us/companion-moc.aspx> Site:** searchable, easy-to-browse digital content with integrated premium online resources that supplement the Course Handbook.

- **Modules:** include companion content, such as questions and answers, detailed demonstration steps, and additional reading links, for each lesson. Additionally, they include Lab Review questions and answers and Module Reviews and Takeaways sections, which contain the review questions and answers, best practices, common issues and troubleshooting tips with answers, and real-world issues and scenarios with answers.
- **Resources:** include well-categorized additional resources that give you immediate access to the most current premium content on TechNet, MSDN, or Microsoft Press.
- **Course evaluation:** at the end of the course, you will have the opportunity to complete an online evaluation to provide feedback on the course, training facility, and instructor.
  - To provide additional comments or feedback on the course, to [mcspprt@microsoft.com](mailto:mcspprt@microsoft.com). To inquire about the Microsoft Certification Program, send an email to [mcp@microsoft.com](mailto:mcp@microsoft.com).

## Virtual Machine Environment

This section provides the information for setting up the classroom environment to support the business scenario of the course.

### Virtual Machine Configuration

In this course, you will use Hyper-V to perform the labs.



**Note:** At the end of each lab, you must revert the virtual machines to a snapshot. You can find the instructions for this procedure at the end of each lab.

The following table shows the role of each virtual machine that is used in this course:

Virtual machine	Role
20742A-LON-DC1	Domain controller in the Adatum.com domain
20742A-LON-DC2	Domain controller in the Adatum.com domain
20742A-TOR-DC1	Domain controller in the Adatum.com domain (in another site)
20742A-TREY-DC1	Domain controller in Treyresearch.com domain
20742A-LON-SVR1	Member server in the Adatum.com domain
20742A-LON-SVR2	Member server in the Adatum.com domain with Web server role
20742A-CA-SRV1	Server not joined to the domain to be used as offline root CA
20742A-LON-CL1	Windows 10 client with Microsoft Office 2016 installed
20742A-LON-CL2	Windows 10 client with Office 2016 installed

### Software Configuration

The following software is installed on each virtual machine:

- Windows Server 2016 TP5
- Windows 10 Enterprise
- Microsoft Office Professional 2016
- Microsoft Active Directory Replication Status tool

### Classroom Setup

Each classroom computer will have the same virtual machine configured in the same way.

## Course Hardware Level

To ensure a satisfactory student experience, Microsoft Learning requires a minimum equipment configuration for trainer and student computers in all Microsoft Certified Partner for Learning Solutions (CPLS) classrooms in which Official Microsoft Learning Product courseware is taught.

- Intel Virtualization Technology (Intel VT) or AMD Virtualization (AMD-V) processor
- Hard Disk: Dual 500 gigabyte (GB) hard disks 7200 RPM SATA labeled C drive and D drive
- 16 GB of random access memory (RAM)
- DVD drive
- Network adapter
- Super VGA (SVGA) 17-inch monitor
- Microsoft mouse or compatible pointing device
- Sound card with amplified speakers

Additionally, the instructor's computer must be connected to a projection display device that supports SVGA 1024×768 pixels, 16-bit colors.



# Module 1

## Installing and configuring domain controllers

### Contents:

Module Overview	1-1
<b>Lesson 1:</b> Overview of AD DS	1-2
<b>Lesson 2:</b> Overview of AD DS domain controllers	1-14
<b>Lesson 3:</b> Deploying a domain controller	1-23
<b>Lab:</b> Deploying and administering AD DS	1-34
Module Review and Takeaways	1-39

## Module Overview

Active Directory Domain Services (AD DS) and its related services form the foundation for enterprise networks that run Windows operating systems. The AD DS database is the central store of all the domain objects, such as user accounts, computer accounts, and groups. AD DS provides a searchable, hierarchical directory and a method for applying configuration and security settings for objects in the enterprise. This module covers the structure of AD DS and its various components, such as forests, domains, and organizational units (OUs).

With an increasing focus on cloud and hybrid environments, Windows Server 2016 includes several new AD DS features that make it easier to manage these environments. This module covers the features and choices available in Windows Server 2016 for installing AD DS on a server along with an overview of domain controllers.

### Objectives

After completing this module, you will be able to:

- Describe AD DS and its main components.
- Describe the purpose of domain controllers and their roles.
- Describe the considerations for deploying domain controllers.
- Deploy a domain controller.

## Lesson 1

# Overview of AD DS

The AD DS database stores information on user identity, computers, groups, services, and resources in a hierarchical structure, called the *directory*. AD DS domain controllers also host the service that authenticates user and computer accounts when they sign in to the domain. Because AD DS stores information about all of the objects in the domain, and all users and computers must connect to AD DS domain controllers when they sign in to the network, AD DS is the primary means by which you can configure and manage user and computer accounts on your network.

This lesson covers the core logical components and physical components that make up an AD DS deployment.

### Lesson Objectives

After completing this lesson, you will be able to:

- Describe the components of AD DS.
- Describe AD DS domains.
- Describe OUs and their purpose.
- Describe AD DS forests and trees and explain how you can deploy them in a network.
- Explain how an AD DS schema provides a set of rules that manage the objects and attributes that are stored in the AD DS domain database.
- Describe Microsoft Azure Active Directory (Azure AD).
- Identify the tools available for administering AD DS.
- Describe what is new for on-premises Active Directory in Windows Server 2016.


### Overview of AD DS

AD DS is composed of both logical and physical components. You need to understand the way the components of AD DS work together so that you can manage your infrastructure efficiently. In addition, you can use many other AD DS options to perform actions such as installing, configuring, and updating apps; managing the security infrastructure; enabling Remote Access Service and DirectAccess; and issuing and managing digital certificates.

One of the most-used AD DS features is Group Policy, which allows you to configure centralized policies that you can use to manage most objects in AD DS. Understanding the various AD DS components is important for using Group Policy successfully.

AD DS is composed of both logical and physical components

Logical components	Physical components
<ul style="list-style-type: none"> <li>• Partitions</li> <li>• Schema</li> <li>• Domains</li> <li>• Domain trees</li> <li>• Forests</li> <li>• Sites</li> <li>• OUs</li> <li>• Containers</li> </ul>	<ul style="list-style-type: none"> <li>• Domain controllers</li> <li>• Data stores</li> <li>• Global catalog servers</li> <li>• RODCs</li> </ul>

 **Note:** Group Policy is covered in more detail in Module 5, “Implementing Group Policy.”

## Logical components


AD DS logical components are structures that you use to implement an AD DS design that is appropriate for an organization. The following table describes the types of logical structures that an AD DS database contains.

Logical component	Description
Partition	A partition, also called a naming context, is a portion of the AD DS database. Although the database is one file named Nds.dit, different partitions contain different data. For example, the schema partition contains a copy of the Active Directory schema. The configuration partition contains the configuration objects for the forest, and the domain partition contains the users, computers, groups, and other objects specific to the domain. Copies of a partition can be stored on multiple domain controllers and updated through directory replication.
Schema	A schema is the set of definitions of the object types and attributes that you use to define the objects created in AD DS.
Domain	A domain is a logical administrative container for objects such as users and computers. A domain maps to a specific partition and can be organized with parent-child relationships to other domains.
Domain tree	A domain tree is a hierarchical collection of domains that share a common root domain and a contiguous Domain Name System (DNS) namespace.
Forest	A forest is a collection of domains that share a common AD DS root and schema, which have a two-way trust relationship.
Site	A site is a container for AD DS objects, such as computers and services that are defined by their physical location. This is in comparison to a domain, which represents the logical structure of objects, such as users and groups in addition to computers.
Subnet	A subnet is a portion of the network IP addresses of an organization assigned to computers in a site. A site can have more than one subnet.
OU	An OU is a container object for users, groups, and computers that provides a framework for delegating administrative rights and administration by linking Group Policy Objects (GPOs).
Container	A container is an object that provides an organizational framework for use in AD DS. Some containers are created by default, or you can create custom containers. Containers cannot have GPOs linked to them.

## Physical components

The following table describes some of the physical components of AD DS.

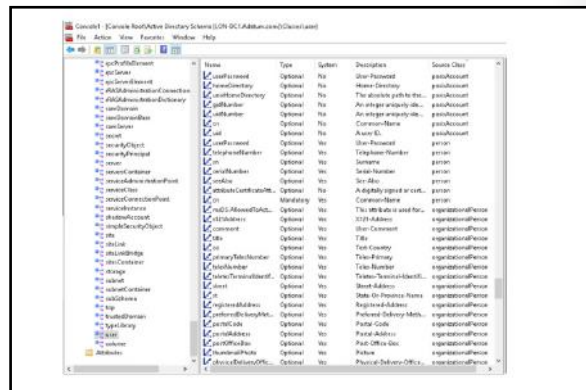
Physical component	Description
Domain controller	A domain controller contains a copy of the AD DS database. For most operations, each domain controller can process changes and replicate the changes to all the other domain controllers in the domain.
Data store	A copy of the data store exists on each domain controller. The AD DS database uses Microsoft Jet database technology and stores the directory information in the Ntds.dit file and associated log files. Those files are stored in the C:\Windows\NTDS folder by default.
Global catalog server	A global catalog server is a domain controller that hosts the <i>global catalog</i> , which is a partial, read-only copy of all the objects in a multiple-domain forest. A global catalog speeds up searches for objects that might be stored on domain controllers in a different domain in the forest.
Read-only domain controller (RODC)	An RODC is a special, read-only installation of AD DS. RODCs are often used in branch offices where physical security cannot be guaranteed, IT support is less advanced than in the main corporate centers, or line-of-business applications exist that need to run on a domain controller.

 **Additional Reading:** For more information on domains and forests, refer to: "Active Directory Domain Services Overview" at: <http://aka.ms/M2lr5a>

## What is the AD DS schema?

The *AD DS schema* is the component that defines all the object classes and attributes that AD DS uses to store data. All domains in a forest contain a copy of the schema that applies to that forest. Any change that is made to the schema is replicated to every domain controller in the forest from the schema master, which is typically the first domain controller in the forest.

AD DS stores and retrieves information from a wide variety of applications and services. It does this, in part, by standardizing how data is stored in the AD DS directory. By standardizing data storage, AD DS can retrieve, update, and replicate data while helping to ensure that the data integrity is maintained.



## Objects

AD DS uses objects as units of storage. All object types are defined in the schema. Each time the directory handles data, the directory queries the schema for an appropriate object definition. Based on the object definition in the schema, the directory creates the object and stores the data.

Object definitions specify both the types of data that the objects can store and the syntax of the data. You can create only objects that are defined by the schema. Because the data is stored in a rigidly defined format, AD DS can store, retrieve, and validate the data that it manages, regardless of which application supplies it.

## Relationships among objects, rules, attributes, and classes

In AD DS, the schema defines the following:

- Objects that store data in the directory
- Rules that define the structure of the objects
- The structure and content of the directory itself

AD DS schema objects consist of attributes, which are grouped together into classes. Each class has rules that define which attributes are required and which are optional. For example, the **user** class consists of more than 400 possible attributes, including **cn** (the common name attribute), **givenName**, **displayName**, **objectSID**, and **manager**. Of these attributes, the **cn** and **objectSID** attributes are mandatory. The **cn** attribute is defined as a single-value Unicode string that is from 1 through 64 characters long and that is replicated to the global catalog.

## Changing the schema

Only members of the Schema Admins group can modify the AD DS schema. You cannot remove anything from the AD DS schema. You can only extend the AD DS schema by using AD DS schema extensions or by modifying the attributes of existing objects. For example, when you are preparing to install Exchange Server 2016, you must apply the Exchange Server 2016 Active Directory schema changes. These changes add or modify hundreds of classes and attributes.

You should change the schema only when necessary because the schema dictates how information is stored, and any changes made to the schema affect every domain controller. Before you change the schema, you should review the changes through a tightly controlled process and implement them only after you have performed testing to help ensure that the changes will not adversely affect the rest of the forest or any applications that use AD DS.

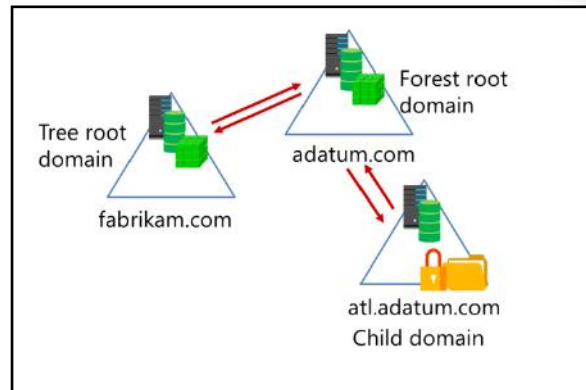
The schema master is one of the operations master roles that is hosted on a single domain controller in AD DS. Because it is a single master, you must make changes to the schema by targeting the domain controller that holds the schema master, using the Active Directory Schema snap-in. To target the schema master in a separate forest, you will need to target the appropriate forest from within the snap-in.



**Note:** Operations master roles are discussed in detail in the topic, “What are operations masters?”.

## What is an AD DS forest?

A forest is a top-level container in AD DS. Each *forest* is a collection of one or more domain trees that share a common directory schema and a global catalog. A domain tree is a collection of one or more domains that share a contiguous namespace. The first domain that is created in the forest is called the *forest root domain*. The forest root domain contains a few objects that do not exist in other domains in the forest. Because these objects are always created on the first domain controller that is created, a forest can consist of as little as one domain with a single domain controller, or it can consist of hundreds of domains across multiple domain trees. The following objects exist only in the forest root domain:



- The schema master role. This is a special, forest-wide domain controller role. Only one schema master exists in any forest. The schema can be changed only on the domain controller that holds the schema master.
- The domain naming master role. This is also a special, forest-wide domain controller role. Only one domain naming master exists in any forest. Only the domain naming master can add new domain names to the directory.
- The Enterprise Admins group. By default, the Enterprise Admins group has the Administrator account for the forest root domain as a member. The Enterprise Admins group is a member of the local Administrators group in every domain in the forest. This allows members of the Enterprise Admins group to have full control administrative rights to every domain throughout the forest.
- The Schema Admins group. By default, the Schema Admins group has no members. Only members of the Enterprise Admins group or the Domain Admins group (in the forest root domain), can add members to the Schema Admins group. Only members of the Schema Admins group can make changes to the schema.

### Security boundary

An AD DS forest is a security boundary. By default, no users from outside the forest can access any resources inside the forest. Typically, an organization creates only one forest, although you can create multiple forests to isolate administrative permissions among different parts of the organization.

By default, all the domains in a forest automatically trust the other domains in the forest. This helps to make it easy to enable access to resources, such as file shares and websites, for all the users in a forest, regardless of the domain in which a user account is located.

### Replication boundary

An AD DS forest is the replication boundary for the configuration and schema partitions in the AD DS database. As a result, all the domain controllers in the forest must share the same schema. Because of this, organizations that want to deploy applications with incompatible schemas need to deploy additional forests.

The AD DS forest is also the replication boundary for the global catalog. The global catalog makes it possible to find objects from any domain in the forest. For example, the global catalog is used whenever user principal name (UPN) sign-in credentials are used or when Microsoft Exchange Server address books are used to find users.

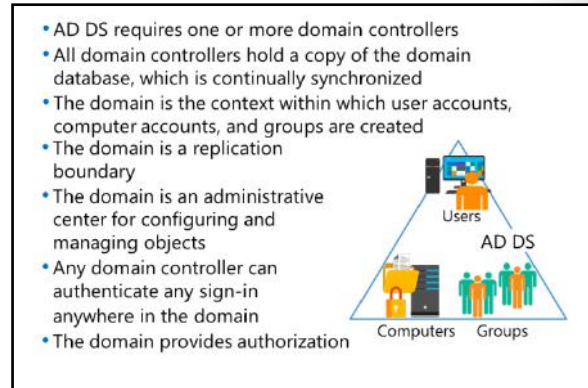
## What is an AD DS domain?

### AD DS domain: a container for users, computers, groups, and more

An AD DS domain is a logical container used to manage user, computer, group, and other objects. All of the domain objects are stored in the AD DS database, a copy of which is stored on each domain controller.

Many types of objects exist in the AD DS database. You most often work with user accounts, computer accounts, and groups. The following list briefly describes these three object types:

- User accounts. User accounts contain information about users, including the information required to authenticate a user during the sign-in process and build the user's access token.
- Computer accounts. Each domain-joined computer has an account in AD DS. Computer accounts are used for domain-joined computers in the same way that user accounts are used for users.
- Groups. Groups are used to organize users or computers to make it easier to manage permissions and Group Policy in the domain.



### The AD DS domain is a replication boundary

When changes are made to any object in the domain, the domain controller where the change occurred replicates that change to all the other domain controllers in the domain. If multiple domains exist in the forest, only subsets of the changes are replicated to other domains. AD DS uses a multimaster replication model that allows every domain controller to make changes to objects in the domain.

AD DS allows a single domain to contain nearly 2 billion objects. With this much capacity, most organizations can deploy only a single domain to ensure that all domain controllers contain all the domain information. However, organizations that have decentralized administrative structures or that are distributed across multiple locations might consider implementing multiple domains in the same forest to accommodate the administrative needs of their environments.

### The AD DS domain is an administrative center


The domain contains an Administrator account and a Domain Admins group. By default, the Administrator account is a member of the Domain Admins group, and the Domain Admins group is a member of every local Administrators group of domain-joined computers. Also, by default, the Domain Admins group members have full control over every object in the domain. The Administrator account in the forest root domain has additional rights, as detailed in the topic, "What is an AD DS forest?" later in this module.

### The AD DS domain provides authentication

Whenever a domain-joined computer starts or a user signs in to a domain-joined computer, AD DS authenticates it. Authentication helps to verify that the computer or user has the proper credentials for an AD DS account.

## The AD DS domain provides authorization

Windows operating systems use authorization and access control technologies to allow authenticated users to access resources. Typically, the authorization process is performed locally at the resource level. Domain-based Dynamic Access Control enables central access rules to control the access to resources. Central access rules do not replace the current access control technology but provide an additional level of control.

 **Note:** Dynamic Access Control (DAC) is a feature introduced in Windows Server 2012 that allows administrators to define rules that control access permissions. DAC is covered in more detail in course 20744A, "Securing Windows Server 2016," Module 11, "Implementing data access for users and devices," Lesson 3, "Understanding Dynamic Access Control."

## What are OUs?

An *organizational unit* (OU) is a container object within a domain that you can use to consolidate users, computers, groups, and other objects. You can link Group Policy Objects (GPOs) directly to an OU in order to manage the objects contained in the OU. You can also assign an OU manager and associate a COM+ partition with an OU.

You can create new OUs in AD DS at any time using Active Directory Administrative Center. Two reasons exist to create an OU:

- To group objects together to make it easier to manage them by applying GPOs to the whole group. When you assign GPOs to an OU, the settings apply to all the objects within the OU. GPOs are policies that administrators create to manage and configure settings for computers and/or users. You deploy the GPOs by linking them to OUs, domains, or sites.
- To delegate administrative control of objects within the OU. You can assign management permissions on an OU, thereby delegating control of that OU to a user or group within AD DS in addition to the Domain Admins group.

- Use containers to group objects within a domain:
  - You cannot apply GPOs to containers
  - Containers are used for system objects and as the default for new objects
- Create OUs to:
  - Configure objects by assigning GPOs to them
  - Delegate administrative permissions

You can use OUs to represent the hierarchical, logical structures within your organization. For example, you can create OUs that represent the departments within your organization, the geographic regions within your organization, or a combination of both departmental and geographic regions. You can use OUs to manage the configuration and use of user, group, and computer accounts based on your organizational model.

## Generic containers

AD DS contains several built-in containers, known as generic containers, such as Users and Computers. These containers are used to store system objects or used as the default parents to the new objects when they are created. These generic container objects should not be confused with OUs. The primary difference between OUs and containers are the management capabilities. Containers have limited management capabilities. For example, you cannot apply a GPO directly to a container.



When you install AD DS, the Domain Controllers OU and several generic container objects are created by default. Some default objects are used primarily by AD DS and are hidden by default. The following objects are visible by default within the AD Administrative Center:

- Domain. The top level of the domain organizational hierarchy.
- Built-in container. A container that stores several default groups.
- Computers container. The default location for new computer accounts that you create in the domain.
- Foreign Security Principals container. The default location for trusted objects from domains outside the AD DS forest. Typically, these are created when an object from an external domain is added to a group in the AD DS domain.
- Managed Service Accounts. The default location for managed service accounts. AD DS provides automatic password management in managed service accounts.
- Users container. The default location for new user accounts and groups that you create in the domain. The Users container also holds the administrator and guest accounts for the domain and for some default groups.
- Domain Controllers OU. The default location for domain controllers' computer accounts. This is the only OU that is present in a new installation of AD DS.

Several containers exist that you can see only when you click **Advanced Features** on the **View** menu. The following objects are hidden by default:

- LostAndFound. This container holds orphaned objects.
- Program Data. This container holds Active Directory data for Microsoft applications, such as Active Directory Federation Services (AD FS).
- System. This container holds the built-in system settings.
- NTDS Quotas. This container holds directory service quota data.
- TPM Devices. This container is new with Windows Server 2016. It stores the recovery information for Trusted Platform Module (TPM) devices.



**Note:** Containers in an AD DS domain cannot have GPOs linked to them. To link GPOs to apply configurations and restrictions, create a hierarchy of OUs and then link the GPOs to them.

## Hierarchy design

The design of an OU hierarchy is dictated by the administrative needs of the organization. The design could be based on geographic, functional, resource, or user classifications. Whatever be the order, the hierarchy should make it possible to administer AD DS resources as effectively and with as much flexibility as possible. For example, if all the computers that IT administrators use must be configured in a certain way, you can group all the computers in an OU and then assign a GPO to manage those computers.

You also can create OUs within other OUs. For example, your organization might have multiple offices, and each office might have a team of IT administrators who are responsible for managing user and computer accounts in their office. In addition, each office might have different departments with different computer configuration requirements. In this situation, you can create an OU for each office, and then within each of those OUs, create an OU for the IT administrators and an OU for each of the other departments.

Although there is no technical limit to the number of levels in your OU structure, to help ensure manageability, limit your OU structure to a depth of no more than 10 levels. Most organizations use 5 levels or fewer to simplify administration. Note that applications that work with AD DS can impose restrictions on the OU depth within the hierarchy for the parts of the hierarchy that they use.


## What is new in AD DS in Windows Server 2016?

Windows Server 2016 has several new features as part of AD DS that make it easier for you to help secure your AD DS environment and migrate to cloud-based or hybrid environments.

- PAM
- Azure AD Join
- Microsoft Passport


### Privileged Access Management

Privileged Access Management (PAM) is based on Microsoft Identity Manager. PAM allows you to separate the permissions required for certain administrative activities from the permissions of members of the current AD DS environment. With PAM, users request permission to perform activities that require privileged access instead of having that access granted on a permanent basis. Granting those permissions can mean that you have to provide additional authentication steps, such as Multi-Factor Authentication. When the user is granted access, the access is granted on a temporary basis through a shadow group in a *bastion forest*. The bastion forest is a cleaner environment that is meant to be devoid of any access from hackers or any stolen credentials of privileged users. Because the user's personal work account does not have the required permissions on a permanent basis, there is a decrease in the possibility of a security breach, such as unlawful access by a malicious hacker that has stolen an administrator's password.

 **Additional Reading:** For more information on PAM, refer to: "Privileged Access Management for Active Directory Domain Services (AD DS)" at: <http://aka.ms/lbsyai>


### Azure AD Join


Azure Active Directory Join (Azure AD Join) supports connecting on-premises, domain-joined devices to Azure AD for improved cloud-only and hybrid environments. For corporate-owned devices, users no longer need a personal Microsoft account. Azure AD also supports connecting devices that normally cannot join an on-premises domain, such as mobile devices. Users can access the Windows Store with their on-premises accounts and even with their personal devices. Support also exists for mobile device management (MDM), setting up shared devices, and imaging corporate-owned devices.

 **Additional Reading:** For more information on Azure AD Join, refer to: "Windows 10 for enterprise: Ways to use devices for work" at: <http://aka.ms/F7dfxe>

### Microsoft Passport

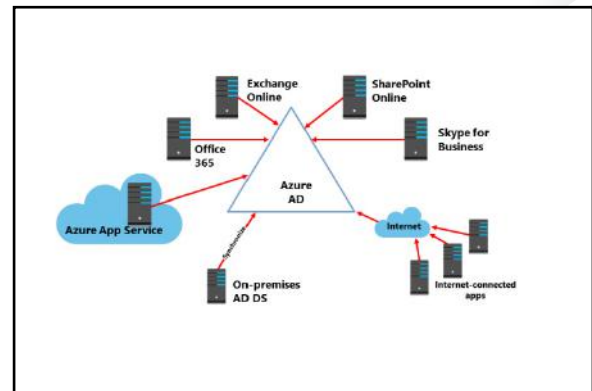
AD DS in Windows Server 2016 supports Microsoft Passport, which provides a certificate-based approach to authentication that can replace the use of passwords. Microsoft Passport allows users to authenticate to an on-premises AD DS account, an Azure AD account, or any service that supports Fast Identity Online (FIDO) authentication. Microsoft Passport is covered in detail in course, 20744: Securing Windows Server 2016.

 **Additional Reading:** For more information on using Microsoft Passport with AD DS in Windows Server 2016, refer to: "Authenticating identities without passwords through Microsoft Passport" at: <http://aka.ms/Nyrund>

 **Additional Reading:** For more information on the new AD DS features in Windows Server 2016, refer to: "What's new in Active Directory Domain Services Technical Preview" at: <http://aka.ms/Nzrl6u>

## What is Azure AD?

Azure AD is a service that provides identity management and access control for your cloud-based applications. You use Azure AD when you subscribe to Microsoft Office 365, Microsoft SharePoint Online, Exchange Online, or Skype for Business. Additionally, you can use Azure AD with Azure apps or Internet-connected apps that require authentication. You can synchronize your on-premises AD DS with Azure AD to allow your users to use the same identity across both internal resources and cloud-based resources.




Azure AD does not include all the services available with an on-premises Active Directory solution that uses Windows Server 2016. On-premises Active Directory in Windows Server 2016 supports five services:

- AD DS
- AD FS
- Active Directory Lightweight Directory Services (AD LDS)
- Active Directory Certificate Services (AD CS)
- Active Directory Rights Management Services (AD RMS)

Azure AD includes only:

- Azure AD, which supports identity management in the cloud.
- Azure Access Control Service, which supports federation with external identity management services, including your on-premises instance of AD DS.

Azure AD does not support applications that are integrated with on-premises Active Directory. For applications to integrate with Azure AD, they must be written for Azure AD.

 **Note:** You cannot create AD DS domain controllers in Azure AD. You can use Azure AD as a standalone service or integrate it with your existing on-premises Active Directory infrastructure. However, you do not create or manage the Azure AD systems. Instead, you manage your users in the Azure AD service.

## Overview of AD DS administration tools

Managing the AD DS environment is one of the most common tasks an IT professional performs. You typically manage your domain controllers remotely, even though you can sign in to the computer either directly or by using Remote Desktop. The primary tool you will use is the Active Directory Administrative Center.

### Active Directory Administrative Center

The Active Directory Administrative Center provides a graphical user interface (GUI) that is built on Windows PowerShell. This enhanced interface allows you to perform AD DS object management by using task-oriented navigation, and it replaces the functionality of Active Directory Users and Computers. Tasks that you can perform by using the Active Directory Administrative Center include:

- Creating and managing user, computer, and group accounts.
- Creating and managing OUs.
- Connecting to and managing multiple domains within a single instance of the Active Directory Administrative Center.
- Searching and filtering AD DS data by building queries.
- Creating and managing fine-grained password policies.
- Recovering objects from the Active Directory Recycle Bin.
- Managing objects that are required for the Dynamic Access Control feature.

You can install the Active Directory Administrative Center only on servers running Windows Server 2008 R2 or later or on client computers running Windows 7 or later.

Other management tools you will use to perform AD DS administration include:

- Active Directory Users and Computers

Active Directory Users and Computers is a Microsoft Management Console (MMC) snap-in that manages most of the common day-to-day resources, including users, groups, and computers. Although this snap-in is well known to many administrators, the Active Directory Administrative Center replaces it and provides more capabilities.

- Active Directory Sites and Services

The Active Directory Sites and Services MMC snap-in manages replication, network topology, and related services.

- Active Directory Domains and Trusts

The Active Directory Domains and Trusts MMC snap-in configures and maintains trust relationships at the domain and forest functional levels.

- Active Directory Schema snap-in

The Active Directory Schema MMC snap-in examines and modifies the definitions of AD DS attributes and object classes. The schema provides the definitions for AD DS objects and attributes, and you typically do not view or change it very often. Therefore, by default, the Active Directory Schema snap-in is not fully installed.

You typically perform AD DS management by using the following tools:

- Active Directory Administrative Center
- Active Directory Users and Computers
- Active Directory Sites and Services
- Active Directory Domains and Trusts
- Active Directory Schema snap-in
- Active Directory module for Windows PowerShell

- Active Directory module for Windows PowerShell

The Active Directory module for Windows PowerShell supports AD DS administration, and it is one of the most important management components. Server Manager and the Active Directory Administration Center are built on Windows PowerShell and use cmdlets to perform their tasks.

## Demonstration: Using the Active Directory Administrative Center to administer and manage AD DS

The Active Directory Administrative Center is the most-powerful administrative interface for managing your AD DS environment. This demonstration will show you how to:

- Navigate within the Active Directory Administrative Center.
- Perform an administrative task within the Active Directory Administrative Center.
- Create objects.
- View all object attributes.
- Use the Windows PowerShell History viewer in the Active Directory Administrative Center.

### Demonstration Steps

#### Navigate within the Active Directory Administrative Center

1. On **LON-DC1**, open the **Active Directory Administrative Center**.
2. Select **Adatum (local)**, **Dynamic Access Control**, and **Global Search** in the navigation pane.
3. In the navigation pane, switch to the tree view, and then expand **Adatum.com**.

#### Perform an administrative task within the Active Directory Administrative Center

1. Go to the **Overview** view.
2. Reset the password for **Adatum\Adam** to **Pa\$\$w0rd** so that the user does not have to change the password at the next sign-in.
3. Use the **Global Search** section to find any objects that match the **lon** search string.

#### Create an object

- Create a new computer object named **LON-CL4** in the **Computers** container.

#### View all object attributes

1. Open the **Properties** page for **LON-CL4**, scroll down to the **Extensions** section, and then click the **Attribute Editor** tab.
2. View the object's AD DS attributes.

#### Use the Windows PowerShell History viewer

1. Open the **Windows PowerShell History** pane.
2. View the Windows PowerShell cmdlet that you used to perform the most recent task.
3. On **LON-DC1**, close all open windows.

**Question:** What are the two main purposes of OUs?

**Question:** Why would you need to deploy an additional tree in the AD DS forest?

## Lesson 2

# Overview of AD DS domain controllers

Because domain controllers authenticate all users and computers in the domain, domain controller deployment is critical for the network to function correctly.

This lesson examines domain controllers, the sign-in process, and the importance of DNS in that process. In addition, this lesson discusses the purpose of the global catalog.

All domain controllers are essentially the same, with two exceptions. RODCs contain a read-only copy of the AD DS database, whereas other domain controllers have a read/write copy. Also, certain operations can be performed only on specific domain controllers called *operations masters*, which are discussed at the end of this lesson.

### Lesson Objectives

After completing this lesson, you will be able to:

- Describe the purpose of domain controllers.
- Understand what is contained in the SYSVOL folder.
- Describe the purpose of the global catalog.
- Describe the AD DS sign-in process and the importance of DNS and service records (SRV records) in that process.
- Explain the functions of operations masters.
- Describe operations master role transfer and seizing.

### What is a domain controller?

A *domain controller* is a server that is configured to store a copy of the AD DS directory database (Ntds.dit) and a copy of the SYSVOL folder. All domain controllers except RODCs store a read/write copy of both Ntds.dit and the SYSVOL folder. Ntds.dit is the database itself, and the SYSVOL folder contains all the template settings and files for GPOs.


Domain controllers use a multimaster replication process to copy data from one domain controller to another. This means that for most operations, data can be modified on any domain controller, except for an RODC. The AD DS replication service then synchronizes the changes that have been made to the AD DS database with all the other domain controllers in the domain. In Windows Server 2016, you can use only Distributed File System (DFS) replication to replicate the SYSVOL folders. Earlier versions of Windows Server used the file replication service (FRS) to replicate the folders, but FRS is obsolete for several versions of Windows.

Domain controllers host several other services related to AD DS, including the Kerberos authentication service, which user and computer accounts use for sign-in authentication, and the Key Distribution Center (KDC), which issues the ticket-granting ticket (TGT) to an account that signs in to the AD DS domain. Optionally, you can configure domain controllers to host a copy of the global catalog.

#### Domain controllers:


- Are servers that host the AD DS database (Ntds.dit) and SYSVOL
- Host the Kerberos authentication service and KDC services to perform authentication
- Have best practices for:
  - Availability:
    - Use at least two domain controllers in a domain
  - Security:
    - Use an RODC or BitLocker

All the users in an AD DS domain exist in the AD DS database. If the database is unavailable for any reason, all operations that depend on domain-based authentication will fail. As a best practice, an AD DS domain should have at least two domain controllers. This makes the AD DS database more available and spreads the authentication load during peak sign-in times.

 **Note:** Consider two domain controllers as the absolute minimum for most enterprises, to ensure high availability and performance.

When you deploy a domain controller in a branch office where physical security is less than optimal, you can use additional measures to reduce the impact of a breach of security. One option is to deploy an RODC.

The RODC contains a read-only copy of the AD DS database, and by default, it does not cache any user passwords. You can configure the RODC to cache the passwords for users in the branch office. If an RODC is compromised, the potential loss of information is much lower than with a full read/write domain controller. Another option is to use BitLocker Drive Encryption to encrypt the domain controller's hard drive. If the hard drive is stolen, BitLocker will help to ensure that a malicious hacker has difficulty getting any useful information from it.

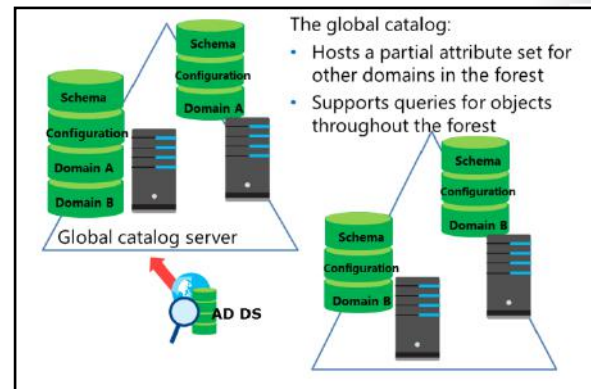
 **Note:** BitLocker is a drive encryption feature that is available for Windows Server operating systems and certain Windows client operating systems. BitLocker encrypts the entire drive to help prevent the computer from starting unless it receives a private key and (optionally) passes an integrity check. A hard drive remains encrypted even if you transfer it to another computer.

## What is a global catalog?

A *global catalog* is a partial, read-only, searchable copy of all the objects in the forest. It speeds up searches for objects that might be stored on domain controllers in a different domain in the forest.

Within a single domain, the AD DS database on each domain controller contains all the information about every object in that domain. However, only a subset of this information is replicated on the global catalog servers in other domains in the forest. Within a particular domain, a query for an object is directed to one of the domain controllers in that domain, but that query does not include results about objects in other domains in the forest. For a query to include results from other domains in the forest, you must query a domain controller that is a global catalog server. By default, the first domain controller in the forest root domain is the only hosted global catalog server. To enhance searching across domains in a forest, you should configure additional domain controllers to each store a copy of the global catalog.

The global catalog does not contain all the attributes for each object. Instead, the global catalog maintains the subset of attributes that are most likely to be useful in cross-domain searches. These attributes include **givenName**, **displayName**, and **mail**. You can modify the set of attributes replicated to the global catalog by modifying the partial attribute set (PAS) in the schema.



For various reasons, you might perform a search against a global catalog rather than a domain controller that is not a global catalog. For example, when a server that is running Exchange Server receives an incoming email, it needs to search for the recipient's account so that it can decide how to route the message. By automatically querying a global catalog, the server that is running Exchange Server can locate the recipient in a multiple domain environment.

For another example, when users sign in to their Active Directory account, the domain controller that performs the authentication must contact a global catalog to check for universal group memberships before the user is authenticated.

In a single domain, you should configure all the domain controllers to hold a copy of the global catalog. However, in a multiple-domain environment, the infrastructure master should not be a global catalog server unless all the domain controllers in the domain are also global catalog servers. When you have multiple sites, you should also make at least one DC at each site a global catalog server, so that you are not dependent on other sites when global catalog queries are required. Deciding which domain controllers should be configured to hold a copy of the global catalog depends on replication traffic and network bandwidth. Many organizations opt to make every domain controller a global catalog server.

## Overview of domain controller SRV records

When users sign in to AD DS, their computer looks in DNS for SRV records to locate the nearest domain controller. SRV records specify information about available services. Each domain controller dynamically registers its addresses in DNS at startup by registering an updated SRV record in DNS.

Clients can locate a suitable domain controller to service their sign-in requests by using DNS lookups which use these SRV records.

SRV records for AD DS are created in the following pattern.

```
_Service._Protocol.DomainName
```

For example, if a client is looking for a server that is running the Lightweight Directory Access Protocol (LDAP) service in the Adatum.com domain, it queries for **\_ldap.\_tcp.Adatum.com**.

### Sites and SRV records

A client uses sites when it needs to contact a domain controller. It starts by looking up SRV records in DNS. The response to the DNS query includes:

- A list of the domain controllers in the same site as the client.
- A list of the domain controllers from the next closest site that does not include an RODC, if no domain controllers were available in the same site and the Try Next Closest Site Group Policy setting is enabled.
- A random list of available domain controllers in the domain, if no domain controller was found in the next closest site.

- Clients find domain controllers through DNS lookup
- Domain controllers dynamically register their addresses with DNS
- The results of DNS queries for domain controllers are returned in this order:
  1. A list of domain controllers in the same site as the client
  2. A list of domain controllers in the next closest site, if none are available in the same site
  3. A random list of domain controllers in other sites, if no domain controller is available in the next closest site



Administrators can define sites in AD DS. When you define sites, you should consider which parts of the network have good connectivity and bandwidth. For example, if a branch office is connected to the main datacenter by an unreliable wide area network (WAN) link, you should define the branch office and the datacenter as separate sites.

The Net Logon service that runs on each domain controller registers the SRV records in DNS. If the SRV records are not entered in DNS correctly, you can trigger the domain controller to reregister those records by restarting the Net Logon service on that domain controller. Note that this process reregisters only the SRV records. If you want to reregister the host (A) record information in DNS, you must run **ipconfig /registerdns** from a command prompt, just as you would for any other computer.

## Demonstration: Viewing the SRV records in DNS

This demonstration shows you how to display the various types of SRV records that the domain controllers register in DNS. These records are crucial to how AD DS operates because they are used to find domain controllers for signing in, changing passwords, and editing GPOs. Domain controllers also use SRV records to find replication partners.

### Demonstration Steps

#### View the SRV records by using DNS Manager

1. On **LON-DC1**, sign in with the user name **Adatum\Administrator** and the password **Pa\$\$w0rd**.
2. Open the **DNS Manager** window, and then explore the DNS domains that begin with an underscore (\_).
3. View the SRV records that are registered by domain controllers.

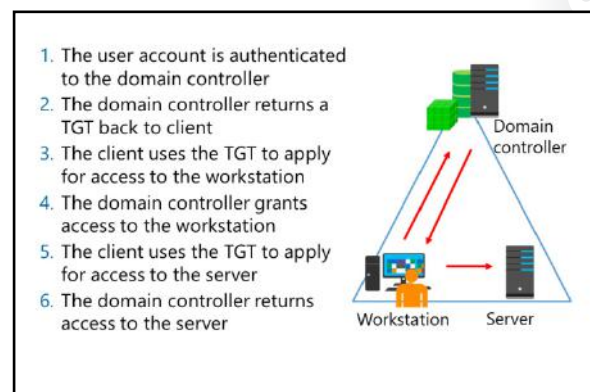


**Note:** These records provide alternate paths so that clients can discover them.

## AD DS sign-in process

When a user attempts to sign in to a computer, the computer first searches for a domain controller to authenticate the user by using DNS lookup. The computer then sends the user's name and password to the domain controller for authentication. The local security authority (LSA) on the domain controller handles the actual authentication process.

If the sign-in succeeds, the LSA builds an access token for the user that contains the security IDs (SIDs) for the user and any groups in which the user is a member. The token provides the access credentials for any process initiated by that user. For example, say that after signing in to AD DS, a user runs Microsoft Word and attempts to open a file. Word then uses the credentials in the user's access token to verify the level of the user's permissions for that file.





**Note:** A SID is a unique string in the form S-R-X-Y1-Y2-Yn-1-Yn. For example, a user SID can be S-1-5-21-322346712-1256085132-1900709958-500.

The following table explains the parts of this SID.

Component	Definition	In the example
S	Indicates that the string is an SID	S
R	Revision level	1
X	Identifier authority value	5 (NT Authority)
Y1-Y2-Yn-1	Domain identifier	21-322346712-1256085132-1900709958
Yn	relative ID (RID)	500

Every user and computer account and every group that you create has a unique SID. They differ from each other only by virtue of the unique RID. The SID in the example is a well-known SID for the domain administrator account. Default accounts and groups use well-known SIDs. The Domain Administrator account's SID always ends with 500.

Although the sign-in process appears to the user as a single event, it is actually made up of two parts:

- The user provides credentials, usually a user account name and password, which are checked against the AD DS database. If the user account name and password match the information that is stored in the AD DS database, the user becomes an authenticated user and is issued a TGT by the domain controller. At this point, the user does not have access to any resources on the network.
- A secondary process in the background submits the TGT to the domain controller and requests access to the local computer. The domain controller issues a service ticket to the user, who then can interact with the local computer. At this point in the process, the user is authenticated to AD DS and signed in to the local computer.

When a user subsequently attempts to connect to another computer on the network, the secondary process runs again, and the TGT is submitted to the nearest domain controller. When the domain controller returns a service ticket, the user can access the computer on the network, which generates a logon event at that computer.



**Note:** A domain-joined computer also signs in to AD DS when it starts—a fact that is often overlooked. You do not see the transaction when the computer uses its computer account name and a password to sign in to AD DS. After it is authenticated, the computer becomes a member of the Authenticated Users group. Although the computer logon event does not have visual confirmation in a GUI, it is recorded in the event log. Also, if auditing is enabled, additional events are recorded in the security log of Event Viewer.

## What are operations masters?

Certain operations can be performed only by a specific role, on a specific domain controller. A domain controller that holds one of these roles is called an *operations master*. An operations master role is also known as a *flexible single master operations (FSMO) role*. Five operations master roles exist, and all five can be located on a single domain controller or they can be spread across several domain controllers. By default, the first domain control installed in a forest contains all five roles. However, these roles can be moved after more domain controllers are built. By

allowing changes only on a single domain controller, the operations master roles help to prevent conflicts in AD DS caused by replication latency. When making changes to data held on one of the operations masters, you must connect to the domain controller that holds the role.

The five operations master roles are distributed as follows:

- Each forest has one schema master and one domain naming master.
- Each AD DS domain has one RID master, one infrastructure master, and one primary domain controller (PDC) emulator.

### Forest operations masters


A forest contains the following single master roles:

- Domain naming master. This is the domain controller that must be contacted when you add or remove a domain or make domain name changes.

If the domain naming master is unavailable, you will not be able to add domains to the forest.

- Schema master. This is the domain controller in which you make all schema changes. To make changes, you typically sign in to the schema master as a member of both the Schema Admins and the Enterprise Admins group. A user who is a member of both of these groups and who has the appropriate permissions can also edit the schema by using a script.

If the schema master is unavailable, you will not be able to make changes to the schema. This prevents the installation of applications that require schema changes, such as Exchange Server.

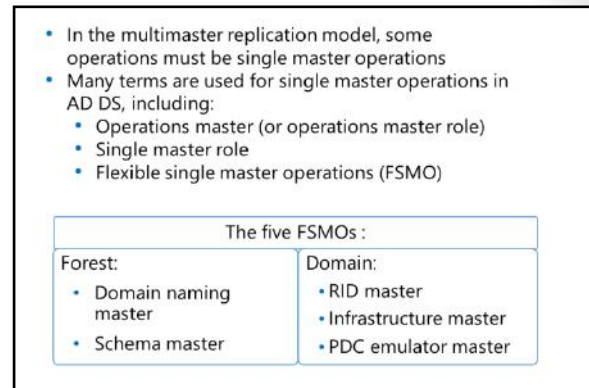
 **Note:** The Windows PowerShell command **Get-ADForest**, from the Active Directory module for Windows PowerShell, shows the forest properties, including the current domain naming master and schema master.

### Domain operations masters

A domain contains the following single master roles:

- RID master. Whenever an object is created in AD DS, the domain controller where the object is created assigns the object a unique identifying number known as a SID. To ensure that no two domain controllers assign the same SID to two different objects, the RID master allocates blocks of RIDs to each domain controller within the domain to use when building the SID.

If the RID master is unavailable, you might experience difficulties adding new objects to the domain. As domain controllers use their existing RIDs, they eventually run out of them and are unable to create new objects.



- Infrastructure master. This role maintains interdomain object references, such as when a group in one domain contains a member from another domain. In this situation, the infrastructure master is responsible for maintaining the integrity of this reference. For example, when you look at the **Security** tab of an object, the system looks up the SIDs that are listed and translates them into names. In a multiple-domain forest, the infrastructure master looks up SIDs from other domains.

If the infrastructure master is unavailable, domain controllers that are not global catalogs will not be able to check universal group memberships or to authenticate users.


The infrastructure role should not reside on a global catalog server, unless you have a single-domain forest. The exception is when you follow best practices and make every domain controller a global catalog. In that case, the infrastructure role is not required because every domain controller knows about every object in the forest.


- PDC emulator master. The domain controller that holds the PDC emulator master is the time source for the domain. The PDC emulator masters in each domain in a forest synchronize their time with the PDC emulator master in the forest root domain. You set the PDC emulator master in the forest root domain to synchronize with a reliable external time source.

The PDC emulator master is also the domain controller that receives urgent password changes. If a user's password is changed, the information is immediately sent to the domain controller holding the PDC emulator master role. This means that if the user tries to sign in, even if the user had been authenticated by a domain controller in a different location that had not yet received the new password information, the domain controller in the user's current location will contact the domain controller holding the PDC emulator master role to check for recent changes.

If the PDC emulator master is unavailable, users might have trouble signing in until their password changes have replicated to all the domain controllers.

The PDC emulator master is also used for editing GPOs. When a GPO other than a local GPO is opened for editing, the edited copy is stored on the PDC emulator master. This prevents conflicts if two administrators attempt to edit the same GPO at the same time on different domain controllers. However, you can choose to use a specific domain controller to edit the GPOs. This is especially useful when editing GPOs in a remote office with a slow connection to the PDC emulator.

 **Note:** The Windows PowerShell command **Get-ADDomain**, from the Active Directory module for Windows PowerShell, shows the domain properties, including the current RID master, infrastructure master, and PDC emulator master.

 **Note:** The global catalog is not one of the operations master roles.

## Transferring and seizing roles

In an AD DS environment where FSMO roles are split among domain controllers, you might need to move a role from one domain controller to another. When you plan this role move—for example, to decommission servers or balance workloads—the move is known as *transferring* the role. If you do not plan the move—for example, in the case of a hardware or system failure—the move is known as *seizing* the role.

For transferring a role, the latest data from the domain controller in that role is replicated to the target server. You should seize a role only as a last resort. For seizing a role, the original domain controller is not available, so the available data might be incomplete or out of date.

- Transferring is:
  - Planned
  - Done with the latest data
  - Performed through snap-ins, Windows PowerShell, or ntdsutil.exe
- Seizing is:
  - Unplanned and a last resort
  - Done with incomplete or out-of-date data
  - Performed through Windows PowerShell or ntdsutil.exe

### Transferring FSMO roles

You can transfer FSMO roles through the GUI by using the AD DS snap-ins that are listed in the following table.

Role	Snap-in
Schema master	Active Directory Schema
Domain naming master	Active Directory Domains and Trusts
Infrastructure master	Active Directory Users and Computers
RID master	Active Directory Users and Computers
PDC emulator	Active Directory Users and Computers

### Seizing FSMO roles

You cannot use the snap-ins to seize FSMO roles. Instead, you must use the ntdsutil.exe command-line tool or Windows PowerShell to seize roles. You can also use these tools to transfer roles.

The syntax for transferring or seizing a role is similar within Windows PowerShell, as shown in the following syntax line.

```
Move-ADDirectoryServerOperationsMasterRole -Identity "<servername>" -OperationsMasterRole <rolenamelist> -Force
```

For the preceding syntax, the noteworthy definitions are as follows:

- *<servername>*. The name of the target domain controller to transfer one or more roles to.
- *<rolenamelist>*. A comma-separated list of AD DS role names to move to the target server.
- **-Force**. An optional parameter that you include to seize a role instead of simply transfer it.



**Additional Reading:** For more information on using Windows PowerShell to transfer or seize FSMO roles, refer to: "Move (Transferring or Seizing) FSMO Roles with AD-Powershell Command to Another Domain Controller" at: <http://aka.ms/Rn7kfi>



**Additional Reading:** For information on using ntdsutil.exe to transfer or seize FSMO roles, refer to: "Using Ntdsutil.exe to transfer or seize FSMO roles to a domain controller" at: <http://aka.ms/Npye86>

**Question:** Should a domain controller be a global catalog?

**Question:** Verify the correctness of the statement by placing a mark in the column to the right.

Statement	Answer
In a multiple-domain forest, a copy of the global catalog should be stored on every domain controller.	

## Lesson 3

# Deploying a domain controller

Sometimes you need to install additional domain controllers in your Windows Server 2016 domain. Several reasons exist for why you might want to do this:

- You need additional resources at a site because the existing domain controllers are overworked.
- You are opening a new remote office that requires you to deploy one or more domain controllers.
- You are creating an off-site disaster recovery location.

The installation method that you use varies with the circumstances.

This lesson examines several ways to install additional domain controllers. These include installing AD DS on a local computer and on a remote server by using Server Manager, installing AD DS on a Server Core installation, and installing AD DS by using a snapshot of the AD DS database that is stored on removable media. This lesson also examines how to upgrade a domain controller from an earlier Windows operating system to Windows Server 2016. Finally, the lesson discusses Azure AD and how to install a domain controller in Azure.

### Lesson Objectives

After completing this lesson, you should be able to:

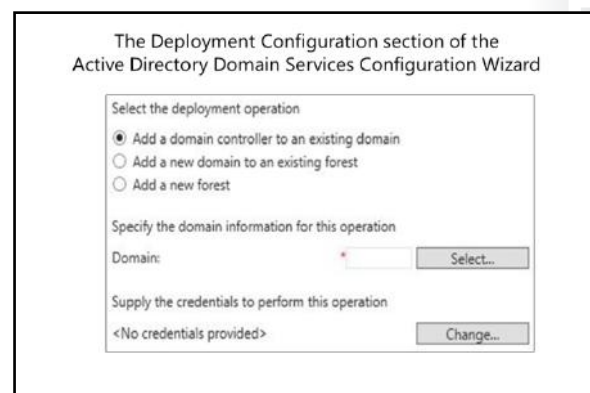
- Explain how to install a domain controller by using the GUI.
- Explain how to install a domain controller on a Server Core installation of Windows Server 2016.
- Explain how to upgrade a domain controller by installing from media.
- Explain how to install a domain controller by installing from media.
- Describe the process of cloning domain controllers.
- Explain best practices for virtualizing domain controllers.

### Installing a domain controller from Server Manager

The domain controller installation and promotion has two steps. First, you need to install the files that the domain controller role uses. You do this by installing the AD DS role using Server Manager. At the end of the initial installation process, the AD DS files are installed but AD DS is not yet configured on the server.


To configure AD DS, you use the **Active Directory Domain Services Configuration Wizard**. You start the wizard by clicking the AD DS link in Server Manager. The wizard allows you to do one of the following:

- Add a domain controller to an existing domain.
- Add a new domain to an existing forest.
- Add a new forest.





Before installing a new domain controller, you need to have answers to the questions in the following table.

Question	Comments
Are you installing a new forest, a new tree, or an additional domain controller for an existing domain?	Answering this question determines what additional information you might need, such as the parent domain name.
What is the DNS name for the AD DS domain?	When you create the first domain controller for a domain, you must specify the fully qualified domain name (FQDN). When you add a domain controller to an existing domain or forest, the wizard provides the existing domain information.
What will you set the forest functional level at?	The forest functional level determines the forest features that will be available and the supported domain controller operating system. This also sets the minimum domain functional level for the domains in the forest.
What will you set the domain functional level at?	The domain functional level determines the domain features that will be available and the supported domain controller operating system.
Will the domain controller be a DNS server?	Your DNS must be functioning well to support AD DS.
Will the domain controller host the global catalog?	This option is selected by default for the first domain controller in a forest, and it cannot be changed.
Will the domain controller be an RODC?	This option is not available for the first domain controller in a forest.
What will the Directory Services Restore Mode (DSRM) password be?	This is required to recover the AD DS database from a backup.
What is the NetBIOS name for the AD DS domain?	When you create the first domain controller for a domain, you must specify the NetBIOS name for the domain.
Where will the database, log files, and SYSVOL folders be created?	By default, the database and log files folder is C:\Windows\NTDS. By default, the SYSVOL folder is C:\Windows\SYSVOL.

 **Note:** If you need to restore the AD DS database from a backup, restart the domain controller in DSRM. The typical process to enter DSRM is to restart the domain controller and then press F8 during the initial startup process. When the domain controller starts, it is not running the AD DS services. Instead, it is running as a member server in the domain. To sign in to that server in the absence of AD DS, use the DSRM password.



 **Note:** Windows Server 2016 supports cloning AD DS servers. Before it is cloned, an AD DS server must be a member of the Cloneable Domain Controllers group. Additionally, the PDC emulator must be online and available to the cloned DC, and it must be running Windows Server 2016.

 **Note:** The **Active Directory Domain Services Installation Wizard (dcpromo.exe)**, commonly used to install domain controllers in Windows Server 2008 and earlier, is obsolete starting with Windows Server 2012.

## Installing a domain controller on a Server Core installation of Windows Server 2016

A Windows Server 2016 server that is running a Server Core installation does not have the Server Manager GUI, so you need to use alternative methods to install the files for the domain controller role and to install the domain controller role itself. You can use Server Manager, Windows PowerShell, or Remote Server Administration Tools (RSAT) installed on a client running Windows 8.1 or later.


To install the AD DS files on the server, you can do one of the following:

- Use Server Manager to connect remotely to the server running the Server Core installation, and then install the AD DS role as described in the previous topic.
- Use the Windows PowerShell command **Install-WindowsFeature AD-Domain-Services** to install the files.

- Using Server Manager:
  1. Install the AD DS role
  2. Run the Active Directory Domain Services Configuration Wizard
- Using Windows PowerShell:
  1. Install the files by running the command **Install-WindowsFeature AD-Domain-Services**
  2. Install the domain controller role by running the command **Install-ADDSDomainController**

After you install the AD DS files, you can complete everything, except for the hardware installation and configuration, in one of the following ways:

- Use Server Manager to start the Active Directory Domain Services Configuration Wizard as described in the previous topic.
- Run the Windows PowerShell cmdlet **Install-ADDSDomainController**, supplying the required information on the command line.

 **Note:** In Windows Server 2016, running a cmdlet automatically loads the cmdlets' module, if it is available. For example, running the **Install-ADDSDomainController** cmdlet automatically loads the **ADDSDeployment** module into your current Windows PowerShell session. If a module is not loaded or available, you will receive an error message when you run the cmdlet that says it is not a valid cmdlet.

You can still manually import the module that you need. However, you do not need to do this in Windows Server 2016, unless you have an explicit need to do so, such as pointing to a particular source to install the module.

**Additional Reading:**

- For more information on using the Windows PowerShell cmdlet **Install-ADDSDomainController**, refer to: "Install Active Directory Domain Services (Level 100)" at: <http://aka.ms/A9jlvk>
- For more information, refer to: "AD DS Deployment Cmdlets in Windows PowerShell" at: <http://aka.ms/Lnxifx>

## Upgrading a domain controller

The process for upgrading a domain controller is the same for any version of Windows Server starting from Windows Server 2008 through Windows Server 2016. You can upgrade to a Windows Server 2016 domain in one of the following two ways.

- You can upgrade the operating system on existing domain controllers that are running Windows Server 2008 or later.
- You can add servers running Windows Server 2016 as domain controllers in a domain that already has domain controllers running earlier versions of Windows Server.

**Options to upgrade AD DS to Windows Server 2016:**

- Perform an in-place upgrade from Windows Server 2008 or later to Windows Server 2016:
  - Benefit: Except for the prerequisite checks, all the files and programs stay in place, and no additional work is required
  - Risk: It might leave obsolete files and dynamic-link libraries (DLLs)
- Introduce a new server running Windows Server 2016 into the domain, and then promote it to be a domain controller (this option is usually preferred):
  - Benefit: The new server has no obsolete files and settings
  - Risk: It might require additional work to migrate administrators' files and settings

Of the two methods, the latter is preferred because when you finish, you will have a clean installation of the Windows Server 2016 operating system and the AD DS database. Whenever a new domain controller is added, the domain DNS records are updated, and clients will immediately find and use this domain controller.

### Upgrading to Windows Server 2016

To upgrade an AD DS domain running at the functional level of an earlier version of Windows Server to an AD DS domain running at the functional level of Windows Server 2016, you must first upgrade all the domain controllers to the Windows Server 2016 operating system. You can perform this upgrade by upgrading all of the existing domain controllers to Windows Server 2016 or by introducing new domain controllers that are running Windows Server 2016 and then phasing out the existing domain controllers.


An in-place operating system upgrade does not perform automatic schema and domain preparation. To perform an in-place upgrade of a computer that has the AD DS role installed, you must first use the command-line commands **adprep.exe /forestprep** and **adprep.exe /domainprep** to prepare the forest and domain. The **adprep** tool is included on the installation media in the `\Support\Adprep` folder. No additional configuration steps exist after that point, and you can continue to run the Windows Server 2016 operating system upgrade.

When you promote a server running Windows Server 2016 to be a domain controller in an existing domain, and you are signed in as a member of the Schema Admins and Enterprise Admins groups, the AD DS schema automatically updates to Windows Server 2016. In this scenario, you do not need to run the **adprep** command before you start the installation.

## Deploying Windows Server 2016 domain controllers

To upgrade the operating system of a domain controller running Windows Server 2008 or later to Windows Server 2016, perform the following steps:

1. Insert the installation disk for Windows Server 2016, and then run **Setup**. The **Windows Setup Wizard** opens.
2. After the **Language Selection** page appears, click **Install now**.
3. After the **Operating System Selection** page and the **License Acceptance** page appears, on the **Which type of installation do you want?** page, click **Upgrade: Install Windows and keep files, settings, and applications**.

 **Note:** With this type of upgrade, you do not need to preserve users' settings and reinstall applications; everything is upgraded in place. Remember to check for hardware and software compatibility before you perform an upgrade.

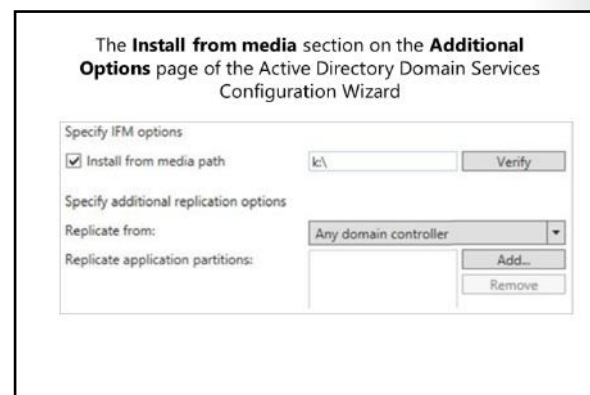
To introduce a clean installation of Windows Server 2016 as a domain controller, perform the following steps:

1. Deploy and configure a new installation of Windows Server 2016, and then join it to the domain.
2. Promote the new server to be a domain controller in the domain by using Server Manager or one of the other methods described previously.
3. Update the client DNS settings that refer to the old domain controllers to use the new domain controller.

## Installing a domain controller by installing from media

If you have a network connection between sites that is slow, unreliable, or costly, you might find it necessary to add another domain controller at a remote location or branch office. In this scenario, it is often better to deploy AD DS to a server by installing it from media rather than by deploying it over the network.

For example, if you connect to a server that is in a remote office and use Server Manager to install AD DS, the entire AD DS database and the SYSVOL folder will be copied to the new domain controller over a potentially unreliable WAN connection. As an alternative and to significantly reduce the amount of traffic moving over the WAN link, you can create a backup of AD DS (perhaps to a USB drive) and take this backup to the remote location. When you are at the remote location and run Server Manager to install AD DS, you can select the **Install from media** option. Most of the copying is then done locally, and the WAN link is used only for security-related traffic and to help ensure that the new domain controller receives any changes that were made to the central AD DS after you created the **Install from media** backup.



To install a domain controller by installing from media, browse to a domain controller that is not an RODC. Use the **ntdsutil** command-line tool to create a snapshot of the AD DS database, and then copy the snapshot to the server that will be promoted to a domain controller. Use Server Manager to promote the server to a domain controller by selecting the **Install from Media** option and then providing the local path to the **Install from media** directory that you previously created.

The procedure is as follows:

1. On the full domain controller, at an administrative command prompt, type the following commands (where C:\IFM is the destination directory that will contain the snapshot of the AD DS database).

```
Ntdstl
Activate instance ntds
Ifm
create SYSVOL full C:\IFM
```

2. On the server that you are promoting to a domain controller, perform the following steps:

- a. Use **Server Manager** to add the AD DS role.
- b. Wait while the AD DS files install.
- c. In **Server Manager**, click the **Notification** icon, and then under **Post-Deployment Configuration**, click **Promote this server to a domain controller**.

The Active Directory Domain Services Configuration Wizard runs.

- d. On the appropriate page of the wizard, select the **Install from media** option, and then provide the local path to the snapshot directory.

AD DS installs from the snapshot.

3. Note that when the domain controller restarts, it contacts the other domain controllers in the domain and updates AD DS with any changes that were made after the snapshot was created.



**Additional Reading:** For more information on the steps required to install AD DS, refer to "Install Active Directory Domain Services (Level 100)" at: <http://aka.ms/Rvcwlz>

## Cloning domain controllers

The fastest way to deploy multiple computers that are identically configured, especially when those computers run in a virtualized environment such as Microsoft Hyper-V, is to clone those computers. Cloning means that the virtual hard disks of the computers are copied, and minor configurations such as computer names and IP addresses are changed to be unique. Then the computers are instantly operational. This process, also referred to as *provisioning* computers, is one main technology of private clouds. Prior to Windows Server 2012, you were able to clone domain members, but you were not able to clone domain controllers. In Windows Server 2016, as in Windows Server 2012, you are able to clone domain controllers.

- You might clone domain controllers for:
  - Rapid deployment
  - Private clouds
  - Recovery strategies
- To clone a source domain controller:
  - Add the domain controller to the Cloneable Domain Controllers group
  - Verify app and service compatibility
  - Create a DCCloneConfig.xml file
  - Export it once, and then create as many clones as needed
  - Start the clones

The following scenarios benefit from virtual domain controller cloning:

- Rapidly deploying additional domain controllers in a new domain.
- Quickly restoring business continuity during disaster recovery by restoring AD DS capacity via the rapid deployment of domain controllers by using cloning.
- Optimizing private cloud deployments by taking advantage of the flexible provisioning of domain controllers to accommodate increased scale requirements.
- Rapidly provisioning test environments, which allows for the deployment and testing of new features and capabilities before a production rollout.
- Quickly meeting increased capacity needs in branch offices either by cloning existing domain controllers in branch offices or by cloning them in the datacenter and then transferring them to branches by using Hyper-V.

Cloning domain controllers requires the following:

- A hypervisor that supports virtual machine generation identifiers, such as Hyper-V in Windows Server 2012 and later.
- Domain controllers as guest operating systems based on Windows Server 2012 and later.
- The domain controller to clone, or a source domain controller, that must run as a virtual machine guest on the supported hypervisor.
- A PDC emulator that runs on Windows Server 2012 or later. Although it is possible to clone domain controllers running Windows Server 2012 when earlier versions of domain controllers exist, the domain controller that holds the PDC emulator FSMO role needs to support the cloning process. The PDC emulator must be online when the virtual domain controller clones start for the first time.

To help ensure that cloning virtualized domain controllers is authorized by the AD DS administrators, a member of the Domain Admins group needs to prepare a computer to be cloned. Hyper-V administrators are unable to clone a domain controller without AD DS administrators, and vice versa.

### Preparing the source virtual domain controller

To prepare to deploy virtual domain controllers, follow these steps:

1. Add the source domain controller to the group Cloneable Domain Controllers.
2. Verify that the apps and services on the source domain controller support the cloning process. You can do this by running the following Windows PowerShell cmdlet.

```
Get-ADDCCloneingExcludedApplicationList
```

If apps or services that do not support cloning exist, you need to remove or test them first. If they work after cloning, put the apps or services in the CustomDCCloneAllowList.xml file. You can create CustomDCCloneAllowList.xml by using the same cmdlet, appending the parameter *GenerateXML*, and optionally appending the parameter *-Force* if an existing CustomDCCloneAllowList.xml file should be overwritten, as shown in the following syntax.

```
Get-ADDCCloneingExcludedApplicationList -GenerateXML [-Force]
```

3. Create a DCCloneConfig.xml file. You need to create this file so that the cloning process recognizes it and creates a new domain controller from the clone. By creating this file, you can specify a custom computer name, TCP/IP address settings, and the site name where the new domain controller should reside. If you do not specify one or all of these parameters, a computer name is automatically generated, and the IP address settings are set to **dynamic**. This requires a Dynamic Host Configuration Protocol (DHCP) server on the network and assumes that the domain controller clones reside in the same site as the source domain controller. You can use Windows PowerShell to create the DCCloneConfig.xml file, as shown in the following syntax.

```
New-ADDCCloneConfigFile [-CloneComputerName <String>] [-IPv4DNSResolver <String[]>]
[-Path <String>] [-SiteName <String>]
```

If you want to create more than one clone, and you want to specify settings such as computer names and TCP/IP addressing information, you need to modify the DCCloneConfig.xml file or create a new, individual one for each clone prior to starting it for the first time.

4. Export the source virtual domain controller.

### Preparing multiple domain controller clones

If you want to prepare multiple domain controller clones, do not provide any additional parameters, and let the computer name be automatically generated. In addition, use DHCP to provide TCP/IP addressing information.

Alternatively, you can customize each clone by creating individual DCCloneConfig.xml files. To do this, follow these steps:

1. Create the cloned virtual hard disks by exporting and importing the virtual computer.
2. Mount the newly cloned virtual hard disks by doing one of the following:
  - o Double-click them in File Explorer.
  - o Use **Diskpart.exe** with the **assign** command at an elevated command prompt.
  - o Use the **Mount-DiskImage** Windows PowerShell cmdlet.
3. Use the *-Offline* and *-Path* parameters with the **New-ADDCCloneConfigFile** cmdlet. Change **E** to the drive letter that you used when mounting the .vhdx file in the previous step, as shown in the following cmdlet.

```
New-ADDCCloneConfigFile -CloneComputerName <LON-DC3> -Offline -Path
<E>:\Windows\NTDS
```

4. Unmount the virtual hard disk files by using **Diskpart.exe** or the **Dismount-DiskImage** Windows PowerShell cmdlet.

### Using dynamically assigned computer names

If you do not configure DCCloneConfig.xml with a static computer name—for example, to create multiple clones without individual configurations—the computer name of the new clone is automatically generated based on the following algorithm:

- The prefix consists of the first eight characters of the computer name of the source domain controller. For example, the source computer name *SourceComputer* is abbreviated into the prefix *SourceCo*.
- A unique naming suffix of the format *-CLnnnn* is appended to the prefix, where *nnnn* is the next available value from 0001 through 9999 that the PDC emulator determines is not currently in use.

## Creating the virtual domain controller clones

To create the virtual domain controller clones, follow these steps:

1. Ensure that the domain controller, which holds the PDC emulator FSMO role, runs on Windows Server 2012 or later.
2. Ensure that the PDC emulator and a domain controller hosting the global catalog are online.
3. By using the exported files from the preparation steps, use the **import** function to create as many clones as needed. When using Hyper-V, select **Copy the virtual machines (create a new unique ID)** to allow you to import multiple individual instances of the same exported computer.
4. Individually configure clones as required by following the previously outlined steps.
5. Start the clones.

## Finalizing the domain controller cloning

When a new domain controller clone starts, the following steps are automatically performed:

1. The clone checks whether a virtual machine generation identifier exists. This is required, and if a virtual machine generation identifier does not exist, the computer either starts normally when no DCCloneConfig exists or renames DCCloneConfig and restarts in DSRM. Starting in DSRM is a safeguard, and a domain administrator needs to pay close attention and fix the issue to make the domain controller work as intended.
2. The clone checks whether the virtual machine generation identifier changed, and takes one of the following actions, accordingly:
  - o If it did not change, it is the original source domain controller. If DCCloneConfig exists, it is renamed. In both cases, a normal startup occurs, and the domain controller is functional again.
  - o If it did change, the virtualization safeguards trigger, and the process continues.
3. The clone checks whether DCCloneConfig exists. If not, a check for a duplicate IP address decides whether to start normally or in DSRM. If the DCCloneConfig file exists, the computer gets the new computer name and IP address settings from the file. The AD DS database is modified, and the initialization steps are performed so that a new domain controller is created.

## Demonstration: Cloning a domain controller

In this demonstration, you will learn how to:

- Prepare a source domain controller to be cloned.
- Export the source virtual machine.
- Create and start the cloned domain controller.

### Demonstration Steps

#### Prepare a source domain controller to be cloned

1. On **LON-DC1** open **Active Directory Administrative Center**.
2. Add the domain controller **LON-DC1** to the group **Cloneable Domain Controllers**.
3. Verify that the apps and services on **LON-DC1** support cloning.
4. Create the **DCCloneConfig.xml** file, for cloning **LON-DC3**.
5. Shut down **LON-DC1**.

### Export the source virtual machine

1. On the host computer, in Hyper-V Manager, export **LON-DC1**.
2. Restart **LON-DC1**.

### Create and start the cloned domain controller

1. Import a new virtual machine by using the exported files.
2. Name the new virtual machine **20742A-LON-DC3**, and then select **Copy the virtual machine (create a new unique ID)**.
3. In Hyper-V Manager, start **LON-DC3**.

## Best practices for domain controller virtualization

Virtualization provides many benefits, such as hardware independence, the efficient use of resources, and scalability in private cloud scenarios. It also provides flexibility when you move virtual machines across virtualization infrastructures. In the past, virtualizing domain controllers required the administrators of the virtual infrastructure to know the requirements specific to AD DS and to take precautions to prevent adding risks to an AD DS infrastructure.

When considering virtual domain controllers, you should know about the following best practices:

- Avoid single points of failure
- Use the time services
- Use virtualization technology with the virtual machine generation identifier feature
- Use Windows Server 2012 or later as virtualization guests
- Avoid or disable checkpoints
- Be aware of improving security
- Consider taking advantage of cloning in your deployment or recovery strategy
- Start a maximum number of 10 new clones at the same time
- Consider using virtualization technologies that allow virtual machine guests to move between sites
- Adjust your naming strategy to allow for domain controller clones

- Avoid single points of failure. Ensure that you have at least two virtualized domain controllers per domain on different virtualization hosts, which reduces the risk of losing all domain controllers if a single virtualization host fails. Also, diversify the hardware, storage networks, and storage systems. Ensure that you maintain domain controllers in different datacenters or regions to reduce the impact of disasters.
- Verify time services. Ensure that all computers, including the hypervisor host and domain controller guests, are participating in the same time services infrastructure. Also, ensure that the time on the host and on the guests does not differ.
- Use virtualization technology that allows for virtual machine generation identifiers. Only virtualization infrastructures that support the new virtual machine generation identifiers also support the safeguards and cloning of virtual domain controllers.
- Use Windows Server 2012 or later as the guest operating system for virtual domain controllers. Only these versions support the safeguards for virtual domain controllers.
- Avoid or disable checkpoints. If the virtualization host or the guest operating systems of the domain controllers do not support the safeguards for virtualizing domain controllers, disable the possibility of creating checkpoints—for example, by using a pass-through disk instead of a virtual hard disk. When the safeguards are supported, use a virtual hard disk to support cloning, but avoid using checkpoints.
- Be aware of improving security, and help to ensure that the virtualization administrators are as trusted as your domain admins.
- Consider taking advantage of cloning. Cloning can be a deployment or a recovery strategy. It helps to provide a fast and simple way to create many domain controllers in a short time.



- Clone in batches of 10 at a maximum. Do not start more than 10 new clones at the same time, because the file replication used for SYSVOL allows only 10 replication connections at the same time.
- Consider using virtualization technologies that allow you to move virtual machines across site boundaries. This can be beneficial in your deployment and recovery strategies. For example, you can create 10 clones in a central location and then move them to remote offices during off-peak hours.
- Adjust your naming strategy to allow for domain controller clones. It might be possible to adjust your naming strategy to allow cloned domain controllers to retain the first eight characters of the source domain controller name, and then have -CLnnnn attached.



**Additional Reading:** For more information on virtualizing domain controllers, refer to: "Running Domain Controllers in Hyper-V" at: <http://aka.ms/Tjil9g>

**Question:** What is the fastest way to replicate domain controllers in a virtualized environment?

**Question:** What are the two major considerations for deploying domain controllers to Azure?

## Lab: Deploying and administering AD DS

### Scenario

You are an IT administrator at A. Datum Corporation. The company is expanding its business and has several new locations. The AD DS administration team is currently evaluating the methods available in Windows Server 2016 for a rapid and remote domain controller deployment. Also, the team is looking for a way to automate certain AD DS administrative tasks. The team wants a fast and seamless deployment of new domain controllers for new locations, and it wants to promote servers to domain controllers from a central location.

### Objectives

After completing this lab, you will be able to:

- Deploy AD DS.
- Deploy domain controllers by performing domain controller cloning.
- Administer AD DS.

### Lab Setup

Estimated Time: **45 minutes**

Virtual machines: **20742A-LON-DC1**, **20742A-LON-DC2**, and **20742A-LON-SVR1**

User name: **Adatum\Administrator**

Password: **Pa\$\$w0rd**

For this lab, you will use the available virtual machine environment. Before you begin the lab, complete the following steps:

1. On the host computer, start **Hyper-V Manager**.
2. In Hyper-V Manager, click **20742A-LON-DC1**, and in the **Actions** pane, click **Start**.
3. In the **Actions** pane, click **Connect**. Wait until the virtual machine starts.
4. Sign in by using the following credentials:
  - o User name: **Adatum\Administrator**
  - o Password: **Pa\$\$w0rd**
5. Repeat steps 2 through 4 for virtual machines **20742A-LON-DC2** and **20742A-LON-SVR1**.

## Exercise 1: Deploying AD DS

### Scenario


As a part of the business expansion, A. Datum Corporation wants to deploy new domain controllers in remote sites with minimal engagement from the remote IT staff. You will use Windows PowerShell to deploy new domain controllers.


The main tasks for this exercise are as follows:

1. Install AD DS binaries.
2. Prepare the AD DS installation and promote a remote server.
3. Run the AD DS Best Practices Analyzer.

### ► Task 1: Install AD DS binaries

1. Switch to **LON-DC1**.
2. From **Server Manager**, open **Windows PowerShell**.
3. Use the **Install-WindowsFeature** cmdlet in Windows PowerShell to install the AD DS role on **LON-SVR1**.
4. Use the **Get-WindowsFeature** cmdlet to verify the installation.
5. Ensure that the check boxes for **Active Directory Domain Services**, **Remote Server Administration Tools** and **Role Administration Tools** are selected. For the node **AD DS and AD LDS Tools**, only the **Active Directory module for Windows PowerShell** should be installed, and not the graphical tools, such as the **Active Directory Administrative Center**.

 **Note:** If you centrally manage your servers, you will not usually need GUI tools on each server. If you want to install them, you need to specify the AD DS tools by running the **Add-WindowsFeature** cmdlet with the **RSAT-ADDS** command name.

 **Note:** You might need to wait a short period of time after the installation process completes before verifying that the AD DS role has been installed. If you do not see the expected results from the **Get-WindowsFeature** command, you can try again after a few minutes.

### ► Task 2: Prepare the AD DS installation and promote a remote server

#### Add LON-SVR1 to Server Manager on LON-DC1

- On **LON-DC1**, from **Server Manager**, on the **All Servers** node, add **LON-SVR1** as a managed server.

#### Remotely configure AD DS by using Server Manager

1. On **LON-DC1**, from **Server Manager**, configure **LON-SVR1** as an AD DS domain controller by using the following settings:
  - Type: **Additional domain controller for existing domain**
  - Domain: **Adatum.com**
  - Credentials: **Adatum\Administrator** with the password of **Pa\$\$w0rd**
  - Directory Services Restore Mode (DSRM) Password: **Pa\$\$w0rd**
  - Remove the selections for DNS and the global catalog.
2. On the **Review Options** page, click **View Script**.
3. In Microsoft Notepad, edit the generated Windows PowerShell script:
  - Delete the comment lines, which begin with the number sign (#).
  - Remove the **Import-Module** line.
  - Remove the grave accents (`) at the end of each line.
  - Remove the line breaks.
4. Now that the Install-ADDSDomainController command and all the parameters are on one line, copy the command.
5. Switch to the **Active Directory Domain Services Configuration Wizard**, and then click **Cancel**.

6. Start **Windows PowerShell**, and at the command prompt, type the following command:

```
Invoke-Command -ComputerName LON-SVR1 { }
```

7. Paste the copied command between the braces ( { } ), and then press Enter to start the installation.
8. Provide the following credentials:
  - o User name: **Adatum\Administrator**
  - o Password: **Pa\$\$w0rd**
9. Type and confirm the **SafeModeAdministratorPassword** as **Pa\$\$w0rd**.
10. After **LON-SVR1** restarts, on **LON-DC1**, switch to **Server Manager**, and on the left side, click the **AD DS** node. Note that **LON-SVR1** has been added as a server and that the warning notification has disappeared. You might have to click **Refresh**.

### ► Task 3: Run the AD DS Best Practices Analyzer

1. On **LON-DC1**, in **Server Manager**, go to the AD DS dashboard view.
2. Start the **BPA** scan for **LON-DC1** and **LON-SVR1**.
3. Review the results of the BPA.

**Results:** After this exercise, you should have successfully created a new domain controller and reviewed the AD DS Best Practices Analyzer (BPA) results for that domain controller.

## Exercise 2: Deploying domain controllers by performing domain controller cloning

### Scenario

An IT team at A. Datum Corporation wants to rapidly deploy new virtual domain controllers when they are needed. They are considering the domain controller clones in Windows Server 2016. You must perform a domain controller cloning procedure to verify that it is a valid option to speed up the deployment of domain controllers.

The main tasks for this exercise are as follows:

1. Check for domain controller clone prerequisites.
2. Copy the source domain controller.
3. Perform domain controller cloning.

### ► Task 1: Check for domain controller clone prerequisites

1. Switch to **LON-DC1**.
2. In **Server Manager**, open the **Active Directory Administrative Center** and add **LON-DC1** to the group **Cloneable Domain Controllers**.
3. Open **Windows PowerShell** and use **Get-ADDCCloningExcludedApplicationList** to verify that the apps and services on **LON-DC1** support cloning.
4. Use the **Get-ADDCCloningExcludedApplicationList -GenerateXML** and **New-ADDCCloneConfigFile** cmdlets to create a **DCCloneConfig.xml** file.

► **Task 2: Copy the source domain controller**

1. Shut down **LON-DC1**.
2. On the host computer, in Hyper-V Manager, export **LON-DC1** to **D:\Program Files\Microsoft Learning\20742\**.
3. Start **LON-DC1**, and then sign in as **Adatum\Administrator** with the password **Pa\$\$w0rd**.

► **Task 3: Perform domain controller cloning**

1. On the host computer, start the **Import Virtual Machine Wizard** in Hyper-V Manager.
2. On the **Locate Folder** page, go to the **D:\Program Files\Microsoft Learning\20742\20742A-LON-DC1** folder.
3. On the **Select Virtual Machine** page, select **20742A-LON-DC1**.
4. On the **Choose Import Type** page, select **Copy the virtual machine (create a new unique ID)**.
5. On the **Choose Folders for Virtual Machine Files** page, select the **Store the virtual machine in a different location** check box. For each folder location, provide the path **D:\Program Files\Microsoft Learning\20742\**.
6. On the **Choose Folders to Store Virtual Hard Disks** page, provide the path **D:\Program Files\Microsoft Learning\20742\**.
7. Rename the new virtual machine **20742A-LON-DC3**.
8. In Hyper-V Manager, start and connect to **20742A-LON-DC3**.
9. While the server is starting, you may see the message **Domain Controller cloning is at x% completion**.

**Results:** After completing this exercise, you should have successfully deployed a domain controller by cloning it in Hyper-V.

## Exercise 3: Administering AD DS

### Scenario

The IT team at A. Datum Corporation is evaluating the tools that are available in Windows Server 2016 for AD DS administration. You should evaluate the use of both the Active Directory Administrative Center and Windows PowerShell for AD DS administration and management.

The main task for this exercise is as follows:

1. Use the Active Directory Administrative Center.
2. Prepare for the next module.

► **Task 1: Use the Active Directory Administrative Center**

### Navigate within the Active Directory Administrative Center

1. On **LON-DC1**, from **Server Manager**, open the **Active Directory Administrative Center**.
2. Switch to the tree view, and then expand **Adatum (local)**.

### Perform an administrative task within the Active Directory Administrative Center

1. Go to the **Overview** view.
2. Reset the password for **Adatum\Adam** to **Pa\$\$w0rd** without requiring the user to change the password at the next sign-in.
3. Use the **Global Search** section to find any objects that match the "Lon" search string.

### Create objects

- Create a new computer object named **LON-CL4** in the **Computers** container.

### View all object attributes

- Open the **Properties** page for **LON-CL4**, scroll to the **Extensions** section, and then select the **Attribute Editor** tab. View the objects' AD DS attributes.

### Use the Windows PowerShell History viewer

1. Open the **Windows PowerShell History** pane.
2. View the Windows PowerShell cmdlet that you used to perform the most recent task.

**Results:** After completing this exercise, you should have successfully used the Active Directory Administrative Center to manage AD DS and reviewed the Windows PowerShell cmdlets that run behind the scenes.

### ► Task 2: Prepare for the next module

When you are finished with the lab, revert all virtual machines to their initial state:

1. On the host computer, start **Hyper-V Manager**.
2. In the **Virtual Machines** list, right-click **20742A-LON-DC1**, and then click **Revert**.
3. In the **Revert Virtual Machine** dialog box, click **Revert**.
4. Repeat steps 2 and 3 for **20742A-LON-DC2** and **20742A-LON-SVR1**.

## Module Review and Takeaways

In this module, you received a basic overview of AD DS and learned the main components. You can now describe the purpose of a domain controller and the various roles it can hold. You are now familiar with the considerations for deploying domain controllers, and you now know various methods of deploying domain controllers.

### Review Questions

**Question:** Which deployment method would you use if you had to install an additional domain controller in a remote location that had a limited WAN connection?

**Question:** If you need to promote a Server Core installation of Windows Server 2016 to be a domain controller, which tool or tools can you use?

**Question:** If you want to run a domain controller in the cloud, which service should you consider using: Azure AD or Infrastructure as a Service (IaaS) Azure virtual machines?

### Common Issues and Troubleshooting Tips

Common Issue	Troubleshooting tip
Syntax errors	
Prerequisite problems	
Network and forest configuration problems	

**MCT USE ONLY. STUDENT USE PROHIBITED**



# Module 2

## Managing objects in AD DS

### Contents:

Module Overview	2-1
<b>Lesson 1:</b> Managing user accounts	2-2
<b>Lesson 2:</b> Managing groups in AD DS	2-11
<b>Lesson 3:</b> Managing computer objects in AD DS	2-21
<b>Lab A:</b> Managing AD DS objects	2-28
<b>Lesson 4:</b> Using Windows PowerShell for AD DS administration	2-33
<b>Lesson 5:</b> Implementing and managing OUs	2-48
<b>Lab B:</b> Administering AD DS	2-56
Module Review and Takeaways	2-61

## Module Overview

Active Directory Domain Services (AD DS) can help you manage your network more effectively. For instance, you can use it to manage user and computer accounts as part of groups instead of managing one account at a time. It also provides ways to group objects together in containers called organizational units (OUs) and the means to delegate administrative tasks to people to help you distribute workload efficiently.

Managing device identities is becoming increasingly complex as more employees bring their own devices into the workplace. As Bring Your Own Device (BYOD) programs expand, you will be managing device identities for many types of personal devices and the various operating systems that they run. AD DS has many features that can make this easier.

This module describes how to use both graphical tools and Windows PowerShell to manage user and computer accounts and groups. It covers how to manage an enterprise network by performing bulk operations to modify object attributes.

### Objectives

After completing this module, students will be able to:

- Manage user accounts in AD DS.
- Manage groups in AD DS.
- Manage computer objects in AD DS.
- Use Windows PowerShell for AD DS administration.
- Implement and manage OUs.
- Administer AD DS.

## Lesson 1

# Managing user accounts

A user object in AD DS is far more than just properties related to the user's security identity or account. It is the cornerstone of identity and access in AD DS. Therefore, consistent, efficient, and secure processes regarding the administration of user accounts are the cornerstone of enterprise security management.

In this lesson, you will learn about managing users' accounts, which is more complex than just creating and deleting them. User accounts have many attributes that you can use for a variety of purposes, such as storing additional user contact information or application-specific information for Active Directory-aware applications. Additionally, there are user-specific files and settings that are not stored in Active Directory but instead typically stored in the user profile. Lastly, you will learn about using user templates to help you create user accounts more easily.

### Lesson Objectives

After completing this lesson, you will be able to:

- Create user accounts.
- Configure user account attributes.
- Manage user accounts.
- Create user profiles.
- Manage inactive and disabled user accounts.
- Explain user account templates.
- Use user account templates to manage accounts.


### Creating user accounts

In AD DS, you must configure all users who require access to network resources with a user account. With this user account, users can authenticate to the AD DS domain and access network resources.

In Windows Server 2016, a user account is an object that contains all of the information that defines a user. A user account includes the user name, user password, and group memberships. A user account also contains many other settings that you can configure based on your organizational requirements. With a user account, you can:

- Allow or deny users permission to sign in to a computer based on their user account identity.
- Grant users access to processes and services for a specific security context.
- Manage users' access to resources such as AD DS objects and their properties, shared folders, files, directories, and printer queues.

- **Users accounts:**
  - Allow or deny access to sign into computers
  - Grant access to processes and services
  - Manage access to network resources
- **User accounts can be created by using:**
  - Active Directory Users and Computers
  - Active Directory Administrative Center
  - Windows PowerShell
  - Directory command line tool **dsadd**
- **Considerations for naming users include:**
  - Naming formats
  - UPN suffixes



A user account enables a user to sign in to computers and domains with an identity that the domain can authenticate. When you create a user account, you must provide a user logon name, which must be unique in the domain and forest in which the user account is created.

To maximize security, you should avoid multiple users sharing a single account and instead ensure that each user who signs in to the network has a unique user account and password.



**Note:** This course focuses on AD DS accounts. You can also store user accounts in the local Security Accounts Manager database of each computer, enabling local sign in and access to local resources. Local user accounts are, for the most part, beyond the scope of this course.

### Creating user accounts

A user account includes the user name and password, which serve as the user's sign-in credentials. A user object also includes several other attributes that describe and manage the user. You can use Active Directory Users and Computers, Active Directory Administrative Center, Windows PowerShell, or the **dsadd** command-line tool to create a user object.

### Considerations for naming users

Your naming convention is an important consideration. Having a formalized naming convention will allow you to deal with duplicate user names and name changes in a standardized way. When you create user accounts, consider the following elements:

- **Full Name** attribute. **Full Name** is used to create several attributes of a user object, most notably, the common name and display name attributes. The common name of a user is the name displayed in the details pane of the snap-in, and it must be unique within the container or OU. If you create a user object for a person with the same name as an existing user in the same container or OU, you need to give the new user object a unique Full Name.
- **UPN logon.** User Principal Name (UPN) logons follow the format *user logon name@* (UPN suffix). User names in AD DS can contain special characters, including periods, hyphens, and apostrophes. These special characters enable you to generate accurate user names, such as O'Hare and Smith-Bates. However, certain programs and applications might have other restrictions, so we recommend that you use only standard letters and numbers until you test the applications in your enterprise environment fully for compatibility with special characters.

You can manage the list of available UPN suffixes by using the Active Directory Domains and Trusts snap-in. Right-click the root of the snap-in, click **Properties**, and then use the **UPN Suffixes** tab to add or remove suffixes. The Domain Name System (DNS) name of your AD DS domain is always available as a suffix, and you cannot remove it. In a multi-domain environment, you can assign different UPN suffixes to users for purposes such as email domain suffixes.



**Note:** It is important that you implement a user account naming strategy, especially in large networks in which users might have the same full name. A combination of last name and first name, and where necessary, additional characters, should yield a unique user account name. Specifically, it is only the UPN name that must be unique within your AD DS forest. The full name property needs to be unique only within the OU where it resides. The **User SAMAccountName** name must be unique within that domain.


## Configuring user account attributes

When you create a user account in AD DS, you also configure all the associated account properties. You have to define the attributes that allow the user to sign in using the account in addition to a few other attributes. Because you can associate a user object with many attributes, it is important that you understand what these attributes are and how you can use them in your organization.

You can configure user attributes by using Active Directory Administrative Center, Active Directory Users and Computers, Windows PowerShell, or the **dsmod** tool.

User properties include the following categories:

- Account
- Organization
- Member of
- Password Settings
- Profile
- Policy
- Silo
- Extensions

 **Note:** The attributes that are associated with a user account are defined as part of the AD DS schema, which members of the Schema Admins security group can modify. Generally, the schema does not often change. However, when you introduce an enterprise-level program (such as Microsoft Exchange Server), many schema changes are required. These changes enable objects, including user objects, to have additional attributes.

### Attribute categories

The attributes of a user object fall into several broad categories. These categories appear in the navigation pane of the **User Properties** dialog box in the Active Directory Administrative Center:

- **Account.** In addition to the user's user name properties (**First name, Middle initial, Last name, Full name**) and the user's various logon names (**User UPN logon, User SAMAccountName logon**), you can configure the following additional properties:
  - **Log on hours.** This property defines when the account can be used to access domain computers. You can use the weekly calendar style view to define Logon permitted hours and Logon denied hours.
  - **Log on to.** Use this property to define which computers a user can use to sign in to the domain. Specify the computer's name and add it to a list of allowed computers.
  - **Account expires.** This value is useful when you want to create temporary user accounts. For example, you might want to create user accounts for interns who will be at your organization for just one year. You can set the account expiration date in advance. No one can use the account after the expiration date until an administrator reconfigures it manually.
  - **User must change password at next log on.** This property enables you to force users to reset their own password the next time they sign in. This is something you might enable after you reset a user's password.
  - **Smart card is required for interactive log on.** This value resets the user's password to a complex, random sequence of characters and sets a property that requires that the user use a smart card to authenticate during logon.

- **Password never expires.** This is a property that you normally use with service accounts; that is, those accounts that are not used by regular users but by services. By setting this value, you must remember to update the password manually on a periodic basis. However, you are not forced to do this at a predetermined interval. Consequently, the account can never be locked out due to password expiration—a feature that is particularly important for service accounts.
- **User cannot change password.** You use this option generally for service accounts.
- **Store password by using reversible encryption.** This policy provides support for programs that use protocols that require knowledge of the user's password for authentication purposes. Storing passwords by using reversible encryption is essentially the same as storing plain text versions of the passwords. For this reason, you should never enable this policy unless program requirements outweigh the need to protect password information. This policy is required when you use Challenge Handshake Authentication Protocol (CHAP) authentication through remote access or Internet Authentication Service (IAS). It is also required when using Digest authentication in Internet Information Services (IIS).
- **Account is trusted for delegation.** You can use this property to allow a service account to impersonate a standard user to access network resources on behalf of a user.
- **Organization.** This includes properties such as the user's **Display name**, **Office**, **Email Address**, various contact telephone numbers, managerial structure, department and organization names, addresses and other properties.
- **Member of.** Use this section to define group memberships for the user.
- **Password Settings.** This section includes password settings that are applied directly to the user.
- **Profile.** Use this section to configure a location for the user's personal data and to define a location in which to save the user's desktop profile when he or she logs out.
- **Policy.** Use authentication policies to control Kerberos ticket-granting ticket (TGT) lifetimes and the authentication access control for a specific account, such as high-level administrative accounts.
- **Silo.** Authentication policy silos are containers that you can assign a user account to. You can assign authentication policies to these silos.
- **Extensions.** This section exposes many additional user properties, most of which do not normally require manual configuration.

## Demonstration: Managing user accounts

In this demonstration you will see how to use Active Directory Administrative Center to:

- Create a new user account
- Delete a user account
- Move a user account
- Configure user attributes:
  - Change department
  - Change group membership

## Demonstration Steps

### Create a new user account

- Use **Active Directory Administrative Center** to create a new user as follows:
  - First name: **Sales**
  - Last name: **Manager**
  - User UPN logon: **SalesManager**
  - Password: **Pa\$\$w0rd**

### Delete a user account

- Delete the Art Odum account.

### Move a user account

1. Move the **Burton Bartels** account from the **Managers** OU to the **Development** OU.
2. Open the **Development** OU to verify that **Burton Bartels** account is present.

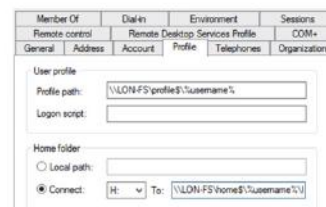
### Configure user attributes

- Modify the **Burton Bartels** account as follows:
  - Change the **Department** field from **Managers** to **Development**.
  - Remove the account from the Managers group.
  - Add the account to the Development group.

## Creating user profiles

When users sign out, their desktop and app settings are saved to a subfolder that matches their user name in the C:\Users folder on the local hard disk. This folder contains their user profile. Within this folder, subfolders contain documents and settings that represent the user's profile, including **Documents**, **Videos**, **Pictures**, and **Downloads** and application data. If a user is likely to sign in interactively at more than one client workstation, then it is preferable for these settings and documents to be available on those other client workstations. There are a number of ways that you can ensure that users can access their profiles from multiple workstations.

The Profile section of the User Properties window



### Configuring user account properties to manage profiles

You can configure the following properties of a user's desktop profile by using the user account settings in the Active Directory Administrative Center:

- **Profile path.** This path is either a local, or more usually, a Universal Naming Convention (UNC) path. The user's desktop settings are stored in the profile. If a user profile has a UNC path, then the user will have access to their desktop settings regardless of the domain computer they sign in at. We refer to this as a roaming profile.

- **Logon script.** This is a batch file that contains commands that execute when the user signs in. Typically, you use these commands to create drive mappings. If you use a login script, the name of the script should be a file name (with extension) only. Scripts should be stored in the C:\Windows\SYSVOL\domain\scripts folder on all domain controllers. Rather than use a logon script batch file, you will typically implement logon scripts by using Group Policy Objects (GPOs) or Group Policy preferences.
- **Home folder.** This is a storage area in which users can save their personal documents. You can specify either a local path or typically a UNC path to the user's folder. You also must specify a drive letter that is used to map a network drive to the specified UNC path. You can then configure a user's personal documents to this redirected home folder.



**Note:** When you create user accounts to use as templates and use a common location for the profile path and home folder, you should use the `%username%` variable in the path so that AD DS can create these folders automatically when the account is used as a template. For example, you can use the following paths, where the file server is named LON-FS and shares have been created for the profiles and home folders, `profile$` and `home$`, respectively:

- Profile Path: `\\LON-FS\profile$\%username%`
- Home folder Connect H: to `\\LON-FS\home$\%username%`

### Using group policy to manage profiles

As an alternative to using the individual user account settings, you can use GPOs to manage these settings. You can configure Folder Redirection settings by using the Group Policy Management Editor to open a GPO for editing and then expand **User Configuration**, expand **Policies**, and then expand **Windows Settings**. Windows Settings contains the sub-nodes listed in the following table.

Sub-nodes in the Windows Settings node		
<ul style="list-style-type: none"> <li>□ AppData (Roaming)</li> <li>□ Desktop</li> <li>□ Start Menu</li> <li>□ Document</li> </ul>	<ul style="list-style-type: none"> <li>□ Pictures</li> <li>□ Music</li> <li>□ Videos</li> <li>□ Favorites</li> <li>□ Contacts</li> </ul>	<ul style="list-style-type: none"> <li>□ Downloads</li> <li>□ Links</li> <li>□ Searches</li> <li>□ Saved Games</li> </ul>

You can use these sub-nodes to configure all aspects of a user's desktop profile and app settings. For a given sub-node, such as Documents, you can choose between Basic and Advanced redirection. In Basic redirection, all users affected by the GPO have their Documents folder redirected to an individually named subfolder off a common root folder defined by a UNC name, for example, `\\LON-SVR1\Users\`. In Advanced redirection, you can use security group membership to specify where a user's settings and documents will be stored. For example, you might store the Research and Development user's documents on a highly secured server.

## Managing inactive and disabled user accounts

User accounts can become inactive for different reasons. Users leave the organization, go on maternity or paternity leave, and take sabbaticals. In these cases, if a user does not need access to their account for a period, you should disable the account rather than deleting it. Even if a user has left the organization, it is a best practice to disable the user account until you are sure there is no requirement for that user account to exist. This is particularly true if a user has a mailbox on your Microsoft Exchange Server. If you delete the user from AD DS, then you also delete the user's mailbox. There are many reasons why you might need to retain the user's mail and restoring a user account and the associated mailbox is time consuming.

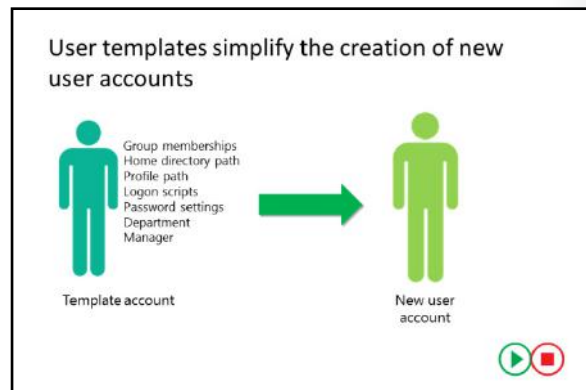
- Users accounts that will be inactive for a period of time should be disabled rather than deleted
- To disable an account in Active Directory Users and Computers, right-click the account and click Disable Account from the menu


To disable a user account, locate and select the account in Active Directory Administrative Center, and then in the **Tasks** pane, click **Disable**. To enable an account, click **Enable** in the **Tasks** pane.

## User account templates

Creating new users usually involves setting multiple attributes for the user. This can be time consuming and tedious, especially if you are creating multiple users. User templates can reduce the effort required to create new user accounts. They also reduce the chance of errors when setting properties for users.

Most users in a given department, business unit, or OU will share many common attributes such as group memberships and home directory locations. In AD DS, a user template is simply an account that you configure with all the properties that are common to that job role or department. For example, you might create a user account named Sales\_Template that has all the attributes that apply to your salespeople. Then, when a new salesperson is hired, you can copy the template to create the new account.



 **Note:** Best practices include disabling the template account so that it cannot be used to sign in and putting an underscore at the beginning of the name so that the template account is always at the top of the user list and easy to locate.

Only the most commonly used attributes are copied from the template over to the new user account. These include:

- Group memberships
- Home directories
- Profile settings
- Logon scripts



- Logon hours
- Password settings
- Department name
- Manager

When you copy an account you must provide the following information for the new account:

- First name
- Last name
- Full name
- User logon name
- Password

Attribute fields that are not copied from the template include:

- Office
- Phone numbers
- Street address
- Job title

## Demonstration: Using templates to manage accounts

In this demonstration, you will see how to create a template account and create a new user based on that template account.

### Demonstration Steps

#### Create a user template

1. Use **Active Directory Users and Computers** to create a new user as follows:
  - First name: **\_sales**
  - Last name: **template**
  - User logon name: **salestemplate**
  - Password: **Pa\$\$w0rd**
2. Clear the **User must change password at next logon** check box.
3. Set the password to never expire.
4. Disable the account.

#### Configure template properties

- Double-click the **\_sales** template account, and then set the following attributes:
  - Member Of: **Sales**
  - Department: **Sales**
  - Manager: **Erin Bull**
  - Logon Script: **\\lon-dc1\netlogon\logon.bat**

### Create a new user by copying the template

1. Right-click the **\_sales template** account, and then click **Copy**.
2. Create a new user named **Sales User** with a password of **Pa\$\$w0rd**.
3. Enable the account and clear the **Password never expires** attribute.
4. Require the account to change the password the next time the user signs in.
5. View the properties of the newly created **Sales User** account and ensure that the template properties are present.
6. Close **Active Directory Users and Computers**.

**Question:** What is the purpose of a roaming profile?

**Question:** What is the difference between disabling an account and an account being locked out?

## Lesson 2

# Managing groups in AD DS

Although it might be practical to assign permissions and abilities to individual user accounts in small networks, this becomes impractical and inefficient in large enterprise networks. For example, if many users need the same level of access to a folder, it is more efficient to create a group that contains the required user accounts and then assign the required permissions to the group. This has the added benefit of enabling you to change a user's file permissions by adding or removing them from groups rather than editing the file permissions directly. Before you implement groups in your organization, you must understand the scope of various Windows Server group types and how best to use these to manage access to resources or to assign management rights and abilities.

### Lesson Objectives



After completing this lesson, you will be able to:

- Describe group types.
- Describe group scopes.
- Explain how to implement group management.
- Manage group membership by using Group Policy.
- Describe default groups.
- Describe special identities.
- Manage groups in Windows Server.

### Group types

In a Windows Server 2016 enterprise network, there are two types of groups: security and distribution. When you create a group, you choose the group type and scope. Group type determines the capabilities of the group.

Email applications mainly use distribution groups, which are not security enabled. Security groups are security enabled and you use them to assign permissions to various resources. You can use security groups in permission entries in access control lists (ACLs) to control security for resource access. You also can use security groups as a means of distribution for email applications. If you want to use a group to manage security, it must be a security group.


<ul style="list-style-type: none"> <li>• Distribution groups               <ul style="list-style-type: none"> <li>• Used only with email applications</li> <li>• Not security enabled (no SID)</li> <li>• Cannot be given permissions</li> </ul> </li> </ul>	
<ul style="list-style-type: none"> <li>• Security groups               <ul style="list-style-type: none"> <li>• Security principal with a SID</li> <li>• Can be given permissions</li> <li>• Can also be email-enabled</li> </ul> </li> </ul>	
<p>Security groups and distribution groups can be converted to the other type of group</p>	




**Note:** The default group type for newly created groups is security.

Because you can use security groups for both resource access and email distribution, many organizations use only security groups. However, we recommend that if you use a group for email distribution only, you should create the group as a distribution group. Otherwise, the group is assigned a SID, and the SID is added to the user's security access token, which can make the token unnecessarily large.

You can convert a security group to a distribution group at any time. When you do this, the **groupType** attribute changes. A security group that has been converted to a distribution group therefore loses all permissions assigned to it, even though the ACLs still contain the SID. If a distribution group is converted to a security group the reverse occurs, the **groupType** attribute changes and it can now be assigned permissions to resources.

 **Note:** Consider that when you add a user to a security group, the user's access token—which authenticates user processes—updates only when the user signs in. Therefore, if the user is currently signed in, the user must sign out and sign back in to update their access token with any changed group memberships.

 **Note:** The benefit of using distribution groups becomes more evident in large-scale Exchange Server deployments, especially when there is a need to nest these distribution groups across the enterprise.

## Group scopes

Windows Server 2016 supports group scoping. The scope of a group determines both the range of a group's abilities or permissions and the group membership.

There are four group scopes:

- Local. You use this type of group for stand-alone servers or workstations, on domain member servers that are not domain controllers, or on domain member workstations. Local groups are truly local, which means that they are available only on the computer where they exist. The important characteristics of a local group are:
  - You can assign abilities and permissions on local resources only, meaning on the local computer.
  - Members can be from anywhere in the AD DS forest, and can include:
    - Any security principals from the domain: users, computers, global groups, or domain local groups.
    - Users, computers, and global groups from any domain in the forest.
    - Users, computers, and global groups from any trusted domain.
    - Universal groups defined in any domain in the forest.
- Domain local. You use this type of group primarily to manage access to resources or to assign management responsibilities (rights). Domain local groups exist on domain controllers in an AD DS forest, and consequently, the group's scope is local to the domain in which they reside. The important characteristics of domain-local groups are:
  - You can assign abilities and permissions on domain-local resources only, which means on all computers in the local domain.

- Local groups can contain users, computers, global groups, domain local groups and universal groups from the same domain, domains in the same forest and other trusted domain and can be given permissions to resources on the local computer only
- Domain local groups have the same membership possibilities but can be given permission to resources anywhere in the domain
- Universal groups can contain users, computers, global groups and other universal groups from the same domain or domains in the same forest and can be given permissions to any resource in the forest
- Global groups can only contain users, computers and other global groups from the same domain and can be given permission to resources in the domain or any trusted domain

- Members can be from anywhere in the AD DS forest and can include:
  - Any security principals from the domain: users, computers, global groups, or domain local groups.
  - Users, computers, and global groups from any domain in the forest.
  - Users, computers, and global groups from any trusted domain.
  - Universal groups defined in any domain in the forest.
- Global. You use this type of group primarily to consolidate users who have similar characteristics. For example, global groups are often used to consolidate users who are part of a department or geographic location. The important characteristics of global groups are:
  - You can assign abilities and permissions anywhere in the forest.
  - Members can be from the local domain only and can include users, computers, and global groups from the local domain.
- Universal. You use this type of group most often in multidomain networks because it combines the characteristics of both domain-local groups and global groups. Specifically, the important characteristics of universal groups are:
  - You can assign abilities and permissions anywhere in the forest, as with global groups.
  - Members can be from anywhere in the AD DS forest, and can include:
    - Users, computers, and global groups from any domain in the forest.
    - Universal groups defined in any domain in the forest.
  - Properties of universal groups are propagated to the global catalog and are made available across the enterprise network on all domain controllers that host the global catalog role. This makes universal groups' membership lists more accessible, which is useful in multidomain scenarios. For example, if a universal group is used for email distribution purposes, the process for determining the membership list typically is quicker in distributed multidomain networks.

The following table summarizes and compares the basic properties of the four group scopes.

Group scope	Can include members from	Can be assigned permissions to	Can be converted to
Local	Domain users, domain computers, global groups, and universal groups from any domain in the forest Domain-local groups from the same domain Local Users from the computer	Local computer resources only	N/A
Domain local	Domain users, domain computers, global groups, and universal groups from any domain in the forest Domain-local groups from the same domain	Local domain resources only	Universal groups (as long as no other domain local groups exist as members)
Global	Domain users, domain computers, and global groups from the same domain	Any domain resource in the forest	Universal groups (as long as it is not a member of any other global groups)

Group scope	Can include members from	Can be assigned permissions to	Can be converted to
Universal	Domain users, domain computers, global groups, and universal groups from any domain in the forest	Any domain resource in the forest	Domain local groups and global groups (as long as no other universal groups exist as members)

## Implementing group management

Adding groups to other groups is a process called nesting. Nesting creates a hierarchy of groups that supports your business roles and management rules.

A best practice for group nesting is known as IGDLA, which is an acronym for the following:

- Identities
- Global groups
- Domain-local groups
- Access



These parts of IGDLA are related in the following way:

- Identities (user and computer accounts) are members of global groups, which represent business roles.
- Global groups (also known as role groups) are members of domain-local groups, which represent management rules: for example, determining who has Read permission to a specific collection of folders.
- Domain-local groups (also known as rule groups) are granted access to resources. In the case of a shared folder, access is granted by adding the domain-local group to the folder's ACL, with a permission that provides the appropriate level of access.

In a multidomain forest, the best practice for group nesting is known as IGUDLA. The additional letter U stands for universal groups:

- Identities
- Global groups
- Universal groups
- Domain-local groups
- Access

In this case, global groups from multiple domains are members of a single universal group. That universal group is a member of domain-local groups in multiple domains.

## IGDLA example

The figure on the slide represents a group implementation that reflects the technical view of group management best practices (IGDLA) and the business view of role-based, rule-based management. Consider the following scenario.

The sales force at Contoso, Ltd. has just completed its fiscal year. Sales files from the previous year are in a folder called Sales. The sales force needs Read access to the Sales folder. Additionally, a team of auditors from Woodgrove Bank, a potential investor, require Read access to the Sales folder to perform the audit. You can implement the security for this scenario by following these steps:

1. Assign users with common job responsibilities or other business characteristics to role groups, which are implemented as global security groups. Do this separately in each domain. Salespeople at Contoso Ltd. are added to a Sales role group; Auditors at Woodgrove Bank are added to an Auditors role group.
2. Create a group to manage access to the Sales folders with Read permission. You implement this in the domain that contains the resource that is being managed. In this case, the Sales folder is in the Contoso domain. Therefore, you create the resource access management rule group as a domain-local group named ACL\_Sales\_Read.
3. Add the role groups to the resource access management rule group to represent the management rule. These groups can come from any domain in the forest or from a trusted domain, such as Woodgrove Bank. Global groups from trusted external domains, or from any domain in the same forest, can be members of a domain-local group.
4. Assign the permission that implements the required level of access. In this case, grant the Allow Read permission to the domain-local group.

This strategy results in two single points of management, thereby reducing the management burden. One point of management defines who is in Sales, and the other point of management defines who is an Auditor. Because these roles are likely to have access to a variety of resources beyond the Sales folder, you have another single point of management to determine who has Read access to the Sales folder. Furthermore, the Sales folder might not be a single folder on a single server; it could be a collection of folders across multiple servers, each of which assigns the Allow Read permission to the single domain-local group.

## Configuring a group manager

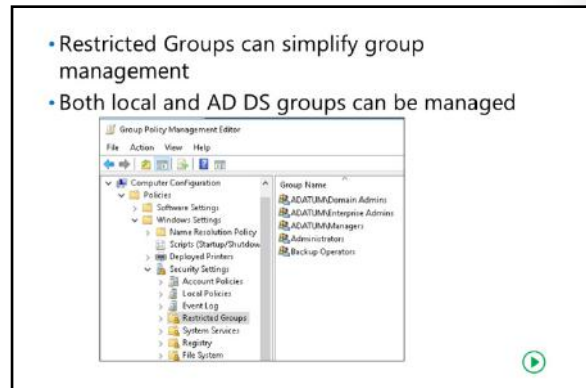
The properties page of a group has a **Managed By** tab. Use this to provide information about which manager is responsible for this group. By adding a user or group to the **Name** field, information about that user—such as office, address, and telephone number—will be pulled from AD DS and displayed. There is also a check box called **Manager can update membership list** that allows the manager of the group to manage group membership. This is useful in distributed administrative environments in which managers are responsible for controlling their own departmental groups.

## Managing group membership by using Group Policy


Managing group membership can be a time-consuming task; especially if you have to modify the membership of groups on workstations or servers distributed throughout the enterprise. For example, you might need to add a user or a global group to the local Administrators group on client computers or add a global group to the Backup Operators group on servers.

Group Policy provides a setting called **Restricted Groups** that enables you to control the membership of local groups on domain-joined computers and control the membership of AD DS groups by configuring a GPO and assigning that GPO to the OU holding those computer accounts.


You can find the **Restricted Groups** setting in the Computer Configuration policy under **Windows Settings**, then under **Security Settings**. It contains no groups by default.



- Restricted Groups can simplify group management
- Both local and AD DS groups can be managed


 **Note:** To configure membership in AD DS groups, you must assign the GPO to the OU that holds the Domain Controllers computer accounts.

You can also configure group nesting by using the **Restricted Groups** setting. For example, you could use **Restricted Groups** to nest global groups into universal groups. All the rules governing group nesting still apply when using **Restricted Groups**.

 **Note:** The **Restricted Groups** setting is only available in domain-level group policies. It does not exist in local group policies on Windows client and server operating systems.

### Removal of non-designated members

One of the benefits of **Restricted Groups** is that it will also remove any user (or group) from the targeted group if they are not on the list of users or groups that the setting assigns. This is useful to control the membership of high-level administrative groups, such as Enterprise Admins, Domain Admins and local Administrators groups on servers and client computers. If a user is manually added to a controlled group they will be removed the next time group policy refreshes.

 **Note:** The only exception to this rule is that the local default Administrator account can never be removed from the local Administrators group.

### Policy removal

If the group policy that was used to configure the restricted group membership is unlinked from the container holding the computer accounts, or if the restricted group entry is deleted from the GPO, then the group memberships that it assigned are not removed. Those group memberships must be modified manually.



## Default groups

Windows Server 2016 creates a number of groups automatically. These are called default local groups, and they include well-known groups such as Administrators, Backup Operators, and Remote Desktop Users. There are additional groups that are created automatically in a domain, both in the Built-in container and the Users container, including Domain Admins, Enterprise Admins, and Schema Admins.

### Default groups that provide administrative privileges

A subset of default groups have significant permissions and user rights related to the management of AD DS. Because of the rights that these groups have, they are protected groups. Protected groups are described later in this topic. The following list summarizes the capabilities of these groups:

- Enterprise Admins (in the Users container of the forest root domain). This group is a member of the Administrators group in every domain in the forest, which gives it complete access to the configuration of all domain controllers. It also owns the Configuration partition of the directory and has full control of the domain naming context in all forest domains.
- Schema Admins (Users container of the forest root domain). This group owns and has full control of the Active Directory schema.
- Administrators (Built-in container of each domain). Members of this group have complete control over all domain controllers and data in the domain-naming context. They can change the membership of all other administrative groups in the domain, and the Administrators group in the forest root domain can change the membership of Enterprise Admins, Schema Admins, and Domain Admins. The Administrators group in the forest root domain is generally considered the most powerful service administration group in the forest.
- Domain Admins (Users container of each domain). This group is added to the Administrators group of its domain. It therefore inherits all of the capabilities of the Administrators group. It is also, by default, added to the local Administrators group of each domain member computer, thus giving Domain Admins ownership of all domain computers.
- Server Operators (Built-in container of each domain). Members of this group can perform maintenance tasks on domain controllers. They have the right to sign in locally, start and stop services, perform backup and restore operations, format disks, create or delete shares, and shut down domain controllers. By default, this group has no members.
- Account Operators (Built-in container of each domain). Members of this group can create, modify, and delete accounts for users, groups, and computers located in any OU in the domain (except the Domain Controllers OU) and in the Users and Computers containers. Account Operator group members cannot modify accounts that are members of the Administrators or Domain Admins groups, nor can they modify those groups. Account Operator group members also can sign in locally to domain controllers. By default, this group has no members.
- Backup Operators (Built-in container of each domain). Members of this group can perform backup and restore operations on domain controllers and can sign in locally and shut down domain controllers. By default, this group has no members.

Carefully manage the default groups that provide administrative privileges, because these groups:

- Typically have broader privileges than are necessary for most delegated environments
- Often apply protection to their members

Group	Location
Enterprise Admins	Users container of the forest root domain
Schema Admins	Users container of the forest root domain
Administrators	Built-in container of each domain
Domain Admins	Users container of each domain
Server Operators	Built-in container of each domain
Account Operators	Built-in container of each domain
Backup Operators	Built-in container of each domain
Print Operators	Built-in container of each domain
Cert Publishers	Users container of each domain

- Print Operators (Built-in container of each domain). Members of this group can maintain print queues on domain controllers. They also can sign in locally and shut down domain controllers. By default, this group has no members.
- Cert Publishers (Users container of each domain). Members of this group are permitted to publish certificates to the directory. By default, this group has no members.

### **Managing groups that provide administrative privileges**

You need to carefully manage the default groups that provide administrative privileges, because they typically have broader privileges than are necessary for most delegated environments, and because they often apply protection to their members.

The Account Operators group is a good example of this. If you examine the capabilities of the Account Operators group in the preceding list, you can see that members of this group have very broad rights—they can even sign in locally to a domain controller. In very small networks, such rights might be assigned to one or two individuals who are typically domain administrators anyway. However, in large enterprises, the rights and permissions granted to Account Operators are usually far too broad. Additionally, the Account Operators group is, like the other administrative groups, a protected group.

### ***Protected groups***

Protected groups are defined by the operating system and cannot be unprotected. Members of a protected group become protected by association and no longer inherit permissions (ACLs) from their OU but instead receive a copy of an ACL from the protected group. This protected group ACL offers considerable protection to the members. For example, if you add Jeff Ford to the Account Operators group, his account becomes protected, and the Help desk, which has rights to reset all other user passwords in the Employees OU, cannot reset Jeff Ford's password.

Protected groups include:

- Account Operators
- Administrators
- Backup Operators
- Cert Publishers
- Domain Admins
- Enterprise Admins
- Krbtgt
- Print Operators
- Read-only Domain Controllers
- Replicator
- Server Operators

## Custom groups

You should try to avoid adding users to the groups that do not have members by default (Account Operators, Backup Operators, Server Operators, and Print Operators). Instead, create custom groups to which you assign permissions and user rights that achieve your business and administrative requirements.

For example, Scott Mitchell should be able to perform backup operations on a domain controller but should not be able to perform restore operations that could lead to database rollback or corruption. In addition, Scott should not be able to shut down a domain controller, so do not put Scott in the Backup Operators group. Instead, create a local group and assign it only the Backup Files And Directories user right, and then create a global group and add Scott as a member. Then add that global group to the local group.

## Special identities

Windows and AD DS also support special identities, which are groups where the operating system controls membership. You cannot view the groups in any list (in Active Directory Users and Computers, for example), you cannot view or modify the membership of these special identities, and you cannot add them to other groups. You can, however, use these groups to assign rights and permissions.

The most important special identities—often called *groups* (for convenience)—are described in the following list:

- Special identities:
  - Are groups for which membership is controlled by the operating system
  - Can be used by the Windows Server operating system to provide access to resources Based on the type of authentication or connection, not on the user account
- Important special identities include:
  - Anonymous Logon
  - Authenticated Users
  - Everyone
  - Interactive
  - Network
  - Creator Owner

- Anonymous Logon. This identity represents connections to a computer and its resources that are made without supplying a user name and password. Before Windows Server 2003, this group was a member of the Everyone group. Beginning with Windows Server 2003, this group is no longer a default member of the Everyone group.

Authenticated Users. This identity represents identities that are authenticated. This group does not include Guest, even if the Guest account has a password.

- Everyone. This identity includes Authenticated Users and the Guest account.
- Interactive. This identity represents users who access a resource while signed on locally to the computer that is hosting the resource, as opposed to accessing the resource over the network. When a user accesses any given resource on a computer on which the user is signed on locally, the user is added automatically to the Interactive group for that resource. Interactive also includes users who sign on through a Remote Desktop Connection (RDC).
- Network. This identity represents users who access a resource over the network, as opposed to users who are signed on locally at the computer that is hosting the resource. When a user accesses any given resource over the network, the user is added automatically to the Network group for that resource.
- Creator Owner. This identity represents the security principal that created an object. The Creator Owner automatically has full control permission on the object by virtue of being the entity that created the object.

The importance of these special identities is that you can use them to provide access to resources based on the type of authentication or connection, rather than the user account. For example, you could create a folder on a system that allows users to view its contents when they are signed on locally to the system but that does not allow the same users to view the contents from a mapped drive over the network. You could achieve this by assigning permissions to the Interactive special identity.

A common scenario for the Creator Owner group is when NTFS permissions are set on a root folder to allow users to create subfolders, such as home directories. The Creator Owner group grants users full control permission on those home directories because the user created the subfolder.

## Demonstration: Managing groups in Windows Server

In this demonstration, you will see how to create a new group and add members to a group. In addition, you will learn to add users to the group, change the group type and scope, and configure a manager for the group.

### Demonstration Steps

#### Create a new group and add members

1. Use **Active Directory Administrative Center** to create a new global security group named **IT Managers** in the IT OU of Adatum.com.
2. Add the following members to the group:
  - **Beth Burke**
  - **Logan Boyle**

#### Add a user to the group

- Locate the user **Maj Hojski** and then add the user to the **IT Managers** group.

#### Change the group type and scope

- Access the **IT Managers** group properties, change the **Group** type to **Distribution**, and then change the **Group** scope to **Universal**.

#### Configure a manager for the group

1. Edit the **Managed By** section to add **Parsa Schoonen** as a manager of the group.
2. Allow **Parsa** to update the group membership list.
3. Close the **IT Managers** properties.
4. Close **Active Directory Administrative Center**.

## Lesson 3

# Managing computer objects in AD DS

Computers, like users, are security principals:

- They have an account with a logon name and password that Windows Server changes automatically on a periodic basis.
- They authenticate with the domain.
- They can belong to groups, have access to resources, and you can configure them by using Group Policy.

A computer account begins its lifecycle when you create it and join it to your domain. Thereafter, day-to-day administrative tasks include:

- Configuring computer properties.
- Moving the computer between OUs.
- Managing the computer itself.
- Renaming, resetting, disabling, enabling, and eventually deleting the computer object.

If you know how to perform these computer-management tasks, then you can configure and maintain the computer objects within your organization.

## Lesson Objectives

After completing this lesson, you will be able to:

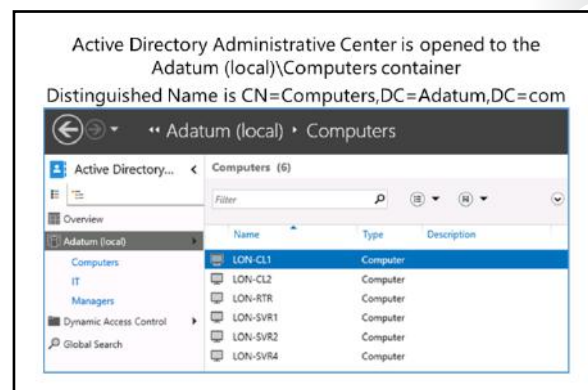
- Explain the purpose of the Computers container.
- Describe how to configure the location of computer accounts.
- Explain how to control who has permission to create computer accounts.
- Explain how to join a computer to a domain.
- Describe computer accounts and secure channels.
- Explain how to reset the secure channel.
- Explain how to perform an offline domain join.

## What is the Computers container?

Before you create a computer object in the AD DS, you must have a place to put it.

When you create a domain, the Computers container is created by default. This container is the default location for the computer accounts when a computer joins the domain.

This container is not an OU; instead, it is an object of the container class. Its common name is CN=Computers. There are subtle but important differences between a container and an OU. You cannot create an OU within a container, so you cannot subdivide the Computers container. You



also cannot link a GPO to a container. Therefore, we recommend that you create custom OUs to host computer objects, instead of using the Computers container.

## Specifying the location of computer accounts


Most organizations create at least two OUs for computer objects: one for servers and another to host computer accounts for client computers, such as desktops, laptops, and other user devices. These two OUs are in addition to the domain controllers OU that is created by default during the AD DS installation.

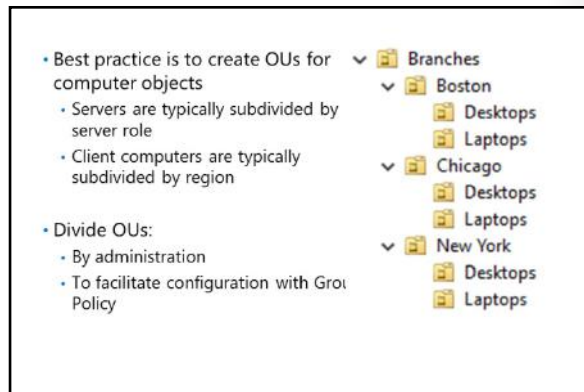
You can create computer objects in any OU in your domain. There is no technical difference between a computer object in a client OU, a computer object in a server OU, a computer object in the domain controllers OU, and even a computer object in an OU intended for users. However, administrators typically create separate OUs to provide unique scopes of management, so that they can delegate management of client objects to one team and management of server objects to another.

Your administrative model might require you to divide your client and server OUs into smaller groups. Many organizations create sub-OUs beneath a server OU to classify and manage specific types of servers. For example, you might create an OU for file and print servers, an OU for database servers, or any number of OUs that categorize the server types in your organization. By doing so, you can delegate permissions to manage computer objects in the appropriate OU to the team of administrators for each type of server. Similarly, geographically distributed organizations with local desktop support teams often divide a parent OU for clients into sub-OUs for each site. This approach enables each site's support team to create computer objects in the site for client computers and to join computers to the domain by using those computer objects.

Your OU structure should reflect your administrative model so that your OUs can provide single points of management for the delegation of administration.

Additionally, by using separate OUs, you can create various baseline configurations by using different GPOs that are linked to the client and the server OUs. With Group Policy, you can specify configuration for collections of computers by linking GPOs that contain configuration instructions to OUs. It is common for organizations to separate clients into desktop and laptop OUs. You then can link GPOs that specify desktop or laptop configuration to the appropriate OUs.

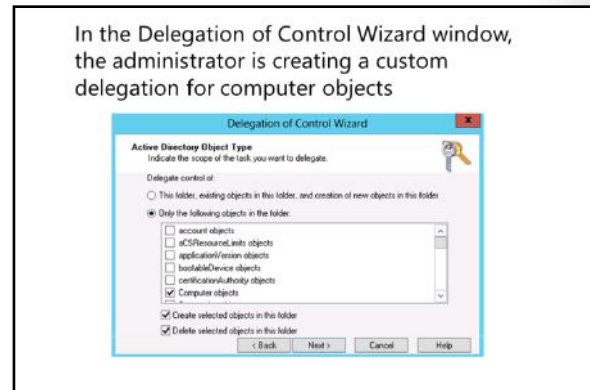
 **Note:** You can use the `redircmp` command-line tool to reconfigure the default container for computers. For example, if you want to change the default container for computers to an OU called `mycomputers`, use the following syntax: `redircmp ou=mycomputers,DC=contoso,dc=com`.




## Controlling permissions to create computer accounts

Before you join a computer to a domain, you should first create a computer object in the appropriate OU. To join a computer to an AD DS domain, three conditions must be met:

- You must have appropriate permissions on the computer object that allow you to join a physical computer with the same name to the domain.
- You must be a member of the local Administrators group on the computer. This allows you to change the computer's domain or workgroup membership.
- You must not have exceeded the maximum number of computer accounts that you can add to the domain. By default, users can add a maximum of 10 computers to the domain; this value is known as the *machine account quota* and is controlled by the `MS-DS-MachineQuota` value. You can modify this value by using the Active Directory Service Interfaces Editor (ADSI Edit) snap-in.



 **Note:** We recommend that you pre-create the computer account in the correct OU prior to joining the computer to the domain. This allows the computer to receive the appropriate group policies immediately. If you do not pre-create the computer account, it will be created in the Computers container.

### Delegating permissions

By default, the Enterprise Admins, Domain Admins, Administrators, and Account Operators groups have permission to create computer objects in any new OU. However, as discussed earlier, we recommend that you tightly restrict membership in the first three groups and that you not add users who are members of the Enterprise Admins, Domain Admins, or Administrators groups to the Account Operators group. Instead, we recommend that you delegate the permission to create computer objects to appropriate administrators or support personnel. This permission, which is assigned to the group that you are delegating administration to, allows group members to create computer objects in a specified OU. For example, you might allow your desktop support team to create computer objects in the clients OU and allow your file server administrators to create computer objects in the file servers OU.

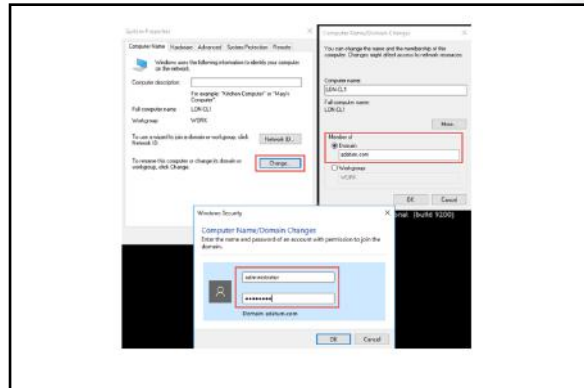
To delegate permissions to create computer accounts, you can use **Delegation of Control Wizard** to choose a custom task to delegate. When you delegate permissions to manage computer accounts, you might consider granting additional permissions beyond those required to create computer accounts. For example, you might decide to allow a delegated administrator to manage the properties of existing computer accounts, to delete the computer account, or to move the computer account.


## Joining a computer to a domain

The actual joining of the computer to the domain happens on the client computer. In Windows operating systems this happens on the **Computer Name** tab of Advanced system settings in the System applet in Control Panel.

Any user can access the Computer Name tab; however, to join the domain you must know the name of the domain and provide the credentials of a domain user that has the required permissions to join a computer to the domain.

To leave a domain is a similar process. Enter the name of the workgroup or other domain that you wish to join, and provide the proper credentials.



 **Note:** If you remove a computer from the domain to a workgroup, ensure that you know the credentials of a local account that has admin rights on the local computer.

The computer requires a restart when joining or leaving a domain.

## Computer accounts and secure channels

Every member computer in an AD DS domain maintains a computer account with a user name (SAMAccountName) and password, just like a user account does. The computer stores its password in the form of a local security authority (LSA) secret and changes its password with the domain approximately every 30 days. The Net Logon service uses the credentials to sign on to the domain, which establishes the secure channel with a domain controller.

Computer accounts and the secure relationships between computers and their domain are robust.

Nevertheless, there are certain scenarios in which a computer cannot authenticate with the domain. When this happens, users are unable to sign in and the computer cannot access resources, such as Group Policy. Examples of scenarios where this can happen include:

- After reinstalling the operating system on a workstation, the workstation cannot authenticate, even though the technician used the same computer name used in the previous installation. Because the new installation generated a new SID, and because the new computer does not know the original computer account password in the domain, it does not belong to the domain and cannot authenticate to the domain.
- A computer has not been used for an extended period, perhaps because the user was working away from the office or the computer was pre-built as a spare and was not needed for a long time. During this period, an administrator might have reset or deleted the computer account.

- Computers have accounts:
  - SAMAccountName and password
  - Used to create a secure channel between the computer and a domain controller
- Scenarios in which a secure channel might be broken:
  - Reinstalling a computer, even with same name, generates a new SID and password
  - Restoring a computer from an old backup or rolling back a computer to an old snapshot
  - The computer and domain disagreeing about what the password is



- A computer's LSA secret gets out of synchronization with the password that the domain knows. You can think of this as the computer forgetting its password. The computer did not actually forget its password: it just disagrees with the domain over what the password really is. When this happens, the computer cannot authenticate and the secure channel cannot be created.

The next topic discusses the steps to take when one of these scenarios happens.

## Resetting the secure channel

Occasionally, the security relationship between a computer account and its domain is broken. This results in numerous potential symptoms and errors. The most common signs of computer account problems are:

- Messages at sign in indicate that a domain controller cannot be contacted, that the computer account might be missing, that the password on the computer account is incorrect, or that the trust relationship (also called the secure relationship) between the computer and the domain has been lost.
- Error messages or events in the event log indicate similar problems or suggest that passwords, trusts, secure channels, or relationships with the domain or a domain controller have failed. One such error is NETLOGON Event ID 3210: Failed To Authenticate, which appears in the computer's event log.
- A computer account is missing in AD DS.

- Do not delete a computer from the domain and then rejoin it; this creates a new account, resulting in a new SID and lost group memberships
- Options for resetting the secure channel:
  - **nltest**
  - **netdom**
    - Active Directory Users and Computers
    - Active Directory Administrative Center
    - Windows PowerShell
  - **dsmod**

When the secure channel fails, you must reset it. Many administrators do this by removing the computer from the domain, putting it in a workgroup, and then rejoining the computer to the domain. When you remove the computer from the domain, the computer account in AD DS is disabled. When you rejoin the computer to the domain, the same computer account is reused and activated, but group memberships are lost. Do not rename the computer when you rejoin it to the domain.

You also can reset the secure channel between a domain member and the domain by using:

- Active Directory Users and Computers
- Active Directory Administrative Center
- The dsmod command-line tool
- The netdom command-line tool
- The nltest command-line tool

If you reset the account, the computer's SID remains the same, and the computer maintains its group memberships.

To reset the secure channel by using Active Directory Users and Computers or Active Directory Administrative Center, follow this procedure:

1. Right-click the computer and then click **Reset Account**.
2. Click **Yes** to confirm your choice.
3. Rejoin the computer to the domain, and then restart the computer.

To reset the secure channel by using **dsmod**, follow this procedure:

1. At a command prompt, type the following command:

```
dsmod computer "ComputerDN" -reset
```

2. Rejoin the computer to the domain, and then restart the computer.

To reset the secure channel by using **netdom**, type the following command at a command prompt, where the credentials belong to the local Administrators group of the computer:

```
netdom reset MachineName /domain DomainName /User0 UserName /Password0 {Password | *}
```

This command resets the secure channel by attempting to reset the password on both the computer and the domain, so it does not require rejoining or rebooting.

To reset the secure channel by using **nltest**, on the computer that has lost its trust, type the following command at a command prompt:

```
nltest /server:servername /sc_reset:domain\domaincontroller
```

You also can use Active Directory module for Windows PowerShell to reset a computer account. To reset the secure channel between the local computer and the domain to which it is joined, run this command on the local computer:

```
Test-ComputerSecureChannel -Repair
```

You can use this command as well:

```
invoke-command -computername Workstation1 -scriptblock {reset-computermachinepassword}
```

## Performing an offline domain join

Typically, when you want to join a computer to a domain, the computer must be able to communicate with an online domain controller. Beginning with the Windows Server 2008 R2 operating system, Microsoft introduced *offline domain join*, a feature that makes it possible for you to join a computer to a domain without communicating directly with an online domain controller. Offline domain join works with client computers that run Windows 7 and later and Windows Server 2008 R2 and later. This feature is useful in situations when connectivity is intermittent, such as when you are deploying a server to a remote site that is connected via satellite uplink.

Use offline domain join to join computers to a domain when they cannot contact a domain controller

- Create a domain join file by using:

```
djoin.exe /Provision /Domain <DomainName>  
/Machine <MachineName> /SaveFile <filepath>
```

- Import the domain join file by using:

```
djoin.exe /requestODJ /LoadFile <filepath>  
/WindowsPath <path to the Windows directory of  
the offline image>
```

Use the command-line tool **djoin** to perform an offline domain join. This generates a domain join file and then imports it to the client computer. When you perform an offline domain join you need to specify the following information:

- The domain that you are joining the computer to.
- The name of the computer that you are joining to the domain.
- The name of the savefile that you are transferring to the target of the offline domain join.

To perform an offline domain join, follow this procedure:

1. To provision a computer account in the domain and create the domain join file, open an elevated command prompt and use the **djoin** command with the **/provision** option. The format for this command is:

```
djoin.exe /Provision /Domain <DomainName> /Machine <MachineName> /SaveFile <filepath>
```

For example, to join the computer Canberra to the domain adatum.com by using the savefile CanberraJoin.txt, type the following command:

```
djoin.exe /provision /domain adatum.com /machine canberra /savefile  
c:\canberra-join.txt
```

If the computer account is not prestaged, it will be created in the Computers container. If the computer is prestaged, then you must include the **/reuse** option in the **djoin** command.

2. To transfer the savefile to the provisioned computer, use the **djoin** command with the **/requestODJ** option. The format for this command is:

```
djoin.exe /requestODJ /LoadFile <filepath> /WindowsPath <path to the Windows  
directory of the offline image>
```

Optionally, you can perform the import on an online operating system by using the **/localOS** option. If you are using the **/localOS** option, then set the **/WindowsPath** option to **%systemroot%** or **%windir%**. For example, to transfer the savefile Canberra-join.txt to the computer Canberra, type the following command on Canberra:

```
djoin.exe /requestODJ /loadfile canberra-join.txt /windowspath %systemroot% /localos
```

3. Start or restart the computer to complete the domain join operation.

**Question:** What causes a computer to lose its trust relationship with the domain?

## Lab A: Managing AD DS objects

### Scenario

You have been working for A. Datum Corporation as a desktop support specialist and have visited desktop computers to troubleshoot app and network problems. You recently accepted a promotion to the server support team. One of your first assignments is to configure the infrastructure service for a new branch office.

To begin deployment of the new branch office, you are preparing AD DS objects. As part of this preparation, you need to create users and groups for the new branch office that will house the Research department. Finally, you need to reset the secure channel for a computer account that has lost connectivity to the domain in the branch office.

### Objectives

After completing this lab, you will be able to:

- Create and configure groups in AD DS.
- Create and configure user accounts in AD DS.
- Manage computer objects in AD DS.

### Lab Setup

Estimated Time: 45 minutes

Virtual machines: **20742A-LON-DC1**, **20742A-LON-DC2** and **20742A-LON-CL1**

User name: **Adatum\Administrator**

Password: **Pa\$\$w0rd**

For this lab, you need to use the available VM environment. Before you begin the lab, you must complete the following steps:

1. On the host computer, start **Hyper-V Manager**.
2. In Hyper-V Manager, click **20742A-LON-DC1**, and then in the **Actions** pane, click **Start**.
3. In the **Actions** pane, click **Connect**. Wait until the VM starts.
4. Sign in by using the following credentials:
  - User name: **Administrator**
  - Password: **Pa\$\$w0rd**
  - Domain: **Adatum**
5. Repeat steps 1-4 for **20742A-LON-DC2**.
6. Repeat steps 1-3 for **20742A-LON-CL1**. Do not sign on to **LON-CL1** until instructed to do so in the lab steps.

## Exercise 1: Creating and managing groups in AD DS

### Scenario

You need to create groups for the Research department. A distribution global group is required to facilitate email delivery to the research users. This group will be managed by Cai Chu. You will also create a research managers group and add Cai Chu and Vera Pace as members of the group. You also need to create a universal group in the Managers OU that will contain all the departmental managers' global groups. After creating the research distribution group, you are told that the group needs access to network resources so you must convert the group to become a security group.

The main tasks for this exercise are as follows:

1. Create groups and add members.
2. Configure group nesting.
3. Convert a group type from distribution to security.

#### ► Task 1: Create groups and add members

1. On **LON-DC1** use **Active Directory Administrative Center** to create the following groups:
  - In the **Managers** OU, create a universal group named **Enterprise Managers**.
  - In the **Research** OU, create a global distribution group named **Research Mail**.
2. Configure the email address of the **Research Mail** group to be **Research@adatum.com**.
3. Configure the **Research Mail** group to be managed by **Cai Chu**.
4. Provide **Cai Chu** with the right to update the group membership list.
5. In the **Research** OU, create a new global security group named **Research Managers**.
6. Add **Cai Chu** and **Vera Pace** as members.

#### ► Task 2: Configure group nesting

- Browse to the **Managers** OU, add the **Managers** global group and the **Research Managers** global group as members to the **Enterprise Managers** universal group.

#### ► Task 3: Convert a group type from distribution to security

- In the **Research** OU, change the group type of the **Research Mail** group to be a **Security** group.

**Results:** After completing this exercise you will have:

- Created groups and added members
- Configured group nesting
- Converted a group type

## Exercise 2: Creating and configuring user accounts in AD DS

### Scenario

You have been given a list of new users to be created for the branch office. You have decided to create a template to facilitate the quick creation of users for the branch. You will validate that template by creating a new test user and checking the properties.

The main tasks for this exercise are as follows:

1. Create and configure a user template for the Research department.
2. Create new users for the Research branch office based on the template.
3. Validate the template.

#### ► Task 1: Create and configure a user template for the Research department

1. Create a new user in the **Research** OU with the following properties:
  - Name: **\_Research Template**
  - User UPN Logon: **ResearchTemplate**
  - Password: **Pa\$\$w0rd**
  - Department: **Research**
  - Company: **Adatum**
  - Manager: **Cai Chu**
  - Member of: **Research**
  - Logon script: **\\LON-DC1\Netlogon\Logon.bat**
  - Disable the account.
2. Close Active Directory Administrative Center.

#### ► Task 2: Create new users for the Research branch office based on the template

1. Use **Active Directory Users and Computers** to copy the **\_Research Template** account.
2. Create the new user from the template with the following properties:
  - First name: **Research**
  - Last name: **User**
  - Password: **Pa\$\$w0rd**
  - Account status: **Enabled**

### ► Task 3: Validate the template

- Inspect the properties of the Research User and ensure that the properties are:
  - Logon script: `\\LON-DC1\Netlogon\Logon.bat`
  - Department: **Research**
  - Company: **Adatum**
  - Member Of: **Research**

**Results:** After completing this exercise, you will have:

- Created and configured a user template for research users.
- Created three new users based on the template.
- Signed on to test that the accounts are functioning as expected.

## Exercise 3: Managing computer objects in AD DS

### Scenario

A user is unable to sign on and a workstation has lost its connectivity to the domain and cannot authenticate users properly. When users attempt to access resources from this workstation, access is denied. You need to repair the trust relationship between the computer and the domain.

The main tasks for this exercise are as follows:

1. Reset a computer account.
2. Observe the behavior when a client attempts to sign on.
3. Resolve the computer issue.

### ► Task 1: Reset a computer account

- Right-click **LON-CL1** in the computers container and reset the account.

### ► Task 2: Observe the behavior when a client attempts to sign on

- Restart **LON-CL1** and attempt to sign in as **Adatum\Adam** with a password of **Pa\$\$w0rd**.

**Question:** What is the message displayed?

**Answer:** The trust relationship between this workstation and the primary domain failed.

► **Task 3: Resolve the computer issue**

1. Sign on to **LON-CL1** as **Adatum\Administrator** with a password of **Pa\$\$w0rd**.
2. Start an elevated session of Windows PowerShell and run the following command:

```
Test-ComputerSecureChannel -Repair
```

3. Sign out of **LON-CL1**, and then attempt to sign in as **Adatum\Adam**. The sign in will succeed now.
4. Sign out of **LON-CL1**.
5. Leave the VMs running for the next lab.

**Results:** After completing this exercise, you will have:

- Reset a computer account.
- Observed the behavior when a client signs on.
- Resolved the computer issue.

**Question:** What types of objects can be members of global groups?

**Question:** What credentials are necessary for any computer to join a domain?



## Lesson 4

# Using Windows PowerShell for AD DS administration

You can use Windows PowerShell to automate AD DS administration. Automating administration speeds up processes that you might otherwise perform manually. Windows PowerShell includes cmdlets for performing AD DS administration and for performing bulk operations. You can use bulk operations to change many AD DS objects in a single step rather than updating each object manually.

## Lesson Objectives

After completing this lesson, you will be able to:

- Use Windows PowerShell to manage user accounts.
- Use Windows PowerShell to manage groups.
- Use Windows PowerShell to manage computer accounts.
- Use Windows PowerShell to manage OUs.
- Describe bulk operations.
- Use graphical tools to perform bulk operations.
- Use Windows PowerShell to query objects.
- Use Windows PowerShell to modify objects.
- Work with comma separated value (CSV) files.
- Use Windows PowerShell to perform bulk operations.

## Using Windows PowerShell cmdlets to manage user accounts

You can use Windows PowerShell cmdlets to create, modify, and delete user accounts. You can use these cmdlets for individual operations or as part of a script to perform bulk operations. The following table lists some of the commonly used cmdlets for managing user accounts.

Cmdlet	Description
New-ADUser	Creates user accounts
Set-ADUser	Modifies properties of user accounts
Remove-ADUser	Deletes user accounts
Set-ADAccountPassword	Resets the password of a user account
Set-ADAccountExpiration	Modifies the expiration date of a user account
Unlock-ADAccount	Unlocks a user account after it has become locked after too many incorrect sign in attempts
Enable-ADAccount	Enables a user account
Disable-ADAccount	Disables a user account
<b>New-ADUser "Sten Faerch" -AccountPassword (Read-Host -AsSecureString "Enter password") -Department IT</b>	

Cmdlet	Description
<b>New-ADUser</b>	Creates user accounts.
<b>Set-ADUser</b>	Modifies properties of user accounts.
<b>Remove-ADUser</b>	Deletes user accounts.
<b>Set-ADAccountPassword</b>	Resets the password of a user account.
<b>Set-ADAccountExpiration</b>	Modifies the expiration date of a user account.

Cmdlet	Description
<b>Unlock-ADAccount</b>	Unlocks a user account when it is locked after exceeding the accepted number of incorrect sign-in attempts.
<b>Enable-ADAccount</b>	Enables a user account.
<b>Disable-ADAccount</b>	Disables a user account.

### Create new user accounts

When you use the **New-ADUser** cmdlet to create new user accounts, you can set most user properties including a password. For example:

- If you do not use the **-AccountPassword** parameter, then no password is set and the user account is disabled. The **-Enabled** parameter cannot be set as **\$true** when no password is set.
- If you use the **-AccountPassword** parameter to specify a password, then you must specify a variable that contains the password as a secure string or choose to receive a prompt for the password. A secure string is encrypted in memory. If you set a password, then you can enable the user account by setting the **-Enabled** parameter as **\$true**.

The following table lists commonly used parameters for the **New-ADUser** cmdlet.

Parameter	Description
<b>AccountExpirationDate</b>	Defines the expiration date for the user account.
<b>AccountPassword</b>	Defines the password for the user account.
<b>ChangePasswordAtLogon</b>	Requires the user account to change passwords at the next sign in.
<b>Department</b>	Defines the department for the user account.
<b>HomeDirectory</b>	Defines the location of the home directory for a user account.
<b>HomeDrive</b>	Defines the drive letters that are mapped to the home directory for a user account.
<b>GivenName</b>	Defines the first name for a user.
<b>Surname</b>	Defines the last name for a user.
<b>Path</b>	Defines the OU or container where the user account is created.

The following command is an example of a command that you could use to create a user account with a prompt for a password:

```
New-ADUser "Sten Faerch" -AccountPassword (Read-Host -AsSecureString "Enter password")
-Department IT
```

## Using Windows PowerShell cmdlets to manage groups

You can use Windows PowerShell to create, modify, and delete groups in much the same way that you do for users. You can use these cmdlets for individual operations or as part of a script to perform bulk operations. Some of the cmdlets for managing groups are listed in the following table.

Cmdlet	Description
<b>New-ADGroup</b>	Creates new groups
<b>Set-ADGroup</b>	Modifies properties of groups
<b>Get-ADGroup</b>	Displays properties of groups
<b>Remove-ADGroup</b>	Deletes groups
<b>Add-ADGroupMember</b>	Adds members to groups
<b>Get-ADGroupMember</b>	Displays membership of groups
<b>Remove-ADGroupMember</b>	Removes members from groups
<b>Add-ADPrincipalGroupMembership</b>	Adds group membership to objects
<b>Get-ADPrincipalGroupMembership</b>	Displays group membership of objects
<b>Remove-ADPrincipalGroupMembership</b>	Removes group membership from an object

```
New-ADGroup -Name "CustomerManagement" -Path
"ou=managers,dc=adatum,dc=com" -GroupScope Global
-GroupCategory Security

Add-ADGroupMember -Name "CustomerManagement"
-Members "Joe"
```

Cmdlet	Description
<b>New-ADGroup</b>	Creates new groups.
<b>Set-ADGroup</b>	Modifies properties of groups.
<b>Get-ADGroup</b>	Displays properties of groups.
<b>Remove-ADGroup</b>	Deletes groups.
<b>Add-ADGroupMember</b>	Adds members to groups.
<b>Get-ADGroupMember</b>	Displays members of groups.
<b>Remove-ADGroupMember</b>	Removes members from a group.
<b>Add-ADPrincipalGroupMembership</b>	Adds group membership to objects.
<b>Get-ADPrincipalGroupMembership</b>	Displays group membership of objects.
<b>Remove-ADPrincipalGroupMembership</b>	Removes group membership from an object.

### Create new groups

You can use the **New-ADGroup** cmdlet to create groups. However, when you create groups by using the **New-ADGroup** cmdlet, you must use the **GroupScope** parameter in addition to the group name. This is the only required parameter. The following table lists commonly used parameters for **New-ADGroup**.

Parameter	Description
<b>Name</b>	Defines the name of the group.
<b>GroupScope</b>	Defines the scope of the group as <b>DomainLocal</b> , <b>Global</b> , or <b>Universal</b> . You must provide this parameter.
<b>DisplayName</b>	Defines the Lightweight Directory Access Protocol (LDAP) display name for the object.
<b>GroupCategory</b>	Defines whether it is a security group or a distribution group. If you do not specify either, a security group is created.

Parameter	Description
<b>ManagedBy</b>	Defines a user or group that can manage the group.
<b>Path</b>	Defines the OU or container in which the group is created.
<b>SamAccountName</b>	Defines a name that is backward compatible with older operating systems.


The following command is an example of what you could type at a Windows PowerShell prompt to create a new group:

```
New-ADGroup -Name "CustomerManagement" -Path "ou=managers,dc=adatum,dc=com" -GroupScope Global -GroupCategory Security
```

### Manage group membership

There are two sets of cmdlets that you can use to manage group membership: **\*-ADGroupMember** and **\*-ADPrincipalGroupMembership**. The distinction between these two sets of cmdlets is the perspective used when modifying group membership:

- The **\*-ADGroupMember** cmdlets modify the membership of a group. For example, you add or remove members of a group.
  - You cannot pipe a list of members to these cmdlets.
  - You can pass a list of groups to these cmdlets.
- The **\*-ADPrincipalGroupMembership** cmdlets modify the group membership of an object such as a user. For example, you can modify a user account to add it as a member of a group.
  - You can pipe a list of members to these cmdlets.
  - You cannot provide a list of groups to these cmdlets.

 **Note:** Piping is a common process in scripting languages that allows you to use the output of one cmdlet as input for the next cmdlet in the command. For example, this command creates a user account and then enables the account:

```
New-ADUser -Name "Sten Faerch" -AccountPassword (Read-Host -AsSecureString "Enter password") | Enable-Account
```

### Using Windows PowerShell cmdlets to manage computer accounts

You can use Windows PowerShell to create, modify, and delete computer accounts. You can use these cmdlets for individual operations or as part of a script to perform bulk operations. The following table lists cmdlets that you can use to manage computer accounts.

Cmdlet	Description
<b>New-ADComputer</b>	Creates new computer accounts
<b>Set-ADComputer</b>	Modifies properties of computer accounts
<b>Get-ADComputer</b>	Displays properties of computer accounts
<b>Remove-ADComputer</b>	Deletes computer accounts
<b>Test-ComputerSecureChannel</b>	Verifies or repairs the trust relationship between a computer and the domain
<b>Reset-ComputerMachinePassword</b>	Resets the password for a computer account

```
New-ADComputer -Name "LON-SVR8" -Path "ou=marketing,dc=adatum,dc=com" -Enabled $true
```

```
Test-ComputerSecureChannel -Repair
```

Cmdlet	Description
<b>New-ADComputer</b>	Creates a new computer account.
<b>Set-ADComputer</b>	Modifies properties of a computer account.
<b>Get-ADComputer</b>	Displays properties of a computer account.
<b>Remove-ADComputer</b>	Deletes a computer account.
<b>Test-ComputerSecureChannel</b>	Verifies or repairs the trust relationship between a computer and the domain.
<b>Reset-ComputerMachinePassword</b>	Resets the password for a computer account.

### Create new computer accounts

You can use the **New-ADComputer** cmdlet to create a new computer account before you join the computer to the domain. You do this so that you can create the computer account in the correct OU before deploying the computer.

The following table lists commonly used parameters for **New-ADComputer**.

Parameter	Description
<b>Name</b>	Defines the name of the computer account.
<b>Path</b>	Defines the OU or container where the computer account is created.
<b>Enabled</b>	Defines whether the computer account is enabled or disabled. By default, the computer account is enabled and a random password is generated.

The following command is an example of a command that you can use to create a computer account:

```
New-ADComputer -Name LON-SVR8 -Path "ou=marketing,dc=adatum,dc=com" -Enabled $true
```

### Repair the trust relationship for a computer account

You can use the **Test-ComputerSecureChannel** cmdlet with the **-Repair** parameter to repair a lost trust relationship between a computer and the domain. You must run the cmdlet on the computer with the lost trust relationship.

## Using Windows PowerShell cmdlets to manage OUs

You can use Windows PowerShell cmdlets to create, modify, and delete OUs. You can use these cmdlets for individual operations or as part of a script to perform bulk operations. The following table lists cmdlets that you can use to manage OUs.

Cmdlet	Description
<b>New-ADOrganizationalUnit</b>	Creates OUs
<b>Set-ADOrganizationalUnit</b>	Modifies properties of OUs
<b>Get-ADOrganizationalUnit</b>	Views properties of OUs
<b>Remove-ADOrganizationalUnit</b>	Deletes OUs

```
New-ADOrganizationalUnit -Name "Sales"
-Path "ou=marketing,dc=adatum,dc=com"
-ProtectedFromAccidentalDeletion $true
```

Cmdlet	Description
<b>New-ADOrganizationalUnit</b>	Creates OUs.
<b>Set-ADOrganizationalUnit</b>	Modifies properties of OUs.
<b>Get-ADOrganizationalUnit</b>	Displays properties of OUs.
<b>Remove-ADOrganizationalUnit</b>	Deletes OUs.

### Create new OUs

You can use **New-ADOrganizationalUnit** cmdlet to create a new OU to represent departments or physical locations within in your organization.

The following table shows commonly used parameters for the **New-ADOrganizationalUnit** cmdlet.

Cmdlet	Description
<b>Name</b>	Defines the name of the new OU.
<b>Path</b>	Defines the location of the new OU.
<b>ProtectedFromAccidentalDeletion</b>	Prevents the OU from being deleted accidentally. The default value is <b>\$true</b> .

The following command is an example of a command that you can use when you want to create a new OU:

```
New-ADOrganizationalUnit -Name Sales -Path "ou=marketing,dc=adatum,dc=com"
-ProtectedFromAccidentalDeletion $true
```

## What are bulk operations?

A *bulk operation* is a single action that changes multiple objects. Performing a bulk operation is much faster than changing many objects individually. It might also be more accurate, because performing many individual actions increases the likelihood of making a typographical mistake. However, due to the nature of bulk operations, if you introduce a mistake, it will be multiplied to every single object being changed. Therefore, ensure that you test your bulk operation on a smaller object set before executing it on all the elements that you want to modify.

- A bulk operation is a single action that changes multiple objects
- Sample bulk operations:
  - Create user accounts based on data in a spreadsheet
  - Disable all accounts not used in six months
  - Rename the department for many users
- You can perform bulk operations by using:
  - Graphical tools
  - Command-line tools
  - Scripts

Common bulk operations in a Windows Server environment include:

- Create new user accounts based on information from a spreadsheet.
- Disable all user accounts that have not been used in the past six months.
- Change the department name for all users belonging to a given department.

You can perform bulk operations with graphical tools, at a command prompt, or by using scripts. Each method for performing bulk operations has different capabilities. Consider that:

- Graphical tools tend to be limited in the properties that they can modify.
- Command-line tools tend to be more flexible than graphical tools when defining queries, and they have more options for modifying object properties.
- Scripts can combine multiple command-line actions for the most complexity and flexibility.

## Demonstration: Using graphical tools to perform bulk operations

In this demonstration, you will see how to use Active Directory Users and Computers to change the **Office** attribute for users in the Research OU as a bulk operation.

### Demonstration Steps

1. Open **Active Directory Users and Computers**, and then select the **Research** OU.
2. Sort the object by **Type**, and then select all the **User** objects.
3. Modify the properties to set the **Office** attribute to be **Winnipeg**.
4. Check the **General** tab in the properties of one of the users to ensure the update has occurred.
5. Close **Active Directory Users and Computers**.

## Querying objects with Windows PowerShell

In Windows PowerShell, you use the **Get-\*** cmdlets to obtain lists of objects, such as user accounts. You can also use these cmdlets to generate queries for objects on which you can perform bulk operations. The following table lists parameters that are commonly used with the **Get-AD\*** cmdlets.

Parameter	Description
SearchBase	Defines the AD DS path to begin searching
SearchScope	Defines at what level below the SearchBase a search should be performed
ResultSetSize	Defines how many objects to return in response to a query
Properties	Defines which object properties to return and display
Filter	Defines a filter by using PowerShell syntax
LDAPFilter	Defines a filter by using LDAP query syntax

Descriptions of operators

-eq	Equal to	-gt	Greater than
-ne	Not equal to	-ge	Greater than or equal to
-lt	Less than	-like	Uses wildcards for pattern matching
-le	Less than or equal to		

Parameter	Description
<b>SearchBase</b>	Defines the AD DS path to begin searching: for example, the domain or an OU.
<b>SearchScope</b>	Defines at what level below <b>SearchBase</b> that the search should be performed. You can choose to search only in the base, one level down, or the entire subtree.
<b>ResultSetSize</b>	Defines how many objects to return in response to a query. To ensure that all objects are returned, set this to <b>\$null</b> .
<b>Properties</b>	Defines which object properties to return and display. To return all properties, type an asterisk (*). You do not need to use this parameter to use a property for filtering.

### Create a query

You can use the **Filter** parameter or the **LDAPFilter** parameter to create queries for objects with the **Get-AD\*** cmdlets. Use the **Filter** parameter for queries that you write in Windows PowerShell, and use the **LDAPFilter** parameter for queries that you write as LDAP query strings.

Windows PowerShell is preferable because:

- It is easier to write queries in Windows PowerShell.
- You can use variables inside the queries.
- There is automatic conversion of variable types when it is required.

The following table lists commonly used operators in Windows PowerShell.

Operator	Description
<b>-eq</b>	Equal to
<b>-ne</b>	Not equal to
<b>-lt</b>	Less than
<b>-le</b>	Less than or equal to
<b>-gt</b>	Greater than



Operator	Description
<b>-ge</b>	Greater than or equal to
<b>-like</b>	Uses wildcards and pattern matches

## Filter

As previously mentioned, you can use the **Filter** parameter to filter data retrieved by a **Get-\*** cmdlet. The **Filter** parameter uses the same syntax as the **Where-Object** cmdlet in Windows PowerShell. As an example, this command retrieves all user accounts that have Smith as their last name, followed by the output of the command:

```
Get-ADUser -Filter {sn -eq "Smith"}
DistinguishedName : CN=Denise Smith,OU=Marketing,DC=Adatum,DC=com
Enabled           : True
GivenName        : Denise
Name             : Denise Smith
ObjectClass      : user
ObjectGUID       : 1ff1b2cb-38c1-4bc7-bda7-511e19744d2a
SamAccountName   : Denise
SID              : S-1-5-21-322346712-1256085132-1900709958-1407
Surname          : Smith
UserPrincipalName : Denise@adatum.com
DistinguishedName : CN=Tony Smith,OU=IT,DC=Adatum,DC=com
Enabled           : True
GivenName        : Tony
Name             : Tony Smith
ObjectClass      : user
ObjectGUID       : ac7eb8db-3cf1-4e6d-91d3-7527e540c284
SamAccountName   : Tony
SID              : S-1-5-21-322346712-1256085132-1900709958-1408
Surname          : Smith
UserPrincipalName : Tony@adatum.com
```

One of the characteristics of all **Get-\*** cmdlets that you use to retrieve data from AD DS is that they do not always return all properties for the objects that they retrieve. For instance, looking at the output above you see only some of the properties that a user account has in AD DS. You do not see, for instance, the **mail** property. You can use the **-Properties** parameters to retrieve properties not returned by default when you run **Get-\*** cmdlets. For example, the code below returns the same list of users, but this time with the **mail** and **PasswordLastSet** properties:

```
Get-ADUser -Filter {sn -eq "Smith"} -Properties mail,passwordlastset
DistinguishedName : CN=Denise Smith,OU=Marketing,DC=Adatum,DC=com
Enabled           : True
GivenName        : Denise
Name             : Denise Smith
ObjectClass      : user
ObjectGUID       : 1ff1b2cb-38c1-4bc7-bda7-511e19744d2a
PasswordLastSet  : 7/9/2016 12:51:30 PM
SamAccountName   : Denise
SID              : S-1-5-21-322346712-1256085132-1900709958-1407
Surname          : Smith
UserPrincipalName : Denise@adatum.com
DistinguishedName : CN=Tony Smith,OU=IT,DC=Adatum,DC=com
Enabled           : True
GivenName        : Tony
Name             : Tony Smith
ObjectClass      : user
ObjectGUID       : ac7eb8db-3cf1-4e6d-91d3-7527e540c284
PasswordLastSet  : 7/9/2016 12:51:30 PM
SamAccountName   : Tony
SID              : S-1-5-21-322346712-1256085132-1900709958-1408
Surname          : Smith
UserPrincipalName : Tony@adatum.com
```

Use the following command to display all of the properties for a user account:

```
Get-ADUser -Name "Administrator" -Properties *
```

Use the following command to return all the user accounts in the Marketing OU and all of its child OUs:

```
Get-ADUser -Filter * -SearchBase "ou=Marketing,dc=adatum,dc=com" -SearchScope subtree
```

Use the following command to show all of the user accounts with a last sign in date older than a specific date:

```
Get-ADUser -Filter {lastlogondate -lt "January 1, 2016"}
```

Use the following command to show all of the user accounts in the Marketing department that have a last sign in date older than a specific date:

```
Get-ADUser -Filter {(lastlogondate -lt "January 1, 2016") -and (department -eq "Marketing")}
```



**Additional Reading:** For more information, refer to: "about\_ActiveDirectory\_Filter" at: <http://aka.ms/Kv5dy3>

## LDAPFilter

You can also use the **LDAPFilter** parameter to filter data retrieved by a **Get-\*** cmdlet. The **LDAPFilter** parameter takes a string value that uses the same syntax you use to build an LDAP query. For example, this command retrieves all users whose last name is Smith:

```
Get-ADUser -LDAPFilter "(sn=Smith)"
```

## Search-ADAccount

One of the downfalls of the **Get-AD\*** cmdlets is how they deal with the **UserAccountControl** property. This property is a 4-byte bitmap, where each bit corresponds to a different property linked to an Active Directory account. The table below shows some of the bits in the bit map.

Hexadecimal value	Decimal value	Identifier	Description
0x00000001	1	ADS_UF_SCRIPT	Logon script is executed.
0x00000002	2	ADS_UF_ACCOUNTDISABLE	User account is disabled.
0x00000008	8	ADS_UF_HOMEDIR_REQUIRED	A home folder is required.
0x00000010	16	ADS_UF_LOCKOUT	User account is locked out.



**Additional Reading:** For more information, refer to: "How to use the UserAccountControl flags to manipulate user account properties" at: <http://aka.ms/Mxt8a1>

When you read the **UserAccountControl**, you receive a numerical value not a group of true/false values per individual flag. For example, the following code shows the **UserAccountControl** property for all users whose last name begins with *Sm*:

```
Get-ADUser -Filter {sn -like "Sm*"} -Properties userAccountControl|Select Name,
userAccountControl|FT -AutoSize
Name          userAccountControl
----          -
Denise Smith   66048
Tony Smith     66048
```

Imagine that you need to retrieve a list of all disabled accounts in AD DS. To do that, you need to retrieve all accounts in which the **UserAccountControl** property has the second to last bit enabled. You can do this by using this code:

```
Get-ADUser -LDAPFilter "(userAccountControl:1.2.840.113556.1.4.803:=2)"|Select Name
```

Memorizing, or even looking up, flags in the **UserAccountControl** property is a time-consuming job. Of course, you can create scripts that already have the code built in and just reuse them. However, it would be much better to have a command that abstracts all that work for you, which is what the **Search-ADAccount** cmdlet does. You can retrieve a list of disabled accounts by using the **Search-ADAccount** cmdlet as follows:

```
Search-ADAccount -AccountDisabled | Select name
```

That is much easier than using **Get-ADUser**. The following table lists the parameters that the **Search-ADAccount** cmdlet uses.

Parameter	Description
<b>AccountDisabled</b>	Retrieves a list of disabled accounts.
<b>AuthType</b>	Specifies the authentication type used when running this command.
<b>AccountExpired</b>	Retrieves a list of accounts that have expired.
<b>AccountExpiring</b>	Retrieves a list of accounts that expire within a given time span.
<b>AccountInactive</b>	Retrieves a list of accounts that will become inactive within a given time span.
<b>LockedOut</b>	Retrieves a list of accounts that are locked out.
<b>PasswordExpired</b>	Retrieves a list of accounts that have expired passwords.
<b>PasswordExpiring</b>	Retrieves a list of accounts that have passwords that will expire within a period.
<b>PasswordNeverExpires</b>	Retrieves a list of accounts that have passwords that never expire.
<b>ComputersOnly</b>	Retrieves computer accounts.
<b>UsersOnly</b>	Retrieves user accounts.
<b>TimeSpan</b>	Used in conjunction with <b>PasswordExpiring</b> , <b>AccountExpiring</b> , and <b>AccountInactive</b> to specify the time span for those parameters.
<b>DateTime</b>	Used in conjunction with <b>PasswordExpiring</b> , <b>AccountExpiring</b> , and <b>AccountInactive</b> to specify the expiration date for those parameters.

Parameter	Description
<b>SearchBase</b>	Specifies the base LDAP container for the search.
<b>SearchScope</b>	Specifies the scope for the search.
<b>Server</b>	Specifies the server to connect to.

Here are some examples of the **Search-ADAccount** cmdlet:

```
# Retrieve all disabled user accounts
Search-ADAccount -AccountDisabled -UsersOnly
# Retrieve all user accounts inactive for the last 5 days
Search-ADAccount -AccountInactive -TimeSpan -5 -UsersOnly
# Retrieve all user accounts whose password will expire on 7/4/2016
Search-ADAccount -AccountExpiring -DateTime "4/7/2016" -UsersOnly
# Retrieve all computer accounts that are locked out
Search-ADAccount -ComputersOnly -LockedOut
```

## Modifying objects with Windows PowerShell

To perform a bulk operation, you need to pass the list of objects that you have queried to another cmdlet to modify the objects. In most cases, you use the **Set-AD\*** cmdlets to modify the objects.

To pass the list of queried objects to another cmdlet for further processing, you use the pipe (|) character. The pipe character passes each object from the query to a second cmdlet, which then performs a specified operation on each object.

You can use the following command for those accounts that do not have the **Company** attribute set. It generates a list of user accounts and sets the **Company** attribute to A. Datum.

Use the pipe character (|) to pass a list of objects to a cmdlet for further processing

```
Get-ADUser -Filter {company -notlike "*"} |
Set-ADUser -Company "A. Datum"
```

```
Get-ADUser -Filter {lastlogondate -lt "January 1,
2016"} | Disable-ADAccount
```

```
Get-Content C:\users.txt | Disable-ADAccount
```

```
Get-ADUser -Filter {company -notlike "*"} | Set-ADUser -Company "A. Datum"
```



**Additional Reading:** For more information, refer to: "Set-ADUser" at: <http://aka.ms/K34c8d>

There are many possible commands that you can use. Here are some examples. To generate a list of user accounts that have not signed on since a specific date and then disable those accounts you could use the following command:

```
Get-ADUser -Filter {lastlogondate -lt "January 1, 2012"} | Disable-ADAccount
```

### Use objects from a text file

Instead of using a list of objects from a query to perform a bulk operation, you can use a list of objects in a text file. This is useful when you have a list of objects to modify or remove, and it is not possible to generate that list by using a query. For example, the Human Resources department might generate a list of user accounts to be disabled. There is no query that can identify a list of users that have left the organization.

When you use a text file to specify a list of objects, the text file needs to have the name of each object on a single line.

This is a possible command you could use to disable the user accounts that are listed in a text file:

```
Get-Content C:\users.txt | Disable-ADAccount
```

### Working with CSV files

A .csv file can contain much more information than a simple list. Similar to a spreadsheet, a .csv file can have multiple rows and columns of information. Each row in the .csv file represents a single object, and each column in the .csv file represents a property of the object. This is useful for bulk operations such as creating user accounts when multiple pieces of information about each object are required.

You can use the **Import-Csv** cmdlet to read the contents of a .csv file into a variable and then work with the data. After the data is imported into the variable, you can refer to each individual row of data and each individual column of data. Each column of data has a name that is based on the header row (the first row) of the .csv file, and you can refer to each column by its name.

Here is an example of a .csv file with a header row:

```
FirstName,LastName,Department
Greg,Guzik,IT
Robin,Young,Research
Qiong,Wu,Marketing
```

Use **foreach** to process CSV data.

In many cases, you will create scripts that you will reuse for multiple .csv files, and you will not know how many rows there are in each .csv file. In these cases, you can use a **foreach** loop to process each row in a .csv file. You do not need to know how many rows there are. During each iteration of the **foreach** loop, a row from the .csv is imported into a variable that is then processed.

The first line of a .csv file defines the names of the columns

```
FirstName,LastName,Department
Greg,Guzik,IT
Robin,Young,Research
Qiong,Wu,Marketing
```

A **foreach** loop processes the contents of a .csv file that have been imported into a variable

```
$users=Import-Csv -LiteralPath "C:\users.csv"
foreach ($user in $users) {
    Write-Host "The first name is:"
    $user.FirstName
}
```

Use this command to import a .csv file into a variable, and use a **foreach** loop to display the first name from each row in a .csv file:

```
$users=Import-CSV -LiteralPath "C:\users.csv"
foreach ($user in $users)
{
    Write-Host "The first name is:" $user.FirstName"
}
```

## Demonstration: Performing bulk operations with Windows PowerShell

You can use a script to combine multiple Windows PowerShell commands to perform more complex tasks. Within a script, you often use variables and loops to process data. Windows PowerShell scripts have a .ps1 extension.

The execution policy on a server determines whether scripts are able to run. The default execution policy on Windows Server 2016 is **RemoteSigned**. This means that local scripts can run without being signed digitally. You can control the execution policy by using the **Set-ExecutionPolicy** cmdlet.

### Demonstration Steps

#### Create a new global group in the IT department

1. On **LON-DC1**, start a **Windows PowerShell** session with elevated permissions.
2. Run the following command:

```
New-ADGroup -Name Helpdesk -Path "ou=IT,dc=Adatum,dc=com" -GroupScope Global
```

#### Add all users in the IT department to the Helpdesk group

- In the Administrator: Windows PowerShell window, run the following command:

```
Get-ADUser -Filter "Department -eq 'IT'" | foreach {Add-ADGroupMember "Helpdesk" -members $_}
```

#### Set the address for all users in the Research department

- In the Administrator: Windows PowerShell window, run the following command:

```
Get-ADUser -Filter {Department -eq "Research"} | Set-ADUser -StreetAddress "1530 Taylor Ave." -City "Winnipeg" -State "Manitoba" -Country "CA"
```



**Note:** Notice that this command filters using brackets rather than quotes and uses the **Set-ADUser** cmdlet rather than a **foreach** loop.

#### Create a new OU

- In the Administrator: Windows PowerShell window, run the following command:

```
New-ADOrganizationalUnit London -Path "dc=Adatum,dc=com"
```

**Run a script to create new users from a .csv file**

1. Open **E:\Labfiles\Mod02**, and then use Notepad to open **DemoUsers.csv**. Describe the makeup of the .csv file.
2. Close the file.
3. In Windows PowerShell, change to the root directory **E:\Labfiles\Mod02**.
4. Run the **DemoUsers.ps1** script.

**Verify that the user accounts were created and that the accounts were modified**

- In **Active Directory Users and Computers** confirm that:
  - The **London** OU exists.
  - There are three users in the **London** OU.
  - The **Helpdesk** group exists in the **IT** OU and that it is populated with IT users.
  - The users in the **Research** OU have their address fields populated.

**Question:** What is Windows PowerShell Integrated Scripting Environment?

## Lesson 5

# Implementing and managing OUs

When designing your OU structure, planning the Active Directory administrative tasks delegation model is essential. Although you can use OUs to apply group policies, partition objects, or represent your organization's business structure, the most important design consideration for the OU structure is the administrative tasks delegation model, which depends on the processes and administrative requirements in your organization. In this lesson, you will learn about planning and considerations for OU structure, how permissions work for OUs, and how to delegate permissions for administrative tasks.

### Lesson Objectives

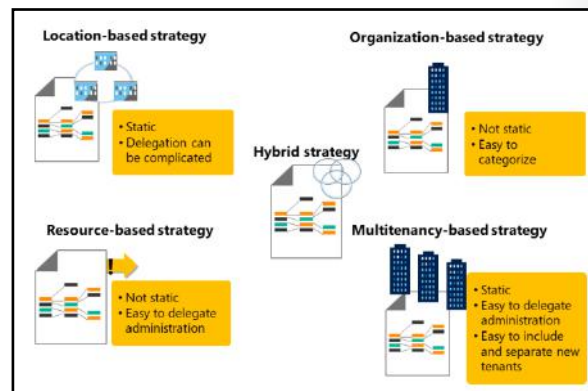
After completing this lesson, you will be able to:

- Plan OUs.
- Describe OU hierarchy considerations.
- Describe considerations for using OUs.
- Explain AD DS permissions.
- Delegate AD DS permissions.
- Delegate administrative permissions on an OU.

### Planning OUs

As one of the most important administrative components in your Active Directory domain, OUs enable you to partition and organize all the objects in the domain into a hierarchical structure. OUs can help you to:

- Delegate rights to administrative groups, enabling them to administer certain objects or attributes of objects below that OU.
- Apply group policies to users and computer objects below that OU.
- Create a hierarchy that enables you to administer the objects in the domain quickly.



There are several strategies for designing OU structures. The following OU design strategies are the most common:

#### Location-based strategy

This strategy uses locations for each top-level OU in the root of the domain. These location-based OUs are the main organizational element of the OU structure. For example, A. Datum Corporation might use a location-based strategy to create OUs for each of its physical locations—in London, Toronto, and Sydney—and then create additional OUs for their branch distribution centers. Each AD DS resource (such as users, groups, and computers) is located in the OU that corresponds to the location where the resource resides.



The location-based strategy is commonly used when each location operates relatively independently or when many tasks are delegated to decentralized administrators. For example, the administrative staff in London can perform the main administrative duties. Administrators in Sydney or Toronto who have some delegated rights can access their users, groups, and computers quickly. It is advantageous for the local staff to fulfill some administrative duties across different types of objects in the same branch. In addition, you do not have to move objects frequently between the top-level OUs, unless the objects move to another physical location. This likely requires moving home folders or Microsoft Exchange Server mailboxes. The location-based strategy also works well for organizations that expect to expand into new locations, because you can add new locations easily to the OU structure.

### **Resource-based strategy**

This strategy is built around the functions of resources that are in the OU structure. Typically, you separate resources by function (or objects by type), and you create OUs to represent these functions. For example, some common top-level OUs are Servers, Workstations, Groups, and Users. The resource-based strategy is typically used in smaller organizations, in organizations that are maintained centrally by the same administrative staff, and where administrative delegation is based on the object type rather than on the location or department. Examples of these administrative groups include User Helpdesk, Client Support, Virtualization Administration, and Application-Specific Support. In large organizations, it is likely that those top-level OUs are more defined in the next subordinate level. For example, the Servers OU might contain child OUs named after their applications, such as Microsoft Exchange Server or Microsoft SQL Server.

**Organization-based strategy.** This strategy reflects the structure of an organization's business logic. Top-level OUs represent departments within the organization, such as Sales, Research, or Finance. This strategy works well if resources move frequently or if they are not affiliated with a physical location, and if there are few employee changes between departments. You should consider this strategy when administrative tasks are delegated on a per department basis rather than a per location basis. For example, an organization with traveling sales teams and other units that are not location-bound would benefit from an organization-based strategy. However, this strategy is not a good choice for organizations that frequently realign their business model or that encourage employees to shift between roles.

### **Multitenancy-based strategy**

This strategy is suitable for organizations that provide the Active Directory infrastructure as a service (IaaS) to other organizations. This might be a group of affiliated organizations that share the same domain, a hosted environment, an outsourced environment, or even a private or public cloud provider. This strategy is appropriate when one organization is responsible for maintaining the Active Directory infrastructure while another organization is delegated to manage certain Active Directory objects or if the first organization relies completely on the administration of the hosting organization. For example, A. Datum might maintain AD DS for Trey Research and Contoso, Ltd. Trey Research might want to administer their Users, Groups, and Computers OUs independently but might not want to manage Active Directory replication and DNS, while Contoso, Ltd. relies fully on the IT staff from A. Datum for all of those tasks. In this scenario, A. Datum would create a top-level OU for ITServices, where they maintain all administrative accounts and groups, and top-level OUs named ADatum, Contoso, Ltd., and TreyResearch for each of the managed organizations. Under these OUs, regular user, group, workstations, and perhaps server accounts are represented as deeper levels. The IT staff of Trey Research would be delegated to maintain their own accounts as designed. In the multitenancy-based strategy, it is possible to allow different tenants to work together or to create privacy settings so that each organization only sees its own resources. In this strategy, it can also be a more straightforward process to include or separate new organizations.

## Hybrid strategy

This strategy uses a combination of OUs based on location, organization, and resources. The multitenancy-based strategy is also a hybrid strategy. Other hybrid strategies might assign the location at the top level and separate object types on the next level. Hybrid strategies can be completely mixed, depending on the organizational requirements. For example, the Servers OU could contain OUs for FileServers, IIS, SQL Server, Exchange Server, and other application servers. The Users OU might contain location or departmental OUs, the Workstations OU might distinguish between Desktops and Laptops, and the Groups OU could incorporate departmental, location, project, or application-specific groups.

Regardless of which strategy you use to design your OU structure, always remember that the main purpose is to enable the implementation of an Active Directory administrative tasks model, while a second priority might be group policies. We also recommended separating administrative accounts and groups from regular user accounts and groups that might be administered by delegated administrators.

## OU hierarchy considerations

When planning Active Directory functionality, you should consider the following high-level aspects of OU design:

- **Administrative purpose.** The OU structure should align primarily to administrative purposes, such as your Active Directory tasks delegation model and your GPOs. Avoid mimicking your organizational chart, unless it benefits the administrative model. Organization charts change frequently, and it is not practical to change your OU structure that often. If you have requests for department-specific GPOs, it might be preferable to reflect those departments in a lower level of the OU structure. However, it is also likely that you have a security and distribution group to reflect the users in this department, and you can instead use security filtering for that purpose. Users and managers usually do not see the OU structure, so there is no benefit in having corporate hierarchies listed in there. If you want to enable users to browse the organizational structure, ensure that you fill in the **Manager** attribute of the user objects, which enables users to use current and previous versions of Microsoft Office Outlook in combination with an Exchange Server messaging infrastructure, Microsoft Office 365, or Microsoft SharePoint Server to navigate through the organizational structure. The OU is for administrative purposes only.
- **Inheritance.** Inheritance is an important aspect of OU functionality, both for delegation of control and GPO application. You should design the OU structure to include objects that require the same administrative control or Group Policy settings within the same OU structure. This way, you can assign the delegation of control or the GPO setting only once at a higher level in the OU structure, rather than individually at each child level. Remember that you can block inheritance for certain child OUs if you do not want AD DS to apply the settings for a higher OU level to certain child OUs.
- **Change.** Design your OU structure to accommodate change. After you implement an OU structure, it can be difficult to change, especially if you also change design strategies, such as changing from an organization-based strategy to a resource-based strategy. Ensure that your OU structure leaves room for organizational growth and a reasonable level of structural change.

Align OU strategy to administrative requirements, not the organizational chart because organizational charts are more subject to change than your IT administration model

AD DS inheritance behavior can simplify group policy administration because it allows group policies to be set on an OU and flow down to lower OUs in the hierarchy

Plan to accommodate for changes in the IT administration model

## Considerations for using OUs

When AD DS is first implemented there is only one OU: the Domain Controllers OU. You must create any other OUs.

### OU creation

You can create OUs by using graphical tools such as Active Directory Users and Computers or Active Directory Administrative Center. You can also create OUs by using command-line tools such as Windows PowerShell.

- OUs can be created using AD DS graphical tools or command-line tools
- New OUs are protected from accidental deletion by default
- When objects are moved between OUs:
  - Directly assigned permissions remain in place
  - Inherited permissions will change
- Appropriate permissions are required to move objects between OUs



**Note:** You must create all new OUs by using an administrative tool. There is no mechanism to copy existing OUs to create new ones.

In most cases, you will use a graphical tool or a script to accomplish this.

### Preventing accidental deletion

Accidental deletion is one of the major causes of Active Directory recoveries. Therefore, Windows Server 2016 supports the Protect OUs from Accidental Deletion feature of AD DS. OUs that are protected from accidental deletion share the following benefits:

- OUs cannot be accidentally deleted. If administrators want to purposely delete an OU, they must remove the protection prior to deleting the OU.
- OUs cannot be accidentally moved.
- OUs that are newly created by using Active Directory Administrative Center or Active Directory Users and Computers in Windows Server 2008 or newer are protected automatically against accidental deletion.

You can enable or disable the protection from accidental deletion in the Active Directory Administrative Center on the properties of the OU. You can also use Active Directory Users and Computers to enable or disable the protection from accidental deletion on the **Object** Tab in the **OU Properties** dialog box.



**Note:** You must enable the advanced view in Active Directory Users and Computers before you can see the **Object** tab in the OU properties.

You can also use Windows PowerShell to enable or disable protection. For example, you can search for OUs that are not protected and enable protection with the following command:

```
Get-ADOrganizationalUnit -filter * -properties ProtectedFromAccidentalDeletion | where
{$_ .ProtectedFromAccidentalDeletion -eq $false} | Set-ADOrganizationalUnit -
protectedFromAccidentalDeletion $true
```

## Moving objects between OUs

As job roles change or computers are reassigned there will be times when objects in AD DS need to be moved to different OUs. Moving objects between OUs in the same domain is a simple task. You can right-click the object and move it or you can click and drag the object to the new OU. Moving objects has the following effects on the objects' permissions:

- Permissions assigned directly to the object remain in place after the object is moved.
- The object will inherit new permissions from its new OU and will lose any inherited permissions from the previous OU.

## Permissions required to move objects

The following permissions are required to move AD DS objects:

- Delete\_Child permission on the source OU (or Delete permission on the object being moved).
- Write\_Prop permission on the object for the relative distinguished name (RDN), distinguished name (DN), and common name (CN) properties.
- Create\_child permission on the target OU.

## AD DS permissions

You implement the Active Directory administrative delegation model by merging the OU design with the permissions on the OUs. This enables delegated administrators to fulfil administrative tasks. To create the administrative task model and design the OU structure to support it, you must understand how Active Directory administrative delegation works, and the options for delegating administrative control.

- Users receive their token (list of SIDs) during sign in
- Objects have a security descriptor, that describes:
  - Who (SID) has been granted or denied access
  - Which permissions (Read, Write, Create or Delete child)
  - What kind of objects
  - Which sublevels
- When users browse the Active Directory structure, their token is compared to the security descriptor to evaluate their access rights

### How do users get permissions?

When users sign in to an Active Directory domain, they receive a token, which is a list of the SIDs of their individual account, historical accounts, if they have been migrated, and every group they belong to (even recursively). If any group was migrated from another domain, it is likely that they also received the historical SIDs of those groups in the former domain.

In Windows operating systems, many objects (such as files, folders, registry keys, processes, and Active Directory objects) contain a security descriptor. Based on the SID, the security descriptor defines which rights are granted or denied and to whom.

When a user browses files and folders or registry keys or navigates through the Active Directory domain structure the list of SIDs in the token is compared with the list of SIDs that are in the security descriptor. If there are any matching SIDs, the system validates the type of access and allows or prohibits the current operation.

### Active Directory OU permissions

In Active Directory, the permission model is more complex than in most other Windows operating system services. Security settings on the Active Directory domain are inherited hierarchically in the OU structure of that domain. At any point in the structure, you can configure additional security settings that could be inherited throughout the hierarchy—depending on the scope of inheritance that is defined in the security setting and whether inheritance is blocked at a lower level. New objects obtain default security settings

(which are defined in the schema class) and inherit security settings from their parents. For example, in the OU schema definition, Account Operators is granted full rights to create and delete objects for computer accounts, user accounts, group objects, and **inetOrgPerson** objects. Therefore, if you remove the default Account Operators group from the security permissions of an OU, and then create a child OU, the child OU retains the explicit security settings of the Account Operators.

### Active Directory object security descriptors

A security descriptor of an Active Directory object contains the following parts:

- The owner of the object. The owner can reset security settings even when he or she accidentally configured them to have no permissions on the object.
- The primary group of the owner (SID).
- A control field that specifies whether the discretionary access control list (DACL) or security access control list (SACL) is present and/or is blocking inheritance.
- An optional DACL. The optional DACL contains permissions for granting or denying access.
- An optional SACL. The optional SACL contains the auditing permissions when Success or Failure auditing is enabled.

The DACL and SACL are containers that contain one or more access control entries (ACEs). An ACE stores the following information:

- Who (which security principal, such as a user or group) is allowed or denied access
- What permissions are granted to the security principal. To Read, Write, Create, or Delete
- Which objects, or object attributes can the action be performed on
- At what sublevels (on the OU-level only, on objects only in the OU, or objects in any sub-OU)

In the OU properties, you use the **Security** tab—in particular, the **Advanced Security** dialog box—to verify or adjust security settings. **Security Delegation Wizard** assists with some common tasks, but you cannot use it to review the security settings.

## Delegating AD DS permissions

Domain administrators have full rights to all objects in the domain. Other default built-in groups have limited rights to objects in the domain. For example, the Account Operators group has full rights over Users, Computers, and Group objects but not other types of objects. If you want certain users or groups to have permission to do only specific tasks in specific areas of the directory, then you must delegate those tasks.

- Permissions on AD DS objects can be granted to users or groups
- Permission models are usually object based or role based
- The Delegation of Control Wizard can simplify assigning common administrative tasks
- The OU advanced security properties allow you to grant granular permissions

### Delegation control methods

When you delegate control of objects in your Active Directory OU, you must consider two factors: to whom you are granting permissions and where in the directory hierarchy. In AD DS, you can grant specific rights on resources. You can allow the creation or deletion of only certain object types, or you can select the individuals who have rights on a particular attribute of a specific object type, such as group account descriptions or their members. Except in rare cases (such as service accounts), you should always grant administrative control to groups rather than

users. Even if the group contains only one user, this individual might leave the organization, and it would be harder to determine where that individual had permissions than it would be to change the appropriate group memberships.

There are two methods for delegating administrative control over Active Directory domain resources:

- **Object-type delegation.** In this delegation model, you can delegate various levels of control to groups based on the objects that the groups control. An example of an object-type delegation would be if you delegated control to the Toronto Admins group for objects within the Toronto OU. In this case, the Toronto Admins group is likely responsible for the majority of administrative tasks within the Toronto OU.

You typically use object-type delegation if there are only a few administrators or if minor delegation is required. This type of delegation also works well if many administrators require the same level of control, typically over most of the domain structure.

We do not recommend object-type delegation in an environment where different users require various levels of control over different objects, because it can be difficult to determine which level of control is granted to which users for a specific object.

- **Role-based delegation.** This delegation model involves creating several specific groups to which you delegate administrative control. These groups usually relate to a specific resource (or resources), and you can name groups for the level of control that you assign to them. Unlike object-based delegation, role-based delegation involves granting permissions to modify only some of the attributes of an object. For example, you could create the role-based group Change Finance User Password and then assign permissions to that group to change passwords for any users in the Finance OU.

To ensure that your role-based delegation is effective, all functions or roles within the Active Directory domain structure should have an associated group. This level of specificity can help you to determine which level of control you have assigned to an individual user, because you simply examine the role-based groups to which the user belongs.

Role-based delegation can take longer to implement than object-type delegation. However, if you design the OU and group structure properly, role-based delegation saves administrative effort and frustration, especially for larger organizations.

### The Delegation of Control Wizard

This tool can be very useful in delegating administrative rights to objects in AD DS to groups or individuals. It helps to simplify what permissions are required to perform everyday administrative tasks such as resetting passwords or modifying group memberships.

The wizard provides a list of common tasks that you can assign or allows you to create a custom task based on the type of object you want to delegate control of.

To start the **Delegation of Control Wizard**, right-click the container, and then click **Delegate Control**. Then, select the user or group that you wish to assign rights to and select the tasks that you want them to perform.



**Note:** Running **Delegation of Control Wizard** at the domain level provides a common task to **Join a computer to the domain**. This task only appears when the wizard runs at the domain level.

## Assigning permissions manually

The advanced security properties of an OU allow you to be very granular about what permissions are granted to users and groups. For example, you might wish to grant the ability to modify only certain user attributes, such as **home address** and **job title**, to Human Resources employees.

## Demonstration: Delegating administrative permissions on an OU

In this demonstration, you will see how to create a new OU, use the **Delegation of Control Wizard** to assign a task, and use advanced OU security to assign granular permissions to the Research group.

### Demonstration Steps

#### Create a new OU

- Use **Active Directory Users and Computers** to create a new OU named **Human Resources** in **Adatum.com**.

#### Use the Delegation of Control Wizard to assign a task

1. Start **Delegation of Control Wizard** at the **Adatum.com** level.
2. Select the **Helpdesk** group and assign the following tasks:
  - **Reset user passwords and force password change at next logon**
  - **Join a computer to the domain**

#### Assign the Research group the right to modify user addresses and job titles in the Research OU

1. Turn on **Advanced Features**.
2. Open the **Research** OU properties.
3. In the advanced security section, select the **Research** group, and then assign the following permissions on the **Descendant User** objects:
  - **Write Home Address**
  - **Write Job Title**

**Question:** What is the advantage of using the **Delegation of Control Wizard**?

## Lab B: Administering AD DS

### Scenario

You have been working for the A. Datum Corporation as a desktop support specialist and have performed troubleshooting tasks on desktop computers to resolve application and network problems. You recently accepted a promotion to the server support team. One of your first assignments is to configure the infrastructure service for a new branch office.

To begin the deployment of the new branch office, you are preparing AD DS objects. As part of this preparation, you need to create an OU for the branch office and delegate permission to manage it. Also, you need to evaluate Windows PowerShell to manage AD DS more efficiently.

### Objectives

After completing this lab, you will be able to:

- Delegate administration for OUs.
- Use Windows PowerShell to manage AD DS objects.

### Lab Setup

Estimated Time: 45 minutes

Virtual machine: **20742A-LON-DC1**, **20742A-LON-DC2**, **20742A-LON-SVR1** and **20742A-LON-CL1**

User name: **Adatum\Administrator**

Password: **Pa\$\$w0rd**

For this lab, you need to use the available VM environment. Before you begin the lab, you must complete the following steps:

1. On the host computer, start **Hyper-V Manager**.
2. In Hyper-V Manager, click **20742A-LON-DC1**, and then in the **Actions** pane, click **Start**.
3. In the **Actions** pane, click **Connect**. Wait until the VM starts.
4. Sign in by using the following credentials:
  - User name: **Administrator**
  - Password: **Pa\$\$w0rd**
  - Domain: **Adatum**
5. Repeat steps 1-4 for **20742A-LON-DC2** and **20742A-LON-SVR1**.
6. Repeat steps 1-3 for **20742A-LON-CL1**. Do not sign on to **LON-CL1** until instructed to do so in the lab steps.



## Exercise 1: Delegating administration for OUs

### Scenario

A. Datum Corporation delegates management of each branch office to a specific group. This allows IT employees who work onsite to be configured as administrators for the branch. Each branch office has a branch administrators group that can perform full administration within the branch office OU. There is also a branch office help-desk group that is able to manage users in the branch office OU but not other objects. You need to create the OU and these groups for the new branch office and delegate permissions to the groups. You will also validate the permissions.

The main tasks for this exercise are as follows:

1. Create a new OU for the branch office.
2. Create groups for branch administrators and branch Help-desk personnel.
3. Add members to the group.
4. Delegate permissions to the group.
5. Test permissions.

#### ► Task 1: Create a new OU for the branch office

- On **LON-DC1**, use **Active Directory Users and Computers** to create a new OU named **London**.

#### ► Task 2: Create groups for branch administrators and branch Help-desk personnel

- In the **London** OU, create the following global security groups:
  - **London Admins**
  - **London Helpdesk**

#### ► Task 3: Add members to the group

1. Select the **IT** OU.
2. Add **Beth Burke** to the **London Admins** group.
3. Add **Dante Danby** to the **London Helpdesk** group.

#### ► Task 4: Delegate permissions to the group

1. In **Active Directory Users and Computers**, enable the **Advanced Features** view.
2. Set permissions on the **Security** tab of the **London** OU properties to give the **London Admins** group **Full Control**.
3. Use the **Delegation of Control Wizard** to grant **Full Control** over **User objects** in the **London** OU to the **London Helpdesk** group.

### ► Task 5: Test permissions

- On **LON-SVR1**, use the **Add Roles and Features Wizard** in **Server Manager** to install the **AD DS Tools** feature. When this task is complete, sign out of **LON-SVR1**.

#### Test permissions for London Admins

1. Sign in to **LON-SVR1** as **Beth** with a password of **Pa\$\$w0rd**.
2. Open **Active Directory Users and Computers**.
3. Click the **Research** OU. Notice that the icons on the toolbar for creating users, groups, or OUs are grayed out.
4. Click the **London** OU, and then notice that those icons are live now.
5. Create a sub-OU in the **London** OU named **Laptops**.
6. Sign out of **LON-SVR1**.

#### Test permissions for London Helpdesk

1. Sign in to **LON-SVR1** as **Dante** with a password of **Pa\$\$w0rd**.
2. Open **Active Directory Users and Computers**.
3. Select the **London** OU. Notice that the only icon not grayed out is the create user icon.

**Results:** After completing this exercise you will have:

- Created a new OU for the branch office.
- Created groups for branch administrators and branch Help-desk personnel.
- Added members to the group.
- Delegated permission to the groups.
- Installed AD DS tools and tested permissions.

## Exercise 2: Creating and modifying AD DS objects with Windows PowerShell

### Scenario

A. Datum Corporation has a number of scripts that have been used in the past to create user accounts by using command-line tools. However, an enterprise-wide mandate specifies that all future scripting will be done by using Windows PowerShell. As the first step in creating scripts, you need to identify the syntax required to manage AD DS objects in Windows PowerShell.

You have a .csv file that contains a large list of new users for the branch office. It is inefficient to create these users individually with graphical tools, so you will use a Windows PowerShell script instead. A colleague who has experience with scripting has given you a script that she created. You need to sign in as branch administrator and modify the script to match the format of your .csv file.

The main tasks for this exercise are as follows:

1. Create a user account using Windows PowerShell.
2. Create a new group by using Windows PowerShell.
3. Add a member to the group by using Windows PowerShell.
4. Modify the .csv file.

5. Modify the script.
6. Run the script.
7. Prepare for the next module.

► **Task 1: Create a user account using Windows PowerShell**

1. Switch to **LON-DC1**.
2. Start an elevated session of Windows PowerShell.
3. Create a user account for **Ty Carlson** in the **London** OU by running the following command:

```
New-ADUser -Name Ty -DisplayName "Ty Carlson" -GivenName Ty -Surname Carlson -Path "ou=London,dc=adatum,dc=com"
```

4. Run the following command to set the password to be **Pa\$\$w0rd**:

```
Set-ADAccountPassword Ty
```

The current password is blank.

5. Run the following command to enable the account:

```
Enable-ADAccount Ty
```

6. Test the account by switching to **LON-CL1**, and then sign in as **Ty** with a password of **Pa\$\$w0rd**.

► **Task 2: Create a new group by using Windows PowerShell**

- On **LON-DC1**, in the **Administrator: Windows PowerShell** window, run the following command:

```
New-ADGroup LondonBranchUsers -Path "ou=London,dc=adatum,dc=com" -GroupScope Global -GroupCategory Security
```

► **Task 3: Add a member to the group by using Windows PowerShell**

1. In the **Administrator: Windows PowerShell** window, run the following command:

```
Add-ADGroupMember LondonBranchUsers -Members Ty
```

2. Confirm that the user is in the group by running the following command:

```
Get-ADGroupMember LondonBranchUsers
```

► **Task 4: Modify the .csv file**

1. Use Notepad to modify the .csv file by adding the following header:

```
FirstName,LastName,Department,DefaultPassword
```

2. Save and close the file.

► **Task 5: Modify the script**

1. In the **Administrator: Windows PowerShell (ISE)** window, replace these variables:

**C:\path\file.csv** with **E:\Labfiles\Mod02\LabUsers.csv**  
**"ou=orgunit,dc=domain,dc=com"** with **"ou=London,dc=adatum,dc=com"**

2. Save the file, and then close the **Administrator: Windows PowerShell (ISE)** window.

**► Task 6: Run the script**

1. Switch to the **Administrator: Windows PowerShell** window.
2. Change the root directory to **E:\Labfiles\Mod02**.
3. Type **.\LabUsers.ps1** to run the script.
4. Run the following command to ensure that users were created:

```
Get-ADUser -Filter * -SearchBase "ou=London,dc=adatum,dc=com"
```

**► Task 7: Prepare for the next module**

When you are finished with the lab, revert all virtual machines to their initial state:

1. On the host computer, start **Hyper-V Manager**.
2. In the **Virtual Machines** list, right-click **20742A-LON-DC1**, and then click **Revert**.
3. In the **Revert Virtual Machine** dialog box, click **Revert**.
4. Repeat steps 2 and 3 for **20742A-LON-DC2**, **20742A-LON-SVR1**, and **20742A-LON-CL1**.

**Results:** After completing this lab, you will have:

- Created a user account by using Windows PowerShell.
- Created a group by using Windows PowerShell.
- Added a user to a group by using Windows PowerShell.
- Modified the .csv file.
- Modified the script.
- Run the script.

**Question:** Why are the users created by this script enabled?

**Question:** What is the status of accounts created by the **New-ADUser** cmdlet?

## Module Review and Takeaways

### Real-world Issues and Scenarios

Many organizations will create some user accounts based on job role rather than the user filling the role. For example, the organization will always have a receptionist. To provide continuity, the person filling that role uses a generic account named reception. That way, when a new person fills the position all that is required is to change the password of the reception user. Applications, settings, documents, emails, and so on will stay consistent.

### Tools

The following table lists the tools that this module references:

Tool	Used for	Where to find it
Windows PowerShell	Command-line and scripting of all administrative tasks.	Native to the operating system.
Active Directory Administrative Center	Performing day-to-day administrative tasks in AD DS.	In Server Manager, under the <b>Tools</b> menu or in <b>Control Panel</b> in <b>Administrative Tools</b> .
Active Directory Users and Computers	Performing day to day administrative tasks in AD DS.	In Server Manager, under the <b>Tools</b> menu or in <b>Control Panel</b> in <b>Administrative Tools</b> .
Delegation of Control Wizard	Assigning permissions to perform administrative tasks.	Right-click on an OU in Active Directory Users and Computers.

### Best Practices

Take away the following best practices for AD DS administration:

- Avoid using the built-in groups to delegate administrative access unless you understand all the permissions that the group membership grants.
- Create specialized administrative groups and assign them only the rights and permissions required to complete the tasks assigned.
- Develop Windows PowerShell scripts to perform repetitive tasks.
- Do not sign in with your administrative account for day-to-day activities. Only use it when you need to perform an administrative task.

### Common Issues and Troubleshooting Tips

Common Issue	Troubleshooting Tip
Users are unable to access network resources.	
You have assigned a user some administrative rights in AD DS, but he says that he has no tool to perform the task.	

**MCT USE ONLY. STUDENT USE PROHIBITED**

# Module 3

## Advanced AD DS infrastructure management

### Contents:

Module Overview	3-1
<b>Lesson 1:</b> Overview of advanced AD DS deployments	3-2
<b>Lesson 2:</b> Deploying a distributed AD DS environment	3-10
<b>Lesson 3:</b> Configuring AD DS trusts	3-24
<b>Lab:</b> Domain and trust management in AD DS	3-30
Module Review and Takeaways	3-34

## Module Overview

For most organizations, the Active Directory Domain Services (AD DS) deployment may be the single most important component in the IT infrastructure. When organizations deploy AD DS or any of the other Active Directory-linked services within the Windows Server 2016 operating system, they are deploying a central authentication and authorization service that provides single sign-on (SSO) access to many other network services and applications in the organization. AD DS also enables policy-based management for user and computer accounts.

Most organizations deploy only a single AD DS domain. However, some organizations also have requirements that necessitate a more complex AD DS deployment, which may include multiple domains or multiple forests.

This module describes the key components of an advanced AD DS environment and explains how to install and configure an advanced AD DS deployment.

### Objectives

After completing this module, you will be able to:

- Describe the components of advanced AD DS deployments.
- Explain how to deploy a distributed AD DS environment.
- Explain how to configure AD DS trusts.

## Lesson 1

# Overview of advanced AD DS deployments

Before you start to configure an advanced AD DS deployment, it is important to know the components that constitute the AD DS structure and how they interact with each other to help provide a scalable and secure IT environment. The lesson starts by examining the various components of an AD DS environment, and then explores reasons why an organization may choose to deploy a complex AD DS environment.

### Lesson Objectives

After completing this lesson, you will be able to:

- Explain how AD DS domains and forests form boundaries for security and administration.
- Describe the reasons for having more than one domain in an AD DS environment.
- Explain the reasons for having more than one forest in an AD DS environment.
- Explain the scenarios and considerations for deploying AD DS in Microsoft Azure infrastructure as a service (IaaS).
- Explain how to manage user, group, and computer objects in complex AD DS deployments.

### Overview of domain and forest boundaries in an AD DS structure

AD DS domains and forests provide different types of boundaries within an AD DS deployment. An understanding of the different types of boundaries is essential to manage a complex AD DS environment.

#### AD DS domain boundaries

The AD DS domain provides the following boundaries:

- Replication boundary for the domain partition. All AD DS objects that exist in a single domain are stored in the domain partition in the AD DS database on each domain controller in the domain. The replication process ensures that all originating updates are replicated to all of the other domain controllers in the same domain. Data in the domain partition is not replicated to domain controllers in other forests.
- Administration boundary. By default, an AD DS domain includes several groups, such as the Domain Admins group. The Domain Admins group has full administrative control over the domain. You can also assign administrative permissions to user accounts and groups within domains. With the exception of the Enterprise Admins group in the forest root domain, administrative accounts do not have any administrative rights in other domains in the forest or in other forests.
- Group Policy application boundary. You can link Group Policies at the following levels: local, site, domain, and organizational unit (OU). Apart from site-level Group Policies, the scope of Group Policies is the AD DS domain. There is no inheritance of Group Policies from one AD DS domain to another, even if one AD DS domain is lower in the hierarchy than another in a domain tree.

AD DS object	Boundary type
Domain	Domain partition replication
	Administrative permissions
	Group Policy application
	Auditing
	Password and account policies
	Domain DNS zone replication
Forest	Security
	Schema partition replication
	Configuration partition replication
	Global catalog replication
	Forest DNS zone replication



- Auditing boundary. Auditing is centrally managed by using Group Policy Objects (GPOs). The maximum scope of these settings is the AD DS domain. You can have the same audit settings in different AD DS domains, but you must manage them separately in each domain.
- Password and account policy boundaries. By default, password and account policies are defined at the domain level and applied to all domain accounts. Although it is possible to configure fine-grained password policies to configure different policies for specific users within a domain, you cannot apply the password and account policies beyond the scope of a single domain.
- Replication boundary for Domain Name System (DNS) zones. One of the options when you configure DNS zones in an AD DS environment is to configure Active Directory-integrated zones. This means that instead of the DNS records being stored locally on each DNS server in text files, they are stored and replicated in the AD DS database. The administrator can then decide whether to replicate the DNS information to:
  - All domain controllers in the domain (regardless of whether they are DNS servers).
  - All domain controllers that are DNS servers in the domain.
  - All domain controllers that are DNS servers in the forest.

By default, when you deploy the first domain controller in an AD DS domain and configure that server as a DNS server, two separate replication partitions called `domainDnsZones` and `forestDnsZones` are created. The `domainDnsZones` partition contains the domain-specific DNS records and is replicated only to other DNS servers that are also AD DS domain controllers in the domain.

### **AD DS forest boundaries**

The AD DS forest provides the following boundaries:

- Security boundary. The forest boundary is a security boundary because, by default, no account outside the forest has any administrative permissions inside the forest.
- Replication boundary for the schema partition. The schema partition contains the rules and syntax for the AD DS database. This is replicated to all the domain controllers in the AD DS forest.
- Replication boundary for the configuration partition. The configuration partition contains the details of the AD DS domain layout, including: domains, domain controllers, replication partners, site and subnet information, and Dynamic Host Configuration Protocol (DHCP) authorization or Dynamic Access Control configuration. The configuration partition also contains information about applications that are integrated with the AD DS database. An example of one application is Exchange Server. This partition is replicated to all domain controllers in the forest.
- Replication boundary for the global catalog. The global catalog is the read-only list containing every object in the entire AD DS forest. To keep it to a manageable size, the global catalog contains only some attributes for each object. The global catalog is replicated to all domain controllers in the entire forest that are also global catalog servers.
- Replication boundary for the forest DNS zones. The `forestDnsZones` partition is replicated to all domain controllers in the entire forest that are also DNS servers. This zone contains records that are important to enable forest-wide DNS name resolution.


## Why implement multiple domains?

Many organizations can function adequately with a single AD DS domain. However, some organizations have requirements that necessitate the deployment of multiple domains. These requirements can include:


- Domain replication requirements. In some cases, organizations have several large offices that are connected by slow or unreliable wide area networks (WANs). The network connections may not have enough bandwidth to support AD DS replication of the domain partition. In such cases, installing a separate AD DS domain in each office might be better.
- DNS namespace requirements. Some organizations require more than one DNS namespace in an AD DS forest. This is typically the case when one company acquires another company or merges with another organization, and preserving the domain names from the existing environment is necessary. It is possible to provide multiple user principal names (UPNs) for users in a single domain, but many organizations choose to deploy multiple domains in this scenario.
- Distributed administration requirements. Organizations may have corporate security or political requirements to have a distributed administration model. Organizations can achieve administrative autonomy by deploying a separate domain. With this deployment, domain administrators have complete control over their domains.

Organizations may choose to deploy multiple domains to meet:

- Domain replication requirements
- DNS namespace requirements
- Distributed administration requirements
- Forest administrative group security requirements
- Resource domain requirements

 **Note:** Deploying separate domains provides administrative autonomy, but not administrative isolation. The only way to ensure administrative isolation is to deploy a separate forest.

- Forest administrative group security requirements. Some organizations may choose to deploy a dedicated or empty root domain. This is a domain that does not have any user accounts other than the default forest root domain accounts. The AD DS forest root domain has two groups—the Schema Admins group and the Enterprise Admins group—that do not exist in any other domain in the AD DS forest. Because these groups have far-reaching rights in the AD DS forest, you may decide to restrict the use of these groups by using only the AD DS forest root domain to store them.
- Resource domain requirements. Some organizations deploy resource domains to deploy specific applications. With this deployment, all user accounts are located in one domain, whereas the application servers and application administration accounts are deployed in a separate domain. This enables the application administrators to have complete domain administrative permissions in the resource domain without enabling any permissions in the domain that contains the regular user accounts.

 **Note:** As a best practice, choose the simplest design that achieves the required goal; it is less costly to implement and more straightforward to administer.


## Why implement multiple forests?

Organizations may sometimes require that their AD DS design contains more than one forest. There are several reasons why one AD DS forest may not be sufficient:

- Security isolation requirements. If an organization requires administrative isolation between two or more parts of the organization, it must deploy multiple AD DS forests. Separate AD DS forests are often deployed by government defense contractors and other organizations for whom the isolation of security is a requirement. In Windows Server 2016, AD DS includes a new feature called Privileged Access Management (PAM), which uses a separate bastion forest to isolate privileged accounts in order to protect against credential theft techniques.
- Incompatible schema requirements. Some organizations may require multiple forests because they require incompatible schemas or incompatible schema change processes. All domains in a forest share the schema.
- Multinational requirements. Some countries have strict regulations regarding the ownership or management of enterprises within the country. Having a separate AD DS forest may provide the administrative isolation required by legislation.
- Extranet security requirements. Some organizations deploy several servers in a perimeter network. These servers may need AD DS to authenticate user accounts or may use AD DS to enforce policies on the servers in the perimeter network. To ensure that the extranet AD DS is as secure as possible, organizations often configure a separate AD DS forest in the perimeter network.
- Business merger or divestiture requirements. Business mergers are among the most common reasons why organizations have multiple AD DS forests. When organizations merge or one organization purchases another, they must evaluate the necessity of merging their AD DS forests. Merging the AD DS forests provides benefits related to simplified collaboration and administration. However, if the two different groups in the organization are to be managed separately, and if there is little need for collaboration, the expense of merging the two forests may not be worth it. In particular, if there is a plan to sell one part of the company, retaining the two organizations as separate forests is preferable.

Organizations may choose to deploy multiple forests to meet:

- Security isolation requirements:
  - PAM in Windows Server 2016 AD DS uses a separate bastion forest to isolate privileged accounts in order to protect against credential theft techniques
- Incompatible schema requirements
- Multinational requirements
- Extranet security requirements
- Business merger or divestiture requirements


 **Best Practice:** As a best practice, choose the simplest design that achieves the required goal; it is less expensive to implement and more straightforward to administer.

## Deploying a domain controller in Azure IaaS

Microsoft Azure provides infrastructure as a service (IaaS), which essentially is virtualization in the cloud. All the considerations for virtualizing applications and servers in an on-premises infrastructure apply to deploying the same applications and servers to Azure. When deploying Active Directory in Azure, you are installing the domain controller on a virtual machine, so all the rules that apply to virtualizing a domain controller apply to deploying Active Directory in Azure. You can install AD DS on Azure virtual machines to support a variety of scenarios:


- Scenarios in which you might deploy AD DS on an Azure virtual machine:
  - Disaster recovery
  - Geo-distributed domain controllers
  - Isolated applications
- Considerations during deployment include:
  - Network topology
  - Site topology
  - Service healing
  - IP addressing
  - DNS
  - Hard disk read/write caching

- Disaster recovery. In a scenario in which your on-premises domain controllers are destroyed or otherwise unavailable, Azure-based virtual machines running as replica domain controllers will have a complete copy of your AD DS database. This can help speed recovery and is a low-cost alternative for organizations that do not have a physical disaster recovery site.
- Geo-distributed domain controllers. If your organization is highly decentralized, Azure-based virtual machines running as replica domain controllers can provide lower latency connections for improved authentication performance. You can achieve this by running domain controllers in different Azure regions that correspond to the locations where it is not cost effective for your organization to deploy physical infrastructure.
- User authentication for isolated applications. If you need to deploy an application with an AD DS dependency, but that application does not require connectivity with the corporate AD DS environment, you could deploy a separate forest on Azure virtual machines.

 **Note:** Although on-premises member servers and clients can communicate with Azure-based domain controllers, these domain controllers should never be the only domain controllers in a hybrid environment. Loss of connectivity from your on-premises environment to Azure prevents authentication and other domain functions if you are not also running AD DS services in your on-premises environment.

When you implement AD DS in Azure, consider the following:

- Network topology. To meet the requirements for AD DS, you must create a Microsoft Azure Virtual Network and attach your virtual machines to it. If you intend to join an existing on-premises AD DS infrastructure, you can opt to extend network connectivity to your on-premises environment. This is achieved either through a standard virtual private network (VPN) connection or Azure ExpressRoute circuit, depending on the speed, reliability, and security your organization requires.

 **Note:** An Azure ExpressRoute circuit is a method of connecting your on-premises infrastructure to Microsoft cloud services through a dedicated connectivity provider that does not use the public Internet.

- Site topology. As with a physical site, you should define and configure an AD DS site that corresponds to the IP address space of your Azure Virtual Network. Because the use of an Azure Virtual Network incurs additional gateway costs for all outbound traffic to your on-premises environment, you should carefully plan your AD DS sites and site links to minimize cost. Because AD DS site link transitivity is enabled by default, you should consider disabling the option to bridge all site links if you have more than 2 sites. If you leave site link bridging enabled, AD DS assumes that all sites in your deployment have direct connectivity with one another and it may result in your Azure AD DS site having multiple replication partners. Ensure you do not enable change notification on site links that contain your Azure AD DS site. This is because this will override any replication intervals configured on the site link, resulting in frequent and often unnecessary replication. If a writeable copy of AD DS is not required, you should consider deploying a read-only domain controller (RODC) to further limit the amount of outbound traffic created by AD DS replication.



**Note:** AD DS sites, site links, and replication are covered in more detail in a later module.

- Service healing. Although Azure does not provide rollback services directly to customers, Azure servers may be rolled back as a regular part of maintenance when recovering from a service failure. Domain controller replication depends on the update sequence number (USN); when an AD DS system is rolled back, duplicate USNs could be created. To prevent this, Windows Server 2012 AD DS introduced a new identifier named *VM-Generation ID*. VM-Generation ID can detect a rollback and prevent a virtualized domain controller from replicating changes outbound until the virtualized AD DS has converged with the other domain controllers in the domain.



**Note:** Azure virtual machines running the domain controller role should always be shut down through the guest operating system and never through the Azure portal. Initiating a shutdown through the Azure portal deallocates the virtual machine, causing a reset of the VM-Generation ID identifier.

- IP addressing. All Azure virtual machines receive DHCP addresses by default, but you can configure static addresses through Azure PowerShell that will persist across restarts, shutdowns, and service healing. Azure virtual machines that are to host a domain controller and/or DNS role should have the initial dynamic IP address configured as static by using the **Set-AzureStaticVNetIP** cmdlet so that the IP is never deallocated if the virtual machine is shut down. You must first provision the Azure Virtual Network before you provision the Azure-based domain controllers.
- DNS. Azure built-in DNS does not meet the requirements of AD DS, such as Dynamic DNS and service records (SRV records). Before you can extend your on-premises AD DS environment to an Azure virtual machine, you must provision and configure the Azure Virtual Network to an on-premises DNS server.
- Disks. Azure virtual machines use read-write host caching for operating system (OS) virtual hard disks. Although this can improve the performance of the virtual machine, if AD DS components are installed on the OS disk, data loss is possible in the event of a disk failure. Caching can be turned off in additional Azure hard disks attached to a virtual machine. When you install Active Directory in Azure, you should locate the NTDS.DIT and SYSVOL folders on an additional data disk in the Azure virtual machine with the **Host Cache Preference** setting configured to **NONE**. However, keep in mind that Azure data disks are constrained to a maximum size of 1 terabyte (TB).

## Managing objects in complex AD DS deployments

In smaller AD DS deployments consisting of a single domain and forest, built-in tools such as the **Active Directory Administrative Center** or **Active Directory Users and Computers** management console are generally sufficient for managing the associated user, group, and computer objects in your organization. However, as the administrator of a complex AD DS environment, you will be managing millions of objects across multiple forests and domains, which makes tasks increasingly tedious and difficult if these are the only tools available to you. In these situations, you may need to implement advanced identity management processes to handle the various issues associated with administration. Consider the following scenarios:

- Potential issues include:
  - User and group management
  - User self-service
  - Certificate management
  - Identity synchronization
- Microsoft Identity Manager 2016 provides:
  - Cloud-ready identities for Azure Active Directory
  - Powerful user self-service features with multi-factor authentication
  - Privileged access management

- **User management.** In complex AD DS deployments, it is generally not feasible for an administrator to manually maintain user objects. Tasks such as creating new user accounts, updating a user's department, or provisioning a Microsoft Exchange Server mailbox should generally be handled by an automated workflow that is initiated by the authoritative data source. For example, you may decide to automatically create AD DS user accounts in a specific domain for new employees based on data from your organization's HR application. If the employee's department changes in the HR application, you may want the same change to be reflected on the corresponding AD DS user object. Handling these tasks using an automated workflow is generally more efficient and less prone to human error.
- **Group management.** Similar to managing user objects, manually managing groups in complex AD DS deployments can present several challenges. Because group membership changes may often require authorization, you may decide to delegate management of group objects to a designated individual or group of individuals. However, for nonadministrators, managing group objects may not be an intuitive process. In some cases, delegating management of groups may still result in inefficiencies that could be better handled by automation. For example, role-based access in your organization may depend on what department a user object is assigned to. Rather than manually maintaining a security group for each department in the organization, leveraging automation to update group memberships based upon the user's assigned department may be more efficient.
- **User self-service.** Implementing user self-service for tasks such as account unlock and password reset can help you alleviate much of the administrative overhead associated with complex AD DS deployments.
- **Certificate management.** In a typical AD DS deployment, you may have one Active Directory Certificate Services (AD CS) certificate authority per forest. Therefore, in complex AD DS deployments with multiple forests, you may have multiple certificate authorities to manage. In this situation, maintaining the required templates, auto enrollment policies, and certificate revocation of deprovisioned users across multiple forests can be a challenge.
- **Identity synchronization.** As organizations become more cloud-based, you may need to synchronize user identities with cloud services such as Azure Active Directory in order to leverage offerings such as Office 365 or multifactor authentication. You may also have multiple on-premises authentication stores and/or legacy line-of-business applications necessitating synchronization of user data so that it is consistent in each source.

## Microsoft Identity Manager 2016

To address many of the scenarios above, you may consider deployment of an identity and access management platform such as Microsoft Identity Manager (MIM) 2016. MIM 2016 can seamlessly make your existing AD DS identities cloud-ready; it also provides powerful user self-service capabilities and enhanced security features to support your on-premises or hybrid infrastructure:

- Cloud-ready identities. MIM 2016 can automatically prepare AD DS identities for synchronization with Azure Active Directory by standardizing AD DS user attributes and values.
- User self-service. MIM 2016 allows your users to do account unlock or password reset functions using multi-factor authentication. It also allows users to create and maintain groups using workflow approval and supports certificate management for multiforest scenarios.
- Enhanced security. PAM in MIM 2016 leverages a separate AD DS forest to provide additional time-bound security of administrator accounts.

### Check Your Knowledge

Question	
Which of the following requirements necessitates the implementation of a multiple forest AD DS deployment?	
Select the correct answer.	
<input type="checkbox"/>	Security isolation requirements
<input type="checkbox"/>	Schema requirements
<input type="checkbox"/>	DNS namespace requirements
<input type="checkbox"/>	Business mergers
<input type="checkbox"/>	Distributed administration requirements

### Check Your Knowledge

Question	
Before you deploy a replica AD DS domain controller on an Azure virtual machine, which of the following requirements must be met?	
Select the correct answer.	
<input type="checkbox"/>	Create an AD DS site to control replication from your on-premises networks to the Azure Virtual Network.
<input type="checkbox"/>	Add an additional hard disk to the virtual machine that has read and write caching disabled.
<input type="checkbox"/>	Create and configure an Azure Virtual Network.
<input type="checkbox"/>	Manually create required SRV records in an Azure DNS zone for your domain.
<input type="checkbox"/>	Configure the initial dynamic IP address of the virtual machine as static by using the <b>Set-AzureStaticVNetIP</b> cmdlet.

## Lesson 2

# Deploying a distributed AD DS environment

Some organizations must deploy multiple domains or even multiple forests. Deploying AD DS domain controllers in this scenario is similar to deploying domain controllers in a single domain environment, but there are some special factors that you must consider.

In this lesson, you will learn how to deploy a complex AD DS environment, and you will see how to upgrade from a previous version of AD DS.

### Lesson Objectives


After completing this lesson, you will be able to:

- Describe AD DS domain functional levels.
- Describe AD DS forest functional levels.
- Describe how to deploy new AD DS domains.
- Install a domain controller in a new domain in a forest.
- Explain how to upgrade a previous version of AD DS to a Windows Server 2016 version.
- Explain how to migrate to Windows Server 2016 AD DS from a previous version.
- Describe the considerations for implementing a complex AD DS environment.

### AD DS domain functional levels

AD DS domains can run at different functional levels. Generally, upgrading the domain to a higher functional level introduces additional features. The following table lists some of the domain functional levels.


- New functionality requires that domain controllers are running a particular version of Windows:
  - Windows Server 2003
  - Windows Server 2008
  - Windows Server 2008 R2
  - Windows Server 2012
  - Windows Server 2012 R2
  - Windows Server 2016 Technical Preview
- You cannot raise the functional level while domain controllers are running previous Windows Server versions
- You cannot add domain controllers running previous Windows Server versions after raising the functional level


Domain functional level	Features
Microsoft Windows 2000 Server native	Features include: <ul style="list-style-type: none"> <li>• Universal groups.</li> <li>• Group nesting.</li> <li>• Group conversion, from security to distribution or vice versa.</li> <li>• Security identifier (SID)-History.</li> </ul> <p> <b>Note:</b> You cannot install Windows Server 2016 domain controllers in a domain running at the Windows 2000 Server native level.</p>




Domain functional level	Features
Windows Server 2003	<p>Features include:</p> <ul style="list-style-type: none"> <li>• Netdom.exe. This domain management tool makes it possible to rename domain controllers.</li> <li>• LastLogonTimestamp. This attribute remembers the time of last domain sign in for users and replicates this to other AD DS domain controllers in the AD DS domain.</li> <li>• InetOrgPerson object support. The InetOrgPerson object is defined in Internet RFC 2798 and is used for federation with external directory services.</li> <li>• Redirection. This feature provides you the ability to redirect the default location for user and computer objects.</li> <li>• Constrained delegation. This feature enables applications to take advantage of the secure delegation of user credentials by using Kerberos-based authentication.</li> <li>• Selective authentication. This feature allows you to specify the users and groups that are allowed to authenticate to specific resource servers in a trusting forest.</li> <li>• Application partitions. These are used to store information for Active Directory-integrated applications. Active Directory-integrated DNS uses an application partition, which allows the DNS partition to be replicated on domain controllers that are also DNS servers in the domain, or even across the forest.</li> </ul>
Windows Server 2008	<p>Features include:</p> <ul style="list-style-type: none"> <li>• Distributed File System (DFS) Replication is available as a more efficient and robust file replication mechanism than the file replication service (FRS) used for the SYSVOL folders.</li> <li>• Additional interactive logon information is stored for each user, instead of just the last logon time.</li> <li>• Fine-grained password settings allow password and account lockout policies to be set for users and groups, replacing the default domain settings for those users or group members.</li> <li>• Personal virtual desktops are available for users to connect to by using RemoteApp and Remote Desktop.</li> <li>• Advanced Encryption Services (AES 128 and 256) support for Kerberos is available.</li> <li>• RODCs provide a secure and economical way to provide AD DS sign-in services in remote sites, without storing confidential information (such as passwords) in untrusted environments.</li> </ul>
Windows Server 2008 R2	<p>Features include:</p> <ul style="list-style-type: none"> <li>• Authentication mechanism assurance, which packages information about a user's sign-in method, can be used in conjunction with application authentication—for example, with Active Directory Federation Services (AD FS). In another example, you can grant users who sign in by using a smart card access to more resources than when they sign in with a user name and password.</li> <li>• Automatic service principal name (SPN) management of managed service accounts is available. Managed service accounts allow account passwords to be managed by the Windows operating system.</li> </ul>

Domain functional level	Features
Windows Server 2012	Windows Server 2012 domain functional level does not implement new features from Windows 2008 R2 functional level. However, there is one exception. If the Key Distribution Center (KDC) support for claims, compound authentication, and Kerberos armoring is configured for <b>Always provide claims</b> or <b>Fail unarmored authentication requests</b> , these functionalities will not be enabled until the domain is also set to Windows Server 2012 level.
Windows Server 2012 R2	<p>Features include:</p> <ul style="list-style-type: none"> <li>• Domain Controller-side protections for Protected Users. The Protected Users group was introduced in Windows Server 2012 R2. Members of the Protected Users group can no longer: <ul style="list-style-type: none"> <li>○ Authenticate with NTLM authentication, Digest Authentication, or CredSSP. Windows 8.1 devices do not cache Protected Users passwords.</li> <li>○ Use Data Encryption Standard (DES) or Rivest Cipher 4 (RC4) cipher suites in Kerberos preauthentication. Domains must be configured to support at least the AES cipher suite.</li> <li>○ Be delegated with unconstrained or constrained delegation. Connections for Protected Users to other systems may fail.</li> <li>○ Renew user tickets (TGTs) beyond the initial four-hour lifetime. After four hours, Protected Users must authenticate again.</li> </ul> </li> <li>• Authentication Policies can be applied to accounts in Windows R2 2012 domains.</li> <li>• Authentication Policy Silos are used to create a relationship between user accounts, managed service accounts, and computer accounts for Authentication Policies.</li> </ul>
Windows Server 2016 Technical Preview	<p>Features include:</p> <ul style="list-style-type: none"> <li>• Privileged access management is an expiring links feature. It allows time-bound membership in a security group that is expressed as a Time to Live (TTL) value bound to the Kerberos ticket lifetime. Expiring links are available on all linked attributes and are not limited to the member/memberOf relationship.</li> <li>• Azure Active Directory join enhances the identity experience for the business customer by improving the capabilities extended to both corporate and personal devices.</li> <li>• Microsoft Passport is a new authentication feature allowing biometric or PIN sign in.</li> <li>• Because Windows Server 2003 is no longer supported, we recommend that you raise your domain and forest functional levels to a minimum of Windows Server 2008 in order to ensure SYSVOL replication consistency.</li> </ul>

 **Note:** Generally, you cannot roll back the AD DS domain functional level after it has been configured. If you have implemented a feature that is only available in a higher domain functional level, you cannot roll back to an earlier state. You can only lower the domain functional level by using the **Set-ADDomainMode** PowerShell cmdlet.

 **Additional Reading:** For more information on AD DS features in the Windows Server 2016 Technical Preview release, refer to: <http://aka.ms/Bxg2z0>

 **Additional Reading:** For more information on the AD DS domain functional levels, refer to: <http://aka.ms/Ynmvma>

## AD DS forest functional levels

The AD DS forest can run at different functional levels, and sometimes raising the AD DS forest functional level makes additional features available. The most noticeable additional features come with the upgrade to a new Windows Server forest functional level. When you raise the forest functional level, adding new domains is limited by the forest functional level. Domain controllers must use domain functional levels that are the same as the forest functional level. For example, if the forest functional level is Windows Server 2012 R2, you cannot add a new domain based on

Windows Server 2008 R2 domain controllers. Additional features that are available with versions of Windows Server, starting with Windows Server 2003, include:

Windows Server 2003:	
• Forest trusts	• Support for RODCs
• Domain rename	• Conversion of inetOrgPerson objects to user objects
• Linked-value replication	• Deactivation and redefinition of attributes and object classes
• Improved KCC	
Windows Server 2008:	
• No new features; sets minimum level for all new domains	
Windows Server 2008 R2:	
• Active Directory Recycle Bin	
Windows Server 2012 and Windows Server 2012 R2:	
• No new features; sets minimum level for all new domains	
Windows Server 2016:	
• No new features; sets minimum level for all new domains	

- Trusts. The basic feature of forests is that all domain trusts are transitive trusts, so that, with permission, any user in any domain in the forest can access any resource in the forest.
- Forest trusts. It is possible to set up trusts between AD DS forests to enable resource sharing. There are full trusts and selective trusts.
- Linked-value replication. This feature improved Windows 2000 Server replication and the management of group membership. In previous versions of AD DS, the membership attribute of a group was replicated as a single value. This meant that if two administrators changed the membership of the same group in two different instances of AD DS during the same replication period, the last write won. The first changes made would be lost, because the new version of the group membership attribute replaced the previous one entirely. With linked-value replication, group membership is treated at the value level; therefore, all updates are merged together. This also greatly reduces replication traffic. An additional benefit from this feature is the removal of the previous group membership restriction that limited the maximum number of members to 5,000.
- Improved AD DS replication calculation algorithms. The Knowledge Consistency Checker (KCC) and Intersite Topology Generator (ISTG) use improved algorithms to speed up the calculation of the AD DS replication infrastructure and provide much faster site link calculations.
- Support for RODCs. RODCs are supported at the Windows Server 2003 forest functional level. The RODC must be running Windows Server 2008 or newer and requires at least one Windows Server 2008 or newer full domain controller as a replication partner.
- Conversion of inetOrgPerson objects to user objects. You can convert an instance of an inetOrgPerson object—used for compatibility with certain nonMicrosoft directory services—into an instance of class user object. You can also convert a user object to an inetOrgPerson object.

- 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.

The Windows Server 2008 forest functional level does not add new forest-wide features. The Windows Server 2008 R2 forest functional level adds the ability to activate Active Directory features, such as the Active Directory Recycle Bin feature. This feature allows the ability to restore deleted Active Directory objects. You cannot roll back the forest functional level if features requiring a certain forest level, such as the Active Directory Recycle Bin feature, have been enabled.

Although the Windows Server 2008 R2 AD DS forest functional level introduced Active Directory Recycle Bin, the Recycle Bin had to be managed with Windows PowerShell. However, the version of Remote Server Administration Tools (RSAT) that comes with Windows Server 2012 has the ability to manage the Active Directory Recycle Bin by using graphical user interface (GUI) tools.

The Windows Server 2012 forest functional level does not provide any new forest-wide features. For example, if you raise the forest functional level to Windows Server 2012, you cannot add a new domain running at Windows Server 2008 R2 domain functional level.

The Windows Server 2012 R2 forest functional level does not provide any new forest-wide features. Any domains added to the forest operate at the Windows Server 2012 R2 domain functional level.

At the time of writing this course, the Windows Server 2016 Technical Preview forest functional level did not provide any new forest wide features. Any domains added to the forest will operate at the Windows Server 2016 Technical Preview domain functional level.

## Deploying new AD DS domains

When you create a new forest in AD DS, a new domain called the forest root domain is automatically created and forms the base of your AD DS infrastructure. Domain controllers in the forest root domain hold the schema master and domain-naming master Flexible Single Master Operation (FSMO) roles for the forest in addition to the domain FSMO roles. If your organization only requires a single domain, the forest root domain will also contain all the user, group, and computer objects used by your organization. If you are deploying multiple domains because of replication, DNS namespace, or administrative requirements, your forest root domain may only contain the necessary administrative objects for the forest. You can choose to create additional domains in one of the following two ways:

- **Forest root domain:**
  - Is automatically created with a new forest
  - Is the base of an AD DS infrastructure
  - Can be the only domain in an AD DS deployment
- **Child domain:**
  - Is a child of a parent domain
  - Shares the same namespace with the parent domain
- **Tree domain:**
  - Creates a new domain tree and a new namespace
  - Are commonly used in merger and acquisition scenarios

- Create a child domain. Child domains share a common namespace with a parent domain. They are common in scenarios where you may decide to deploy multiple domains which align to specific departments or regions within your organization. For example, if you are the forest administrator for the adatum.com forest, you may deploy child domains named europe.adatum.com and asia.adatum.com which align to the continents where A. Datum conducts operations. Child domains can also be the parent of other child domains such as sales.europe.adatum.com or test.asia.adatum.com.

- Create tree domain. Tree domains are domains which establish a new namespace that differs from the forest root domain. Tree domains are common in merger and acquisition scenarios or in organizations which have multiple subsidiaries. For example, if you are the forest administrator for the adatum.com forest, you may deploy tree domains named treyresearch.net and tailspintoys.com which align to autonomous companies owned by A. Datum. Tree domains can also contain child domains such as europe.treyresearch.net or asia.tailspintoys.com.

## Demonstration: Installing a domain controller in a new domain in an existing forest

In this demonstration, you will see how to:

- Install the AD DS binaries on TOR-DC1.
- Configure TOR-DC1 as an AD DS domain controller using the Active Directory Domain Services Configuration Wizard.

### Demonstration Steps

#### Install the AD DS binaries on TOR-DC1

1. On **TOR-DC1**, in **Server Manager**, use the **Add Roles and Features Wizard** to install the Active Directory Domain Services binaries.
2. Complete the AD DS **Add Roles and Features Wizard** using default settings.

#### Configure TOR-DC1 as an AD DS domain controller using the Active Directory Domain Services Configuration Wizard

1. Use **Promote this server to a domain controller** to start the **Active Directory Domain Services Configuration Wizard**.
2. Use the **Active Directory Domain Services Configuration Wizard** to configure AD DS on **TOR-DC1** with the following settings:
  - Deployment operation: **Add a new domain to an existing forest**
  - New domain name: **NA**
  - Directory Services Restore Mode (DSRM) password: **Pa\$\$w0rd**
3. Complete the **Active Directory Domain Services Configuration Wizard** with default settings.
4. Restart, and then sign in as **NA\Administrator** with the password as **Pa\$\$w0rd**, on the newly-created AD DS domain controller **TOR-DC1**.

## Upgrading a previous version of AD DS to Windows Server 2016

To upgrade a previous version of AD DS to Windows Server 2016 AD DS, you can use either of the following two methods:


- Upgrade the operating system on the existing domain controllers to Windows Server 2016.
- Introduce Windows Server 2016 servers as domain controllers in the existing domain. You can then decommission AD DS domain controllers that are running earlier versions of AD DS.

### Methods to upgrade AD DS to Windows Server 2016:

- In-place upgrade from Windows Server 2012 R2 or Windows Server 2012
  - Introduce a new Windows Server 2016 server into the domain and promote it to be a domain controller (recommended method)
- Both methods require that the schema is at the Windows Server 2016 level:
- The Active Directory Domain Services Installation Wizard will upgrade the schema automatically when run with appropriate permissions
  - Adprep is available

Of these two methods, the second is preferred, because upgrading operating systems—especially on servers that have been running for several years—is often difficult due to all the changes made through the years. By installing new domain controllers running Windows Server 2016, you will have a clean installation of Windows Server 2016.

You can deploy Windows Server 2016 servers as member servers in a domain with domain controllers running Windows Server 2008 or newer versions. However, before you can install the first domain controller that is running Windows Server 2016, you must upgrade the schema. In versions of AD DS prior to Windows Server 2012 R2, you ran the Adprep.exe tool to perform the schema upgrades. However, when you deploy new Windows Server 2016 domain controllers in an existing domain, and if you are signed in with an account that is a member of the Schema Admins and Enterprise Admins groups, the Active Directory Domain Services Installation Wizard automatically upgrades the AD DS forest schema.


 **Note:** Windows Server 2016 still provides a 64-bit version of Adprep, so you can run Adprep.exe separately. For example, if the administrator who is installing the first Windows Server 2016 domain controller is not a member of the Enterprise Admins or Schema Admins group, you might have to run the command separately. You only have to run adprep.exe if you are planning an in-place upgrade for the first Windows Server 2016 domain controller in the domain.

### The upgrade process

To upgrade the operating system of a Windows Server 2012 domain controller to Windows Server 2016, perform the following steps:

1. Insert the installation media for Windows Server 2016, and then run **Setup**.
2. After the **language selection** page, click **Install now**.
3. After the **operating system selection** window and the **license acceptance** page, on the **Which type of installation do you want?** window, click **Upgrade: Install Windows and keep files, settings, and apps**.

With this type of upgrade, AD DS on the domain controller is upgraded to Windows Server 2016 AD DS. As a best practice, you should check for hardware and software compatibility before you perform an upgrade. After performing the operating system upgrade, remember to update your drivers and other services (such as monitoring agents) and to check for updates for both Microsoft applications and non-Microsoft software.

 **Note:** You can upgrade directly from Windows Server 2012 and Windows Server 2012 R2 to Windows Server 2016. To upgrade servers that are running a version of Windows Server that is older than Windows Server 2012, you must either perform an interim upgrade to Windows Server 2012 or Windows Server 2012 R2, or perform a clean install. Note that Windows Server 2016 AD DS domain controllers can coexist as domain controllers in the same domain as Windows Server 2008 domain controllers or newer.

### The clean installation process

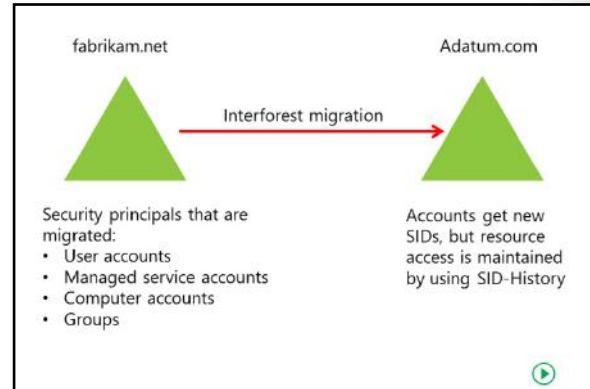
For a clean install of Windows Server 2016 as a domain member, perform these steps:

1. Deploy and configure a new installation of Windows Server 2016, and then join it to the domain.
2. Promote the new server to be a domain controller in the domain by using Server Manager.

### Migrating to Windows Server 2016 AD DS from a previous version

As part of deploying AD DS, you might choose to restructure your environment for the following reasons:

- To optimize the logical AD DS structure. In some organizations, the business may have changed significantly since AD DS was first deployed. As a result, the AD DS domain or forest structure may no longer meet the business requirements.
- To assist in completing a business merger, acquisition, or divestiture.



Restructuring involves the migration of resources between AD DS domains in either the same forest or in different forests. There is no option available in AD DS to detach a domain from one forest and then attach it to another forest. You can rename and rearrange domains within a forest under some circumstances, but there is no way to easily merge domains within or between forests. The only option for restructuring a domain in this way is to move all the accounts and resources from one domain to another.

You can use the Microsoft Active Directory Migration Tool (ADMT) to move user, group, and computer accounts from one domain to another, and to migrate server resources. If managed carefully, the migration can be completed without disrupting user access to the resources they need to do their work. ADMT provides both a GUI and a scripting interface, and supports the following tasks for completing the domain migration:

- User account migration
- Group account migration
- Computer account migration
- Service account migration
- Trust migration
- Exchange Server directory migration

- Security translation on migrated computer accounts
- Reporting features for viewing the migration's results
- Functionality to undo the last migration and retry the last migration

### Premigration steps

Before performing the migration, you must complete several tasks to prepare the source and target domains. These tasks include:

- For domain member computers that are pre-Windows Vista Service Pack 1 (SP1) or Windows Server 2008 R2, configure a registry key on the target AD DS domain controller to allow cryptography algorithms that are compatible with the Microsoft Windows NT Server 4.0 operating system.
- Enable firewall rules on source and target AD DS domain controllers to allow file and printer sharing.
- Prepare the source and target AD DS domains to manage how the users, groups, and user profiles will be handled.
- Create a rollback plan.
- Establish the trust relationships that are required for the migration.
- Configure source and target AD DS domains to enable SID-History migration.
- Specify service accounts for the migration.
- Perform a test migration and fix any errors that are reported.

### Interforest restructuring with ADMT

An interforest restructure involves moving resources from source domains that are in different forests than the target domain. To use ADMT to perform an interforest restructure, do the following:

1. Create a restructure plan. An adequate plan is critical to the success of the restructuring process. Complete the following steps to create your restructure plan:
  - a. Determine the account-migration process.
  - b. Assign object locations and location mapping.
  - c. Develop a test plan.
  - d. Create a rollback plan.
  - e. Create a communication plan.
2. Prepare source and target domains. You must prepare both the source and target domains for the restructure process by performing the following tasks:
  - a. Ensure 128-bit encryption on all domain controllers. Windows Server 2000 SP3 and newer versions natively support 128-bit encryption. For older operating systems, you must download and install a separate encryption pack.
  - b. Establish required trusts. You must configure at least a one-way trust between the source and target domains.
  - c. Establish migration accounts. The ADMT uses migration accounts to migrate objects between source and target domains. Ensure that these accounts have permissions to move and modify objects on the source and target domains.
  - d. Determine whether ADMT will handle SID-History automatically, or if you must configure the target and source domains manually.



- e. Ensure proper configuration of the target domain OU structure. Ensure that you configure the proper administrative rights and delegated administration in the target domain.
  - f. Install ADMT in the target domain.
  - g. Enable password migration.
  - h. Perform a test migration with a small test account group.
3. Migrate accounts. Perform the following steps to migrate accounts:
    - a. Transition service accounts.
    - b. Migrate global groups.
    - c. Migrate accounts. Migrate user and computer accounts in batches to monitor the migration's progress. If you are migrating local profiles as part of the process, migrate the affected computers first, and then the associated user accounts.
  4. Migrate resources. Migrate the remaining resources in the domain by performing the following steps:
    - a. Migrate workstations and member servers.
    - b. Migrate domain local groups.
    - c. Migrate domain controllers.
  5. Finalize migration. Finalize the migration and perform cleanup by performing the following steps:
    - a. Transfer administration processes to the target domain.
    - b. Ensure that at least two operable domain controllers exist in the target domain. Back up these domain controllers.
    - c. Decommission the source domain.

### The SID-History attribute

During the migration, you may have moved user and group accounts to the new domain, but the resources that the users need to access may still be in the old domain. When you migrate a user account, AD DS assigns it a new SID. Because the resource in the source domain grants access based on the user SID from the source domain, the user cannot use the new SID to access the resource until the resource is moved to the new domain.

To address this situation, you can configure the ADMT to migrate the SID from the source domain, and then store the SID in an attribute called **SID-History**. When the **SID-History** attribute is populated, the user's previous SID is used to grant access to resources in the source domain.

SID-History increases the size of the users' access token. After migrating the users to the new domain, the access control lists (ACLs) in your environment should be examined and ACLs migrated as well. After a migration is complete and the original domain has been removed, you should clean up your users' SID-History attribute. You can best accomplish this task by using the **Get-SIDHistory** and **Remove-SIDHistory Windows PowerShell** cmdlets. You should carefully plan and execute these activities because removing SID-History before the environment is properly prepared could cause business interruptions.



**Additional Reading:** For more information on using ADMT, refer to: <http://aka.ms/Jiauyg>

## Considerations for implementing complex AD DS environments

In a single-forest, single-domain AD DS environment, when you install AD DS and DNS with default settings, the configuration works appropriately in most scenarios. However, as your organization grows and your AD DS environment becomes more complex, there are several choices you may have to make in order to facilitate efficient name resolution and user sign in within the AD DS environment.

### DNS considerations

In a multidomain or multiforest environment, client computers may have to locate a variety of cross-forest services, including Key Management Servers for Windows Activation, Terminal Services Licensing servers, licensing servers for specific applications, and domain controllers in any domain to validate trusts when accessing resources in another domain. When organizations deploy multiple trees in an AD DS forest or when they deploy multiple forests, name resolution is more complicated because you must manage multiple domain namespaces. In these scenarios, consider the following points:

- DNS considerations:
  - Centralized vs. decentralized
  - Verify the DNS client configuration and name resolution
  - Optimize DNS name resolution:
    - Conditional forwarders and stub zones
    - DNS devolution and DNS suffix search order
  - Deploy a GlobalNames zone
  - Use AD DS-integrated zones
  - Extending AD DS to Azure
- UPN considerations:
  - UPN suffixes
  - Global catalog
  - Federated authentication scenarios

- Decide on a centralized or decentralized model. In a centralized model, you configure all DNS zones for forest-wide replication, making them locally available on every domain controller in the forest. Although this is easy to accomplish and ensures cross-domain name resolution, you must consider the impact this may have on domain controller replication throughout your AD DS environment. In a decentralized model, zones are configured for domain-wide replication, making them available on every domain controller in the domain. To implement cross-domain name resolution, you create delegations in the parent domain and forwarders in the child domains. A decentralized model is more difficult to maintain but allows you more control over replication and flexibility in administration of the child domains.
- Verify the DNS client configuration. Configure all computers in the AD DS domain with at least two addresses of functional DNS servers. All computers must have good network connectivity with DNS servers.
- Verify and monitor DNS name resolution. Verify that all of your computers, including domain controllers, are able to perform successful DNS lookups for all domain controllers in the forest. Domain controllers must be able to connect to other domain controllers to successfully replicate changes to AD DS. Client computers must be able to locate domain controllers by using SRV resource records, and must be able to resolve the domain controller names to IP addresses.
- Optimize DNS name resolution between multiple namespaces:
  - Use DNS features such as conditional forwarding and stub zones to optimize the process of resolving computer names across the namespaces. By using a conditional forwarder or stub zone, you effectively create a shortcut that prevents the need for recursive queries to the domain tree or forest root. Although a conditional forwarder or stub zone is not required for name resolution to work correctly, it may greatly reduce latency when cross-domain or cross-forest name resolution occurs frequently. When you configure a trust between two forests, you typically use a conditional forwarder in each forest to facilitate name resolution on both sides of the trust.

- Consider DNS devolution and DNS suffix search order. DNS devolution is a feature of the Windows DNS client that allows a client in a child namespace to resolve the IP address of a host in a parent namespace without specifying a fully qualified domain name (FQDN). The devolution process automatically attempts to resolve a single-label name by appending the primary DNS suffix. If a result is not found, devolution recursively appends the parent DNS suffix until the name is resolved or the devolution level is met. The devolution level is determined automatically by comparing the forest root domain to the primary DNS suffix, but it also can be manually configured when precise control is necessary. In complex AD DS environments where you may have a deep domain tree with many levels in the namespace, relying on DNS devolution for name resolution may not be efficient. In these cases, you can configure the DNS suffix search order to manually specify the DNS suffixes to append and the order in which to append them. When the DNS suffix search order is specified either manually or through Group Policy, the DNS devolution process is automatically disabled.
- Deploy a GlobalNames zone. A GlobalNames zone allows you to configure single name resolution for DNS names in your forest. This allows name resolution using a shorter name that is easier to remember than a FQDN. Previously, Windows Internet Name Service (WINS) was configured in a domain to support single-label name resolution. You can use a GlobalNames zone to replace WINS in your environment, especially if you deploy Internet Protocol version 6 (IPv6), because WINS does not support IPv6 addressing. In addition, you can use a GlobalNames zone when relying on DNS suffix search lists is not efficient due to the number of domains that must be searched.
- Use AD DS-integrated DNS zones. When you configure a DNS zone as AD DS integrated, the DNS information is stored in AD DS and replicated through the normal AD DS replication process. This optimizes the process of replicating changes throughout the forest. You can also configure the scope of replication for the DNS zones. By default, domain-specific DNS records are replicated to other domain controllers that are also DNS servers in the domain. DNS records that enable cross-domain lookups are stored in the `_msdcs.forestrootdomainname` zone and are replicated to domain controllers that are also DNS servers in the entire forest. You should not change this default configuration.
- When you extend your AD DS domain into Azure, you must take a few extra steps. Azure's built-in DNS does not support AD DS domains; to support your cloud-based domain components, you must do the following:
  - Configure an Azure Virtual Network.
  - Configure an AD DS site for your Azure subnet.
  - Register your on-premises DNS with the Azure Virtual Network. You must do this to allow an Azure virtual machine to communicate with your on-premises AD DS.
  - After you have successfully promoted an Azure virtual machine to an AD DS domain controller/DNS server, register that virtual machine's IP address as the DNS server for your Azure Virtual Network. This allows local AD DS communication and name resolution for other virtual machines in your Azure subnet.

## UPN considerations

In a multidomain or multiforest environment, sign in becomes more complicated as users must be aware of the domain that contains their user account. Users are able to sign in by using the NetBIOS name of the domain and their SAM Account Name or the friendlier UPN attribute, which is formatted like an email address. The default UPN is *user@DNS-domain-name*. A UPN is generally easier to remember and in many organizations, may match the user's primary email address. If you decide to use the UPN attribute for sign in, there are several things you must consider:

- **UPN suffixes.** By default, the UPN suffix matches the DNS FQDN of the domain where the user account exists. In complex AD DS environments where there are multiple domains in a domain tree, the UPN suffix may become quite long and difficult to remember. For example, in an AD DS environment organized by region and department, a sample default UPN may look like *user@hr.northamerica.contoso.com*. In this situation, you may decide to utilize a common UPN suffix for all users in the domain. The UPN suffix does not have to be a valid DNS domain, but, in many cases, organizations choose to use their email domain name to simplify the sign-in process for users. The **Active Directory Domains and Trusts** console allows you to specify alternate UPN suffixes for a domain. You specify the UPN suffix for a user account upon account creation and you can modify it anytime afterward.
- **Global catalog.** To allow sign in with a UPN, availability of a global catalog server may be necessary. If an alternate UPN suffix is used and the computer account is not in the same domain as the user account, a global catalog server is required to resolve the UPN that is specified during sign in.
- **Federated authentication scenarios.** If your organization is leveraging AD FS to perform federated authentication with a cloud-based service such as Office 365, the UPN suffix used must be a valid external DNS domain owned by your organization. This is necessary because a federation trust cannot be created with a DNS domain that only exists within your internal AD DS infrastructure.

## Check Your Knowledge

Question	
What is the minimum domain functional level in which you should deploy a Windows Server 2016 AD DS domain controller?	
Select the correct answer.	
<input type="checkbox"/>	Windows Server 2003
<input type="checkbox"/>	Windows Server 2008
<input type="checkbox"/>	Windows Server 2008 R2
<input type="checkbox"/>	Windows Server 2012 R2
<input type="checkbox"/>	Windows Server 2016

**Check Your Knowledge**

Question	
Which of the following can you use to optimize name resolution across DNS namespaces?	
Select the correct answer.	
<input type="checkbox"/>	Conditional forwarders
<input type="checkbox"/>	AD DS sites
<input type="checkbox"/>	DNS suffix search order
<input type="checkbox"/>	DNS stub zones
<input type="checkbox"/>	Global catalog servers

## Lesson 3

# Configuring AD DS trusts

AD DS trusts enable access to resources in a complex AD DS environment. When you deploy a single domain, you can easily grant access to resources within the domain to users and groups from the domain. When you implement multiple domains or forests, you should ensure that the appropriate trusts are in place to enable the same access to resources. This lesson describes how trusts work in an AD DS environment, and how you can configure trusts to meet your business requirements.

### Lesson Objectives

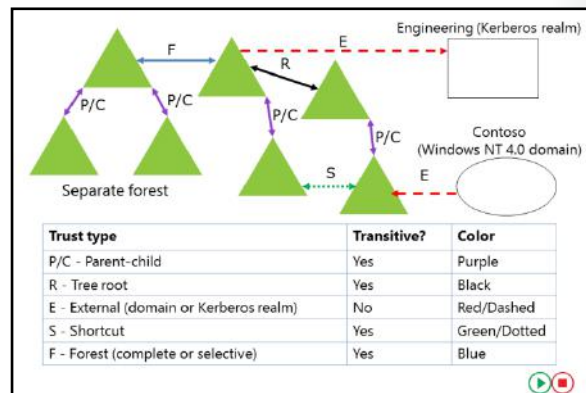
After completing this lesson, you will be able to:

- Describe the types of trusts that you can configure in a Windows Server 2016 environment.
- Explain how trusts work within an AD DS forest.
- Explain how trusts work between AD DS forests.
- Describe how to configure advanced trust settings.
- Configure a forest trust.

### Overview of different AD DS trust types

In a multidomain AD DS forest, two-way transitive trust relationships are generated automatically between the AD DS domains, so that there is a path of trust between all of the AD DS domains. The trusts that are created automatically in the forest are all transitive trusts. This means that if domain A trusts domain B, and domain B trusts domain C, then domain A trusts domain C.

There are other types of trust that you can deploy. The following table describes the main trust types.



Trust type	Transitivity	Direction	Description
Parent and child	Transitive	Two-way	When you add a new AD DS domain to an existing AD DS tree, new parent and child trusts are created.
Tree-root	Transitive	Two-way	When a new AD DS tree is created in an existing AD DS forest, a new tree-root trust is created.
External	Nontransitive	One-way or two-way	External trusts enable resource access to be granted with a Windows NT 4.0 domain or an AD DS domain in another forest. These may also be set up to provide a framework for a migration.

Trust type	Transitivity	Direction	Description
Realm	Transitive or nontransitive	One-way or two-way	Realm trusts establish an authentication path between a Windows Server AD DS domain and a Kerberos v5 realm implemented by using a directory service other than AD DS.
Forest (complete or selective)	Transitive	One-way or two-way	Trusts between AD DS forests allow two forests to share resources.
Shortcut	Nontransitive	One-way or two-way	You can configure shortcut trusts to improve authentication times between AD DS domains that are in different parts of an AD DS forest. There are no shortcut trusts by default; they must be created by an administrator.

## How trusts work within a forest

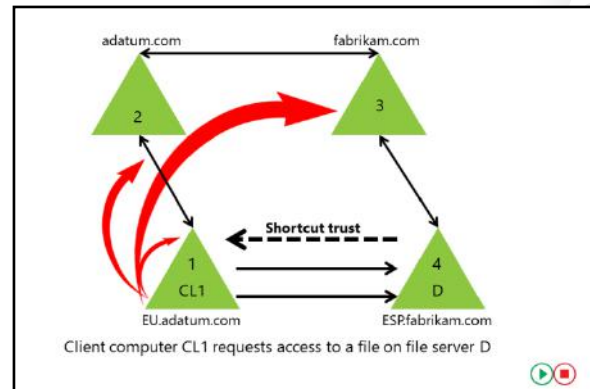
When you set up trusts between domains either within the same forest, across forests, or with an external realm, information about these trusts, such as transitivity and type, is stored in AD DS. A trusted domain object stores this information. This domain object is created and stored in the System container in AD DS whenever you set up a trust.

### How trusts enable users to access resources in a forest

When the user in the domain attempts to access a shared resource in another domain in the forest, the user's computer first contacts a domain controller in its domain to request a session ticket to the resource. Because the resource is not in the user's domain, the domain controller must determine whether a trust exists with the target domain.

The domain controller can use the trust domain object to verify that the trust exists. However, to access the resource, the client computer must communicate with a domain controller in each domain along the trust path. The domain controller in the client computer's domain refers the client computer to a domain controller in the next domain along the trust path. If that is not the domain where the resource is located, that domain controller refers the client computer to a domain controller in the next domain. Eventually, the client computer is referred to a domain controller in the domain where the resource is located, and the client is issued a session ticket to access the resource.

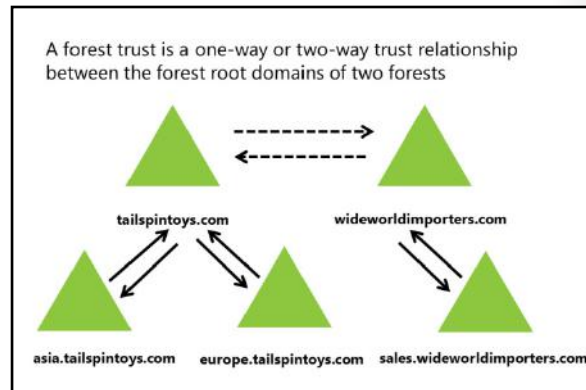
The trust path is the shortest path through the trust hierarchy. In a forest in which only the default trusts are configured, the trust path goes up the domain tree to the forest root domain, and then down the domain tree to the target domain. If shortcut trusts are configured, the trust path may be a single hop from the client computer domain to the domain containing the resource.



## How trusts work between forests

If the AD DS environment contains more than one forest, it is possible to set up trust relationships between the AD DS forest root domains. These forest trusts can be either forest-wide trusts or selective trusts. Forest trusts can be one-way or two-way. Forest trusts are also transitive for domains in each forest.

A forest trust relationship allows users who are authenticated by a domain in one forest to access resources that are in a domain in the other forest, provided they have been granted access rights. If the forest trust is one-way, domain controllers in the trusting forest can provide session tickets to users in any domain in the trusted forest. Forest trusts are significantly easier to establish, maintain, and administer than separate trust relationships between each of the domains in the forests.



Forest trusts are particularly useful in scenarios that involve cross-organization collaboration, mergers and acquisitions, or within a single organization that has more than one forest in which to isolate Active Directory data and services. Forest trusts are also useful for application service providers, for collaborative business extranets, and for companies seeking a solution for administrative autonomy.

Forest trusts provide the following benefits:

- Simplified management of resources across two Windows Server 2008 (or newer version) forests by reducing the number of external trusts necessary to share resources.
- Complete two-way trust relationships with every domain in each forest.
- Use of UPN authentication across two forests.
- Use of the Kerberos v5 protocol to improve the trustworthiness of authorization data that is transferred between forests.
- Flexibility of administration. Administrative tasks can be unique to each forest.

You can create a forest trust only between two AD DS forests; you cannot extend the trust implicitly to a third forest. This means that if you create a forest trust between Forest 1 and Forest 2 and you create a forest trust between Forest 2 and Forest 3, Forest 1 does not have an implicit trust with Forest 3. Forest trusts are not transitive between multiple forests.

You must address several requirements before you can implement a forest trust, including ensuring that the forest functional level is Windows Server 2003 or newer and that DNS name resolution exists between the forests.



## Configuring advanced AD DS trust settings

In some cases, trusts can present security issues. Additionally, if you do not configure a trust properly, users who belong to another domain can gain unwanted access to some resources. There are several technologies that can help you control and manage security in a trust.

### SID filtering

By default, when you establish a forest or domain trust, you enable a domain quarantine, which is also known as SID filtering. When a user authenticates in a trusted domain, the user presents authorization data that includes the SIDs

of all of the groups to which the user belongs. Additionally, the user's authorization data includes the SID-History of the user and the user's groups. SID filtering prevents misuse of the SID-History attribute by allowing reading of the SID only from the objectSID attribute and not the SID-History attribute.

In a trusted domain scenario, an administrator can use administrative credentials in the trusted domain to load SIDs that are the same as SIDs of privileged accounts in your domain into the SID-History attribute of a user. That user would then have inappropriate levels of access to resources in your domain. SID filtering prevents this 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 that 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. SID filtering is enabled by default for all outgoing trusts to external domains and forests.

### Selective authentication

When you create an external trust or a forest trust, you can manage the scope of authentication of trusted security principals. There are two modes of authentication for an external or forest trust:

- Domain-wide authentication (for an external trust) or forest-wide authentication (for a forest trust)
- Selective authentication

Choosing domain-wide or forest-wide authentication enables all trusted users to authenticate for services and access on all computers in the trusting domain. Therefore, trusted users can be given permission to access resources anywhere in the trusting domain. If you use this authentication mode, all users from a trusted domain or forest are considered Authenticated Users in the trusting domain. Thus, if you choose domain-wide or forest-wide authentication, any resource that has permissions granted to Authenticated Users is accessible immediately to trusted domain users.

If 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 specify. When they use selective authentication, users will not become authenticated users in the target domain, but you can explicitly grant them the **Allowed to Authenticate** permission on specific computers.

For example, imagine that you have an external trust with a partner organization's domain. You want to ensure that only users from the partner organization's marketing group 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.

Security considerations in forest trusts include:

- SID filtering
- Selective authentication
- Name suffix routing

An incorrectly configured trust can allow unauthorized access to resources

## Name suffix routing

Name suffix routing is a mechanism for managing how authentication requests are routed across forests running Windows Server 2003 or newer forests that are joined by forest trusts. To simplify the administration of authentication requests, when you create a forest trust, AD DS routes all unique name suffixes by default. A *unique name suffix* is a name suffix within a forest—such as a UPN suffix, SPN suffix, or DNS forest or domain tree name—that is not subordinate to any other name suffix. For example, the DNS forest name fabrikam.com is a unique name suffix within the fabrikam.com forest.

AD DS routes all names that are subordinate to unique name suffixes implicitly. For example, if your forest uses fabrikam.com as a unique name suffix, authentication requests for all child domains of fabrikam.com (childdomain.fabrikam.com) are routed, because the child domains are part of the fabrikam.com name suffix. Child names appear in the **Active Directory Domains and Trusts** snap-in. If you want to exclude members of a child domain from authenticating in the specified forest, you can disable name-suffix routing for that name. You also can disable routing for the forest name itself.



### Additional Reading:

- For more information on configuring SID filter quarantining on external trusts, refer to: <http://aka.ms/Sveqfn>
- For more information on enabling selective authentication over a forest trust, refer to: <http://aka.ms/Blp826>
- For more information on name-suffix routing, refer to: <http://aka.ms/Egc6g7>

## Demonstration: Configuring a forest trust

In this demonstration, you will see how to:

- Configure DNS name resolution by using a conditional forwarder.
- Configure a two-way selective forest trust.

### Demonstration Steps

#### Configure DNS name resolution by using a conditional forwarder

1. Configure DNS name resolution between adatum.com and treyresearch.net by creating a conditional forwarder so that **LON-DC1** has a referral to **TREY-DC1** as the DNS server for the DNS domain **treyresearch.net**.
2. Configure a conditional forwarder on **TREY-DC1** so that it has a referral to **LON-DC1** for the DNS domain **adatum.com**.

#### Configure a two-way selective forest trust

- On **LON-DC1**, in **Active Directory Domains and Trusts**, create a two-way selective forest trust between **adatum.com** and **treyresearch.net** by supplying the credentials of the **treyresearch.net** domain **Administrator** account.

**Check Your Knowledge**

Question	
Which of the following must be in place before you can create a forest trust?	
Select the correct answer.	
<input type="checkbox"/>	Name resolution between the root domains in each forest
<input type="checkbox"/>	Forest functional level of Windows Server 2003 or higher
<input type="checkbox"/>	Forest functional level of Windows Server 2008 or higher
<input type="checkbox"/>	Forest functional level of Windows Server 2012 or higher
<input type="checkbox"/>	Domain controllers must be enabled for selective authentication

**Check Your Knowledge**

Question	
Which AD DS trust setting allows you to control the scope of authentication of trusted security principals?	
Select the correct answer.	
<input type="checkbox"/>	Name suffix routing
<input type="checkbox"/>	Kerberos constrained delegation (KCD)
<input type="checkbox"/>	Selective authentication
<input type="checkbox"/>	SID filtering
<input type="checkbox"/>	SID-History

## Lab: Domain and trust management in AD DS

### Scenario

A. Datum Corporation has deployed a single AD DS domain with all the domain controllers located in its London data center. As the company has grown and added branch offices with a large numbers of users, it has become increasingly apparent that the current AD DS environment does not meet company requirements. The network team is concerned about the amount of AD DS-related network traffic that is crossing WAN links, which are becoming highly utilized.

The company has also become increasingly integrated with partner organizations, some of which need access to shared resources and applications that are located on the A. Datum internal network. The security department at A. Datum wants to ensure that the access for these external users is as secure as possible.

As one of the senior network administrators at A. Datum, you are responsible for implementing an AD DS infrastructure that meets the company requirements. You are responsible for planning an AD DS domain and forest deployment that provides optimal services for both internal and external users, while addressing the security requirements at A. Datum.

### Objectives

After completing this lab, you will be able to:

- Implement forest trusts in AD DS.
- Implement child domains in AD DS.

### Lab Setup

Estimated Time: 45 minutes

Virtual machines: **20742A-LON-DC1**, **20742A-LON-DC2**, **20742A-TOR-DC1**, **20742A-LON-SVR2**, and **20742A-TREY-DC1**

User name: **Adatum\Administrator**

Password: **Pa\$\$w0rd**

For this lab, you will use the available virtual machine environment. Before you begin the lab, you must complete the following steps:

1. On the host computer, start **Hyper-V Manager**.
2. In Hyper-V Manager, click **20742A-LON-DC1**, and in the **Actions** pane, click **Start**.
3. In the **Actions** pane, click **Connect**. Wait until the virtual machine starts.
4. Sign in using the following credentials:
  - User name: **Adatum\Administrator**
  - Password: **Pa\$\$w0rd**
5. Repeat steps 2 through 4 for **20742A-LON-DC2**, **20742A-LON-SVR2**, and **20742A-TOR-DC1**.
6. Start **20742A-TREY-DC1**, and sign in as **TreyResearch\Administrator** with the password **Pa\$\$w0rd**.

## Exercise 1: Implementing forest trusts

### Scenario

A. Datum is working on several high-priority projects with a partner organization named Trey Research. To simplify the process of enabling access to resources located in the two organizations, they have deployed a WAN between London and Munich, where Trey Research is located. You now must implement and validate a forest trust between the two forests and configure the trust to allow access to only selected servers in London.

The main tasks for this exercise are as follows:

1. Configure stub zones for DNS name resolution.
2. Configure a forest trust with selective authentication.
3. Configure a server for selective authentication.

#### ► Task 1: Configure stub zones for DNS name resolution

1. On **LON-DC1**, using the **DNS management** console, configure a DNS stub zone for **treymresearch.net**:
  - o Use **172.16.10.10** as the **Master DNS** server.
2. On **TREY-DC1**, using the **DNS management** console, configure a DNS stub zone for **adatum.com**:
  - o Use **172.16.0.10** as the **Master DNS** server.

#### ► Task 2: Configure a forest trust with selective authentication

1. On **LON-DC1**, create a one-way outgoing trust between the **treymresearch.net** AD DS forest and the **adatum.com** forest. Configure the trust to use selective authentication.
2. Confirm and validate the trust from **treymresearch.net**.

#### ► Task 3: Configure a server for selective authentication

1. On **LON-DC1**, from the **Server Manager**, open **Active Directory Users and Computers**.
2. Configure the **LON-SVR2** computer object permissions so that members of **TreyResearch\IT** group have the **Allowed to authenticate** permission. If you are prompted for credentials, type **TreyResearch\administrator** with the password as **Pa\$\$w0rd**.
3. On **LON-SVR2**, create a shared folder named **IT-Data**, and grant **Read/Write** access to members of the **TreyResearch \IT** group. If you are prompted for credentials, type **TreyResearch\administrator** with the password as **Pa\$\$w0rd**.
4. Add user name **Alice** to the **Domain Admins** group in the **TreyResearch** domain.
5. Sign out of **TREY-DC1**.
6. Sign in to **TREY-DC1** as **TreyResearch\Alice** with the password as **Pa\$\$w0rd**, and verify that you can access the shared folder on **LON-SVR2**.

**Results:** After completing this exercise, you should have implemented forest trusts.

## Exercise 2: Implementing child domains in AD DS

### Scenario

A. Datum has decided to deploy a new child domain in the adatum.com forest for the North American region. The first domain controller will be deployed in Toronto, and the domain name will be na.adatum.com. You need to configure and install the new domain controller.

The main tasks for this exercise are as follows:

1. Install a domain controller in a child domain.
2. Verify the default trust configuration.
3. Prepare for the next module.

#### ► Task 1: Install a domain controller in a child domain

1. On **TOR-DC1**, start **Server Manager** and then install the AD DS binaries.
2. When the AD DS binaries have installed, use the **Active Directory Domain Services Configuration Wizard** to install and configure **TOR-DC1** as an AD DS domain controller for a new child domain named **na.adatum.com**.
3. When prompted, use **Pa\$\$w0rd** as the **Directory Services Restore Mode (DSRM)** password. After the configuration completes, the server restarts automatically.

#### ► Task 2: Verify the default trust configuration

1. Sign in to **TOR-DC1** as **NA\Administrator** with the password as **Pa\$\$w0rd**.
2. Ensure that the Windows Firewall is turned off for all profiles.
3. From **Server Manager**, launch the **Active Directory Domains and Trusts** console, and verify the parent child trusts.



**Note:** If you receive a message that the trust cannot be validated or that the secure channel verification has failed, ensure that you have completed step 2, and then wait for at least 10 to 15 minutes before trying again.

**Results:** After completing this exercise, you should have implemented child domains in AD DS.

► **Task 3: Prepare for the next module**

When you finish the lab, revert the virtual machines to their initial state. To do this, complete the following steps:

1. On the host computer, start **Hyper-V Manager**.
2. In the **Virtual Machines** list, right-click **20742A-LON-DC1**, and then click **Revert**.
3. In the **Revert Virtual Machine** dialog box, click **Revert**.
4. Repeat steps 2 and 3 for **20742A-LON-DC2**, **20742A-TOR-DC1**, **20742A-TREY-DC1**, and **20742A-LON-SVR2**.

**Question:** When creating the forest trust between Adatum.com and TreyResearch.net, DNS stub zones were created to enable name resolution between the two forests. What alternative could you have used in place of a DNS stub zone?

**Question:** When you are creating a forest trust, why would you create a selective trust instead of a complete trust?

## Module Review and Takeaways

### Review Question

**Question:** You are the AD DS administrator for A. Datum Corporation. Currently, your AD DS environment is configured in a single-domain, single-forest model using the adatum.com namespace. A. Datum has recently announced that they are expanding from Europe into new continents through the acquisition of a company named Trey Research. Trey Research currently operates in North America and Asia. The AD DS environment of Trey Research consists of a single forest named treyresearch.net with an empty forest root domain, and child domains which align to each continent they operate in (na.treyresearch.net and asia.treyresearch.net). The long-term objectives for A. Datum are to fully integrate Trey Research into the daily operations of A. Datum. A. Datum leadership also wishes to adopt the regional operations model used by Trey Research. As the AD DS administrator for A. Datum, how would you combine the adatum.com forest with the treyresearch.net forest? Discuss both short-term and long-term objectives for AD DS integration and how different requirements might change your approach.

### Common Issues and Troubleshooting Tips

Common Issue	Troubleshooting Tip
You receive error messages such as: <ul style="list-style-type: none"> <li>o DNS lookup failure</li> <li>o RPC server unavailable</li> <li>o Domain does not exist</li> <li>o Domain controller could not be found</li> </ul>	
User cannot be authenticated to access resources on another AD DS domain or Kerberos realm.	



# Module 4

## Implementing and administering AD DS sites and replication

### Contents:

Module Overview	4-1
<b>Lesson 1:</b> Overview of AD DS replication	4-2
<b>Lesson 2:</b> Configuring AD DS sites	4-10
<b>Lesson 3:</b> Configuring and monitoring AD DS replication	4-18
<b>Lab:</b> Implementing AD DS sites and replication	4-25
Module Review and Takeaways	4-31

## Module Overview

When you deploy Active Directory Domain Services (AD DS), it is important to provide an efficient sign-in infrastructure and a highly available directory service. Implementing multiple domain controllers throughout the infrastructure helps you achieve both of these goals. However, you must ensure that AD DS replicates Active Directory information between each domain controller in the forest.

In this module, you will learn how AD DS replicates information between domain controllers within a single site and throughout multiple sites. You also will learn how to create multiple sites and how to monitor replication to help optimize AD DS replication and authentication traffic.

### Objectives

After completing this module, you will be able to:

- Describe how AD DS replication works.
- Configure AD DS sites to help optimize authentication and replication traffic.
- Configure and monitor AD DS replication.

## Lesson 1

# Overview of AD DS replication

Within an AD DS infrastructure, standard domain controllers replicate Active Directory information by using a multiple master replication model. This means that if a change occurs on one domain controller, that change then replicates to all other domain controllers in the domain, and potentially to all domain controllers throughout the entire forest. This lesson provides an overview of how AD DS replicates information between standard domain controllers and also read-only domain controllers (RODCs).

### Lesson Objectives

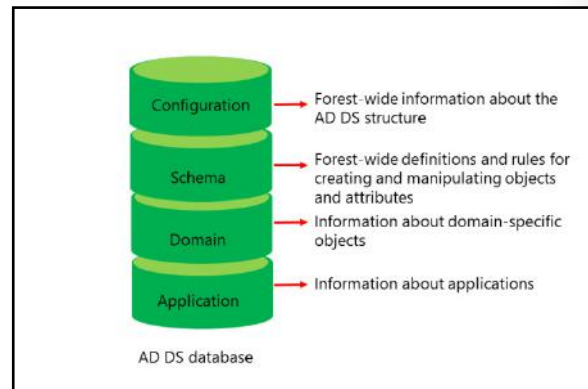
After completing this lesson, you will be able to:

- Describe AD DS partitions.
- Describe characteristics of AD DS replication.
- Explain how AD DS replication works within a site.
- Explain how to resolve replication conflicts.
- Explain how replication topology is generated.
- Explain how SYSVOL replication works.

### What are AD DS partitions?

The Active Directory data store contains information that AD DS distributes to all domain controllers throughout the forest infrastructure. Much of the information that the data store contains is distributed within a single domain. However, some information may be related to, and replicated throughout the entire forest, regardless of the domain boundaries.

To help provide replication efficiency and scalability between domain controllers, the Active Directory data is separated logically into several partitions. Each partition is a unit of replication, and each partition has its own replication topology. The default partitions include the following:



- **Configuration partition.** The configuration partition is created automatically when you create the first domain controller in a forest. The configuration partition contains information about the forest-wide AD DS structure, including which domains and sites exist and which domain controllers exist in each domain. The configuration partition also stores information about forest-wide services such as Dynamic Host Configuration Protocol (DHCP) authorization and certificate templates. This partition replicates to all domain controllers in the forest. It is smaller than the other partitions, and its objects do not change frequently; therefore, replication is also infrequent.
- **Schema partition.** The schema partition contains definitions of all the objects and attributes that you can create in the data store, and the rules for creating and manipulating them. Schema information replicates to all domain controllers in the forest. Therefore, all objects must comply with the schema object and attribute definition rules. AD DS contains a default set of classes and attributes that you cannot modify. However, if you have Schema Admins group credentials, you can extend the schema by adding new attributes and classes to represent application-specific classes. Many applications such

as Microsoft Exchange Server and Microsoft System Center Configuration Manager may extend the schema to provide application-specific configuration enhancements. These changes target the domain controller that contains the forest's schema master role. Only the schema master is permitted to make additions to classes and attributes. Similar to the configuration partition, the schema partition is small and needs to replicate only when changes occur to the data that is stored there, which does not happen frequently, except in those cases when the schema is extended.

- **Domain partition.** When you create a new domain, AD DS automatically creates and replicates an instance of the domain partition to all of the domain's domain controllers. The domain partition contains information about all domain-specific objects, including users, groups, computers, organizational units (OUs), and domain-related system settings. This is usually the largest of the AD DS partitions because it stores all the objects contained in the domain. Changes to this partition are fairly constant because every time an object is created, deleted, or modified by changing an attribute's value, those changes must then be replicated. All objects in every domain partition in a forest are stored in the global catalog with only a subset of their attribute values.
- **Application partition.** The application partition stores non-domain, application-related information that might tend to be updated frequently or have a specified lifetime, such as a Domain Name System (DNS) partition when Active Directory–integrated DNS is enabled. An application typically is programmed to determine how it stores, categorizes, and uses application-specific information that is stored in the Active Directory database. To prevent unnecessary replication of an application partition, you can designate which domain controllers in a forest will host the specific application's partition. Unlike a domain partition, an application partition does not store security principal objects, such as user accounts. Additionally, the global catalog does not store data that is contained in application partitions. The application partition's size and replication frequency can vary widely according to usage. Using Active Directory–integrated DNS with a large and robust DNS zone of many domain controllers, servers, and client computers will result in the frequent replication of the partition.



**Note:** You can use the Active Directory Services Interfaces Editor (ADSI Edit) to connect to the partitions and to view them.

## Characteristics of AD DS replication

An effective AD DS replication design ensures that each partition on a domain controller is consistent with the replicas of that partition that are hosted on other domain controllers. Typically, not all domain controllers have exactly the same information in their replicas at any particular moment because changes occur to the partition constantly. However, AD DS replication ensures that all changes to a partition are transferred to all replicas of the partition. AD DS replication balances accuracy (called *integrity*) and consistency (called *convergence*) with performance, thus keeping replication traffic to a reasonable level.

- Multi-master replication ensures:
  - Accuracy (*integrity*)
  - Consistency (*convergence*)
  - Performance (keeping replication traffic to a reasonable level)
- Key characteristics of AD DS replication include:
  - Multi-master replication
  - Pull replication
  - Store-and-forward replication
  - Partitions
  - Automatic generation of an efficient, robust replication topology
  - Attribute-level and multivalued replication
  - Distinct control of intersite replication
  - Collision detection and management

The key characteristics of AD DS replication are:

- Multiple master replication. Any domain controller except an RODC can initiate and commit a change to AD DS. This provides fault tolerance and eliminates dependency on a single domain controller to maintain the operations of the directory store.
- Pull replication. A domain controller requests, or *pulls*, changes from other domain controllers. Even though a domain controller can notify its replication partners that it has changes to the directory, or poll its partners to see if they have changes to the directory, in the end, the target domain controller requests and pulls the changes themselves.
- Store-and-forward replication. A domain controller can pull changes from one replication partner and then make those changes available to another replication 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. This helps balance the replication load for domains that contain several domain controllers.
- Data store partitioning. A domain's domain controllers host the domain-naming context for their domains, which helps minimize replication, particularly in multidomain forests. The domain controllers also host copies of schema and configuration partitions, which are replicated forest wide. However, changes in configuration and schema partitions are much less frequent than in the domain partition. By default, other data, including application directory partitions and the partial attribute set (the global catalog), do not replicate to every domain controller in the forest. You can enable replication to be universal by configuring all the domain controllers in a forest as global catalog servers.
- Automatic generation of an efficient and robust replication topology. By default, AD DS configures an effective, multidirectional replication topology so that the loss of one domain controller does not impede replication. AD DS automatically updates this topology as domain controllers are added, removed, or moved between sites.
- Attribute-level replication. When an object's attribute changes, only that attribute and minimal metadata describing that attribute replicates. The entire object does not replicate, except on its initial creation. For multivalued attributes, such as account names in the **Member of** attribute of a group account, only changes to actual names replicate, and not the entire list of names.
- Distinct control of intersite replication. You can control replication between sites.
- Collision detection and management. Although rare, within a single replication window, it is possible to modify an attribute on two different domain controllers, thereby creating a conflict. If this occurs, you must reconcile the two changes. AD DS has resolution algorithms that satisfy almost all scenarios.

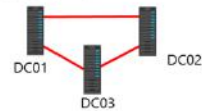
## How AD DS replication works within a site

AD DS replication within a single site, which takes place automatically, is called *intrasite replication*. However, you also can configure it to occur manually if applications in your environment require a more specific replication schedule. The following concepts relate to intrasite replication:

- Connection objects
- The Knowledge Consistency Checker
- Notification
- Polling

Intrasite replication uses:

- Connection objects for inbound replication to a domain controller
- Knowledge Consistency Checker to automatically create a topology that is efficient (maximum three-hop) and robust (two-way)
- Notifications in which the domain controller tells its downstream partners that a change is available
- Polling, in which the domain controller checks with its upstream partners for changes:
  - Downstream domain controller directory replication agent replicates changes
  - Changes to all partitions held by both domain controllers are replicated



### Connection objects

A domain controller that replicates changes from another domain controller is called a *replication partner*. Connection objects link replication partners. A connection object represents a replication path from one domain controller to another. Connection objects are one way, representing inbound-only pull replication.

To view and configure connection objects, open **Active Directory Sites and Services**, and then select the **NTDS Settings** container of a domain controller's server object. You can force replication between two domain controllers by right-clicking the connection object, and then selecting **Replicate Now**. Note that replication is inbound-only, so if you want to replicate both domain controllers, you need to replicate the inbound connection object of each domain controller.

### The Knowledge Consistency Checker

The replication paths that connection objects build between domain controllers create the forest's replication topology. You do not have to create the replication topology manually. By default, AD DS creates a topology that ensures effective replication. The topology is two-way, which means that if a domain controller fails, replication continues uninterrupted. The topology also ensures that no more than three network hops occur between any two domain controllers.

On each domain controller, a component of AD DS called the Knowledge Consistency Checker helps generate and optimize the replication automatically between domain controllers within a site. The Knowledge Consistency Checker evaluates the domain controllers in a site and then creates connection objects to build the two-way, three-hop topology that was described earlier. If you add or remove a domain controller, or if a domain controller is not responsive, the Knowledge Consistency Checker rearranges the topology dynamically, adding and deleting connection objects to rebuild an effective replication topology. The Knowledge Consistency Checker runs at specified intervals (every 15 minutes by default) and designates replication routes between domain controllers that are the most favorable connections available at the time.

You can manually create connection objects to specify replication paths that should persist. However, creating a connection object manually is not typically required or recommended because the Knowledge Consistency Checker does not verify or use the manual connection object for failover. The Knowledge Consistency Checker also will not remove manual connection objects, which means that you must remember to delete connection objects that you create manually.

## Notification

When a change occurs on an Active Directory partition on a domain controller, the domain controller queues the change for replication to its partners. By default, the source server waits 15 seconds to notify its first replication partner of the change. *Notification* is the process by which an upstream partner informs its downstream partners that a change is available. By default, the source domain controller then waits three seconds between notifications to additional partners. These delays, called the *initial notification delay* and the *subsequent notification delay*, are designed to stagger the network traffic that intrasite replication can cause.

After receiving the notification, the downstream partner requests the changes from the source domain controller, and the directory replication agent pulls the changes from the source domain controller. For example, suppose domain controller **DC01** initializes a change to AD DS. When **DC02** receives the change from **DC01**, it makes the change to its directory. **DC02** then queues the change for replication to its own downstream partners.

Next, suppose **DC03** is a downstream replication partner of **DC02**. After 15 seconds, **DC02** notifies **DC03** that it has a change. **DC03** makes the replicated change to its directory, and it then notifies its downstream partners. The change has made two hops, from **DC01** to **DC02**, and then from **DC02** to **DC03**. The replication topology ensures that no more than three hops occur before all domain controllers in the site receive the change. At approximately 15 seconds per hop, the change fully replicates in the site within one minute.

## Polling

Sometimes, a domain controller might not make any changes to its replicas for an extended time, particularly during off hours. Suppose this is the case with **DC01**. This means that **DC02**, its downstream replication partner, will not receive notifications from **DC01**. **DC01** also might be offline, which would prevent it from sending notifications to **DC02**.

It is important for **DC02** to know that its upstream partner is online and simply does not have any changes. This occurs through a process called *polling*. During polling, the downstream replication partner contacts the upstream replication partner with queries as to whether any changes are queued for replication. By default, the polling interval for intrasite replication is once per hour. You can configure the polling frequency from a connection object's properties by clicking **Change Schedule**, although we do not recommend it.

If an upstream partner fails to respond to repeated polling queries, the downstream partner launches the Knowledge Consistency Checker to check the replication topology. If the upstream server is indeed offline, the Knowledge Consistency Checker rearranges the site's replication topology to accommodate the change.

**Question:** Describe the circumstances that result when you manually create a connection object between domain controllers within a site.

## Resolving replication conflicts

Because AD DS supports a multiple master replication model, replication conflicts might occur. Typically, three types of replication conflicts might occur in AD DS:

- Simultaneously modifying the same attribute value of the same object on two domain controllers.
- Adding or modifying the same object on one domain controller at the same time that the container object for the object is deleted on another domain controller.
- Adding objects with the same relative distinguished name into the same container on different domain controllers at the same time.

- In multi-master replication models, replication conflicts arise when:
  - The same attribute is changed on two domain controllers simultaneously
  - An object is moved or added to a deleted container on another domain controller
  - Two objects with the same relative distinguished name are added to the same container on two different domain controllers
- To resolve replication conflicts, AD DS uses:
  - Version number
  - Time stamp
  - Server GUID

To help minimize conflicts, all domain controllers in the forest record and replicate object changes at the attribute or value level rather than at the object level. Therefore, changes to two different object attributes, such as the user’s password and postal code, do not cause a conflict even if you change them at the same time from different locations.

When an originating update is applied to a domain controller, a stamp is created that travels with the update as it replicates to other domain controllers. The stamp contains the following components:

- Version number. The version number starts at one for each object attribute, and increases by one for each update. When performing an originating update, the version of the updated attribute is one number higher than the version of the attribute that is being overwritten.
- Timestamp. The timestamp is the update’s originating time and date in the universal time zone, according to the system clock of the domain controller where the change occurs.
- Server globally unique identifier (GUID). The server GUID identifies the domain controller that performed the originating update.

### Common replication conflicts

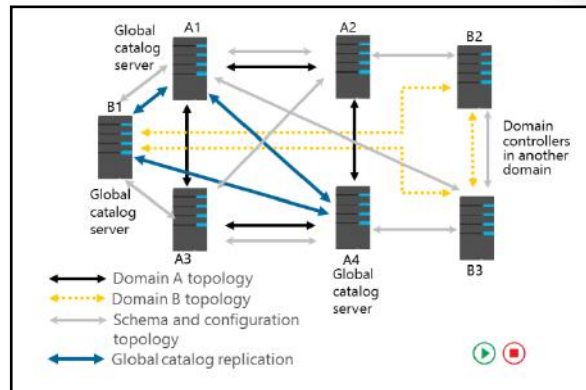
The following table outlines several conflicts, and it describes how AD DS resolves these issues.

Conflict	Resolution
Attribute value	If the version number value is the same but the attribute value differs, then the timestamp is evaluated. The update operation that has the higher stamp value replaces the attribute value of the update operation with the lower stamp value. Certain multivalue attributes can be updated, such as a value in a group’s <b>Member of</b> attribute, and will be processed as separate replicable events.
Add or move under a deleted container object, or the deletion of a container object	After resolution occurs at all replicas, AD DS deletes the container object, and the leaf object is made a child of the <b>LostAndFound</b> container. Stamps are not involved in this resolution.
Adding objects with the same relative distinguished name	The object with the later stamp keeps the relative distinguished name. AD DS assigns the sibling object a unique relative distinguished name by the domain controller. The name assignment is the relative distinguished name + CNF: + a reserved character (the asterisk,) + the object’s GUID. This name assignment ensures that the generated name does not conflict with any other object’s name.

MCT USE ONLY. STUDENT USE PROHIBITED

## How replication topology is generated

*Replication topology* is the route by which replication data travels through a network. To create a replication topology, AD DS must determine which domain controllers replicate data with other domain controllers. AD DS creates a replication topology based on the information that AD DS contains. Because each AD DS partition might be replicated to different domain controllers in a site, the replication topology can differ for schema, configuration, domain, and application partitions.



Because all domain controllers within a forest share schema and configuration partitions, AD DS replicates schema and configuration partitions to all domain controllers. Domain controllers in the same domain also replicate the domain partition. Additionally, domain controllers that host an application partition also replicate the application partition. To optimize replication traffic, a domain controller might have several replication partners for different partitions. In a single site, the replication topology will be fault-tolerant and redundant. This means that if the site contains more than two domain controllers, each domain controller will have at least two replication partners for each AD DS partition.

### How the schema and configuration partitions are replicated

Schema and configuration partition replication follows the same process as all other directory partitions. However, because these partitions are forest-wide rather than domain-wide, connection objects for these partitions might exist between any two domain controllers regardless of the domain controller's domain. Furthermore, the replication topology for these partitions includes all domain controllers in the forest.

### How the global catalog affects replication

The configuration partition contains information about the site topology and other global data for all domains that are members of the forest. AD DS replicates the configuration partition to all domain controllers through normal forest-wide replication. Each global catalog server obtains domain information by contacting a domain controller for that domain and obtaining the partial replica information. Each global catalog server has full access to its own domain's domain partition, and therefore, does not have to request a partial replication set of this information. The configuration partition also provides domain controllers with a list of the forest's global catalog servers.

Global catalog servers register DNS service records in the DNS zone that corresponds to the forest root domain. These records, which are registered only in the forest root DNS zone, help clients and servers locate global catalog servers throughout the forest to provide client logon services.




## How SYSVOL replication works

SYSVOL is a collection of files and folders on each domain controller that is linked to the %SystemRoot%\SYSVOL location. SYSVOL contains logon scripts and objects that relate to Group Policy, such as Group Policy templates. The contents of the SYSVOL folder replicate to every domain controller in the domain using the connection object topology and schedule that the Knowledge Consistency Checker creates.

Depending on the domain controller operating system version, the domain's functional level, and the migration status of SYSVOL, file replication

service (FRS) or Distributed File System (DFS) Replication replicates SYSVOL changes between domain controllers. FRS was used primarily in Windows Server 2003 R2 and older domain structures. FRS has limitations in both capacity and performance, which has led to the adoption of DFS Replication. FRS is no longer available on domain controllers that are running Windows Server 2012 R2 and later when the domain is at the Windows Server 2012 R2 domain functional level or higher. If the forest functional level is Windows Server 2008 R2 or newer, DFS Replication is used.

In Windows Server 2008 and newer domains, you can use DFS Replication to replicate the contents of SYSVOL. DFS Replication supports replication scheduling and bandwidth throttling, and it uses a compression algorithm known as remote differential compression (RDC). By using RDC, DFS Replication replicates only the differences or changes within files between the two servers, resulting in lower bandwidth usage during replication. If any file that is stored in SYSVOL changes, DFS Replication will automatically replicate the file changes to the SYSVOL folders on the other domain controllers in the domain.

 **Note:** You can use the **Dfsrmig.exe** tool to migrate SYSVOL replication from FRS to DFS Replication. For the migration to succeed, the domain functional level must be at least Windows Server 2008.

- SYSVOL contains logon scripts, Group Policy templates, and GPOs with their content
- SYSVOL replication can take place by using:
  - FRS, which is primarily used in Windows Server 2003 and older domain structures
  - DFS Replication, which is used in Windows Server 2008 and newer domains
- To migrate SYSVOL replication from FRS to DFS Replication:
  - The domain functional level must be at least Windows Server 2008
  - Use the **Dfsrmig.exe** tool to perform the migration

**Question:** Why is replication important to the global catalog?

## Lesson 2

# Configuring AD DS sites

Within a single site, AD DS replication occurs automatically without regard for network utilization. However, some organizations have multiple locations that are connected by wide area networks (WANs). If this is the case, you must ensure that AD DS replication does not affect network utilization negatively between locations. You also might need to localize network services to a specific location. For example, you might want users at a branch office to authenticate to a domain controller in their local office rather than over the WAN connection to a domain controller in the main office. You can implement AD DS sites to help manage bandwidth over slow or unreliable network connections and to assist in service localization for authentication and many other site-aware services on the network.

### Lesson Objectives

After completing this lesson, you will be able to:

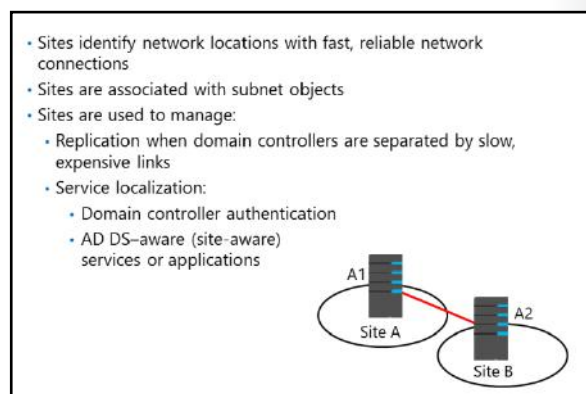
- Describe AD DS sites.
- Explain why organizations might implement additional sites.
- Configure additional AD DS sites.
- Describe how AD DS replication works between sites.
- Describe the intersite topology generator (ISTG).
- Describe service (SRV) resource records.
- Describe how client computers locate domain controllers within sites.
- Explain how to move domain controllers between sites.

### What are AD DS sites?

To most administrators, a site is a physical location such as an office or a city that is typically separated by a WAN connection. These sites connect physically by network links that can vary in available bandwidth. Together, the physical locations and links make up the physical network infrastructure.

AD DS represents the physical network infrastructure with objects called *sites*. AD DS site objects are stored in the **Configuration** container (CN=Sites, CN=Configuration, DC=*forest root domain*) and are used to achieve three primary service management tasks:

- Manage replication traffic. 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. However, you can manage and schedule replication between sites as needed. Typically, there are two types of network connections within an enterprise environment: highly connected and less highly connected. Conceptually, a change made to AD DS should replicate immediately to other domain controllers within the highly connected network in which the change occurred. However, you might not want the change to replicate to another site immediately if you have a slower, more




expensive, or less reliable link. Instead, you might want to optimize performance, reduce costs, and manage bandwidth by managing replication over less highly connected segments of your enterprise.

- Provide service localization. Active Directory sites help you localize services, including those that domain controllers provide. During sign-in, Windows clients are directed automatically to domain controllers in their sites. If domain controllers are not available in their sites, then they are directed to domain controllers in the nearest site that can authenticate the client efficiently. Many other services such as replicated DFS resources are also site-aware, to ensure that users are directed to a local copy of the resource.
- Group Policy Objects (GPOs) can be linked to a site. In that case, the site represents the top of the AD DS GPO hierarchy, and the AD DS GPO settings are applied here first.

### What are subnet objects?

*Subnet objects* identify the network addresses that map computers to AD DS sites. A *subnet* is a segment of a TCP/IP network to which a set of logical IP addresses are assigned. Because subnet objects map to the physical network, so do the sites. A site can consist of one or more subnets. For example, if your network has three subnets in New York and two in London, you can create a site in New York and one in London, respectively, and then add the subnets to the respective sites.

 **Note:** When you design your AD DS site configuration, it is critical that you correctly map IP subnets to sites. Likewise, if the underlying network configuration changes, you must ensure that these changes are updated to reflect the current IP subnet to site mapping. Domain controllers use the IP subnet information in AD DS to map client computers and servers to the correct AD DS site. If this mapping is not accurate, AD DS operations such as sign-in traffic and Group Policy application are likely to occur across WAN links, and may get disrupted.

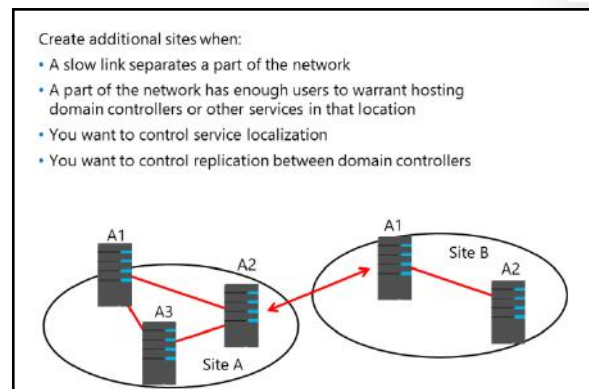
### Default first site

AD DS creates a default site when you install a forest's first domain controller. By default, this site is named **Default-First-Site-Name**. You can rename this site to a more descriptive name. When you install the forest's first domain controller, AD DS automatically places it in the default site. If you have a single site, it is not necessary to configure subnets or additional sites, because all machines will be covered by the **Default-First-Site-Name** default site. However, multiple sites should have subnets associated with them as needed.

### Why implement additional sites?

Every Active Directory forest includes at least one site. You should create additional sites when:

- A slow link separates part of the network. As previously mentioned, a site is characterized by a location with fast, reliable, inexpensive connectivity. If two locations are connected by a slow link, you should configure each location as a separate AD DS site. A slow link typically is one that has a connection of less than 512 kilobits per second (Kbps).



- A part of the network has enough users to warrant hosting domain controllers or other services in that location. Concentrations of users also can influence your site design. 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 you place a domain controller or other distributed service in a location that will support those users, you might want to manage AD DS replication to the location or localize service use by configuring an Active Directory site to represent the location.

- You want to control service localization. By establishing AD DS sites, you can ensure that clients use domain controllers that are nearest to them for authentication, which reduces authentication latency and traffic on WAN connections. In most scenarios, each site will contain a domain controller. However, you might configure sites to localize services other than authentication, such as DFS, Windows BranchCache, and Exchange Server services. In this case, some sites might be configured without a domain controller.
- You want to control replication between domain controllers. Scenarios might exist in which two well-connected domain controllers are allowed to communicate only at certain times of the day. Creating sites allows you to control how and when replication takes place between domain controllers.

## Demonstration: Configuring AD DS sites

In this demonstration, you will see how to configure AD DS sites.

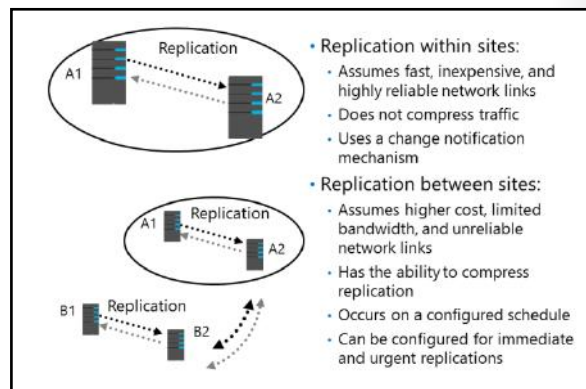
### Demonstration Steps

1. On **LON-DC1**, from **Server Manager**, open **Active Directory Sites and Services**.
2. Rename the **Default-First-Site-Name** site to **LondonHQ**.
3. Right-click the **Sites** node, and then click **New Site**. Specify the name **Toronto**, and then associate the new site with the default site link.
4. Create additional sites as needed.
5. In the navigation pane, right-click **Subnets**, and then click **New Subnet**.
6. Provide the prefix **172.16.0.0/24**, and then associate the IP prefix to an available site object.
7. If required, move a domain controller to the new site.

## How replication works between sites

The main characteristics of replication within a site are as follows:

- The network connections within a site are reliable and have sufficient available bandwidth.
- Replication traffic within a site is not compressed, because a site assumes fast, highly reliable network connections. Not compressing replication traffic helps reduce the processing load on domain controllers. However, uncompressed traffic might increase network bandwidth.



The main characteristics of replication between sites are as follows:


- The network links between sites have limited available bandwidth, might have a higher cost, and might not be reliable.
- Replication traffic between sites can be designed to optimize bandwidth by compressing all replication traffic. Replication traffic is compressed to 10 percent to 15 percent of its original size before it transmits. Although compression optimizes network bandwidth, it imposes an additional processing load on domain controllers when it compresses and decompresses replication data.
- Replication between sites occurs automatically after you define configurable values such as a schedule or a replication interval. You can schedule replication for inexpensive or off-peak hours. By default, changes replicate between sites according to a schedule that you define, and not according to when changes occur. The interval specifies how often domain controllers check for changes during the time that replication can occur.

### Change notifications between AD DS sites

By design, changes in AD DS sites replicate between domain controllers in different sites according to a defined replication schedule, and not according to when changes occur, such as with intrasite replication. Because of this, the replication latency in the forest can equal the sum of the greatest replication latencies along the longest replication path of any directory partition. In some scenarios, this can be inefficient.

To avoid replication latency, you can configure change notifications on connections between sites. By modifying the site link object, you can enable change notification between sites for all connections that occur over that link. Because the replication partner across the site receives notification of changes, the intersite replication interval is effectively ignored. The originating domain controller notifies the domain controller in the other site that it has a change, just as it does within a single site.

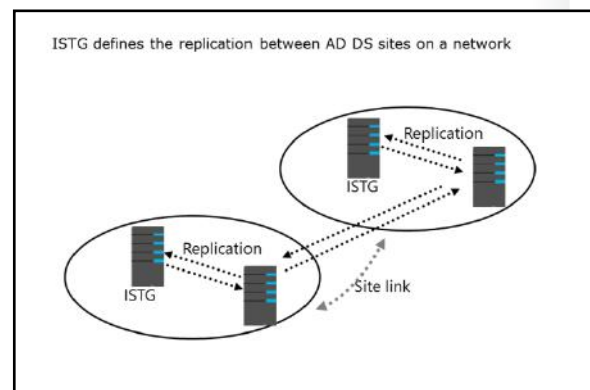
For changes such as account lockout or similar security-related changes, immediate replication is crucial. In these situations, *urgent replication* is used. *Urgent replication* bypasses the notification delay and processes change notifications immediately. This only affects change notifications. If you do not have change notifications enabled between sites, replication still honors the replication interval on the site link.

 **Note:** When a user's password changes, immediate replication is initiated to the primary domain controller emulator operations master. This differs from urgent replication because it occurs immediately, without regard for the intersite replication interval.

### What is the ISTG?

When you configure multiple sites, the Knowledge Consistency Checker on one domain controller in each site is designated as the site's ISTG. There is only one ISTG per site, regardless of how many domains or other directory partitions the site includes. ISTG is responsible for calculating the site's ideal replication topology across site links.

When you add a new site to the forest, each site's ISTG determines which directory partitions are present in the new site. The ISTG then calculates how many new connection objects are necessary to replicate the new site's required information.



## Bridgehead servers

In some networks, you might want to specify that only certain domain controllers are responsible for intersite replication. You can do this by specifying bridgehead servers. Bridgehead servers are responsible for all replication into and out of the site. ISTG creates the required connection agreement in its directory, and this information is then replicated to the bridgehead server. The bridgehead server then creates a replication connection with the bridgehead server in the remote site, and replication begins. If a replication partner becomes unavailable, the ISTG selects another domain controller automatically, if possible. If bridgehead servers were assigned manually, and if they become unavailable, ISTG will not automatically select other servers.

### Selecting bridgehead servers

The ISTG selects bridgehead servers automatically and creates the intersite replication topology to ensure that changes replicate effectively between bridgehead servers that share a site link. Bridgehead servers are selected per partition, so it is possible that one domain controller in a site might be the bridgehead server for the schema, while another is for the configuration. However, you usually will 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 this scenario, bridgehead servers will be chosen for those partitions. Designated bridgehead servers are also useful when you have firewalls between sites that only allow replication between specific domain controllers.

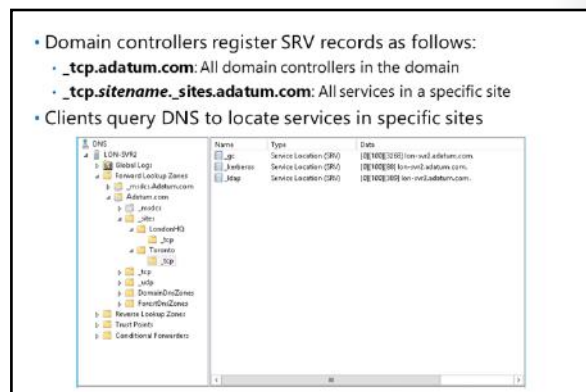
## Overview of SRV records

When you add a domain controller to a domain, the domain controller advertises its services by creating service (SRV) resource records (also known as *locator records*) in DNS. Unlike host (A) resource records, which map host names to IP addresses, SRV records map services to host names. For example, to publish its ability to provide authentication and directory access, a domain controller registers Kerberos version 5 protocol and Lightweight Directory Access Protocol (LDAP) SRV records. These SRV records are added to several folders within the forest's DNS zones.

Within the domain zone, a folder named **\_tcp** contains the SRV records for all domain controllers in the domain. Additionally, within the domain zone is a folder named **\_sites**, which contains subfolders for each site that is configured in the domain. Each site-specific folder contains SRV records that represent services that are available in the site. For example, if a domain controller is located in a site, a SRV record will be located at the path **\_sites\sitename\\_tcp**, where **sitename** is the name of the site.

A typical SRV record contains the following information:

- 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 include LDAP (port 389), Kerberos (port 88), Kerberos V5 authentication protocol (KPASSWD, port 464), and global catalog services (port 3268).
- Protocol. The Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) is 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 both UDP and TCP.



- Host name. The host name corresponds to the host (A) resource record for the server that hosts the service. When a client queries for a service, the DNS server returns the SRV record and associated host (A) resource records, so the client does not need to submit a separate query to resolve the service's IP address.

The service name in a SRV record follows the standard DNS hierarchy with components separated by dots. For example, a domain controller's Kerberos service is registered as:

**kerberos.\_tcp.sitename.\_sites.domainName**, where:

- Kerberos is a Kerberos Key Distribution Center that uses TCP as its transport protocol.
- **\_tcp** is any TCP-based services in the site.
- **sitename** is the site of the domain controller that is registering the service.
- **\_sites** is all sites that are registered with DNS.
- **domainName** is the domain or zone, for example, **contoso.com**.

## How client computers locate domain controllers within sites

When you join a Windows client operating system to a domain and then restart it, the client completes a domain controller location and registration process. The goal of this registration process is to locate the domain controller with the most efficient and closest location to the client's location based on IP subnet information.

The process for locating a domain controller is as follows:

1. The new client queries for all domain controllers in the domain. As the new domain client restarts, it receives an IP address from a DHCP server, and is ready to authenticate to the domain. However, the client does not know where to find a domain controller. Therefore, the client queries for a domain controller by querying the **\_tcp** folder, which contains the SRV records for all domain controllers in the domain.
2. The client attempts an LDAP ping to all domain controllers in a sequence. DNS returns a list of all matching domain controllers, and the client attempts to contact all of them on its first startup.
3. The first domain controller responds. 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 and then queries for domain controllers in the site-specific **\_tcp** folder.
4. The client queries for all domain controllers in the site. DNS returns a list of all domain controllers in the site.
5. The client attempts an LDAP ping sequentially to all domain controllers in the site. The domain controller that responds first authenticates the client.
6. The client forms an affinity. The client forms an affinity with the domain controller that responded first, and then attempts to authenticate with the same domain controller in the future. If the domain controller is unavailable, the client queries the site's **\_tcp** folder again, and again attempts to bind with the first domain controller that responds in the site.

The process for locating a domain controller is as follows:


1. The new client queries for all domain controllers in the domain
2. The client attempts an LDAP ping to find all domain controllers
3. First domain controller responds
4. The client queries for all domain controllers in the site
5. The client attempts an LDAP ping to find all domain controllers in the site
6. The client forms an affinity

If the client moves to another site, which might be the case with a mobile computer, the client attempts to authenticate to its preferred domain controller. The domain controller notices that the client's IP address is associated with a different site, and it then refers the client to the new site. The client then queries DNS for domain controllers in the local site.

### Automatic site coverage

You can configure sites to direct users to local copies of replicated resources, such as shared folders replicated within a DFS namespace. There might be scenarios in which you require only service localization with no need for a domain controller located within the site. In this case, a nearby domain controller will register its SRV records in the site by using a process called *site coverage*.

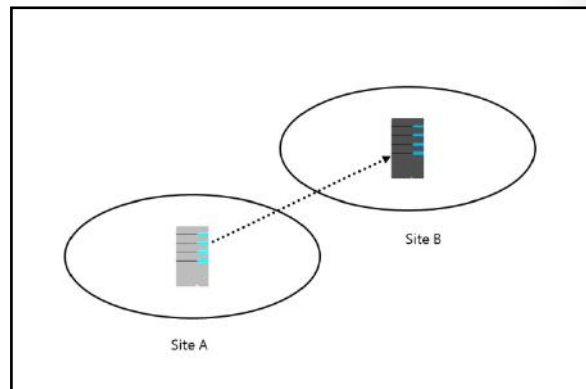
A site without a domain controller generally is covered by a domain controller in a site with the lowest site link cost to the site that requires coverage. You also can configure site coverage and SRV record priority manually if you want to control authentication in sites without domain controllers.

 **Additional Reading:** For more information, refer to: "Finding a Domain Controller in the Closest Site" at: <http://aka.ms/Cjzdd>

### Moving domain controllers between sites

You can move domain controllers between sites if required. To move a domain controller, perform the following steps using an account with domain admin privileges:

1. Relocate the domain controller to the new site.
2. On another domain controller in the same domain, open **Active Directory Sites and Services**.
3. Expand the site that contains the domain controller you want to move.
4. Right-click on the domain controller you want to move, and then click **Move**.
5. Choose the new site from the list.



In certain situations, an organization might have computers in a location that does not have domain controllers, or where having domain controllers is undesirable. You can create sites without domain controllers; however, as noted above, the site would not have a corresponding domain controller listing in the `_sites\sitename\_tcp` path. In this case, several potential solutions exist:

- Deploy RODCs. If maintenance of the domain controller and security of the AD DS database that it contains are the main concerns, you could deploy RODCs.
- Use automatic site coverage. In the case of an empty site, a domain controller from the next closest site will automatically decide to take care of that site and also register its records for that site. You can adjust or force this by using Group Policy.
- Add the subnet to an existing site. If the site is well connected with only a few computers, you might want to avoid the cost of maintaining a server there. In this case, you could add the local subnet of the site to a central location or to a datacenter site location with multiple domain controllers.



In the SRV record section example in the “Overview of SRV records” topic, the client computers at the remote location without a domain controller would be identified as belonging to the central site. This would be a problem only if the central site’s domain controllers were not available. In this case, the clients could use cached credentials to authenticate locally. Because automatic site link bridging, which the next lesson will discuss, is turned on by default, domain authentication could still take place over the site link bridge where multiple sites exist.

### Check Your Knowledge

Question	
Which of the following is not a consideration for implementing AD DS sites?	
Select the correct answer.	
<input type="checkbox"/>	Reducing bandwidth usage between network locations
<input type="checkbox"/>	Applying Group Policy settings to a single location in your organization
<input type="checkbox"/>	Controlling which domain controller client computers use for authentication
<input type="checkbox"/>	Creating a backup site for disaster recovery
<input type="checkbox"/>	Controlling access to apps and services for a certain segment of your network

## Lesson 3

# Configuring and monitoring AD DS replication

After you configure the sites that represent your network infrastructure, the next step is to determine if any additional site links are necessary to help manage AD DS replication. AD DS provides several options that you can configure to control how replication occurs over site links. You also need to understand the tools that you can use to monitor and manage replication in an AD DS network environment.

### Lesson Objectives

After completing this lesson, you will be able to:

- Describe AD DS site links.
- Explain the concept of site link bridging.
- Describe universal group membership caching.
- Describe how to manage intersite replication.
- Configure AD DS intersite replication.
- Describe the tools for monitoring and managing replication.

### What are AD DS site links?

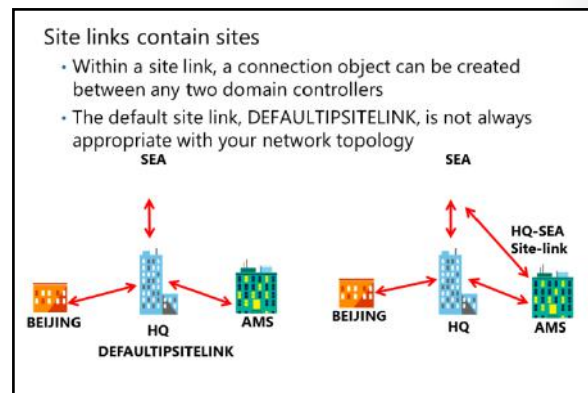
For two sites to exchange replication data, a site link must connect them. A *site link* is a logical path that the Knowledge Consistency Checker and ISTG use to establish replication between sites. When you create additional sites, you must select at least one site link that will connect the new site to an existing site. Unless a site link is in place, the Knowledge Consistency Checker cannot make connections between computers at different sites, nor can replication occur between sites.

### Controlling replication paths with site links

It is important to remember that a site link 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 tell AD DS that it can replicate between any of the sites that are associated with the site link. The ISTG creates connection objects, and those objects will determine the actual replication path. Although the replication topology that the ISTG builds does replicate AD DS effectively, it might not be efficient with your network topology.

To understand this concept better, consider the following example. When you create a forest, one site link object is created: **DEFAULTIPSITELINK**. By default, each new site that you add is associated with **DEFAULTIPSITELINK**. **DEFAULTIPSITELINK** and any other existing site links have a default cost of 100 and a default replication period of 180 minutes.

Consider the example of an organization with three branch offices and a datacenter at the headquarters. The three branch offices each connect to the datacenter with a dedicated link. You create sites for each branch office: Seattle (**SEA**), Amsterdam (**AMS**), and **Beijing**. Each of the sites, including headquarters, is associated with the **DEFAULTIPSITELINK** site link object.



Because all four sites are on the same site link, you are instructing AD DS that all four sites can replicate with each other. That means that Seattle might replicate changes from Amsterdam; Amsterdam might replicate changes from Beijing; and Beijing might replicate changes from the headquarters, which in turn replicates changes from Seattle. In several of these replication paths, replication traffic on the network flows through the headquarters on its way from one branch to another. With a single site link, you do not create a hub-and-spoke replication topology even though your network topology is hub-and-spoke.

To align your network topology with AD DS replication, you must create specific site links. That is, you can manually create site links that reflect your intended replication topology. Continuing the preceding example, you would create three site links as follows:

- **HQ-AMS** includes the headquarters and Amsterdam sites.
- **HQ-SEA** includes the headquarters and Seattle sites.
- **HQ-Beijing** includes the headquarters and Beijing sites.

After you create site links, the ISTG will use the topology to build an intersite replication topology that connects each site, and then create connection objects automatically to configure the replication paths. As a best practice, you should set up your site topology correctly and avoid creating connection objects manually.

## What is site link bridging?

After you create site links and the ISTG generates connection objects to replicate partitions between domain controllers 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 replication properties.

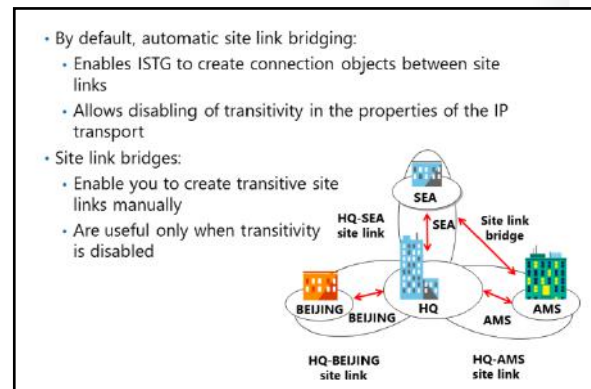
### Automatic site link bridging

By default, all site links are bridged. For example, if the Amsterdam and headquarters sites are linked, and if the headquarters and Seattle sites are linked, then Amsterdam and Seattle are linked with a combined cost. Theoretically, this means that the ISTG could create a connection object directly between a domain controller in Seattle and a domain controller in Amsterdam, if a domain controller were not available at the headquarters for replication. This occurs by working around the hub-and-spoke network topology.

You can disable automatic site link bridging by opening the properties of the IP transport in the **Intersite Transports** container and then clearing the **Bridge All Site Links** check box.

### 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** check box for the transport protocol. Remember that automatic site link bridging is enabled by default, which means that site link bridges are not required. However, you can keep automatic site link bridging enabled for the majority of sites, but also configure a site link bridge with in-between costs. For example, suppose you have many sites, but branches A and B are both directly connected to the corporate headquarters with the default cost of 100. The corporate headquarters has a backup datacenter, **HQ-HA**, which is also connected with a cost of 100

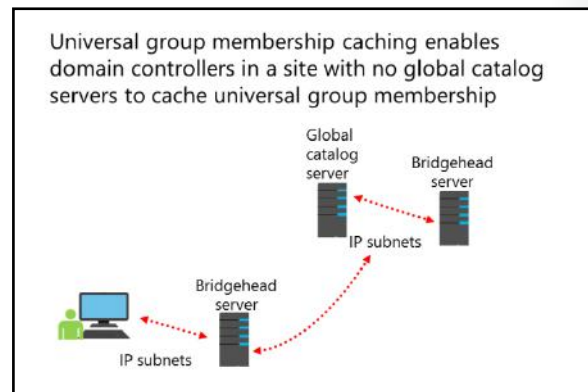


between the corporate headquarters and the site A and site B locations. In the event that not all domain controllers are available in **HQ-HA**, you want to ensure that site A can go to site B. This enables you to keep site link bridging on but to configure a site link bridge with a cost of 150 for site A to site B. This is greater than the cost of 100 for either site to **HQ-HA**, but less than the cost without the site link bridge. That cost would be 200—100 from Site A to HQ-HA, plus the cost of 100 to HQ-HA to Site B. This makes the site link bridge cost of 150 an in-between cost.

The figure on the slide illustrates how you can use a site link bridge in a forest in which automatic site link bridging is disabled. By creating the site link bridge **AMS-HQ-SEA**, which includes the **HQ-AMS** and **HQ-SEA** site links, those two site links become *transitive*, or bridged. Therefore, a replication connection can be made between a domain controller in Amsterdam and a domain controller in Seattle.

## What is universal group membership caching?

One issue that you might need to address when you configure AD DS replication is whether to deploy global catalog servers in each site. Because global catalog servers are required when users sign in to the domain, deploying a global catalog server in each site optimizes the user experience. However, if you deploy a global catalog server in a site, additional replication traffic might occur. That could be an issue if the network connection between AD DS sites has limited bandwidth and there are other domains with a large number of objects in the forest. In these scenarios, you can deploy domain controllers that are running Windows Server 2008 or newer and then enable universal group membership caching for the site.



## How universal group membership caching works

A domain controller in a site that has enabled universal group membership caching stores the universal group information locally after a user attempts to sign in for the first time. The domain controller obtains the user's universal group membership information from a global catalog server in another site. It then caches the information indefinitely and periodically refreshes it. The next time the user tries to sign in, the domain controller obtains the universal group membership information from its local cache without contacting a global catalog server.

By default, the universal group membership information in each domain controller's cache refreshes every eight hours. To refresh the cache, domain controllers send a universal group membership confirmation request to a designated global catalog server.

You can configure universal group membership caching from the **NTDS Site Settings** node settings.

## Managing intersite replication

When you create a site link, you can use several configuration options to help manage intersite replication. These options include:

- Site link costs. Site link costs manage the flow of replication traffic when more than one route for replication traffic exists. You can configure site link costs to indicate that a particular link meets one or more requirements or conditions; for example, it might be faster or more reliable, or it might be preferred. Slow links have higher costs, and fast links have lower costs. AD DS replicates by using the connection with the lowest cost. By default, all site links are configured with a cost of 100.
- Replication frequency. Intersite replication is based only on polling. By default, every three hours a replication partner polls its upstream replication partners to determine whether changes are available. This replication interval might be too long for organizations that want directory changes to replicate more quickly. You can change the polling interval by accessing the properties of the site link object. The minimum polling interval is 15 minutes.
- 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.

- Site link costs:
  - Replication uses connections with the lowest cost
- Replication:
  - During polling, the downstream bridgehead polls its upstream partners
    - Default is 3 hours
    - Minimum is 15 minutes
    - Recommended is 15 minutes
  - Replication schedules:
    - 24 hours a day
    - Can be scheduled



## Demonstration: Configuring AD DS intersite replication

In this demonstration, you will see how to configure AD DS intersite replication.

### Demonstration Steps

1. From **Server Manager**, open **Active Directory Sites and Services**.
2. Rename the **DEFAULTIPSITELINK** to **LON-TOR**.
3. Right-click the site link, and then click **Properties**.
4. Modify the cost, replication interval, and schedule as needed.
5. If necessary, open the properties of the **IP** node, and then modify the **Bridge all site links** option.

## Tools for monitoring and managing replication

After you implement 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 the Domain Controller Diagnostics Tool (**Dcdiag.exe**).

**Repadmin.exe** is a command-line tool that enables you to report the status of replication on each domain controller. The information that **Repadmin.exe** produces can help you spot a potential replication problem 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 AD DS. You can even use **Repadmin.exe** to create the replication topology and force replication between domain controllers.

**Repadmin.exe** supports a number of commands that perform specific tasks. You can learn about each command by typing **repadmin /?:command** at a command prompt. Most commands require arguments. Many commands take a **DC\_LIST** parameter, which is simply a network label (DNS, NetBIOS name, or IP address) of a domain controller. Some of the replication monitoring tasks that you can perform by using **Repadmin.exe** include:

- Displaying the replication partners for a domain controller. To display the replication connections of a domain controller, type **repadmin /showrepl DC\_LIST**. By default, **Repadmin.exe** shows intersite connections only. Add the **/repsto** argument also to see intersite connections.
- Displaying connection objects for a domain controller. Type **repadmin /showconn DC\_LIST** to show the connection objects for a domain controller.
- Displaying metadata about an object, its attributes, and replication. You can learn much about replication by examining an object on two different domain controllers to find out which attributes have or have not replicated. Type **repadmin /showobjmeta DC\_LIST Object**, where **DC\_LIST** indicates the domain controller or controllers to query. You can use an asterisk to indicate all domain controllers. **Object** is a unique identifier for the object—its distinguished name or GUID, for example.

You can also make changes to your replication infrastructure by using the **Repadmin.exe** tool. Some of the management tasks that you can perform include:

- Launching the Knowledge Consistency Checker. Type **repadmin /kcc** to force the Knowledge Consistency Checker to recalculate the inbound replication topology for the server.
- Forcing replication between two partners. You can use **Repadmin.exe** to force replication of a partition between a source and a target domain controller. Type **repadmin /replicate Destination\_DC\_LIST Source\_DC\_Name Naming\_Context**.
- Synchronizing a domain controller with all replication partners. Type **repadmin /syncall DC/A /e** to synchronize a domain controller with all its partners, including those in other sites.

**Dcdiag.exe** performs a number of tests and reports on the overall health of replication and security for AD DS. Run by itself, **Dcdiag.exe** performs summary tests and then reports the results. At the other extreme, **Dcdiag.exe /c** performs almost every test. The tests' output can be redirected to files of various types, including XML. Type **dcdiag /?** for full usage information.

• **Repadmin.exe** examples:

- **repadmin /showrepl Lon-dc1.adatum.com**
- **repadmin /showconn Lon-dc1.adatum.com**
- **repadmin /showobjmeta Lon-dc1 "cn=Linda Miller,ou=..."**
- **repadmin /kcc**

• **Dcdiag.exe /test:testName:**

- FrsEvent or DFSREvent
- Intersite
- KccEvent
- Replications
- Topology

• Monitor replication with Operations Manager

• Windows PowerShell

You also can specify one or more tests to perform by using the **/test:Test Name** parameter. Tests that are directly related to replication include:

- **FrsEvent.** This reports any operation errors in FRS.
- **DFSREvent.** This reports any operation errors in the DFS Replication system.
- **Intersite.** This checks for failures that would prevent or delay intersite replication.
- **KccEvent.** This identifies errors in the Knowledge Consistency Checker.
- **Replications.** This checks for timely replication between domain controllers.
- **Topology.** This checks that the replication topology is connected fully for all domain controllers.
- **VerifyReplicas.** This verifies that all application directory partitions are instantiated fully on all domain controllers that host replicas.

### Monitoring replication with Microsoft System Center Operations Manager

You can install the Active Directory Domain Services Management Pack for Operations Manager on the domain controller. This management pack contains many alerts, views, tasks, and reports for a variety of AD DS functions, including replication.

The **replication monitoring** section collects replication performance data to include AD DS replication alerts, intersite replication, replication latency, and both inbound and outbound replication traffic bytes per second. The management pack also contains several replication topology diagrams that cover site links, connection objects and broken connection objects. It also contains reports on replication connection objects, replication site links, replication bandwidth, and replication latency.

Operations Manager monitors four primary replication areas as part of the management pack:

- **Operations master consistency check.** This critical part of replication allows replication partners to agree on which domain controllers are in an operations master role.
- **Replication latency monitoring.** This ensures that AD DS changes replicate in a timely manner, and this can periodically send replication events of its own to ensure that all replication partners are functioning properly.
- **Replication partner count.** This keeps track of how many replication partners a domain controller has. If the number is either below or above a particular threshold, it will trigger an alert.
- **Replication provider.** This monitors and reports on all replication links for each domain controller. You use Windows Management Instrumentation to find link status.

### New Windows PowerShell cmdlets for AD DS replication

Windows Server 2016 supports several Windows PowerShell cmdlets to create, configure, and monitor AD DS replication. The following table describes some of these cmdlets.

Cmdlet	Data returned
<b>Get-ADReplicationConnection</b>	A specific AD DS replication connection or a set of AD DS replication connection objects based on a specified filter
<b>Get-ADReplicationFailure</b>	A description of an AD DS replication failure
<b>Get-ADReplicationPartnerMetadata</b>	Replication metadata for a set of one or more replication partners
<b>Get-ADReplicationSite</b>	A specific AD DS replication site or a set of replication site objects based on a specified filter

Cmdlet	Data returned
<b>Get-ADReplicationSiteLink</b>	A specific Active Directory site link or a set of site links based on a specified filter
<b>Get-ADReplicationSiteLinkBridge</b>	A specific Active Directory site link bridge or a set of site link bridge objects based on a specified filter
<b>Get-ADReplicationSubnet</b>	A specific Active Directory subnet or a set of Active Directory subnets based on a specified filter



**Additional Reading:** For more information, refer to: "AD DS Administration Cmdlets in Windows PowerShell: at: <http://aka.ms/ltjgof>

Verify the correctness of the statement by placing a mark in the column to the right.

Statement	Answer
The shortest replication duration that you can configure with site replication scheduling is 15 minutes.	



# Lab: Implementing AD DS sites and replication

## Scenario

A. Datum Corporation has deployed a single AD DS domain, with all the domain controllers located in the London datacenter. As the company has grown and added branch offices with large numbers of users, it has become apparent that the current AD DS environment does not meet the company's requirements. Users in some branch offices report that it can take a long time for them to sign in to their computers. Access to network resources such as the company's servers, which are running Microsoft Exchange Server 2016 and Microsoft SharePoint Server 2016, can be slow, and they sporadically fail.

As one of the senior network administrators, you are responsible for planning and implementing an AD DS infrastructure that will help address the organization's business requirements. You are responsible for configuring AD DS sites and replication to optimize the user experience and network utilization within the organization.

## Objectives

After completing this lab, you will be able to:

- Modify the default site that was created in AD DS.
- Create and configure additional sites and subnets.
- Configure AD DS replication.
- Monitor and troubleshoot AD DS replication.

## Lab Setup

Estimated Time: 45 minutes

Virtual machines: **20742A-LON-DC1**, **20742A-LON-DC2**, and **20742A-TOR-DC1**

User name: **Adatum\Administrator**

Password: **Pa\$\$w0rd**

For this lab, you will use the available virtual machine environment. Before you begin the lab, you must complete the following procedure:

1. On the host computer, click **Start**, point to **Administrative Tools**, and then click **Hyper-V Manager**.
2. In Hyper-V Manager, click **20742A-LON-DC1**, and then in the **Actions** pane, click **Start**.
3. In the **Actions** pane, click **Connect**. Wait until the virtual machine starts.
4. Sign in by using the following credentials:
  - User name: **Adatum\Administrator**
  - Password: **Pa\$\$w0rd**
5. Repeat steps 2 through 4 for **20742A-LON-DC2** and **20742A-TOR-DC1**.

## Exercise 1: Modifying the default site

### Scenario

A. Datum has decided to implement additional AD DS sites to optimize the network utilization for AD DS network traffic. Your first step in implementing the new environment is to install a new domain controller for the Toronto site. You then will reconfigure the default site and assign appropriate IP address subnets to the site.

Finally, your task is to change the name of the default site to **LondonHQ** and associate it with the **172.16.0.0/24** IP subnet, which is the subnet range for the London head office.

The main tasks for this exercise are as follows:

1. Install the Toronto domain controller.
2. Rename the default site.
3. Configure IP subnets that are associated with the default site.

#### ► Task 1: Install the Toronto domain controller

1. On **TOR-DC1**, start **Server Manager** and install **Active Directory Domain Services**.
2. When the AD DS binaries have installed, use the **Active Directory Domain Services Configuration Wizard** to install and configure **TOR-DC1** as an additional domain controller for **Adatum.com**. Under **Type the Directory Services Restore Mode (DSRM) password**, type **Pa\$\$w0rd** in both the **Password** and **Confirm password** boxes. Let the server restart as indicated.
3. After the server restarts, sign in as **Adatum\Administrator** with the password **Pa\$\$w0rd**.

#### ► Task 2: Rename the default site

1. If necessary, on **LON-DC1**, open the **Server Manager** console.
2. Open **Active Directory Sites and Services**, and then rename the **Default-First-Site-Name** site to **LondonHQ**.
3. Verify that both **LON-DC1** and **TOR-DC1** are members of the **LondonHQ** site.

#### ► Task 3: Configure IP subnets that are associated with the default site

1. If necessary, on **LON-DC1**, open the **Server Manager** console, and then open **Active Directory Sites and Services**.
2. Create a new subnet with the following configuration:
  - Prefix: **172.16.0.0/24**
  - Site object: **LondonHQ**

**Results:** After completing this exercise, you should have successfully reconfigured the default site and assigned IP address subnets to the site.

## Exercise 2: Creating additional sites and subnets

### Scenario

The next step you take to implement the AD DS site design is to configure the new AD DS site. The first site that you need to implement is the Toronto site for the North American datacenter. The network team in Toronto would also like to dedicate a site named **TestSite** in the Toronto datacenter. You have been instructed that the Toronto IP subnet address is **172.16.1.0/24**, and the test network IP subnet address is **172.16.100.0/24**.

The main tasks for this exercise are as follows:

1. Create the AD DS sites for Toronto.
2. Create IP subnets that are associated with the Toronto sites.

#### ► Task 1: Create the AD DS sites for Toronto

1. If necessary, on **LON-DC1**, open the **Server Manager** console, and then open **Active Directory Sites and Services**.
2. Create a new site with the following configuration:
  - Name: **Toronto**
  - Site link object: **DEFAULTIPSITELINK**
3. Create another new site with the following configuration:
  - Name: **TestSite**
  - Site link object: **DEFAULTIPSITELINK**

#### ► Task 2: Create IP subnets that are associated with the Toronto sites

1. If necessary, on **LON-DC1**, open **Active Directory Sites and Services**.
2. Create a new subnet with the following configuration:
  - Prefix: **172.16.1.0/24**
  - Site object: **Toronto**
3. Create another new subnet with the following configuration:
  - Prefix: **172.16.100.0/24**
  - Site object: **TestSite**
4. In the navigation pane, click the **Subnets** folder. Verify in the details pane that the two subnets are created and associated with their appropriate site.

**Results:** After completing this exercise, you should have successfully created two additional sites representing the IP subnet addresses in Toronto.

## Exercise 3: Configuring AD DS replication

### Scenario

Now that the AD DS sites have been configured for Toronto, your next step is to configure the site links to manage replication between the sites and then to move the **TOR-DC1** domain controller to the **Toronto** site. Currently, all sites belong to **DEFAULTSITELINK**.

You need to modify site linking so that **LondonHQ** and **Toronto** belong to one common site link called **LON-TOR**. You should configure this link to replicate every hour. Additionally, you should link the **TestSite** site only to the **Toronto** site by using a site link named **TOR-TEST**. Replication should not be available from the **Toronto** site to the **TestSite** site during working hours from 9 AM to 3 PM. You then will use tools to monitor replication between the sites.

The main tasks for this exercise are as follows:

1. Configure site links between AD DS sites.
2. Move TOR-DC1 to the Toronto site.
3. Monitor AD DS site replication.

#### ► Task 1: Configure site links between AD DS sites

1. If necessary, on **LON-DC1**, open **Active Directory Sites and Services**.
2. Create a new IP-based site link with the following configuration:
  - Name: **TOR-TEST**
  - Sites: **Toronto, TestSite**
  - Modify the schedule to only allow replication from **Monday 9 AM** to **Friday 3 PM**
3. Rename **DEFAULTSITELINK**, and then configure it with the following settings:
  - Name: **LON-TOR**
  - Sites: **LondonHQ, Toronto**
  - Replication: Every **60** minutes

#### ► Task 2: Move TOR-DC1 to the Toronto site

1. If necessary, on **LON-DC1**, open **Active Directory Sites and Services**.
2. Move **TOR-DC1** from the **LondonHQ** site to the **Toronto** site.
3. Verify that **TOR-DC1** is located under the **Servers** node in the **Toronto** site.

#### ► Task 3: Monitor AD DS site replication

1. On **LON-DC1**, on the taskbar, click the **Windows PowerShell** icon.
2. Use the following commands to monitor site replication:

```
Repadmin /kcc
```

This command recalculates the inbound replication topology for the server.

```
Repadmin /showrep
```

Verify that the last replication with **TOR-DC1** was successful.

```
Repadmin /bridgeheads
```

This command displays the bridgehead servers for the site topology.

```
Repadmin /replsummary
```

This command displays a summary of replication tasks. Verify that no errors appear.

```
DCDiag /test:replications
```

Verify that all connectivity and replication tests pass successfully.

3. Switch to **TOR-DC1**, and then repeat the commands to view information from the **TOR-DC1** perspective.

**Results:** After completing this exercise, you should have successfully configured site links and monitored replication.

## Exercise 4: Monitoring and troubleshooting AD DS replication

### Scenario

After AD DS sites and replication are established, A. Datum experiences replication issues. You must use monitoring and troubleshooting tools to diagnose the issue and resolve it.

The main tasks for this exercise are as follows:

1. Produce an error.
2. Monitor AD DS site replication.
3. Troubleshoot AD DS replication.
4. Prepare for the next module.

#### ► Task 1: Produce an error

1. On **LON-DC1**, open **Server Manager**, and then open **Active Directory Sites and Services**.
2. In **Active Directory Sites and Services**, replicate **TOR-DC1** with **LON-DC1** from the **LondonHQ** site.
3. In Windows PowerShell, run:

```
Get-ADReplicationUpToDatenessVectorTable -Target "adatum.com"
```

4. Observe the results, and then note the date and time of the most recent replication event.
5. Go to **TOR-DC1**, open **Windows PowerShell**, and then run the following Windows PowerShell commands:

```
CD \Labfiles\Mod04.\Mod04Ex4.ps1
```

### ► Task 2: Monitor AD DS site replication

1. On **TOR-DC1**, in **Active Directory Sites and Services**, replicate **LON-DC1** with **TOR-DC1** from the **Toronto** site.
2. On **TOR-DC1**, in Windows PowerShell, run the following cmdlets, and then observe the results:

```
Get-ADReplicationUpToDateenessVectorTable -Target "adatum.com"
Get-AdReplicationSubnet -filter *
Get-AdReplicationSiteLink-filter *
```

### ► Task 3: Troubleshoot AD DS replication

1. On **TOR-DC1**, in Windows PowerShell, determine the IP address settings for the computer, and then run the following cmdlet:

```
Get-DnsClient | Set-DnsClientServerAddress -ServerAddresses
("172.16.0.10", "172.16.0.25")
```

Ensure that the IP address settings are correct.

2. Go to **Active Directory Sites and Services**, and then replicate **LON-DC1** with **TOR-DC1** from the **Toronto** site. Review the objects to determine if any are missing.
3. On **TOR-DC1**, open **File Explorer**. Browse to **C:\Labfiles\Mod04**.
4. Right-click the **Mod04EX4Fix.ps1** file, and then select **Run with PowerShell**.
5. In **Active Directory Sites and Services**, examine all the objects that you created earlier. Ensure that the site link has been created in the **Inter-Site Transports** node, and subnets have been created in the **Subnets** node.
6. On **LON-DC1** and **TOR-DC1**, close all open windows, and then sign out of both virtual machines.

**Results:** After completing this exercise, you should have successfully diagnosed and resolved replication issues.

### ► Task 4: Prepare for the next module

When you finish the lab, revert the virtual machines to their initial state. To do this, complete the following steps:

1. On the host computer, start **Hyper-V Manager**.
2. On the **Virtual Machines** list, right-click **20742A-LON-DC1**, and then click **Revert**.
3. In the **Revert Virtual Machine** dialog box, click **Revert**.
4. Repeat steps 2 and 3 for **20742A-LON-DC2** and **20742A-TOR-DC1**.

**Question:** You decide to add a new domain controller named **LON-DC2** to the **LondonHQ** site. How can you ensure that **LON-DC2** passes all replication traffic to the **Toronto** site?

**Question:** You have added a new domain controller named **LON-DC2** to the **LondonHQ** site. Which AD DS partitions will be modified as a result?

**Question:** In the lab, you created a separate site link for the **Toronto** and **TestSite** sites. What might you also have to do to ensure that **LondonHQ** does not automatically create a connection object directly with the **TestSite** site?

## Module Review and Takeaways

### Best Practices

Implement the following best practices when you manage Active Directory sites and replication in your environment:

- Always provide at least one or more global catalog servers per site.
- Ensure that all sites have appropriate subnets associated.
- When you configure replication schedules for intersite replication, do not set up long intervals without replication.
- Avoid using Simple Mail Transfer Protocol (SMTP) as a protocol for replication.

### Common Issues and Troubleshooting Tips

Common Issue	Troubleshooting Tip
A client cannot locate a domain controller in its site.	
Replication between sites does not work.	
Replication between two domain controllers in the same site does not work.	

### Review Questions

**Question:** In a multisite enterprise, why is it important that all subnets are identified and associated with a site?

**Question:** What are the advantages and disadvantages of reducing the intersite replication interval?

**Question:** What is the purpose of a bridgehead server?

### Tools

The following table lists the tools that this module references.

Tool	Use	Location
<b>Active Directory Sites and Services</b> console	Create sites, subnets, site links, site link bridging, force replication, and restart the Knowledge Consistency Checker.	<b>Server Manager</b> tools
<b>Repadmin.exe</b>	Reports the status of replication on each domain controller, create replication topology and force replication, and view levels of detail down to the replication metadata.	Command line

Tool	Use	Location
<b>Dcdiag.exe</b>	Performs a number of tests and reports on the overall health of replication and security for AD DS.	Command line
<b>Get-ADReplicationConnection</b>	A specific AD DS replication connection or set of AD DS replication connection objects based on a specified filter.	Windows PowerShell
<b>Get-ADReplicationFailure</b>	A description of an AD DS replication failure.	Windows PowerShell
<b>Get-ADReplicationPartnerMetadata</b>	Replication metadata for a set of one or more replication partners.	Windows PowerShell
<b>Get-ADReplicationSite</b>	A specific AD DS replication site or a set of replication site objects based on a specified filter.	Windows PowerShell
<b>Get-ADReplicationSiteLink</b>	A specific Active Directory site link or a set of site links based on a specified filter.	Windows PowerShell
<b>Get-ADReplicationSiteLinkBridge</b>	A specific Active Directory site link bridge or a set of site link bridge objects based on a specified filter.	Windows PowerShell
<b>Get-ADReplicationSubnet</b>	A specific Active Directory subnet or a set of Active Directory subnets based on a specified filter.	Windows PowerShell



# Module 5

## Implementing Group Policy

### Contents:

Module Overview	5-1
<b>Lesson 1:</b> Introducing Group Policy	5-2
<b>Lesson 2:</b> Implementing and administering GPOs	5-13
<b>Lesson 3:</b> Group Policy scope and Group Policy processing	5-21
<b>Lab A:</b> Implementing a Group Policy infrastructure	5-36
<b>Lesson 4:</b> Troubleshooting the application of GPOs	5-40
<b>Lab B:</b> Troubleshooting Group Policy infrastructure	5-48
Module Review and Takeaways	5-53

## Module Overview

Since the release of Microsoft Windows 2000, the Group Policy feature of Windows operating systems has provided an infrastructure with which administrators can define settings centrally and then deploy them to computers across their organizations. In an environment managed by a well-implemented Group Policy infrastructure, very little configuration takes place by an administrator directly touching a user's computer. You can define, enforce, and update the entire configuration by using Group Policy Object (GPO) settings. By using GPO settings, you can affect an entire site or domain within an organization or you can narrow your focus to a single organizational unit (OU). Filtering based on security group membership and other attributes allow you to define the target for your GPO settings even further. This module will explain what Group Policy is and describe how it works and how best to implement it in your organization.

### Objectives

After completing this module, you will be able to:

- Explain what Group Policy is.
- Implement and administer GPOs.
- Describe Group Policy scope and Group Policy processing.
- Troubleshoot GPO application.

## Lesson 1

# Introducing Group Policy

The Group Policy infrastructure has several interacting components. To implement and support Group Policy properly, you must understand what each component does and how they work together. In addition, you must understand how to assemble these components into different configurations. This lesson provides a comprehensive overview of Group Policy components, procedures, and functions.

### Lesson Objectives

After completing this lesson, you will be able to:

- Describe configuration management.
- Describe Group Policy.
- Explain the benefits of using Group Policy.
- Describe GPOs.
- Explain GPO scope.
- Explain GPO inheritance.
- Describe the Group Policy Client service and client-side extensions.
- Describe new features in Group Policy in Windows Server 2016.

### What is configuration management?

If you only have one computer in your environment—at home, for example—and you wish to modify the desktop background, you can do it in several different ways. Often people open **Personalization** from the **Settings** app in Windows 10 and then make the change by using the Windows operating system interface. Although that works well for one computer, it might be tedious if you want to make the change across multiple computers. Implementing any change and maintaining a consistent environment is more difficult with multiple computers.

- *Configuration management* is a centralized approach to applying one or more changes to more than one user or computer
- The key elements of configuration management are:
  - Setting
  - Scope
  - Application

*Configuration management* is a centralized approach to applying one or more changes to more than one user or computer. The key elements of configuration management are:

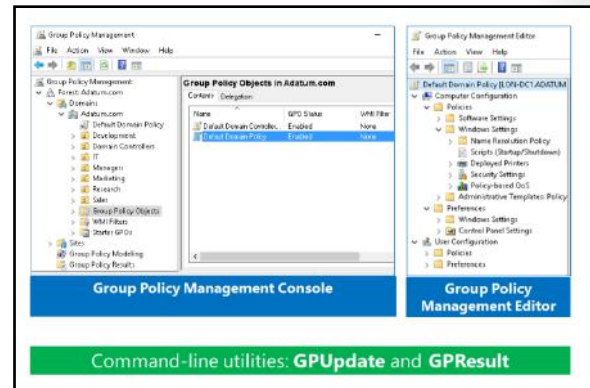
- **Setting.** A setting also is known as a centralized definition of a change. The setting brings a user or computer to a desired configuration state.
- **Scope.** The scope of a change is the number of computers or users that the setting affects.
- **Application.** The application is a mechanism or process that ensures that the setting applies to users and computers within the scope.

Group Policy is a framework in Windows operating systems with components that reside in Active Directory Domain Services (AD DS), on domain controllers, and on each Windows server and client. With these components, you can manage configuration in an AD DS domain.

## Overview of Group Policy tools and consoles

The most basic component of Group Policy is an individual policy setting. An individual policy setting also is known as a policy. The policy defines a specific configuration change that you can apply, such as a policy setting that prevents a user from accessing registry editing tools. If you define that policy setting, and then apply it to the user, the user will be unable to run tools such as REGEDIT (regedit.exe).

It is important to know that some settings affect a user: these settings are called *user configuration settings* (or *user policies*). And some settings affect the computer: these settings are called *computer-configuration settings* (or *computer policies*).



Group Policy manages various policy settings, and the Group Policy framework is extensible. In the end, you can manage just about any configurable setting with Group Policy.

In the **Group Policy Management Editor** window, you can define a policy setting by double-clicking it. The policy setting **Properties** dialog box appears. Policy settings in the area called **Administrative Templates** can have three states: **Not Configured**, **Enabled**, and **Disabled**.

In a new GPO, every policy setting defaults to **Not Configured**. This means that the GPO does not modify the existing configuration of that particular setting for a user or computer. If you enable or disable a policy setting, a change is made to the configuration of users and computers to which the GPO is applied. When you return an **Administrative Template** setting to its **Not Configured** value, you return it to its default value. Some settings remain configured on the computer even if you remove the setting from the GPO.

The effect of the change depends on the policy setting. For example, if you enable the **Prevent Access To Registry Editing Tools** policy setting, users are unable to open the registry editor, regedit.exe. If you disable the policy setting, you ensure that users can open the registry editor. Notice the double negative in this policy setting example: you disable a policy that prevents an action; therefore, you allow the action. Some policy settings bundle several configurations into one policy, and these might require additional parameters.

**Note:** Many policy settings are complex, and the effect of enabling or disabling them might not be obvious. Furthermore, some policy settings affect only certain versions of the Windows operating system. Be sure to review a policy setting's explanatory text in the **Group Policy Management Editor** window or on the **Explain** tab in the policy setting's **Properties** dialog box. Additionally, always test the effects of a policy setting and its interactions with other policy settings before deploying a change in your production environment.

### Computer Configuration and User Configuration

There are two major divisions of policy settings: computer settings, which are contained in the **Computer Configuration node**, and user settings, which are contained in the **User Configuration** node:

- The **Computer Configuration** node contains the settings that are applied to computers, regardless of who logs on to them. Computer settings apply when the operating system starts, during background refreshes, and every 90–120 minutes thereafter.
- The **User Configuration** node contains settings that apply when a particular user signs in to the computer, during background refreshes, and every 90–120 minutes thereafter.

Within the **Computer Configuration** and **User Configuration** nodes are the **Policies** and **Preferences** nodes. You will learn more about configuring settings in both the Policies and Preferences node in Module 6 “Managing user settings with GPO.”

Within the **Policies** nodes, under the **Computer Configuration** node and the **User Configuration** node, are a hierarchy of folders that contain policy settings. Because there are thousands of settings, it is beyond the scope of this course to examine individual settings. However, it is worthwhile to define the broad categories of settings in the folders.

### The Software Settings node

The Software Settings node is the first node. It contains only the software Installation extension, which helps you specify how your organization installs and maintains its applications.

### The Windows Settings node

In both the **Computer Configuration** and **User Configuration** nodes, the **Policies** node contains a **Windows Settings** node, which includes the **Scripts**, **Security Settings**, and **Policy-Based QoS** nodes. It also contains the **Name Resolution Policy** folder that contains settings for configuring DirectAccess.

### The Scripts node

With the scripts extension, you can specify two types of scripts: startup and shutdown scripts in the **Computer Configuration** node and logon and logoff scripts in the **User Configuration** node. Startup and shutdown scripts run at computer startup or shutdown. Logon and logoff scripts run when a user signs in or signs out. When you assign multiple logon and logoff or startup and shutdown scripts to a user or computer, the script’s client-side extension (CSE) executes the scripts from the top to the bottom of the list. You can determine the order of execution for multiple scripts in the **Properties** dialog box. When a computer is shut down, the CSE first processes logoff scripts, followed by shutdown scripts. By default, the timeout value for processing scripts is 10 minutes. If the logoff and shutdown scripts require more than 10 minutes to process, you must adjust the timeout value with a policy setting. You can use any ActiveX scripting language to write scripts. Some possibilities include Microsoft Visual Basic Scripting Edition (VBScript); JScript; Perl; and MS-DOS–style batch files (.bat and .cmd). Logon scripts on a shared network directory in another forest are supported for network logon across forests. Windows 7, Windows 8, and Windows 10 all support Windows PowerShell command-line interface scripts, too. CSEs will be explained in detail later in this lesson.

### The Security Settings node

By using the **Security Settings** node, a security administrator can configure security with GPOs. You can do this after, or instead of, using a security template to configure system security.

### The Policy-Based QoS node

This quality of service (QoS) node, known as the **Policy-Based QoS** node, defines policies that manage network traffic. For example, you might want to ensure that users in the Finance department have priority to run a critical network application during the end-of-year financial reporting period. You can do that by using the **Policy-Based QoS** node.

In the **User Configuration** node only, the **Windows Settings** folder contains the additional **Folder Redirection** node. With folder redirection, you can redirect user data and settings folders such as **AppData**, **Desktop**, **Documents**, **Pictures**, **Music**, and **Favorites** from their default user profile location to an alternate location on the network, where you can manage them centrally.

## The Administrative Templates node

In the **Computer Configuration** and **User Configuration** nodes, the **Administrative Templates** node contains registry-based Group Policy settings. There are thousands of such settings available for configuring the user and computer environment. As an administrator, you might spend a significant amount of time modifying these settings. To assist you with these settings, a description of each policy setting is available in two locations:

- On the **Explain** tab in the **Properties** dialog box for the setting. Additionally, the **Settings** tab in the **Properties** dialog box for each setting also lists the required operating system or software for the setting.
- On the **Extended** tab of the **Group Policy Management Editor** window. The **Extended** tab, which appears on the lower right of the details pane, provides a description of each selected setting in a column between the console tree and the settings pane. Also, it lists the required operating system or software for each setting.

You can use the **gpupdate** command to initiate a Group Policy refresh. You will learn more about **gpupdate** later in this module.

To verify which GPOs and settings apply to a computer and user, you can use the **gpresult** command. The **gpresult** command can show more or less details depending on the options that you type.

## Demonstration: Exploring Group Policy tools and consoles

In this demonstration, you will see how to:

- Navigate Group Policy Management Console (GPMC).
- Create a new GPO.
- Configure a setting.
- Perform a Group Policy refresh.
- Examine which GPOs apply to the computer and user.

### Demonstration Steps

1. Open **Group Policy Management Editor**.
2. In the **Group Policy Management Editor** window, in the navigation pane, navigate to **Group Policy Objects**.
3. Create a new GPO named **Disable Control Panel**, and then edit it.
4. In the **Group Policy Management Editor** window, in the navigation pane, under **User Configuration**, expand **Policies**, expand **Administrative Templates**, and then click **Control Panel**.
5. In the details pane, double-click **Prohibit access to Control Panel and PC Settings**.
6. Enable the setting, type a comment, and then close the **Group Policy Management Editor** window.
7. View the **Scope**, **Details**, and **Settings** tabs.
8. Link the **Disable Control Panel** GPO to the domain.
9. View the **Linked Group Policy Objects** and **Group Policy Inheritance** tabs.
10. Open a **Windows PowerShell** window as **Administrator**.

11. In the **Administrator: Windows PowerShell** window, type the following command, and then press Enter:

```
gpupdate
```

12. Verify that both the computer and user settings updated successfully.
13. Type the following command, and then press Enter:

```
gpresult /r
```

14. Verify that in the output from the command in the **User Settings** section, in the **Applied GPOs** list, the **Disable Control Panel** GPO is listed.
15. Close the **Windows PowerShell** window.

## Benefits of using Group Policy

Group Policy is a powerful administrative tool. You can use GPOs to push various settings to a large number of users and computers. Because you can apply them to different levels, from local computer to domain, you also can focus these settings precisely.

Primarily, you use Group Policy to configure settings that you do not want users to configure. Additionally, you can use Group Policy to standardize desktop environments on all computers in an OU or in an entire organization.

You also can use Group Policy to provide additional security, to configure some advanced system settings and for other purposes that the following sections detail.

- Group Policy is a very powerful administrative tool
- You can use it to enforce various types of settings to a large number of users and computers
- Typically, you use GPOs to:
  - Apply security settings
  - Manage desktop application settings
  - Deploy application software
  - Manage Folder Redirection
  - Configure network settings

### Applying security settings

In the Windows Server 2016 operating system, GPOs include a large number of security-related settings that you can apply to both users and computers. For example, you can enforce settings for Windows Firewall, and you can configure auditing and other security settings. You also can configure full sets of user-rights assignments.

### Managing desktop and application settings

You can use Group Policy to provide a consistent desktop and application environment for all users in your organization. By using GPOs, you can configure each setting that affects the look and feel of the user environment. You also can configure settings for some applications that support GPOs.

### Deploying software

With Group Policy, you can deploy software to users and computers. You can use Group Policy to deploy all software that is available in the .msi format. Additionally, you can enforce automatic software installation, or you can let your users decide whether they want the software to deploy to their computers.



**Note:** Deploying large software packages with GPOs might not be the most efficient way to distribute an application to your organization's computers. In many circumstances, it might be more effective to distribute applications as part of the desktop computer image.

## Managing Folder Redirection


With the Folder Redirection option, it is easier to back up users' data files. By redirecting folders, you also ensure that users have access to their data regardless of the computer they sign in on. Additionally, you can centralize all users' data to one place on a network server, while still providing a user experience that is similar to storing these folders on their computers. For example, you can configure Folder Redirection to redirect users' **Documents** folders to a shared folder on a network server.

## Configuring network settings

By using Group Policy, you can configure various network settings on client computers. For example, you can enforce settings for wireless networks to allow users to connect only to specific service set identifiers and with predefined authentication and encryption settings. You also can deploy policies that apply to wired network settings, and some Windows Server 2016 roles use Group Policy to configure the client side of services, such as DirectAccess.

## Group Policy Objects


You define policy settings within a GPO. A GPO is an object that contains one or more policy settings that apply to one or more configuration settings for a user or a computer.

 **Note:** You manage GPOs by using the GPMC.

The GPMC displays GPOs in a container named **Group Policy Objects**. To create a new GPO in a domain, right-click the **Group Policy Objects** container, click **New**, and then specify a name for the GPO. To modify the configuration settings in a GPO, right-click the GPO, and then click **Edit**. This opens the **Group Policy Management Editor** window. To create a GPO in Windows PowerShell, you run the following cmdlet:

```
New-GPO -Name "Sales GPO" -comment "This is the sales GPO"
```

It is also possible to create a GPO and link it to the domain or an OU when it is created, by right-clicking the container, and then clicking **Create a GPO in the domain and link it here**.

 **Note:** For the settings within the object to take effect, you must apply or link the GPO to a site, domain, or OU in the AD DS hierarchy.

### A GPO is:


- A container for one or more policy settings
- Managed with the GPMC
- Stored in the GPOs container
- Edited with Group Policy Management Editor
- Applied to a specific level in the AD DS hierarchy

## Overview of GPO scope


You define configuration changes by configuring policy settings in GPOs. However, the configuration changes in a GPO do not affect computers or users in your organization until you specify the computers or users to which the GPO applies. This is called *scoping* a GPO. The scope of a GPO is the collection of users and computers that will apply the settings in the GPO.

You can use several methods to manage the scope of GPOs. The first is the GPO link. You can link GPOs to sites, domains, and OUs in AD DS. The site, domain, or OU then becomes the maximum scope of the GPO. All computers and users within the site, domain, or OU, including those in child OUs, are affected by the configurations that the policy settings in the GPO specify.

- The *scope* of a GPO is the collection of users and computers that will apply the settings in the GPO
- You can use several methods to scope a GPO:
  - Link the GPO to a container, such as an OU
  - Filter by using security settings
  - Filter by using WMI filters
- For Group Policy preferences:
  - You can filter or target the settings that you configure by Group Policy preferences within a GPO based on several criteria

 **Note:** You can link a GPO to more than one site, domain, or OU. You should be careful linking GPOs to multiple sites, which can introduce performance issues when the policy is applied. This is because, in a multisite network, the GPOs are stored in the domain controllers of the domain where the policy was created. Consequently, computers in other domains might need to traverse a slow wide area network (WAN) link to obtain the GPOs.

You can further narrow the scope of the GPO with one of two types of filters. With security filters, you can use permissions to specify to which users, computers, or members of security groups the GPO does or does not apply. Windows Management Instrumentation (WMI) filters specify a scope by using the characteristics of a system, such as operating system version or free disk space. Use security filters and WMI filters to narrow or specify the scope within the initial scope created by the GPO link.

 **Note:** Windows Server 2008 introduced a new component of Group Policy called Group Policy preferences. You can filter or target the settings that you configure by Group Policy preferences within a GPO based on several criteria. With targeted preferences, you can further refine the scope of preferences within a single GPO.

## Overview of GPO inheritance

You can create and link GPOs to a site, domain, or OU. When you apply multiple GPOs to the same container, this aggregates the settings in the GPOs. For most policy settings, the GPO with the highest precedence and that contains the specific setting determines the setting's final value. For a few settings, the final value is actually the combination of values across GPOs.

GPOs are processed on a client computer in the following order:

1. Local GPOs
2. Site-level GPOs
3. Domain-level GPOs
4. OU GPOs, including any nested OUs



GPOs are processed on a client computer in the following order:

1. Local GPOs
2. Site-level GPOs
3. Domain-level GPOs
4. OU GPOs, including any nested OUs, starting with the OU farthest from the user or computer object



**Note:** In the following topics, the term *container* describes a site, a domain, and an OU. In this context, it does not describe AD DS containers, because you cannot link GPOs to AD DS containers.

GPOs that apply to higher-level containers pass through to all subcontainers in that part of the Active Directory tree. For example, a policy setting that you apply through a GPO linked to an OU also applies to any child OUs below it. The local GPO is processed first, and the OU to which the computer or user belongs is processed last. The last GPO processed is the effective setting.

Several Group Policy options can alter this default inheritance behavior. These options include:

- **Link Order.** Use this option to set the precedence order for GPOs linked to a given container. The GPO link with a link order of one has the highest precedence on that container. If you change the link order, it does not have an effect unless GPOs that link to the same location have conflicting settings.
- **Enforced.** With this option you can specify that a GPO takes precedence over any GPOs that link to child containers. Additionally, a GPO that the Windows operating system enforces at the domain level overrides a GPO that it enforces at an OU level. You typically enforce a GPO to ensure that computers use company-wide settings and that departmental administrators do not override these settings by creating other GPOs.
- **Block Inheritance.** With this option you can prevent an OU or domain from inheriting GPOs from any parent containers. Enforced GPO links will always be inherited. Typically, you block inheritance to enable a department to manage Group Policy settings separately from the rest of the organization.
- **Link Enabled.** The ability to specify whether a Windows operating system processes a specific GPO link for the container to which it links. When you do not enable a link, the Windows operating system does not process the GPO. Typically this is done during troubleshooting when you want to disable the processing of a GPO to eliminate it as a source of configuration errors.



**Note:** Remember that GPO inheritance is on a per setting basis rather than a per GPO basis.

## The Group Policy Client service and client-side extensions

### Group Policy application

It is important to understand how group policies apply on client computers. The steps below explain the process:

1. When a Group Policy refresh begins, a service that is running on all Windows-based computers, known as the Group Policy Client service in Windows Vista and later and Windows 2008 and later determines which GPOs apply to the computer or user.
2. The Group Policy Client service downloads any GPOs that are not cached already.
3. Group Policy client-side extensions interpret the settings in a GPO and make appropriate changes to the local computer or to the currently signed-in user. There are client-side extensions for each major category of policy setting. For example, there is a security client-side extension that applies security changes, a client-side extension that executes startup and logon scripts, a CSE that installs software, and a client-side extension that makes changes to registry keys and values. Each Windows operating system version has added client-side extensions to extend the functional reach of Group Policy, and there are several dozen client-side extensions in Windows operating systems.

#### • Group Policy application process:


1. Group Policy Client retrieves GPOs
2. Client downloads and caches GPOs
3. Client-side extensions process the settings

• Policy settings in the **Computer Configuration** node apply at system startup and every 90–120 minutes thereafter


• Policy settings in the **User Configuration** node apply at sign-in and every 90–120 minutes thereafter

One of the more important concepts to remember about Group Policy is that it is client driven. The Group Policy Client service pulls GPOs from the domain, triggering the client-side extensions to apply settings locally. Group Policy is not a push technology.

You can see the installed client-side extensions on a computer by locating the **HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\GPExtensions** key in the registry. You can configure the behavior of client-side extensions by using Group Policy. Most client-side extensions apply settings in a GPO only if that GPO has changed. This behavior improves overall policy processing by eliminating redundant applications of the same settings. Most policies apply in such a way that standard users cannot change the setting on their computer—they always will be subject to the configuration enforced by Group Policy. However, standard users can change some settings, and a user can change many settings if that user is an administrator on the system. If users in your environment are administrators on their computers, you should consider configuring client-side extensions to reapply policy settings even if the GPO has not changed. That way, if an administrative user changes a configuration so that it is no longer compliant with policy, the configuration will be reset to its compliant state at the next Group Policy refresh.

 **Note:** You can configure client-side extensions to reapply policy settings at the next refresh even if the GPO has not changed. You can do this by configuring a GPO scoped to computers and then defining the settings in the **Computer Configuration\Policies\Administrative Templates\System\Group Policy** node. For each CSE that you want to configure, open its policy-processing policy setting, such as **Registry Policy Processing for the Registry CSE**. Click **Enabled**, and then select the **Process even if the Group Policy objects have not changed** check box.


The security client-side extension manages an important exception to the default policy-processing settings. The security client-side extension reapplies security settings every 16 hours, even if a GPO has not changed.

 **Note:** Enable the **Always Wait For Network At Startup And Logon** policy setting for all Windows-based clients. Without this setting, by default, Windows XP and later clients perform refreshes asynchronously. The user signs in using cached credentials. The benefit is that the desktop is quicker to display and the user can start work without waiting for Group Policy to apply. This means that when the client computer starts up, and the user signs in, they do not receive the latest policies from the domain. Group Policy will perform a refresh in the background after the user signs in. The setting is located in **Computer Configuration\Policies\Administrative Templates\System\Logon**. Be sure to read the policy setting's explanatory text. The setting changes the Group Policy processing to synchronous mode, which might make processing slower, but it ensures a more consistent environment.

### Group Policy refresh

Policy settings in the **Computer Configuration** node apply at system startup and then every 90–120 minutes thereafter. Policy settings in the **User Configuration** node apply at sign in and then every 90–120 minutes thereafter. The application of policies is called *Group Policy refresh*.

The refresh that occurs at system startup and user sign in is also referred to as foreground refresh. The periodic refresh that occurs every 90-120 minutes and manual refreshes are both referred to as background refreshes. Some client-side extensions only apply settings during foreground processing.

 **Note:** You also can force a policy refresh by using the **gpupdate** command.

## New features in Group Policy in Windows Server 2016

Windows Server 2016 introduces a few changes and improvements to GPOs. These are:

- Limited support for Nano Server. Although Nano Server does not support Group Policy directly, there are PowerShell cmdlets that allow you to import settings from the GPO after exporting them by using Windows PowerShell. You can import the following types of settings on a Nano Server:
  - Registry settings. You export the registry settings to a .POL file before you import them on a Nano Server.
  - Security settings. You export the security settings to an .INF file before you import them on a Nano Server.
  - Audit settings. You export the audit settings to a .CSV file before you import them on a Nano Server.
- Windows 10 administrative templates are included. The files needed to configure Windows 10 specific settings are included in Windows Server 2016.

Windows Server 2016 introduces a few changes and improvements to Group Policy, including:

- Importing the following types of policy settings on Nano Server:
  - Registry settings
  - Security settings
  - Audit settings
- Including Windows 10 administrative templates

**Categorize Activity**

Categorize each item into the appropriate category. Indicate your answer by writing the category number to the right of each item.

Items	
1	Domain
2	User
3	Organizational unit
4	Computer
5	Site
6	Group
7	Users container
8	Computers container

Category 1		Category 2
Can link GPOs to		Cannot link GPOs to

## Lesson 2

# Implementing and administering GPOs

Before deploying a Group Policy solution, you need to be familiar with the procedures for working with GPOs, including how to create, link, edit, and manage GPOs with Windows PowerShell and in the GPMC. You also need to know where GPOs are stored on the domain controllers. In an organization, some users might require some administrative responsibilities regarding GPOs, so you also need to know how to delegate permissions to create GPOs. This lesson teaches about all these things. Starter GPOs, which can hold preconfigured settings, are also part of this lesson.

### Lesson Objectives

After completing this lesson, you will be able to:

- Explain what are domain-based GPOs.
- Describe GPO storage.
- Describe Starter GPOs.
- Describe common GPO management tasks.
- Explain how to delegate administration of group policies.

### What are domain-based GPOs?

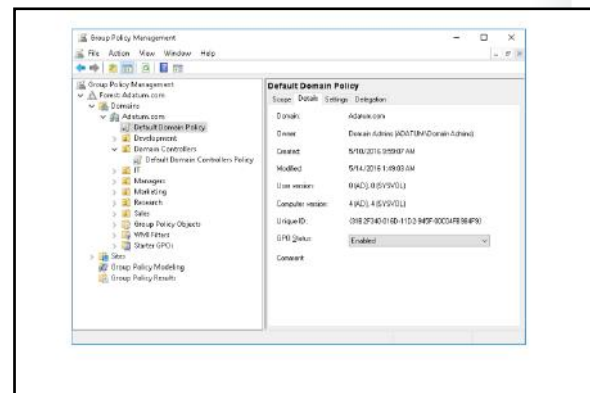
Domain-based GPOs are any GPOs created in AD DS and stored on domain controllers. You can use them to manage configuration centrally for domain users and computers. When you install AD DS and create a domain, two GPOs are created automatically: **Default Domain Policy** and **Default Domain Controllers Policy**.


#### Default Domain Policy


This GPO is linked to the domain and has no security group or WMI filters. Therefore, it affects all users and computers in the domain, including computers that are domain controllers, but there are only settings in the **Computer Configuration** section. This GPO contains policy settings that specify password, account lockout, and Kerberos version 5 protocol policies. You should not add unrelated policy settings to this GPO. If you need to configure other broad settings in your domain, create additional GPOs that link to the domain.

#### Default Domain Controllers Policy

This GPO is linked to the OU of the domain controllers. Because computer accounts for domain controllers are kept exclusively in the **Domain Controllers** OU, and other computer accounts should be kept in other OUs, this GPO affects only domain controllers. You should only modify the **Default Domain Controllers** GPO to implement your auditing policies and to assign the user rights required on domain controllers.



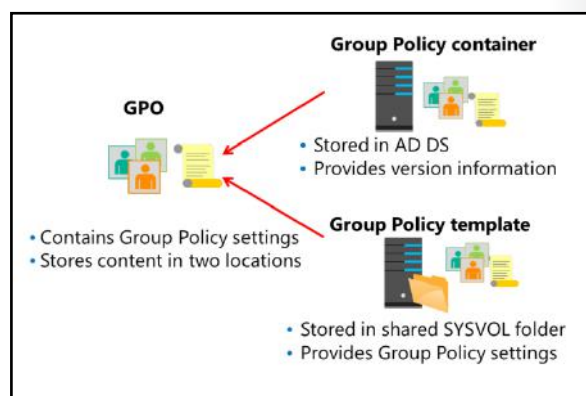
 **Note:** Many administrators prefer not to modify either of the default GPOs and instead rely on the process of creating additional GPOs and linking them to the same container objects. If some incident occurs and you need to restore the default GPOs to their out-of-the-box settings, all your changes would be lost, if you made changes to the two default GPOs.

 **Note:** Computers running Windows operating systems also have local GPOs, which are typically overwritten by higher precedence domain-based GPOs. However, when computers are not connected to a domain, it is only the local GPOs that apply. Windows Vista and later and Windows 2008 and later support the notion of multiple local GPOs. The **Local Computer** GPO is the same as the GPO in previous versions of Windows operating systems. In the **Computer Configuration** node, you can configure all computer-related settings. In the **User Configuration** node, you can configure settings that you want to apply to all users on the computer. You can modify the user settings in the **Local Computer** GPO by using the user settings in two new local GPOs: **Administrators** and **Non-Administrators**. These two GPOs apply user settings to signed-in users according to whether they are members of the local Administrators group, in which case they would use the **Administrators** GPO, or not members of the Administrators group, and therefore use the **Non-Administrators** GPO. You can refine the user settings further with a local GPO that applies to a specific user account. User-specific local GPOs are associated with local—not domain—user accounts.

It is important to understand that domain-based GPO settings combine with those applied by using local GPOs. However, because domain-based GPOs apply last, they take precedence over local GPO settings. You can disable the local GPOs by configuring the **Turn off Local Group Policy Objects processing** setting in a domain-based GPO. Be aware that the local GPO contains many important settings, including security settings that you need to configure in a domain-based GPO.

## GPO storage

Group Policy settings are presented as GPOs in AD DS user interface (UI) tools, but a GPO is actually two components: a Group Policy container and a Group Policy template. The Group Policy container is an AD DS object that is stored in the **Group Policy Objects** container within the domain-naming context of the directory. Similar to all AD DS objects, each Group Policy container includes a globally unique identifier (GUID) attribute that uniquely identifies the object within AD DS. The Group Policy container defines basic attributes of the GPO. The settings are contained in the Group Policy template, which is a collection of files stored in the SYSVOL of each domain controller in the **%SystemRoot%\SYSVOL\Domain\Policies\GPOGUID** path, where *GPOGUID* is the GUID of the Group Policy container. When you make changes to the settings of a GPO, the changes are saved to the Group Policy template of the domain controller from which the GPO was opened, which by default is the domain controller that holds the primary domain controller (PDC) emulator operations master role. By default, when Group Policy refresh occurs, the client-side extensions apply settings in a GPO only if the GPO has been updated.



The Group Policy Client service can identify an updated GPO by its version number. Each GPO has a version number that increments each time a change is made. The version number is stored as a Group Policy container attribute and in a text file, **Gpt.ini**, in the **Group Policy template** folder. Group Policy Client knows the version number of each GPO it has previously applied. If, during Group Policy refresh, Group Policy Client discovers that the version number of the Group Policy container has been changed, the client-side extensions are informed that the GPO is updated.

## GPO replication

Group Policy containers and Group Policy templates are both replicated between all domain controllers in a single domain in AD DS. However, different replication mechanisms are used for these two items. The Group Policy container in AD DS replicates by using a directory replication agent. A directory replication agent uses a topology generated by Knowledge Consistency Checker, which you can define or refine manually. The result is that the Group Policy container is replicated within seconds to all domain controllers in a site and also is replicated between sites based on the intersite replication configuration.

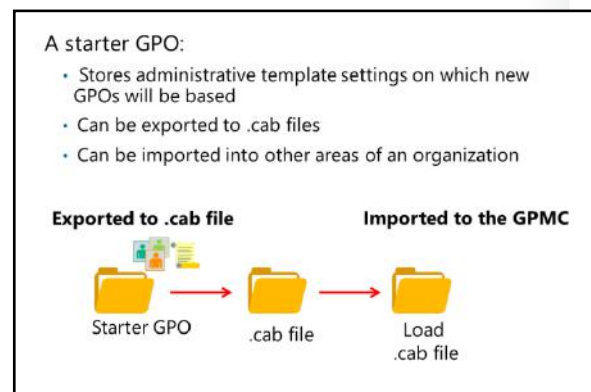
The Group Policy template in the SYSVOL replicates by using one of the following two technologies. The file replication service (FRS) replicates SYSVOL in domains that are running Windows Server 2008, Windows Server 2008 R2, Windows Server 2003, and Microsoft Windows 2000 Server. If all domain controllers are running Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2 or Windows Server 2016, you should configure SYSVOL replication by using Distributed File System Replication (DFS-R), which is a more efficient and reliable mechanism. We recommend that you use DFS-R, because FRS is now deprecated.

Because the Group Policy container and Group Policy template replicate separately, it is possible for them to become out of synchronization for a short time. Typically, when this happens, the Group Policy container replicates to a domain controller first. Systems that obtained their ordered list of GPOs from that domain controller identify the new Group Policy container, attempt to download the Group Policy template, and notice that the version numbers are not the same. A policy-processing error is then recorded in the event logs. If the reverse happens and the Group Policy template replicates to a domain controller before the Group Policy container, then clients obtaining their ordered list of GPOs from that domain controller are not notified of the new GPO until the Group Policy container replicates.

## What are starter GPOs?

You use a starter GPO as a template from which you can create other GPOs within the GPMC. Starter GPOs can contain administrative template settings only. You might use a starter GPO to provide a starting point for new GPOs created in your domain. The starter GPO already might contain specific settings that are Microsoft recommended best practices for your environment. You can export starter GPOs to or import starter GPOs from cabinet (**.cab**) files to make distribution to other environments simple and efficient. The GPMC stores starter GPOs in a folder named **Starter GPOs**, which is located in SYSVOL.

When you click the **Create Starter GPOs Folder** button, located in the **Starter GPOs** node in the GPMC, 10 Starter GPOs are created by default.



## Common GPO management tasks

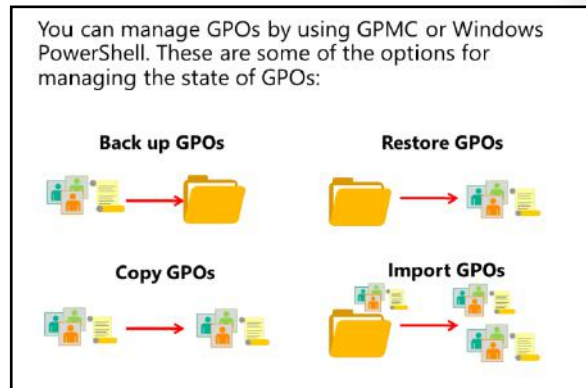
Similar to critical data and AD DS–related resources, you must back up GPOs to protect the integrity of AD DS and GPOs. The GPMC not only provides basic backup and restore options, but it also provides additional control over GPOs for administrative purposes. To manage GPOs, you have the following options:

- **Backing up GPOs.** You can back up GPOs individually or as a whole with the GPMC. You must provide a backup location only, which can be any valid local or shared folder. You must have Read permission on the GPO to back it up. Every time that you perform a backup, a new backup version of the GPO is created, which provides a historical record. If you want to make an automatic backup of all GPOs, you can run the following Windows PowerShell cmdlet:

```
Backup-GPO -all -path E:\GPOBackup -comment "Powershell backup of GPOs"
```

- **Restoring backed up GPOs.** You can restore any version of a GPO. If one becomes corrupt or you delete it, you can restore any of the historical versions of that GPO. The restore interface provides the ability for you to view the settings stored in the backed-up version before restoring it. Restoring a GPO does not restore the GPO links. You must do this manually afterwards.
- **Importing GPO settings from a backed-up GPO.** You can import policy settings from one GPO into another. By importing a GPO, you can transfer settings from a backed up GPO to an existing GPO. Importing a GPO transfers only the GPO settings. The import process does not import GPO links. Security principals defined in the source might need to be migrated to the target by using migration tables.
- **Copying GPOs.** You can copy GPOs by using the GPMC both in the same domain and across domains. A copy operation copies an existing, live GPO to the desired destination domain. A new GPO always gets created during this process. The new GPO is named **Copy of OldGPOName**. For example, if you copied a GPO named **Desktop**, then the new version would be named **Copy of Desktop**. After you copy and paste the file into the **Group Policy Objects** container, you can rename the policy. The destination domain can be any trusted domain in which you have the rights to create new GPOs. When copying between domains, security principals defined in the source might need to be migrated to target.
- **Migration tables.** When importing GPOs or copying them between domains, you can use migration tables to modify references in the GPO that need to be adjusted for the new location. For example, you might need to replace the Universal Naming Convention (UNC) path for Folder Redirection with a UNC path that is appropriate for the new user group to which the GPO will be applied. You can create migration tables prior to this process, or you can create them during the import or cross-domain copy operation. Migration tables are also useful if you want to move GPOs from a test environment into your production domain.

If something happens to the two default GPOs, **Default Domain Policy** and **Default Domain Controllers Policy**, you can restore one or both by using the **DCGPOFix** command-line utility. If you run **DCGPOFix** without any parameters, you will restore both default GPOs. To restore only the **Default Domain Policy** GPO, you add the **/target:Domain** parameter. Likewise you can restore the **Default Domain Controllers Policy** GPO by adding the **/target:DC** parameter.





In addition to using the GPMC and Group Policy Management Editor, you also can perform common GPO administrative tasks by using Windows PowerShell. You can use **get-command -module grouppolicy** to get a list of all Group Policy commands. The following table lists some of the more common administrative tasks possible with Windows PowerShell.

Cmdlet name	Description
<b>New-GPO</b>	Creates a new GPO
<b>New-GPLink</b>	Creates a new GPO link for the specified GPO
<b>Backup-GPO</b>	Backs up the specified GPOs
<b>Restore-GPO</b>	Restores the specified GPOs
<b>Copy-GPO</b>	Copies a GPO
<b>Get-GPO</b>	Gets the specified GPOs
<b>Import-GPO</b>	Imports the backed up settings into a specified GPO
<b>Set-GPInheritance</b>	Grants specified permissions to a user or security group for the specified GPOs

## Delegating administration of Group Policy

By delegating GPO-related tasks, you can distribute the administrative workload across the enterprise. You can task one group with creating and editing GPOs, while another group performs reporting and analysis duties. A third group might be in charge of creating WMI filters.

You can delegate the following Group Policy tasks:

- Creating GPOs
- Editing GPOs
- Managing Group Policy links for a site, domain, or OU
- Performing Group Policy modeling analyses on a given domain or OU
- Reading Group Policy results data for objects in a given domain or OU
- Creating WMI filters in a domain

- Delegation of GPO-related tasks allows the administrative workload to be distributed across the enterprise
- You can delegate the following Group Policy tasks independently:
  - Creating GPOs
  - Editing GPOs
  - Managing Group Policy links for a site, domain, or OU
  - Performing Group Policy modeling analysis in a domain or OU
  - Reading Group Policy results data in a domain or OU
  - Creating WMI filters in a domain

The Group Policy Creator Owners group allows members who create new GPOs to edit or delete them.

### Group Policy default permissions

By default, the following user and groups have full control over GPO management:

- Domain Admins
- Enterprise Admins

- Group Policy Creator Owners
- Local System

The Authenticated Users group has Read and Apply Group Policy permissions to all GPOs.

### Creating GPOs

By default, only Domain Admins, Enterprise Admins, and Group Policy Creator Owners can create new GPOs. You can use two methods to grant a group or user this right:

- Add the user or group to the Group Policy Creator Owners group.
- Explicitly grant the group or user permission to create GPOs by using the GPMC.

### Editing GPOs

To edit a GPO, the user must have both Read and Write access to the GPO. You can grant this permission by using the GPMC.

### Managing GPO links

The ability to link GPOs to a container is a permission that is specific to that container. In the GPMC, you can manage this permission by using the **Delegation** tab on the container. You also can delegate it by using **Delegation of Control Wizard** in Active Directory Users and Computers.

### Group Policy modeling and Group Policy results

You can delegate the ability to use the reporting tools in the same way: by using the GPMC or by using **Delegation of Control Wizard** in Active Directory Users and Computers.

### Creating WMI filters

You can delegate the ability to create and manage WMI filters in the same way: by using the GPMC or by using **Delegation of Control Wizard** in Active Directory Users and Computers.

## Demonstration: Delegating administration of Group Policy

In this demonstration, you will see how to:

- Delegate permissions to create GPOs.
- Delegate permissions to link GPOs.
- Delegate permissions to view Group Policy results.

### Demonstration Steps

#### Make Beth a local administrator on LON-SVR1

1. Switch to **LON-DC1**.
2. Run the Windows PowerShell script located at **E:\Labfiles\Mod05\Set-LocalAdmin.ps1** to make **Beth** a local administrator on **LON-SVR1**.

#### Check user permissions before delegation

1. Switch to **LON-SVR1**.
2. Sign in as **Adatum\Beth** with the password **Pa\$\$w0rd**.
3. In **Server Manager**, add the **Group Policy Management** feature.
4. Start **Group Policy Management**.

5. Try to create a new GPO. The menu item **New** is dimmed, because Beth has not been assigned permissions to create GPOs.
6. Try to link a GPO to the **Adatum.com** domain. The menu item **Link an Existing GPO** is dimmed because Beth does not have permissions to link GPOs to the domain.
7. Try to link a GPO to the **IT OU**. The menu item **Link an Existing GPO** is dimmed because Beth also does not have permissions to link GPOs to IT OU.
8. Open a Windows PowerShell command prompt, and then run the following command:

```
GPResult /r
```

9. In the output from the command, notice that only the **User** settings are displayed because Beth is not allowed to view Group Policy results for computer settings.

### Delegate permissions

1. On **LON-DC1**, switch to the **Group Policy Management** window.
2. On the **Delegation** tab for the **Group Policy Objects** container, add **Beth** to the list.
3. On the **Delegation** tab on the **IT OU**, add **Beth** with the **Link GPOs** permission.
4. On the **Delegation** tab on the **Adatum.com** domain, add **Beth** with the **Read Group Policy Results data** permission.

### Check permissions after delegation

1. Switch to **LON-SVR1**.
2. In the **Group Policy Management** window, click and then right-click the **Adatum.com** domain, and then click **Refresh**.
3. Create a new GPO named **Beth's GPO**.
4. Try to link a GPO to the **Adatum.com** domain. **Link an Existing GPO** is still dimmed, because Beth can only link GPOs to the **IT OU**.
5. Link **Beth's GPO** to the **IT OU**.
6. Switch to the **Windows PowerShell** window.
7. In the **Windows PowerShell** window, type the following command, and then press Enter:

```
GPResult /r
```

8. In the output from the command, notice that both the **Computer** and the **User** settings are displayed.

**Check Your Knowledge**

Question	
Members of which built-in AD DS groups can create GPOs by default? (Select three.)	
Select the correct answer.	
<input type="checkbox"/>	Domain Admins
<input type="checkbox"/>	Account Operators
<input type="checkbox"/>	Enterprise Admins
<input type="checkbox"/>	GPO Admins
<input type="checkbox"/>	Group Policy Creator Owners

## Lesson 3

# Group Policy scope and Group Policy processing

A GPO is, by itself, a collection of configuration instructions that will be processed by the client-side extensions of computers. Until the GPO is scoped, it does not apply to any users or computers. The GPO's scope determines the client-side extensions of which computers will receive and process the GPO, and only the computers or users within the scope of a GPO will apply the settings in that GPO. Consequently, you must design the scoping of GPOs to your environment. In this lesson, you will learn about each of the mechanisms with which you can scope a GPO, and, in the process, you will learn about the concepts of Group Policy application, inheritance, and precedence.

## Lesson Objectives

After completing this lesson, you will be able to:

- Describe GPO links.
- Explain how to link GPOs.
- Describe Group Policy processing order.
- Explain how to configure GPO inheritance and precedence.
- Explain how to use security filtering to modify Group Policy scope.
- Describe WMI filters.
- Explain how to filter Group Policy application.
- Explain how to enable or disable GPOs and GPO nodes.
- Describe loopback policy processing.
- Describe considerations for slow links and disconnected systems.
- Explain how to identify when settings become effective.

## What are GPO links?

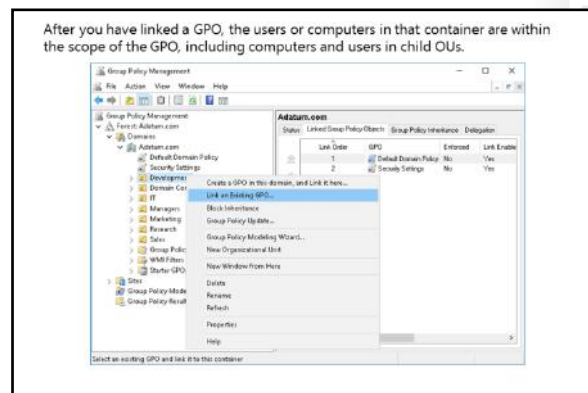
You can link a GPO to one or more AD DS sites, domains, or OUs. After you have linked a GPO, the users or computers in that container are within the scope of the GPO, including computers and users in child OUs.

### Linking a GPO

To link a GPO, either:

1. Right-click the domain or OU in the GPMC console tree, and then click **Link as existing GPO**.
2. If you have not yet created a GPO, click **Create A GPO In This {Domain | OU} And Link It Here**.

You can choose the same commands to link a GPO to a site, but by default, your AD DS sites are not visible in the GPMC. To show sites in the GPMC, right-click **Sites** in the GPMC console tree, and then click **Show Sites**. It is not possible to create and link a GPO to a site in one operation.





**Note:** A GPO that is linked to a site affects all computers in the site, without regard to the domain to which the computers belong, as long as all computers belong to the same Active Directory forest. Therefore, when you link a GPO to a site, that GPO can apply to multiple domains within a forest. Site-linked GPOs are stored on domain controllers in the domain in which you create the GPO. Therefore, domain controllers for that domain must be accessible for site-linked GPOs to be applied correctly. If you implement site-linked policies, you must consider policy application when planning your network infrastructure. You can either place a domain controller from the GPO's domain in the site to which the policy is linked or ensure that WAN connectivity provides accessibility to a domain controller in the GPO's domain.

When you link a GPO to a container, you define the initial scope of the GPO. Select a GPO, and then click the **Scope** tab to identify the containers to which the GPO is linked. In the details pane of the GPMC, the GPO links are displayed in the first section of the **Scope** tab.

The impact of the GPO's links is that the Group Policy Client service downloads the GPO if either the computer or the user objects fall within the scope of the link. The GPO is downloaded only if it is new or updated. Group Policy Client caches the GPO to make policy refresh more efficient.

### Linking a GPO to multiple OUs

You can link a GPO to more than one site or OU. It is common, for example, to apply a configuration to computers in several OUs. You can define the configuration in a single GPO and then link that GPO to each OU. If you later change settings in the GPO, your changes will apply to all OUs to which the GPO is linked.

### Deleting or disabling a GPO link

After you have linked a GPO, the GPO link appears in the GPMC underneath the site, domain, or OU. The icon for the GPO link has a small shortcut arrow. When you right-click the GPO link, a shortcut menu appears. To delete a GPO link, right-click the GPO link in the GPMC console tree, and then click **Delete**.

Deleting a GPO link does not delete the GPO itself, which remains in the **Group Policy Objects** container. However, deleting the link does change the scope of the GPO, so that it no longer applies to computers and users within the previously linked container object.

You also can modify a GPO link by disabling it. To disable a GPO link, right-click the GPO link in the GPMC console tree, and then clear the **Link Enabled** option. When you disable the link, you change the GPO scope so that it no longer applies to computers and users within that container. However, the link remains so that you can more easily re-enable it. You can recognize an unavailable link because it appears to be dimmed.

## Demonstration: Linking GPOs

In this demonstration, you will learn how to:

- Create and edit two GPOs.
- Link the GPOs to different locations.
- Disable a GPO link.
- Delete a GPO link.

## Demonstration Steps

### Create and edit two GPOs

1. Open **Group Policy Management**.
2. Create two new GPOs named **Remove Run Command** and **Do Not Remove Run Command**.
3. Edit the settings of the two GPOs.

### Link the GPOs to different locations

1. Link the **Remove Run Command** GPO to the domain. The **Remove Run Command** GPO is now attached to the **Adatum.com** domain.
2. Link the **Do Not Remove Run Command** GPO to the **IT OU**. The **Do Not Remove Run Command** GPO is now attached to the **IT OU**.
3. View the GPO inheritance on the **IT OU**. The **Group Policy Inheritance** tab shows the order of precedence for the GPOs.

### Disable a GPO link

1. Disable the **Remove Run Command** GPO on the **Adatum.com** domain.
2. Refresh the **Group Policy Inheritance** tab for the **IT OU**, and then notice the results in the details pane. The **Remove Run Command** GPO is no longer listed.

### Delete a GPO link

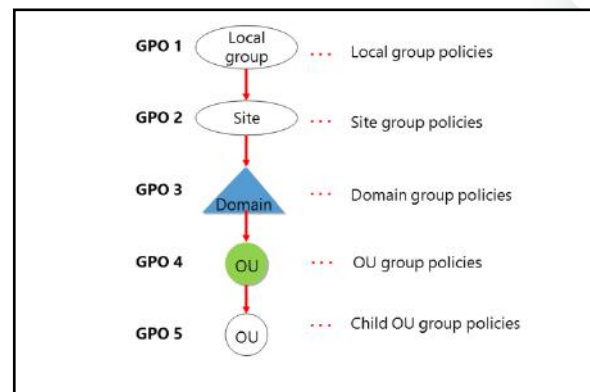
1. Select the **IT OU**, and then delete the **Do Not Remove Run Command** GPO link. Verify the removal of the **Do Not Remove Run Command** and the absence of the **Remove Run Command** GPOs.
2. Enable the **Remove Run Command** GPO on the **Adatum.com** domain. Refresh the **Group Policy Inheritance** window for the **IT OU**, and then notice the results in the details pane.

## Group Policy processing order

The GPOs that apply to a user, computer, or both do not all apply at once. Group Policy applies GPOs in a particular order. This order means that settings processed first might be overwritten by conflicting settings that are processed later.

Group Policy follows the following hierarchical processing order:

1. Local GPOs. Each computer that is running Microsoft Windows 2000 or newer has at least one local GPO. The local GPOs apply first.
2. Site GPOs. GPOs linked to sites apply second. If there are multiple site GPOs, they apply synchronously in the listed order.
3. Domain GPOs. GPOs linked to domains apply third. If there are multiple domain GPOs, they apply synchronously in the listed order.
4. OU GPOs. GPOs linked to top-level OUs apply fourth. If there are multiple top-level OU GPOs, they apply synchronously in the listed order.



5. Child OU GPOs. GPOs linked to child OUs apply fifth. If there are multiple child OU GPOs, they apply synchronously in the listed order. When there are multiple levels of child OUs, GPOs linked to higher-level OUs apply first and GPOs for the lower-level OUs apply next.

In Group Policy application, the general rule is that the last policy applied wins. For example, a policy that restricts access to **Control Panel** applied at the domain level could be reversed by a policy applied at the OU level for the objects contained in that particular OU.

If you link several GPOs to an OU, their processing occurs in the order that the administrator specifies on the OU's **Linked Group Policy Objects** tab in the GPMC. By default, processing is enabled for all GPO links. You can disable a container's GPO link to block the application of a GPO completely for a given site, domain, or OU. Note that if the same GPO is linked to other containers elsewhere in the AD DS hierarchy, the GPO will continue to process in those containers if the links are enabled.

You also can disable the user or the computer configuration section of a particular GPO independently of either the user or computer. If one section of a policy is known to be empty, disabling the other side will make policy processing marginally faster. For example, if you have a policy that only delivers user desktop configuration, you could disable the computer side of the policy.

## Configuring GPO inheritance and precedence

You can configure the same policy setting in more than one GPO, which can result in GPO conflicts. For example, you might enable a policy setting in one GPO, disable it in another, and then not configure it in a third. In this case, the precedence of the GPOs determines which policy setting the client applies. A GPO with higher precedence prevails over a GPO with lower precedence. Precedence is shown as a number in the GPMC. The smaller the number—that is, the closer to 1—the higher the precedence. Therefore, a GPO that has a precedence of 1 will prevail over other GPOs. Select the relevant AD DS container, and then click the **Group Policy Inheritance** tab to view the precedence of each GPO.

- The application of GPOs linked to each container results in a cumulative effect called *policy inheritance*:
  - Default precedence: Local → Site → Domain → OU → Child OU... (LSDOU)
  - Visible on the **Group Policy Inheritance** tab
- Link order (attribute of GPO link):
  - Lower number → Higher on list → Precedence
- Block Inheritance (attribute of OU):
  - Blocks the processing of GPOs from a higher level
- Enforced (attribute of GPO link):
  - Enforced GPOs override Block Inheritance
  - Enforced GPO settings win over conflicting settings in lower GPOs

When you enable or disable a policy setting in a GPO with higher precedence, the configured setting takes effect. However, remember that policy settings are set to **Not Configured**, by default. If a policy setting is not configured in a GPO with higher precedence, the enabled or disabled policy setting in a GPO with lower precedence will take effect.

You can link more than one GPO to an AD DS container object. The link order of GPOs determines the precedence of GPOs in such a scenario. GPOs with a higher link order take precedence over GPOs with a lower link order. When you select an OU in the GPMC, the **Linked Group Policy Objects** tab shows the link order of GPOs linked to that OU.

The default behavior of Group Policy is that GPOs linked to a higher-level container are inherited by lower-level containers. When a computer starts up or a user logs on, Group Policy Client examines the location of the computer or user object in AD DS and evaluates the GPOs with scopes that include the computer or user. Then, the client-side extensions apply policy settings from these GPOs. Policies apply sequentially, beginning with the policies linked to the site, followed by those linked to the domain, followed by those linked to OUs—from the top-level OU down to the OU in which the user or computer object exists. It is a layered application of settings, so a GPO that is applied later in the process, because it has higher precedence, overrides settings applied earlier in the process.



The sequential application of GPOs creates an effect called *policy inheritance*. Policies are inherited, so the resultant set of policies for a user or computer will be the cumulative effect of site, domain, and OU policies.

By default, inherited GPOs have lower precedence than GPOs linked directly to the container. For example, you might configure a policy setting to disable the use of registry-editing tools for all users in the domain by configuring the policy setting in a GPO linked to the domain. That GPO, and its policy setting, are inherited by all users within the domain. However, you probably want administrators to be able to use registry-editing tools, so you can link a GPO to the OU that contains administrators' accounts, and then configure the policy setting to allow the use of registry-editing tools. Because the GPO linked to the administrators' OU takes higher precedence than the inherited GPO, administrators will be able to use registry-editing tools.

### Precedence of Multiple Linked GPOs

If there are multiple GPOs linked to an AD DS container object, the object's link order determines their precedence.

To change the precedence of a GPO link:

1. Select the AD DS container object in the GPMC console tree.
2. Click the **Linked Group Policy Objects** tab in the details pane.
3. Select the GPO.
4. Use the **Up**, **Down**, **Move To Top**, and **Move To Bottom** arrows to change the link order of the selected GPO.

### Block inheritance

You can configure a domain or OU to prevent the inheritance of policy settings. This is known as *blocking inheritance*. To block inheritance, right-click the domain or OU in the GPMC console tree, and then select **Block Inheritance**.

The **Block Inheritance** option is a property of a domain or OU, so it blocks all Group Policy settings from GPOs linked to parents in the Group Policy hierarchy. For example, when you block inheritance on an OU, GPO application begins with any GPOs linked directly to that OU. Therefore, GPOs linked to higher-level OUs, the domain, or the site will not apply.

Use the **Block Inheritance** option sparingly because blocking inheritance makes it more difficult to evaluate Group Policy precedence and inheritance. With security group filtering, you can scope a GPO carefully so that it applies to only the correct users and computers in the first place, making it unnecessary to use the **Block Inheritance** option.

### Enforcing a GPO link

Additionally, you can set a GPO link to be **Enforced**. To enforce a GPO link, right-click the GPO link in the console tree, and then click **Enforced** on the shortcut menu. When you set a GPO link to **Enforced**, the GPO takes the highest level of precedence; policy settings in that GPO will prevail over any conflicting policy settings in other GPOs. Furthermore, a link that is enforced will apply to child containers even when those containers are set to **Block Inheritance**. The **Enforced** option causes the policy to apply to all objects within its scope. The **Enforced** option causes policies to override any conflicting policies and apply regardless of whether the **Block Inheritance** option is in use.

Enforcement is useful when you must configure a GPO that defines a configuration mandated by your corporate IT security and usage policies. Therefore, you should ensure that other GPOs do not override those settings. You can do this by enforcing the GPO's link.

## Evaluating precedence

To facilitate evaluation of GPO precedence, you can simply select an OU or domain, and then click the **Group Policy Inheritance** tab. This tab will display the resulting precedence of GPOs, accounting for GPO link, link order, inheritance blocking, and link enforcement. This tab does not account for policies that are linked to a site, nor does it account for GPO security or WMI filtering.

## Using security filtering to modify Group Policy scope

Although you can use the **Enforcement** and **Block Inheritance** options to control the application of GPOs to container objects, you might need to apply GPOs only to certain groups of users or computers rather than to all users or computers within the scope of the GPO. You cannot directly link a GPO to a security group, but there is a way to apply GPOs to specific security groups. The settings in a GPO apply only to users who have Allow Read and Allow Apply Group Policy permissions to the GPO.

- Apply Group Policy permission:
  - GPO has an ACL (**Delegation** tab → **Advanced**)
  - Members of the Authenticated Users group have Allow Apply Group Policy permissions by default
- To scope only to users in selected global groups:
  - Remove the Authenticated Users group
  - Add appropriate global groups: Must be global groups (GPOs do not scope to domain local)
- To scope to users except for those in selected groups:
  - On the **Delegation** tab, click **Advanced**
  - Add appropriate global groups
  - Deny the Apply Group Policy permission

Each GPO has an access control list (ACL) that defines permissions to the GPO. Two permissions, Allow Read and Allow Apply Group Policy, are required for a GPO to apply to a user or computer. For example, if a GPO is scoped to a computer by its link to the computer's OU, but the computer does not have Allow Read and Allow Apply Group Policy permissions, it will not download and apply the GPO. Therefore, by setting the appropriate permissions for security groups, you can filter a GPO so that its settings apply only to the computers and users that you specify.

By default, members of the Authenticated Users group receive the Allow Apply Group Policy permission on each new GPO. This means that by default, all users and computers are affected by the GPOs set for their domain, site, or OU, regardless of the other groups in which they might be members. Therefore, there are two ways of filtering GPO scope:

- Remove the Apply Group Policy permission—by default set to Allow—for the Authenticated Users group, but do not set this permission to Deny. Then, determine the groups to which the GPO should be applied and set the Read and Apply Group Policy permissions for these groups to Allow.
- Identify the groups that the GPO should not be applied to and then set the Apply Group Policy permission for these groups to Deny. If you deny the Apply Group Policy permission to a GPO, the user or computer will not be able to apply settings in the GPO, even if the user or computer is a member of another group that is granted the Apply Group Policy permission. These groups are also known as *exemption groups*.

You can use security group filtering to manage the scope of a GPO during testing. Instead of creating a child OU to manage the GPO's scope for testing, link the GPO to the location to which it belongs in production. However, instead of allowing the GPO to apply to Authenticated Users, or to the production security group, configure a security group specifically designed to limit the scope of the GPO to appropriate users and computers. The benefit of this practice is that it gives a much more realistic picture of how the GPO will perform in production because you are not artificially limiting its scope or precedence by linking it to a separate test OU. In other words, you get a better picture for how the GPO interacts with other GPOs that are already in production. And yet, you still maintain full control over the specific users and computers that are within the test's scope. You should set the security filtering on the GPO before you link it to the OU or domain.

## Filtering a GPO to apply to specific groups

To apply a GPO to a specific security group:


1. Select the GPO in the **Group Policy Objects** container in the console tree.
2. On the **Scope** tab, in the **Security Filtering** section, select the **Authenticated Users** group, and then click **Remove**.
3. Click **OK** to confirm the change.
4. Click **Add**.
5. Select the group to which you want the policy to apply, and then click **OK**.


## Filtering a GPO to exclude specific groups

The **Scope** tab of a GPO does not allow you to exclude specific groups. To exclude a group—that is, to deny the Apply Group Policy permission—you must use the **Delegation** tab.

To deny a group the Apply Group Policy permission:

1. Select the GPO in the **Group Policy Objects** container in the console tree.
2. Click the **Delegation** tab, and then click **Advanced**.
3. In the **Security Settings** dialog box, click **Add**.
4. Select the group that you want to exclude from the GPO.
5. Click **OK**. The group that you selected receives the Allow Read permission by default.
6. Clear the **Allow Read** permission check box.
7. Select the **Deny Apply Group Policy** check box.
8. Click **OK**. You receive a warning that Deny permissions override other permissions. Because Deny permissions override Allow permissions, we recommend that you use them sparingly. The warning message reminds you of this best practice. The process to exclude groups with the Deny Apply Group Policy permission is far more laborious than the process to include groups in the Security Filtering section of the **Scope** tab.
9. Click **Yes** to confirm that you want to continue.

 **Note:** Deny permissions are not available on the **Scope** tab. Unfortunately, when you exclude a group, the exclusion is not shown in the **Security Filtering** section of the **Scope** tab. This is one more reason to use Deny permissions sparingly.

 **Note:** If you remove the Authenticated Users group, and then scope a GPO to a specific group, users will not be able to read the policy to perform Group Policy management tasks. Be sure to assign appropriate personnel the Read permission to the GPO, but do not assign them the Apply Policy permission.

## What are WMI filters?

Administrators can use the Windows Management Instrumentation (WMI) management infrastructure technology to monitor and control managed objects in a network. A WMI query is capable of filtering systems based on characteristics, including random access memory (RAM), processor speed, disk capacity, IP address, operating system version, service pack level, installed applications, and printer properties. Because WMI exposes almost every property of every object within a computer, the list of attributes that you can use in a WMI query is virtually unlimited. WMI queries are written by using WMI Query Language (WQL).

- WMI queries can filter GPOs based on system characteristics, including:
  - RAM
  - Processor speed
  - Disk capacity
  - IP address
  - Operating system version
- WMI queries are written by using WQL, for example `select * from Win32_OperatingSystem where Version like "10.%"`
- WMI filters can be expensive in terms of Group Policy processing performance

You can use a WMI query to create a WMI filter, which you can use to filter a GPO. You can use Group Policy to deploy software applications and service packs. You might create a GPO to deploy an application and then use a WMI filter to specify that the policy should apply only to computers with a certain operating system and service pack. The WMI query to identify such systems is:

```
select * from Win32_OperatingSystem where Version like "10.%"
```

The query above returns true for computers that are running Windows 10 and Windows Server 2016.

When the Group Policy Client service evaluates GPOs that it has downloaded to determine which should be handed off to client-side extensions for processing, it performs the query against the local system. If the system meets the criteria of the query, the query result is a logical True, and the client-side extensions process the GPO.

WMI exposes namespaces, within which are classes that can be queried. Many useful classes, including **Win32\_OperatingSystem**, are found in a namespace called **root\CIMv2**.

To create a WMI filter:

1. Right-click the **WMI Filters** node in the GPMC console tree, and then click **New**. Type a name and description for the filter, and then click **Add**.
2. In the **Namespace** text box, type the namespace for your query or click **Browse** to select from available namespaces.
3. In the **Query** text box, type the query, and then click **OK**.

To filter a GPO with a WMI filter:

1. Select the GPO or GPO link in the GPMC console tree.
2. Click the **Scope** tab.
3. In the **WMI** drop-down list, select **WMI filter**.

You can filter a GPO with only a single WMI filter, but you can create a WMI filter with a complex query that uses multiple criteria. You can link a single WMI filter to one or more GPOs. The **General** tab of a WMI filter displays the GPOs that use the WMI filter. There are two significant caveats regarding WMI filters:

- First, the WQL syntax of WMI queries can be challenging to master. You often can find examples on the Internet when you search by using the keywords **WMI filter** and **WMI query** with a description of the query that you want to create.

- Second, WMI filters can negatively impact Group Policy processing performance. Because the Group Policy Client service must perform the WMI query at each policy processing interval, there is a slight impact on system performance every 90–120 minutes. With the performance of today's computers, the impact might not be noticeable. However, you should test the effects of a WMI filter prior to deploying it widely in your production environment. Also, some WMI queries are more expensive in terms of processing performance; querying for available disk space might take more time than querying for operating system version.



**Note:** A WMI query is processed only once, even if you use it to filter the scope of multiple GPOs.

## Demonstration: Filtering Group Policy application

In this demonstration, you will learn how to:

- Create a new GPO and link it to the **IT OU**.
- Filter Group Policy application by using security group filtering.
- Filter Group Policy application by using WMI filtering.

### Demonstration Steps

#### Create a new GPO and link it to the IT OU

1. Open **Group Policy Management Console** on **LON-DC1**.
2. Create a new GPO named **Remove Help menu**, and then link it to the **IT OU**.
3. Modify the settings of the GPO to remove the **Help** entry from the **Start** menu.

#### Filter Group Policy application by using security group filtering

1. Remove the **Authenticated Users** entry from the **Security Filtering** list for the **Remove Help** menu GPO in the **IT OU**.
2. Add the user **Beth Burke** to the security-filtering list. Now, only Beth Burke has the Apply Policy permission.

#### Filter Group Policy application by using WMI filtering

1. Create a WMI filter named **OS Version filter**.
2. Add the following query to the filter:

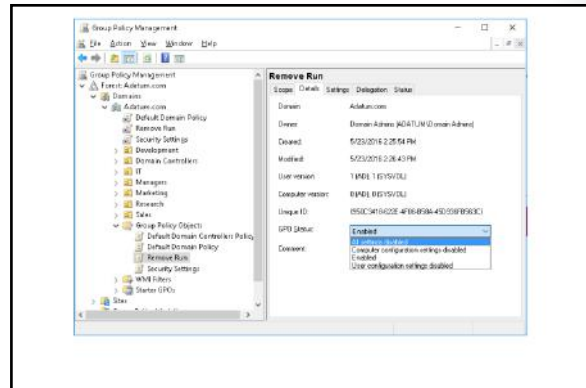
```
select * from Win32_OperatingSystem where Version like "6.%"
```

3. Save the query as **OS Version filter**.
4. Create a new GPO named **Software Updates**, and then link it to the **IT OU**.
5. Modify the policy's properties to use the OS Version filter.
6. Close Group Policy Management Console.

## How to enable or disable GPOs and GPO nodes


You can prevent the settings in the **Computer Configuration** node or **User Configuration** nodes from processing during policy refresh by changing the **GPO Status** option. This is useful if you want to optimize the processing of GPOs or you want to disable a specific part of a GPO for troubleshooting.

To enable or disable a GPO's nodes, select the GPO or GPO link in the console tree, click the **Details** tab (shown in the image on the slide), and then select one of the following option from the **GPO Status** drop-down list:



- **Enabled.** Both the computer configuration settings and user configuration settings will be processed by client-side extensions during policy refresh.
- **All Settings Disabled.** Client-side extensions will not process the GPO during policy refresh.
- **Computer Configuration Settings Disabled.** During computer policy refresh, computer configuration settings in the GPO will not be applied.
- **User Configuration Settings Disabled.** During user policy refresh, user configuration settings in the GPO will not be applied.

You can configure GPO status to optimize policy processing. For example, if a GPO contains only user settings, then setting the **GPO Status** option to disable computer settings prevents the Group Policy Client service from attempting to process the GPO during computer policy refresh. Because the GPO contains no computer settings, there is no need to process the GPO, and you can save a few processor cycles.

 **Note:** You can define a configuration that should take effect in the event of an emergency, security incident, or other disasters in a GPO, and then link the GPO so that it is scoped to appropriate users and computers. Then, disable the GPO. If you require the configuration to be deployed, enable the GPO. You should then use the GPMC to force a policy refresh on all computers.

## Loopback policy processing

By default, a user's settings come from GPOs that are scoped to the user object in AD DS. Regardless of which computer the user signs in to, the resultant set of policies that determine the user's environment is the same. There are situations, however, in which you might want to configure some different Group Policy settings that affect a user, depending on the computer that he or she uses. For example, you might want to standardize and lock user desktops when users sign in to computers in closely managed environments, such as conference rooms, reception areas,

- Provides the ability to apply user Group Policy settings based on the computer to which the user is signing in
- **Replace mode:**
  - Only the list of GPOs based on the computer object is used
- **Merge mode:**
  - The list of the GPOs based on the computer have higher precedence than the list of GPOs based on the user
- Useful in closely managed environments and special-use computers, such as:
  - Terminal servers, public-use computers, and classrooms



laboratories, classrooms, and kiosks. This also is important for Virtual Desktop Infrastructure scenarios, including remote virtual machines and Remote Desktop Services.


Imagine a scenario in which you want to enforce a standard corporate appearance for Windows-based desktops on all the computers in conference rooms and other public areas of your office. How will you manage this configuration centrally by using Group Policy? Policy settings that configure desktop appearance are located in the **User Configuration** node of a GPO. Therefore, by default, the settings apply to users, regardless of which computer they sign in to. Default policy processing does not give you a way to scope user settings to apply to computers, regardless of which user signs in. That is how loopback policy processing can be useful.

*Loopback policy processing* alters the default algorithm that the Group Policy Client service uses to obtain the ordered list of GPOs that should be applied to a user's configuration. Normally the **User Configuration** node of the GPOs scoped to the user object determine the user configuration. When you enable loopback policy processing, it is the **User Configuration** node of the GPOs scoped to the computer object that determine the user configuration.

Similar to all policy settings in the **Administrative Templates** section of a GPO, the **Configure user Group Policy loopback processing mode** policy setting that is located in the **Computer Configuration \Policies\Administrative Templates\System\Group Policy** folder in the **Group Policy Management Editor** window can be set to **Not Configured, Enabled, or Disabled**.

When enabled, the policy can specify the Replace or Merge mode:

- **Replace.** This mode replaces the GPO list for the user entirely by the GPO list already obtained for the computer at computer startup. The settings in the **User Configuration** node of the computer's GPOs apply to the user. The Replace mode is useful in a situation such as a classroom where users should receive a standard configuration, rather than the configuration applied to those users in a less managed environment.
- **Merge.** This mode appends the GPO list obtained for the computer at computer startup to the GPO list obtained for the user when signing in. Because the GPO list obtained for the computer apply later, settings in GPOs on the computer's list have precedence if they conflict with settings in the user's list. This mode is useful for applying additional settings to users' typical configurations. For example, you might allow a user to receive their typical configuration when signing in to a computer in a conference room or reception area but replace the wallpaper with a standard picture and disable the use of certain applications or devices.

 **Note:** When you combine loopback processing with security group filtering, the application of user settings during policy refresh uses the computer's credentials to determine which GPOs to apply as part of the loopback processing. However, the signed-in user also must have the Apply Group Policy permission for the GPO to be applied successfully. Also, the loopback processing flag is configured on a per-session basis, rather than per GPO.

## Considerations for slow links and disconnected systems

By default, only some of the settings that you can configure with Group Policy will apply if the speed of the link that the user's computer has with your domain network is too slow. For instance, deploying software by using GPOs would be inappropriate over slower links. Furthermore, it is important to consider the effect of Group Policy on computers that are disconnected from the domain network.

- **Slow link detection:**
  - By default, connection speeds below 500 kbps
  - The following CSEs apply by default:
    - Security Settings
    - Administrative Templates
- **Disconnected computers:**
  - Cache Group Policy so that settings still apply
  - Perform Group Policy refresh when reconnecting with the domain network if a background refresh has been missed

### Slow links

The Group Policy Client service addresses the issue of slow links by detecting the connection speed to the domain and by determining whether the connection should be considered a slow link. Each CSE determine whether to apply settings. The software extension, for example, is configured to forgo policy processing so that software is not installed if a slow link is detected.



**Note:** By default, a link is considered slow if it is less than 500 kilobits per second (Kbps). However, you can configure this to a different speed.

If Group Policy detects a slow link, it sets a flag to indicate the slow link to the client-side extensions. The client-side extensions then can detect whether to process the applicable Group Policy settings. The following table describes the default behavior of the client-side extensions.


Client-side extension	Slow link processing	Can it be changed?
Registry policy processing	On	No
Internet Explorer maintenance	Off	Yes
Software Installation policy	Off	Yes
Folder Redirection policy	Off	Yes
Scripts policy	Off	Yes
Security policy	On	No
Internet Protocol security (IPsec) policy	Off	Yes
Wireless policy	Off	Yes
Encrypting File System recovery policy	On	Yes
Disk quota policy	Off	Yes



## Disconnected computers

If a user is working while disconnected from the network, the settings previously applied by Group Policy continue to take effect. That way, a user's experience is identical, regardless of whether he or she is on the network or not. There are exceptions to this rule—most notably that startup, shutdown, logon, and logoff scripts will not run if the user is disconnected.

If a remote user connects to the network, the Group Policy Client wakes up and then determines whether a Group Policy refresh was missed. If so, it performs a Group Policy refresh to obtain the latest GPOs from the domain. Again, the client-side extensions determine, based on their policy processing settings, whether settings in those GPOs are applied.

 **Note:** This process does not apply to the Windows XP or Windows Server 2003 and earlier operating systems. It applies only to Windows Vista and later and Windows 2008 and later operating systems.

## Identifying when settings become effective

You must complete several processes before Group Policy settings actually apply to a user or a computer. This topic discusses these processes.

### GPO replication must occur

Before a GPO can take effect, the Group Policy container in AD DS must replicate to the domain controller from which the Group Policy Client service obtains its ordered list of GPOs.

Additionally, the Group Policy template in SYSVOL must replicate to the same domain controller.


- GPO replication must occur
- Group changes must replicate
- Group Policy refresh must occur
- User must sign out and sign in or the computer must restart
- You must perform a manual refresh
- Most CSEs do not reapply unchanged GPO settings

### Group changes must replicate

If you have added a new group or changed the membership of a group that is used to filter the GPO, then that change also must be replicated. Furthermore, the change must be in the security token of the computer and the user, which requires a restart for the computer to update its group membership or a sign-in and a sign-out for the user to update their group membership.

### User or computer Group Policy refresh must occur

Group Policy refresh happens at startup for computer settings, at sign-in for user settings, and every 90–120 minutes thereafter by default.

 **Note:** Remember that the practical impact of the Group Policy refresh interval is that when you make a change in your environment, it will be, on average, one-half that time, or 45–60 minutes before the change starts to take effect.

By default, Windows XP, Windows Vista, Windows 7, Windows 8, Windows 8.1 and Windows 10 clients perform only background refreshes at startup and sign-in, which means that a client might start up and a user might sign in without receiving the latest policies from the domain. We highly recommend that you change this default behavior so that policy changes implement in a managed, predictable way. Enable the policy setting **Always Wait For Network At Startup And Logon for all Windows clients**. The setting is located in **Computer Configuration\Policies\Administrative Templates\System\Logon**. Be sure to read the policy setting's explanatory text. This does not affect the startup or sign-in time for computers

that are not connected to a network. If the computer detects that it is disconnected, it does not wait for a network.

### User must sign out and sign in or computer must restart

Although most settings apply during a background policy refresh, some client-side extensions do not apply the setting until the next startup or logon event. For example, newly added startup and logon script policies do not run until the next computer startup or logon. Software installation will occur at the next startup if the software is assigned in computer settings. Changes to Folder Redirection policies will not take effect until the next logon.

### You must manually refresh Group Policy

When you experiment with Group Policy processing, you need to initiate a Group Policy refresh manually so that you do not have to wait for the next background refresh. You can use the **gpupdate** command to initiate a Group Policy refresh. Used on its own, this command triggers processing identically to a Group Policy background refresh. Both the computer policy and the user policy are refreshed. Use the **/target:computer** or **/target:user** parameter to limit the refresh to computer or user settings, respectively. During background refresh, by default, settings are applied only if the GPO has been updated. The **/force** switch causes the system to reapply all settings in all GPOs scoped to the user or computer. Some policy settings require a sign-out or restart before they take effect. The **/logoff** and **/boot** switches of **gpupdate** cause a sign-out or restart, respectively. You can use these switches when you apply settings that require a sign-out or restart.

For example, the command that will cause a total refresh application, and if necessary, restart and sign-in to apply updated policy settings, is:

```
gpupdate /force /logoff /boot
```

### Most client-side extensions do not reapply settings if the GPO has not changed

Remember that most client-side extensions apply settings in a GPO only if the GPO version has changed. This means that if a user can change a setting that Group Policy originally specified, then the setting will not be brought back into compliance with the settings that the GPO specifies until the GPO changes. Fortunately, most policy settings cannot be changed by a non-administrative user. However, if a user is an administrator of his or her computer, or if the policy setting affects a part of the registry or the system that the user has permissions to change, then this could be a real problem.

You have the option of instructing each client-side extension to reapply the settings of GPOs, even if the GPOs have not been changed. You can configure the processing behavior of each client-side extension in the policy settings found in **Computer Configuration\Administrative Templates\System\Group Policy**.

**Question:** Verify the correctness of the statement by placing a mark in the column to the right.

Statement	Answer
It is possible to link more than one WMI filter to a GPO.	

**Check Your Knowledge**

Question	
Which of the following options can you configure in the GPMC to change the default Group Policy processing order? (Select all that apply.)	
Select the correct answer.	
<input type="checkbox"/>	WMI filters
<input type="checkbox"/>	Security filtering
<input type="checkbox"/>	Block inheritance
<input type="checkbox"/>	Enforce
<input type="checkbox"/>	Loopback processing

## Lab A: Implementing a Group Policy infrastructure

### Scenario

Your manager asked you to use Group Policy to implement standardized security settings to lock computer screens when users leave computers unattended for 10 minutes or more. You also have to configure a policy setting that will prevent access to certain programs on local computers.

You configured Group Policy to lock computer screens when users leave computers unattended for 10 minutes or more. However, after some time, you were made aware that a critical application used by the Research engineering team fails when the screen saver starts. An engineer asked you to prevent the GPO setting from applying to any member of the Research security group. He also asked you to configure conference room computers to be exempt from corporate policy. However, you must ensure that the conference room computers use a 2-hour time out.

Create the policies that you need to evaluate the RSoPs for users in your environment. Make sure to optimize the Group Policy infrastructure and verify that all policies are applied as they were intended.

### Objectives

After completing this lab, you will be able to:

- Create and configure GPOs.
- Manage GPO scope.

### Lab Setup

Estimated Time: **40 minutes**

Virtual machines: **20742A-LON-DC1, 20742A-LON-DC2, 20742A-LON-CL1**

User name: **Adatum\Administrator**

Password: **Pa\$\$w0rd**

For this lab, you need to use the available virtual machine environment. Before you begin the lab, you must complete the following steps:

1. On the host computer, start **Hyper-V Manager**.
2. In Hyper-V Manager, click **20742A-LON-DC1**, and in the **Actions** pane, click **Start**.
3. In the **Actions** pane, click **Connect**. Wait until the virtual machine starts.
4. Sign in by using the following credentials:
  - o User name: **Administrator**
  - o Password: **Pa\$\$w0rd**
  - o Domain: **Adatum**
5. Repeat steps 2 and 4 for **20742A-LON-DC2**.
6. Repeat steps 2 and 3 for **20742A-LON-CL1**. Do not sign in to **LON-CL1** until directed to do so.

## Exercise 1: Creating and configuring GPOs

### Scenario

Your manager asked you to use Group Policy to implement standardized security settings to lock computer screens when users leave computers unattended for 10 minutes or more. She also asked you to configure a policy setting that will prevent access to registry-editing tools on local computers.

The main tasks for this exercise are as follows:

1. Create and edit a GPO.
2. Link the GPO.
3. View the effects of the GPO's settings.

#### ► Task 1: Create and edit a GPO

1. On **LON-DC1**, from **Server Manager**, open **Group Policy Management Console**.
2. Create a GPO named **ADATUM Standards** in the **Group Policy Objects** container.
3. Edit the **ADATUM Standards** policy, and then navigate to **User Configuration\Policies\Administrative Templates\System**.
4. Prevent users from accessing the registry by enabling the **Prevent access to registry editing tools** policy setting.
5. Navigate to the **User Configuration\Policies\Administrative Templates\Control Panel\Personalization** folder, and then configure the **Screen saver timeout** policy to **600 seconds**.
6. Enable the **Password protect the screen saver** policy setting, and then close the **Group Policy Management Editor** window.

#### ► Task 2: Link the GPO

- Link the **ADATUM Standards** GPO to the **Adatum.com** domain.

#### ► Task 3: View the effects of the GPO's settings

1. Sign in to **LON-CL1** as **Adatum\Administrator** with the password **Pa\$\$w0rd**.
2. Open Control Panel. In **Windows Firewall**, allow **Remote Event Log Management** and **Windows Management Instrumentation (WMI)** traffic.
3. Sign out and then sign in as **Adatum\Connie** with the password **Pa\$\$w0rd**.
4. Attempt to change the screen saver wait time and resume settings. You are prevented from doing this by Group Policy.
5. Attempt to run **Registry Editor**. You are prevented from doing this by Group Policy.

**Results:** After completing this exercise, you should have created, edited, and linked the required GPO successfully.

## Exercise 2: Managing GPO scope

### Scenario

You used Group Policy to implement standardized security settings to lock computer screens when users leave computers unattended for 10 minutes or more. However, after some time, an engineer informed you that a critical application used by the Research engineering team fails when the screen saver starts. He asked you to prevent the GPO setting from applying to any member of the Research security group. He also asked you to configure conference room computers to be exempt from corporate policy. However, you must ensure that the conference room computers always use a 2-hour time out.

The main tasks for this exercise are as follows:

1. Create and link the required GPOs.
2. Verify the order of precedence.
3. Configure the scope of a GPO with security filtering.
4. Configure loopback processing.
5. Prepare for the next lab.

#### ► Task 1: Create and link the required GPOs

1. On **LON-DC1**, in **Group Policy Management Console**, create a new GPO named **Research Application Override** that is linked to the **Research** OU.
2. Configure the **Screen saver timeout** policy setting to be disabled, and then close the **Group Policy Management Editor** window.

#### ► Task 2: Verify the order of precedence

- In the **Group Policy Management Console** tree, select the **Research** OU, and then click the **Group Policy Inheritance** tab. Notice that the **Research Application Override** GPO has precedence over the **ADATUM Standards** GPO. The screen saver time-out policy setting that you just configured in the **Research Application Override** GPO will be applied after the setting in the **ADATUM Standards** GPO. Therefore, the new setting will overwrite the standards setting and will prevail. Screen saver time-out will be unavailable for users within the scope of the **Research Application Override** GPO.

#### ► Task 3: Configure the scope of a GPO with security filtering

1. On **LON-DC1**, in Group Policy Management Console, select the **Research Application Override** GPO. Notice that in the **Security Filtering** section, the GPO applies by default to all authenticated users.
2. In the **Security Filtering** section, remove **Authenticated Users** and add the **Research** group.

#### ► Task 4: Configure loopback processing

1. On **LON-DC1**, in **Group Policy Management Console**, create a new OU named **Kiosks** under the domain.
2. Under **Kiosks**, create a child OU named **Conference Rooms**.
3. Create a new GPO named **Conference Room Settings**, and then link it to the **Conference Rooms** OU.
4. Edit the **Conference Room Settings** GPO, and then modify the **Screen saver timeout** policy to launch the screen saver after 120 minutes.

5. In the **Computer Configuration** section of the GPO, modify the **Configure user Group Policy loopback processing mode** policy setting to use **Merge mode**.

**Results:** After completing this exercise, you should have configured the required scope of the GPOs successfully.

► **Task 5: Prepare for the next lab**

- After you finish this lab, leave the virtual machines running for the next lab.

**Question:** Many organizations rely heavily on security group filtering to scope GPOs, rather than linking GPOs to specific OUs. In these organizations, GPOs typically are linked very high in the Active Directory logical structure—to the domain itself or to a first-level OU. What advantages do you gain by using security group filtering rather than GPO links to manage a GPO's scope?

**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?

**Question:** Do you use loopback policy processing in your organization? In which scenarios and for which policy settings can loopback policy processing add value?

## Lesson 4

# Troubleshooting the application of GPOs

With the interaction of multiple settings in multiple GPOs scoped by using a variety of methods, Group Policy application can be complex to analyze and understand. Therefore, you must equip yourself to evaluate and troubleshoot your Group Policy implementation effectively. You must be able to identify potential problems before they arise and solve unforeseen challenges. Windows Server operating systems provides indispensable tools for supporting Group Policy. In this lesson, you will explore the use of these tools in both proactive and reactive troubleshooting and support scenarios.

### Lesson Objectives

After completing this lesson, you will be able to:


- Explain how to refresh GPOs.
- Describe Resultant Set of Policy (RSOP).
- Explain how to generate RSOP reports.
- Perform an analysis with Group Policy Modeling Wizard.
- Explain how to examine Group Policy event logs.
- Detect issues with the health of GPOs.

### Refreshing GPOs

Computer configuration settings apply at startup and are refreshed at regular intervals. Any startup scripts run at computer startup. The default interval is every 90 minutes plus a random time between 0 and 30 minutes, but this period of time is configurable. The exception to the set interval is domain controllers, which have their settings refreshed every five minutes.

User settings are applied at sign-in and are refreshed at regular, configurable intervals—the default also is 90 minutes plus a random time between 0 and 30 minutes. Any logon scripts run at sign-in.

- When you apply GPOs, remember that:
  - Computer settings apply at startup
  - User settings apply at sign-in
  - Policies refresh at regular, configurable intervals
  - Security settings refresh at least every 16 hours
  - Policies refresh manually by using:
    - The **gpupdate** command-line utility
    - The Windows PowerShell cmdlet **Invoke-gpupdate**
  - With the Remote Group Policy Refresh feature, you can refresh policies remotely

 **Note:** A number of user settings require two sign-ins before the user sees the effect of the GPO. This is because users who sign in to the same computer use cached credentials to speed up sign-ins. This means that although the policy settings are being delivered to the computer the user is signed in already and the settings will therefore not take effect until the next sign-in. The **Folder Redirection** setting is an example of this.


You can change the refresh interval by configuring a Group Policy setting. For computer settings, you can find the refresh interval setting in the **Computer Configuration\Policies\Administrative Templates\System\Group Policy** node. For user settings, you can find the refresh interval in the corresponding settings under **User Configuration**. An exception to the refresh interval is security settings. The security



settings section of Group Policy is refreshed at least every 16 hours, regardless of the interval that you set for the refresh. This is not configurable via Group Policy.

You can also refresh Group Policy manually. The command-line utility **gpupdate** refreshes and delivers any new Group Policy configurations and removes settings that no longer apply. The **gpupdate /force** command refreshes all the Group Policy settings. A new Windows PowerShell **Invoke-gpupdate** cmdlet also performs the same function, but the cmdlet requires the Active Directory module to be installed. The advantage of the cmdlet is that you can use it to refresh Group Policy on other computers than the one you are signed in to by using the **-Computer** parameter.

You cannot push Group Policy settings to a client. The client always pulls the settings from the domain controller. A feature introduced in Windows Server 2012 is the possibility to remotely start a Group Policy Refresh. With this feature, administrators can use the GPMC to target an OU and force a Group Policy refresh on all of its computers and currently signed-in users. To do this, you right-click an OU, and then click **Group Policy Update**. The update occurs within 10 minutes. You will see a command-line window open when the refresh is executing on the client.

 **Note:** Sometimes, the failure of a GPO to apply is a result of problems with the underlying technology that is responsible for replicating AD DS and SYSVOL. In Windows Server 2016, you can view the replication status by using the GPMC, selecting the **Domain** node, clicking the **Status** tab, and then clicking **Detect Now**.

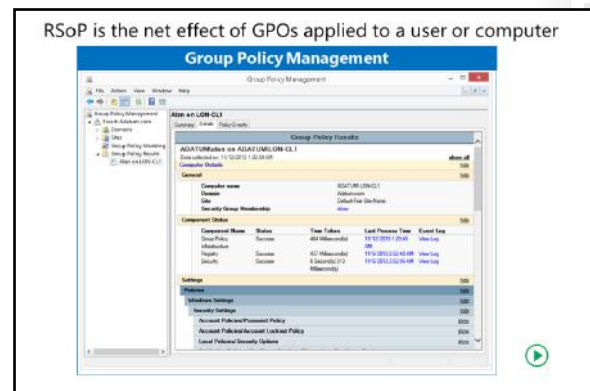
## What is RSoP?

Group Policy inheritance, filters, and exceptions are complex, and it often is difficult to determine which policy settings will apply. *Resultant Set of Policy* (RSoP) is the net effect of GPOs applied to a user or computer, taking into account GPO links, exceptions such as Enforced and Block Inheritance, the application of security and WMI filters, slow links, and loopback processing.

RSoP also is a collection of tools that help you evaluate, model, and troubleshoot the application of Group Policy settings. RSoP can query a local or remote computer and report back the exact settings that were applied to the computer and to any user who has logged on to the computer. RSoP also can model the policy settings that are anticipated to be applied to a user or computer under a variety of scenarios, including moving the object between OUs or sites or changing the object's group membership. With these capabilities, RSoP can help you manage and troubleshoot conflicting policies.

Windows Server 2016 provides the following tools for performing RSoP analysis:

- **Group Policy Results Wizard**
- **Group Policy Modeling Wizard**
- **GPResult.exe**



## Generating RSoP reports


To help you analyze the cumulative effect of GPOs and policy settings on a user or computer in your organization, the GPMC includes **Group Policy Results Wizard**. If you want to understand exactly which policy settings apply to a user or a computer and why they were applied, then **Group Policy Results Wizard** is the tool to use.

### Generating RSoP reports with Group Policy Results Wizard

**Group Policy Results Wizard** can reach into the WMI provider on a local or remote computer that is running Windows Vista or newer operating systems. The WMI provider can report everything there is to know about the way Group Policy was applied to the system. It can report when processing occurred, which GPOs were applied, which GPOs were not applied and why, errors that were encountered, and the exact policy settings and source GPOs that took precedence.

Several requirements for running **Group Policy Results Wizard** are as follows:

- The target computer must be online.
- You must have administrative credentials on the target computer.
- The target computer must be running a Windows XP or newer operating system.
- You must be able to access WMI on the target computer. This means that the computer must be online, connected to the network, and accessible through ports 135 and 445.

 **Note:** Performing RSoP analysis by using **Group Policy Results Wizard** is just one example of remote administration. To perform remote administration, you might need to configure inbound rules for the firewall that your clients and servers use.

- The WMI service must be started on the target computer.
- If you want to analyze RSoP for a user, that user must have signed in at least once to the computer. It is not necessary for the user to be signed in at the moment you run the Group Policy Results Wizard.

After the requirements have been met, you are ready to run an RSoP analysis. To run an RSoP report:

1. Right-click **Group Policy Results** in the **Group Policy Management Console** tree, and then click **Group Policy Results Wizard**.
2. **Group Policy Results Wizard** prompts you to select a computer. It then connects to the WMI provider on that computer and provides a list of users that have signed in to it. You then can select one of the users, or you can skip RSoP analysis for user configuration policies.

- RSoP reports show the actual settings being applied to the user and computer
- Might show the time taken to apply Group Policy
- You can generate RSoP reports by using:
  - **Group Policy Results Wizard**
  - **GPResults**
  - **Get-GPResultantSetOfPolicy**
- Target computer must be online
- Remote WMI must be enabled



3. **Group Policy Results Wizard** produces a detailed RSoP report in dynamic HTML format. If Microsoft Internet Explorer **Enhanced Security Configuration** is configured, you will be prompted to allow the console to display the dynamic content. You can expand or collapse each section of the report by clicking the **Show** or **Hide** links or by double-clicking the heading of the section. The report is displayed on three tabs:
  - **Summary.** The **Summary** tab displays the status of Group Policy processing at the last refresh. You can identify information that was collected about the system, the GPOs that were applied and denied, security group membership that might have affected GPOs filtered with security groups, WMI filters that were analyzed, and the status of client-side extensions.
  - **Settings.** The **Settings** tab displays the RSoP settings applied to the computer or user. This tab shows you exactly the settings that are applied to the user and/or computer through the effects of your Group Policy implementation. You can access a large amount of information from the **Settings** tab, although some data is not reported, including IPsec, wireless, and disk quota policy settings.
  - **Policy Events.** The **Policy Events** tab displays Group Policy events from the event logs of the target computer.
4. After you generate an RSoP report with **Group Policy Results Wizard**, right-click the report to rerun the query, print the report, or save the report as an XML file or an HTML file that maintains the dynamic expanding and collapsing sections. You can open both file types with Internet Explorer, so the RSoP report is portable outside the GPMC.

If you right-click the node of the report itself, under the **Group Policy Results** node in the console tree, you can switch to **Advanced View**. In **Advanced View**, RSoP displays by using the RSoP snap-in, which exposes all the applied settings, including IPsec, wireless, and disk quota policies.

### Generating RSoP reports by using GPRresult.exe

The **GPRresult.exe** command is the command-line version of **Group Policy Results Wizard**. **GPRresult** uses the same WMI provider as the wizard and produces the same information. You can even use it to create the same graphical reports. **GPRresult** runs on Windows Vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016.

When you run the **GPRresult** command, you are likely to use the following options. Each option is followed by its description.

```
/s computername
```

This option specifies the name or IP address of a remote system. If you use a dot (.) as the computer name, or do not include the **/s** option, the RSoP analysis is performed on the local computer.

```
/scope [user | computer]
```

This displays RSoP analysis for user or computer settings. If you omit the **/scope** option, RSoP analysis includes both user and computer settings.

```
/user username
```

This specifies the name of the user for which you want to display RSoP data.

```
/r
```

This option displays a summary of RSoP data.

```
/v
```

This option displays verbose RSoP data, which presents the most meaningful information.

```
/z
```

This displays additional verbose data, including the details of all policy settings applied to the system. Often, this is more information than you will require for typical Group Policy troubleshooting.

```
/u domain\user/p password
```

This provides credentials that are in the Administrators group of a remote system. Without these credentials, **GPResult** runs by using the credentials that you used to sign in.

```
[/x | /h] filename
```

This option saves the reports in XML or HTML format.

### Troubleshooting Group Policy with Group Policy Results Wizard or GPResult.exe

As an administrator, you likely will encounter scenarios that require Group Policy troubleshooting. You might need to diagnose and solve problems, including:

- GPOs are not being applied at all.
- The RSoPs for a computer or user are not what was expected.

**Group Policy Results Wizard** and **GPResult.exe** often will provide the most valuable insight into Group Policy processing and application problems. Remember that these tools examine the WMI RSoP provider to report exactly what happened on a system. Examining the RSoP report often will point you to GPOs that are scoped incorrectly or policy processing errors that prevented the application of GPO settings.

### Using Windows PowerShell to Manage RSoP Reports

You also can use Windows PowerShell to manage RSoP. You use the **Get-GPResultantSetofPolicy** cmdlet to generate RSoP reports. For example, the following command generates a report for the specified computer (**Adatum.com\LON-CL1**) and user (Alan) in HTML format and saves it to the specified file:

```
Get-GPResultantSetofPolicy -user Alan -computer Adatum\LON-CL1 -reporttype html -path c:\Report.html
```

### Demonstration: Performing a what-if analysis with Group Policy Modeling Wizard

If you move a computer or user between sites, domains, or OUs, or change their security group membership, then the GPOs scoped to that user or computer will often change. Therefore, the RSoP for the computer or user will be different. The RSoP also will change if a slow link or loopback processing occurs or if there is a change to a system characteristic that a WMI filter targets.

Before you make any of these changes, you should evaluate the potential impact that these changes will have on the RSoP. You can use **Group Policy Results Wizard** to perform RSoP analysis only on what has actually happened. To predict the future and to perform what-if analyses, you can use **Group Policy Modeling Wizard**. To perform Group Policy modeling, right-click the **Group Policy Modeling** node in the **Group Policy Management Console** tree, click **Group Policy Modeling Wizard**, and then go through the pages in the wizard to model the what-if analysis.

Modeling is performed by conducting a simulation on a domain controller, so the wizard first asks you to select a domain controller. You do not need to be signed in locally to the domain controller, but the modeling request will be performed on the domain controller. Next, the wizard asks you to specify the settings for the simulation. You must:

- Select a user or computer object to evaluate or specify the OU, site, or domain to evaluate.
- Choose whether slow link processing should be simulated.
- Specify whether to simulate loopback processing and, if so, choose Replace or Merge mode.
- Select a site to simulate.
- Select security groups for the user and for the computer.
- Choose which WMI filters to apply in the simulation of user and computer policy processing.

When you have specified the simulation's settings, the wizard produces a report that is very similar to the **Group Policy Results Wizard** report discussed earlier. The **Summary** tab shows an overview of which GPOs will be processed, and the **Settings** tab details the policy settings that will be applied to the user or computer. You can also save this report by right-clicking it, and then clicking **Save Report**.

### Demonstration

In this demonstration, you will learn how to:

- Use **GPRresult.exe** to create a report.
- Use **Group Policy Reporting Wizard** to create a report.
- Use **Group Policy Modeling Wizard** to create a report.

### Demonstration Steps

#### Use GPRresult.exe to create a report

1. On **LON-DC1**, open a **Command Prompt** window.
2. Run the following two commands:

```
Gprresult /r  
Gprresult /h results.html
```

3. Open the **Results.html** report in Internet Explorer, and then review the report.

#### Use Group Policy Reporting Wizard to create a report

1. Close the **Command Prompt** window, and then open **Group Policy Management Console**.
2. From the **Group Policy Results** node, open **Group Policy Results Wizard**.
3. Complete the wizard by using the default settings.
4. Review the report, and then save the report to the desktop.

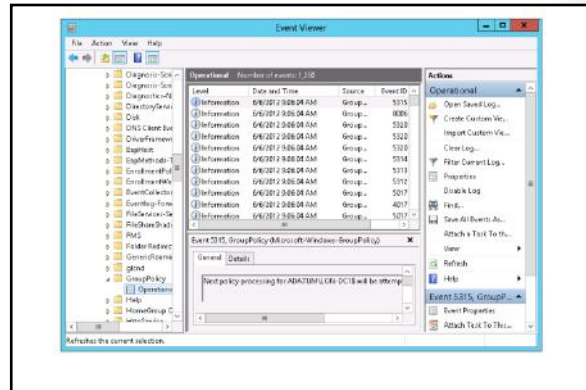
#### Use Group Policy Modeling Wizard to create a report

1. From the **Group Policy Modeling** node, open **Group Policy Modeling Wizard**.
2. Specify the user for the report as **Beth Burke** and the computer container as the **IT** OU.
3. Complete the wizard by using the default settings, and then review the report.
4. Close Group Policy Management Console.

## Examining Group Policy event logs

Windows Vista and later and Windows 2008 and later improve your ability to troubleshoot Group Policy, not only with RSoP tools, but also with improved logging of Group Policy events. Group Policy event logs include the:

- System log. You can find high-level information about Group Policy, including errors created by the Group Policy Client service when it cannot connect to a domain controller or locate GPOs.
- Application log. You can capture events recorded by client-side extensions.
- Group Policy operational log. This log provides detailed information about Group Policy processing.



To find Group Policy logs, open the **Event Viewer** snap-in or console. The System and Application logs are in the **Windows Logs** node. The Group Policy Operational log is found in

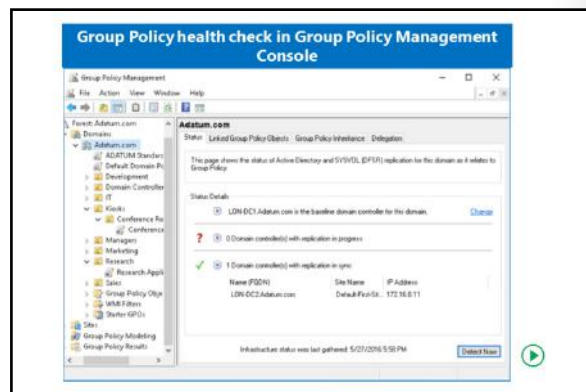
**Applications And Services Logs\Microsoft\Windows\Group Policy\Operational**. You can download the Group Policy Log View tool to create an HTML file containing all events relating to one Group Policy refresh.

 **Additional Reading:** To download Group Policy Log View, go to: <http://aka.ms/E8oi7g>

## Detecting Group Policy health issues

The Group Policy infrastructure has to perform optimally for you to apply policy settings to computers and users correctly. In very large enterprises with thousands of GPOs spread across multiple locations and time zones, there could be a significant replication delay between domain controllers.

A mismatch in version numbers between the Group Policy container and the Group Policy template of a GPO might indicate an issue with Group Policy. In Group Policy Management Console, you can create a report displaying the overall health state of the Group Policy infrastructure for a domain. You can also display the health of a single GPO.



The **Status** tab on the domain in Group Policy Management Console can display information that indicates the health of the Group Policy infrastructure. The information displayed on the tab contains information regarding to domain controllers, GPO replication, and GPO versioning. The health status helps you find any irregularities.

You can perform a health analysis on either the entire domain or on a single GPO. You perform the task from the **Status** tab on the domain or selected GPO by clicking **Detect Now**. You choose which domain controller you want to select as the baseline. Group Policy Management Console then compares both the

Group Policy container and the Group Policy template on all the domain controllers in the selected domain with the baseline domain controller.

The analysis performs the following comparisons:

- Permissions for each Group Policy container
- Version number for each Group Policy template
- Number of Group Policy container objects
- Permissions on each Group Policy template
- Version number stored for each Group Policy container
- Number of Group Policy template folders and files
- Hash information for each file in all Group Policy templates

If Group Policy Management Console cannot contact a domain controller during the analysis, or if a domain controller is not consistent with the domain controller used as a baseline, then Group Policy Management Console adds the analyzed domain controller to the **Domain controller(s) with replication in progress** list.

## Lab B: Troubleshooting Group Policy infrastructure

### Scenario

After configuring settings for the Research department and computers in the conference rooms, you want to make sure that all settings apply as intended. You want to do this by creating RSoP reports from both Group Policy Management Console and a client. You do not have access to a computer in the conference rooms, so you have to simulate how settings will apply by using Group Policy modeling analyses. You want to investigate what events are stored in Event Viewer regarding Group Policy. You have heard about a feature that can discover any errors in the Group Policy infrastructure and want to make sure that both domain controllers have the same information regarding Group Policy.

After some time, you receive a Help desk ticket opened by a user. The issue is that the Screen Saver settings that was applied is not the correct settings for the user. You have to investigate the issue and make sure that the correct settings apply to the user.

### Objectives

After completing this lab, you will be able to:

- Verify GPO application.
- Troubleshoot GPOs.

### Lab Setup

Estimated Time: **40 minutes**

Virtual machines: **20742A-LON-DC1**, **20742A-LON-DC2**, **20742A-LON-CL1**

User name: **Adatum\Administrator**

Password: **Pa\$\$w0rd**

For this lab, you need to use the available virtual machine environment. Before you begin the lab, you must complete the Lab A. Also, ensure that the following virtual machines are running. To start each virtual machine, use the following steps:

1. On the host computer, start **Hyper-V Manager**.
2. In Hyper-V Manager, click **20742A-LON-DC1**, and in the **Actions** pane, click **Start**.
3. In the **Actions** pane, click **Connect**. Wait until the virtual machine starts.
4. Sign in by using the following credentials:
  - User name: **Administrator**
  - Password: **Pa\$\$w0rd**
  - Domain: **Adatum**
5. Repeat steps 2 and 4 for **20742A-LON-DC2**.
6. Repeat steps 2 and 3 for **20742A-LON-CL1**. Do not sign in to **LON-CL1** until directed to do so.



## Exercise 1: Verifying GPO application

### Scenario

After configuring settings for the Research department and computers in the conference rooms, to make sure that all settings apply as intended, you need to create RSoP reports from both Group Policy Management Console and a client. You do not have access to a computer in the conference rooms, so you have to simulate how settings will apply by using Group Policy modeling analyses. You also need investigate what events are stored in Event Viewer regarding Group Policy.

The main tasks for this exercise are as follows:

1. Perform RSoP analysis.
2. Analyze RSoP with GPRresult.
3. Evaluate GPO results by using Group Policy Modeling Wizard.
4. Review policy events and determine GPO infrastructure status.

### ► Task 1: Perform RSoP analysis

1. On **LON-CL1**, verify that you are still signed in as **Adatum\Connie**. If necessary, use the password **Pa\$\$w0rd**.
2. Open a command prompt.
3. Run the **gpupdate /force** command.
4. After the command has completed, make a note of the current system time, which you will need to know for a task later in this lab:

Time

5. Restart **LON-CL1**, and then wait for it to restart before proceeding with the next task.
6. On **LON-DC1**, switch to **Group Policy Management Console**.
7. Use **Group Policy Results Wizard** to run an RSoP report for Connie on **LON-CL1**.
8. Review 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.
9. Click the **Details** tab. Review the settings that were applied during user and computer policy application, and then identify the GPO from which the settings were obtained.
10. Click the **Policy Events** tab, and then locate the event that logs the policy refresh that you triggered with the **gpupdate** command.
11. Click the **Summary** tab, right-click the page, and then choose **Save Report**. Save the report as an HTML file on your desktop. Then open the RSoP report in Internet Explorer from the desktop.

### ► Task 2: Analyze RSoP with GPRresult

1. Sign in to **LON-CL1** as **Adatum\Connie** with the password **Pa\$\$w0rd**.
2. At a command prompt, run the **gprresult /r** command. RSoP summary results are displayed. The information is very similar to the **Summary** tab of the RSoP report that was produced by **Group Policy Results Wizard**.
3. At the command prompt, type **gprresult /v | more**, and then press Enter. A more detailed RSoP report is produced. Notice that many of the Group Policy settings that were applied by the client are listed in this report.

4. At the command prompt, type **gpresult /z | more**, and then press Enter. The most detailed RSoP report is produced.
5. At the command prompt, type **gpresult /h:"%userprofile%\Desktop\RSOP.html"**, and then press Enter. An RSoP report is saved as an HTML file to your desktop.
6. Open the saved RSoP report from your desktop. Compare the report, its information, and its formatting with the RSoP report that you saved in the previous task.
7. Sign out of **LON-CL1**.

► **Task 3: Evaluate GPO results by using Group Policy Modeling Wizard**

1. On **LON-DC1**, in **Group Policy Management Console**, open **Group Policy Modeling Wizard**.
2. Select **Adatum\Connie** as the user and **LON-CL1** as the computer for modeling.
3. When prompted, select the **Loopback Processing** check box, and then click **Merge**. Even though the **Conference Room Settings** GPO specifies loopback processing, you must instruct **Group Policy Modeling Wizard** to include loopback processing in its simulation.
4. When prompted, on the **Alternate Active Directory Paths** page, select the **Conference Rooms** location. You are simulating the effect of **LON-CL1** as a conference room computer.
5. Accept all other options as defaults.
6. On the **Summary** tab, scroll to, and if necessary expand, **User Details**, expand **Group Policy Objects**, and then expand **Applied GPOs**.
7. Check whether the **Conference Room Settings** GPO applies to Connie as a User policy when she signs in to **LON-CL1**, if **LON-CL1** is in the **Conference Rooms** OU.
8. Scroll to, and if necessary expand, **User Details\Policies\Administrative Templates \Control Panel\Personalization**.
9. Confirm that the screen saver timeout is 7,200 seconds (2 hours)—the setting configured by the **Conference Room Settings** GPO that overrides the 10-minute standard configured by the **ADATUM Standards** GPO.

► **Task 4: Review policy events and determine GPO infrastructure status**

1. Switch to **LON-CL1**. Sign in as **Adatum\Administrator** with the password **Pa\$\$w0rd**.
2. Open **Event Viewer**.
3. Go to the **System** log located under **Windows Logs**, and sort events by the **Source** column.
4. Locate event **1500**, **1501**, **1502**, or **1503** with Group Policy as the source and review the information that is associated with Group Policy events.
5. In the console tree, go to the **Operational** log located under **Applications and Services Logs \Microsoft\Windows\Group Policy**.
6. Locate the first event related to the Group Policy refresh that you initiated in the first exercise with the **gpupdate** command. Review that event and the events that followed it.
7. Sign out of **LON-CL1**.
8. Switch to **LON-DC1**.
9. In the **Group Policy Management** window, check the Group Policy status for the domain.

10. Note that **LON-DC1.Adatum.com** is listed as the baseline domain controller and verify that **LON-DC2.Adatum.com** is listed as the domain controller with replication in sync. Some students might see **LON-DC2.Adatum.com** listed as a domain controller with replication in progress. This is due to the lab environment.

**Results:** After completing this exercise, you should have used the RSoP tools successfully to verify the correct application of your GPOs, examined Group Policy events, and verified the health of the Group Policy infrastructure.

## Exercise 2: Troubleshooting GPOs

### Scenario

A user has opened a Help desk ticket because the screen saver settings do not apply as intended. You have to investigate the issue and make sure that the correct settings apply to the user.

You must resolve the reported GPO application problem that Tier 1 help desk staff could not resolve.

Incident Record	
<b>Incident Reference Number: 604531</b>	
Date of Call	July 15
Time of Call	10:02
User	Connie Vaughn
Status	OPEN
<b>Incident Details</b>	
A user reports that the Research configuration does not apply to her anymore.	
<b>Additional Information</b>	
A user reports that suddenly she has a fixed time of 10 minutes before her screen saver activates. Because of an application that the Research department uses, she is unable to complete her work.	
<b>Plan of Action</b>	
<b>Resolution</b>	

The main tasks for this exercise are as follows:

1. Read the Help desk Incident Record and simulate the problem.
2. Update the Plan of Action section of the Incident Record.
3. Troubleshoot and resolve the problem.
4. Prepare for the next module.

► **Task 1: Read the Help desk Incident Record and simulate the problem**

1. Read Help desk Incident Record **604531** in the exercise scenario.
2. On **LON-DC1**, run the **E:\Labfiles\Mod05\Mod05-1.ps1** Windows PowerShell script.

► **Task 2: Update the Plan of Action section of the Incident Record**

1. Read the **Additional Information** section of the Incident Record above.
2. Update the **Plan of Action** section of the Incident Record above with your recommendations.

► **Task 3: Troubleshoot and resolve the problem**

1. On **LON-CL1**, sign in as **Adatum\Connie** with the password **Pa\$\$w0rd**.
2. Open **Control Panel**.
3. In Control Panel, click **Change Screen Saver**.
4. Verify that **Wait** is dimmed and has a value of **10 minutes**.
5. Sign out of **LON-CL1**.
6. Using your knowledge of Windows Server GPOs, and the tools available for troubleshooting GPOs, attempt to resolve the problem.
7. Update the **Resolution** section of the Incident Record.
8. If you are unable to resolve the problem, escalate it by asking your instructor for additional guidance.



**Note:** You have resolved the issue when Connie Vaughn's screen saver is not locked to 10 minutes.

**Results:** After completing this exercise, you will have resolved the GPO application problem.

► **Task 4: Prepare for the next module**

When you finish the lab, revert the virtual machines to their initial state. To do this, perform the following steps:

1. On the host computer, start **Hyper-V Manager**.
2. In the **Virtual Machines** list, right-click **20742A-LON-DC1**, and then click **Revert**.
3. In the **Revert Virtual Machine** dialog box, click **Revert**.
4. Repeat steps 2 and 3 for **20742A-LON-CL1** and **20742A-LON-DC2**.

**Question:** In what situations have you used RSoP reports to troubleshoot Group Policy application in your organization?

**Question:** In what situations have you used Group Policy modeling? If you have not done this yet, in what situations can you anticipate using Group Policy modeling?

## Module Review and Takeaways

### Review Questions

**Question:** You have assigned a logon script to an OU via Group Policy. The script is located in a shared network folder named **Scripts**. Some users in the OU receive the script and others do not. What might be the possible causes?

**Question:** What GPO settings apply across slow links by default?

**Question:** You must ensure that a domain-level policy is enforced, but the Managers group must be exempt from the policy. How would you accomplish this?

### Common Issues and Troubleshooting Tips

Common Issue	Troubleshooting Tip
Group Policy settings are not applied to all users or computers in an OU where a GPO is applied.	
Group Policy settings sometimes require two restarts to apply.	

**MCT USE ONLY. STUDENT USE PROHIBITED**

# Module 6

## Managing user settings with Group Policy

### Contents:

Module Overview	6-1
Lesson 1: Implementing administrative templates	6-2
Lesson 2: Configuring Folder Redirection, Software Installation, and Scripts	6-12
Lesson 3: Configuring Group Policy preferences	6-22
Lab: Managing user settings with Group Policy	6-29
Module Review and Takeaways	6-38

## Module Overview

By using Group Policy Objects (GPOs), you can implement standard desktop environments across your organization with administrative templates, Folder Redirection, Group Policy preferences, and software installation. It is important that you know how to use these Group Policy features so that you can configure your users' computer settings properly.

In this module, you will learn about administrative templates and using them to configure settings. You also will learn about configuring the Folder Redirection feature, and using GPOs to manage software, and apply and configure scripts. This module also covers the different Group Policy preferences and explains how you can use them to manage settings.

### Objectives

After completing this module, you will be able to:

- Implement administrative templates.
- Configure Folder Redirection, software installation, and scripts.
- Configure Group Policy preferences.

## Lesson 1

# Implementing administrative templates

Administrative template files provide the majority of available GPO settings, which modify specific registry keys. The use of administrative templates is known as *registry-based policy*, because all the settings you configure in administrative templates result in changes to the registry. For many apps, using registry-based policy is the simplest and best way to support the centralized management of policy settings. In this lesson, you will learn how to configure administrative templates.

### Lesson Objectives

After completing this lesson, you will be able to:

- Describe administrative templates.
- Describe .adm and .admx files.
- Describe the central store.
- Describe practical uses of administrative templates.
- Configure settings with administrative templates.
- Explain how to import security templates.
- Explain how to manage administrative templates.

### What are administrative templates?

You can use administrative templates to control the environment of an operating system and the user experience. There are two sets of administrative templates:

- User-related settings
- Computer-related settings

When you configure settings in the **Administrative Templates** node of the GPO, you make modifications to the registry. Administrative templates have the following characteristics:

- They are organized into subnodes that correspond to specific areas of the environment, such as network, system, and Windows-based components.
- The settings in the computer section of the **Administrative Templates** node edit the **HKEY\_LOCAL\_MACHINE** hive in the registry, and the settings in the user section of the **Administrative Templates** node edit the **HKEY\_CURRENT\_USER** hive in the registry.
- Some settings exist for both user and computer. For example, there is a setting to prevent Windows Live Messenger from running in both the user and the computer templates. In the case of conflicting settings, the computer setting will prevail.
- Some settings are available only to certain versions of Windows operating systems. For example, you can apply a number of new settings only to Windows 10. Double-clicking the setting displays the supported versions for that setting.

- Administrative templates give you the ability to control the environment of the operating system and the user experience.
- Administrative template section for computers:
  - Control Panel
  - Network
  - Printers
  - System
  - Windows-based components
- Administrative template section for users:
  - Control Panel
  - Desktop
  - Network
  - Start menu and taskbar
  - System
  - Windows-based components
- Each of these main sections contain many subfolders to further organize settings



The following table details the organization of the **Administrative Templates** node.

Administrative template section	Settings
<b>Computer Configuration</b>	<ul style="list-style-type: none"> <li>• <b>Control Panel</b></li> <li>• <b>Network</b></li> <li>• <b>Printers</b></li> <li>• <b>Server</b></li> <li>• <b>Start Menu and Taskbar</b></li> <li>• <b>System</b></li> <li>• <b>Windows Components</b></li> <li>• <b>All Settings</b></li> </ul>
<b>User Configuration</b>	<ul style="list-style-type: none"> <li>• <b>Control Panel</b></li> <li>• <b>Desktop</b></li> <li>• <b>Network</b></li> <li>• <b>Shared Folders</b></li> <li>• <b>Start Menu and Taskbar</b></li> <li>• <b>System</b></li> <li>• <b>Windows Components</b></li> <li>• <b>All Settings</b></li> </ul>

Most of the nodes contain multiple subfolders that enable you to organize settings even further into logical groupings. Even with this organization, finding the setting that you need might be a daunting task. The **All Settings** node contains an alphabetically sorted list of all settings contained in all the other nodes. Later in this lesson, you will learn how to filter settings in the **Administrative Templates** node to help you locate settings.

## What are .adm and .admx files?

All the settings in the **Administrative Templates** node of a GPO are stored in files. All currently supported operating systems store the settings in .admx files. Windows Server 2000 and Windows Server 2003 store the settings in .adm files. Later in this module, you will learn how to expand the number settings you can configure with **Administrative Templates** by adding additional files containing the settings.

### .adm files

Traditionally, *.adm files* define the settings that an administrator can configure through Group Policy.

Each successive Windows operating system and service pack has included a newer version of these files. The .adm files use their own markup language. Therefore, it is difficult to customize them.

- **.adm files:**
  - Are copied into every GPO in SYSVOL
  - Are difficult to customize
  - Are not language-neutral
  - Could cause SYSVOL bloat if there are many GPOs
- **.admx files:**
  - Are language-neutral
  - .adml files provide the localized language
  - Are not stored in the GPO
  - Are extensible through XML

The .adm files are located in the %SystemRoot%\Inf folder. The .adm files include both the settings and the plain language descriptions. Therefore, overwriting a .adm file in the SYSVOL could potentially change the text that you see when editing a GPO.

Another potential drawback of .adm files is that depending on client version, when you create them, they copy into every GPO and consume about 3 megabytes (MB) of space. While not enormous, this can cause the SYSVOL folder to become large and can increase replication traffic. With many GPOs in a domain, this could lead to what is known as *SYSVOL bloat* with SYSVOL taking up several gigabytes (GB) of space.

### .admx files

The Windows Vista and Windows Server 2008 operating systems introduced a new format for displaying registry-based policy settings. These settings use a standards-based XML file format known as *.admx files*. These new files replace .adm files. However, you can still use .adm files.

In all Windows operating systems since Windows Vista and Windows Server 2008, Group Policy continues to recognize the custom .adm files that you have in your existing environment, but ignores any .adm file that .admx files have superseded. Unlike .adm files, .admx files are not stored in individual GPOs. The Local Group Policy Editor automatically reads and displays settings from the local .admx file store. By default, .admx files are stored in the Windows\PolicyDefinitions folder, but they can be stored in a central location, which you will learn about in the next topic.

The .admx files are language-neutral. The plain language descriptions of the settings are not part of the .admx files. Instead, they are stored in language-specific *.adml files*. This means that administrators can look at the same GPO and see the policy descriptions in their own language because they can each use their own language-specific .adml files.

The .adml files are stored in subfolders of the PolicyDefinitions folder. Each language is stored in its own folder. For example, the **en-US** folder stores the English files, and the **es-ES** folder stores the Spanish files. By default, only the .adml language files for the language of the installed operating system are present.

## Overview of the central store

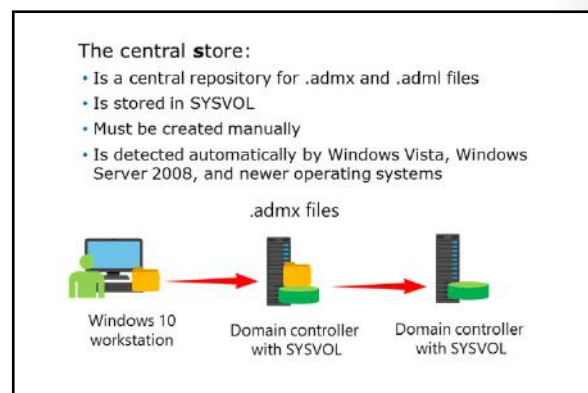
In domain-based enterprises, you can create a central store location for .admx files, which anyone with permissions to create or edit GPOs can access. The Group Policy Management Editor automatically reads and displays administrative templates policy settings from .admx files in the central store, and then ignores the .admx files stored locally. If the domain controller or central store is not available, the local store is used.

The advantages of creating the central store are:

- You ensure that whenever someone edits a GPO, the settings in the **Administrative Templates** node are always the same.
- When Microsoft releases .admx files for new operating systems, you only have to update the .admx files in one location.

You must create the central store manually, and then update it manually on a domain controller.

The use of .admx files is dependent on the operating system of the computer where you create or edit the GPO. Depending on your server's operating system and configuration, the domain controllers use File Replication Service or Distributed File System (DFS) Replication to replicate the data.



To create a central store for .admx and .adml files, create a folder and name it **PolicyDefinitions** in the following location: **\\FQDN\SYSVOL\FQDN\Policies**, where <FQDN> is the domain name for your Active Directory Domain Services (AD DS) domain. For example, to create a central store for the Test.Microsoft.com domain, create a **PolicyDefinitions** folder in the following location: **\\Test.Microsoft.Com\SYSVOL\Test.Microsoft.Com\policies**.

A user must copy all files and subfolders of the **PolicyDefinitions** folder, which on a Windows-based computer resides in the Windows folder. The **PolicyDefinitions** folder stores all .admx files, and subfolders store .adml files for all languages enabled on the client computer. For example, on a Windows Server 2016 server that has English enabled, **C:\Windows\PolicyDefinitions** will contain the .admx files and in the subfolder **en-US**, the .adml files will contain English-based descriptions for the settings defined in the .admx files.



**Note:** You must update the **PolicyDefinitions** folder for each service pack and for other additional software, such as Windows 10 Version 1511 and Microsoft Office 2016 .admx files.

## Discussion: Practical uses of administrative templates

Spend a few minutes examining the administrative templates. Consider how you could employ some of them in your organization.

Be prepared to share information about your organization's current use of GPOs and logon scripts, such as:

- How do you provide desktop security currently?
- How much administrative access do users have to their systems?
- Which Group Policy settings will you find useful in your organization?



**Question:** How do you provide desktop security currently?

**Question:** How much administrative access do users have to their systems?

**Question:** Which Group Policy settings will you find useful in your organization?

## Demonstration: Configuring settings with administrative templates

Group Policy editing tools in Windows Server 2016 provide several functionalities that aid GPO configuration and management. In this demonstration, you will review these options.

### Configuring an administrative templates setting

In the Group Policy Management Editor, you can configure a policy setting by double-clicking it. The policy setting **Properties** dialog box appears. Policy settings in administrative templates can have three states: **Not Configured**, **Enabled**, and **Disabled**. In a new GPO, every policy setting defaults to **Not Configured**. This means that the GPO does not modify the existing configuration of that particular setting for a user or computer.

The effect of the change depends on the policy setting. For example, if you enable the **Prevent Access To Registry Editing Tools** policy setting, users are unable to launch the Registry Editor, Regedit.exe. If you disable the policy setting, you ensure that users can launch the Registry Editor. Notice the double negative in this policy setting example: you disable a policy that prevents an action; therefore, you allow the action.

### Filter policy settings for administrative templates

A disadvantage of previous versions of Group Policy editing tools is the inability to search for a specific policy setting. With thousands of policies to choose from, it can be difficult to locate the exact setting that you want to configure. The Group Policy Management Editor in Windows Server 2016 solves this problem for settings in **Administrative Templates**. You now can create filters to locate specific policy settings.

To create a filter:

1. Right-click **Administrative Templates**, and then click **Filter Options**.
2. To locate a specific policy, select the **Enable keyword filters** check box, enter the words to filter with, and then select the fields in which to search.

You also can filter for Group Policy settings that apply to specific versions of the Windows operating system, Microsoft Internet Explorer, and other Windows-based components. However, the filter only applies to settings in the **Administrative Templates** node.

### Filter Based on Comments

You also can search and filter based on policy-setting comments. Windows Server 2016 enables you to add comments to policy settings in the **Administrative Templates** node. To do so, double-click a policy setting, and then click the **Comment** tab.

As a best practice, you should add comments to configured policy settings. You should document the justification for a setting and its intended effect. You also should add comments to the GPO itself. Windows Server 2016 enables you to attach comments to a GPO:

- In the Group Policy Management Editor, in the console tree, right-click the root node, click **Properties**, and then click the **Comment** tab.

### How to copy GPO settings

Starter GPOs can contain administrative templates policy settings only. In addition to using Starter GPOs, there are two other ways to copy settings from one GPO into a new GPO:

1. You can copy and paste entire GPOs in the Group Policy Objects container of the Group Policy Management Console (GPMC) so that you have a new GPO with all the settings of the source GPO.
2. To transfer settings between GPOs in different domains or forests, right-click a GPO, and then click **Back Up**. In the target domain, create a new GPO, right-click the GPO, and then click **Import Settings**. You will be able to import the settings of the backed up GPO.



**Additional Reading:** For more information, refer to: "Filtering Administrative Template Policy Settings" at: <http://aka.ms/Jcl669>



**Note:** Module 5, "Implementing Group Policy" explains Starter GPOs in detail.

In this demonstration, you will see how to:

- Configure a setting in **Administrative Templates**.
- Filter administrative templates policy settings.
- Add comments to policy settings.
- Add comments to a GPO.
- Create a new GPO by copying an existing GPO.
- Create a new GPO by importing settings that were exported from another GPO.

### Demonstration Steps

#### Configure an administrative templates policy setting

1. On **LON-DC1**, open the **GPMC**.
2. Create a new GPO named **GPO1**, and then open it.
3. Locate the **User Configuration\Policies \Administrative Templates\System** node.
4. Review the three possible values for the **Prevent access to the command prompt** setting.

#### Filter administrative templates policy settings

1. Filter the settings to display only those that contain the keywords **screen saver**, and examine the settings shown.
2. Filter the settings to display only configured values, and verify that no settings display.

#### Add comments to a policy setting

1. Open **User Configuration\Policies\ Administrative Templates\Control Panel**, and locate the **Personalization** value.
2. Add a comment to both the **Password Protect the screen saver** and **Enable screen saver** policy settings.

#### Add comments to a GPO

- Open the GPO1 policy root node, and then add a comment to the **Comment** tab.

#### Create a new GPO by copying an existing GPO

- Copy **GPO1**, and then paste it to the **Group Policy Objects** folder.

#### Create a new GPO by importing settings that were exported from another GPO

1. Back up **GPO1**.
2. Create a new GPO named **ADATUM Import**.
3. Import the settings from the **GPO1** backup into the **ADATUM Import** GPO.

## Importing security templates

Administrators often configure security settings in GPOs. Configuring security settings in a GPO can be tedious work, especially when configuring firewall rules because of the number of rules and settings that you need to configure.

*Security templates* are files that you use to manage and configure security settings on Windows-based computers. Depending on the various categories of security settings, the security templates consist of settings divided into logical sections. When you configure a security template, you can use it to configure a single computer, or to configure multiple computers on a network. You can configure and distribute security templates in several ways:

- Security Templates contain settings for:
  - Account policies
  - Local policies
  - Event log
  - Restricted groups
  - System services
  - Registry
  - File system
- More security settings are available in a GPO
- Security templates created in the Security Templates snap-in can be imported into a GPO
- The Security Compliance Manager can export security baselines in a GPO backup format

- **Secedit.exe** command-line tool. You can use Secedit.exe to compare the current configuration of a computer that is running Windows Server 2016 to specific security templates.
- **Security Templates snap-in.** You can use this snap-in to create a security policy by using security templates.
- **Group Policy.** You can use Group Policy to analyze and configure computer settings and to distribute specific security settings.
- **Security Compliance Manager.** You can use the Microsoft Security Compliance Manager to view security settings, compare settings to *security baselines* (which are groups of settings that are designed on Microsoft security guides and best practices), customize settings, and import or export GPO backups.

### Security Templates snap-in

You can use the Security Templates snap-in to configure security settings in the following sections:

- **Account Policies.** This section includes password, account-lockout, and Kerberos version 5 (v5) policies.
- **Local policies.** This section includes audit policies, user-right assignment, and security options.
- **Event log.** This section includes application, system, and security event log settings.
- **Restricted groups.** This section includes memberships of groups that have special rights and permissions.
- **System services.** This section includes startup and permissions for system services.
- **Registry.** This section includes permissions for registry keys.
- **File system.** This section includes permissions for folders and files.

You can use the snap-in either to save the .inf file to a known location, or to make a note of the standard location of Security Templates, which is the **Documents\Security\Templates** folder in the signed-in user's profile.

## Security Compliance Manager

The security settings for a computer consist of more than what you can configure in a security template. Because of this, using the Security Compliance Manager to configure security might be a better option. Microsoft updates the Security Compliance Manager with new security baselines that you can download and use in your own environment as is or change the settings to adapt to the security needs of your organization. You export the baselines you want to use as a GPO backup, and then import the backup by using either the GPMC or Windows PowerShell.



**Additional Reading:** For more information, refer to: "Security Compliance Manager (SCM)" at: <http://aka.ms/Ypdcmd>

## Import a security template into a GPO

Once you have created your security template, you can import the security template by doing the following:

1. In the GPMC, create a GPO.
2. Edit the GPO.
3. In the **Group Policy Management Editor**, go to the **Computer Configuration\Policies\Windows Settings\Security Settings** section of the GPO.
4. Right-click **Security Settings**, and then click **Import Policy**.
5. In the **Import Policy From** dialog box, select the security template file that you want to import, and then click **Open**.



**Note:** The GPO will now contain the security settings configured in the security template.

In previous versions of Windows Server, you could use the **Security Configuration Wizard** to examine Windows Server configuration, and then create a security policy based on that configuration. You could then convert the security policy to a GPO by using a command-line tool. The **Security Configuration Wizard** is no longer available in Windows Server 2016.

## Managing administrative templates

As discussed previously, administrative templates offer administrators thousands of configurable settings that you can deploy to computers or users. You also can extend the configurable set of administrative templates to include more settings that are not otherwise available. To extend the administrative templates, follow these four high-level steps:

1. Download the administrative templates or create a new custom template from scratch. Many vendors, including Microsoft and other third-party developers, offer free administrative template downloads. One popular administrative template is the Microsoft Office template. This administrative template allows you to customize settings specific to Office, including specific settings for each of the applications included in the Office suite.

- Extend the set of administrative templates by:
  1. Creating new templates or downloading available templates
  2. Adding the templates to the central store so the settings become available in all GPOs
  3. Configuring the settings in a GPO
  4. Deploying the GPO
- .admx files are available for both Microsoft and third-party applications
- Import legacy .adm files to the Administrative Templates section of a GPO

2. Add the administrative templates to the central store. Once you add the administrative templates for an application to the central store, a new folder or set of folders containing new settings becomes available for customization.
3. Customize the administrative template settings. You can customize the administrative template settings in the same way that you customize GPO settings. Using the familiar Group Policy Management Editor may make it easier for administrators to customize their applications.
4. Deploy the GPO along with the administrative template settings. Once deployed, you configure applications through the administrative template settings.

You should download the administrative templates in the .adm format to be able to update the central store. If the administrative templates for a given application are available only in .adm format, you can use the Microsoft Management Console (MMC) snap-in ADMX Migrator to convert the .adm file to a set of .admx and .adml files.



**Additional Reading:** For more information, refer to: "ADMX Migrator" at: <http://aka.ms/Ny5p5c>



**Additional Reading:** For more information, refer to: "Office 2016 Administrative Template files (ADMX/ADML) and Office Customization Tool" at: <http://aka.ms/Nknzlx>

You also can use .adm files to extend the set of administrative templates, but the settings will only be available in the GPO to which you import the .adm file. To extend the set of administrative templates with an .adm file use the following procedure:

1. In the GPMC, create a new GPO.
2. Edit the GPO.
3. In the **Group Policy Management Editor**, right-click the **Administrative Templates** node of the GPO, and then click **Add/Remove Templates**.
4. In the **Add/Remove Templates** dialog box, click **Add**.
5. In the **Policy Templates** dialog box, browse to the location of the .adm file that you want to import, select the file, and then click **Open**.



**Note:** The extra settings should now be available in **Administrative Templates**.



**Check Your Knowledge**

Question	
Which sections are available in the Administrative Templates node under the User Configuration node? (Select all that apply.)	
Select the correct answer.	
<input type="checkbox"/>	Desktop
<input type="checkbox"/>	Windows Components
<input type="checkbox"/>	Server
<input type="checkbox"/>	System
<input type="checkbox"/>	Control Panel

Verify the correctness of the statement by placing a mark in the column to the right.

Statement	Answer
You can create the central store through the GPMC.	<input type="checkbox"/>

## Lesson 2

# Configuring Folder Redirection, Software Installation, and Scripts

You can use GPOs to deploy scripts that run when users sign in or sign out and computers start up or shut down. You also can redirect folders that are included in users' profiles, to a central server. Using Group Policy for software installation enables you to manage software installation on client computers. These features enable you to configure users' desktop settings more easily, and where desirable, to create a standardized desktop environment that meets your organizational needs.

### Lesson Objectives

After completing this lesson, you will be able to:

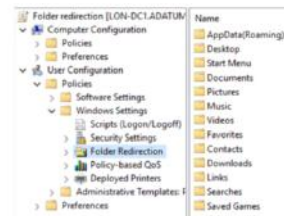
- Describe Folder Redirection.
- Explain the settings for configuring Folder Redirection.
- Describe security settings for redirected folders.
- Configure Folder Redirection.
- Manage software with Group Policy.
- Describe Group Policy settings for applying scripts.
- Configure scripts with GPOs.

### What is Folder Redirection?

*Folder Redirection* is a feature that allows folders to be located on a network server, but appear as if they are located on a local drive. You can use Folder Redirection to manage data effectively, and optionally back up data. By redirecting folders, you can ensure user access to data regardless of the computers to which the users sign in. Folder Redirection has the following characteristics:

- When you redirect folders, you change the folder's storage location from a computer's local hard drive to a shared folder on a network file server.
- After you redirect a folder to a file server, it still displays to the user as if it is stored on the local hard drive.
- You can use Offline Files technology with redirection to synchronize data in the redirected folder to the user's local hard drive. This ensures that users have access to their data even if a network outage occurs or if the user works offline.

- Folder Redirection allows folders to be located on a network server, but appear as if they are located on a local drive
- Folders that can be redirected in Windows Vista and later are:



Computers running Windows Vista and later can redirect the following folders:

- **AppData/Roaming**
- **Contacts**
- **Desktop**
- **Documents**
- **Downloads**
- **Favorites**
- **Links**
- **Music**
- **Pictures**
- **Saved Games**
- **Searches**
- **Start Menu**
- **Videos**

### Advantages of Folder Redirection

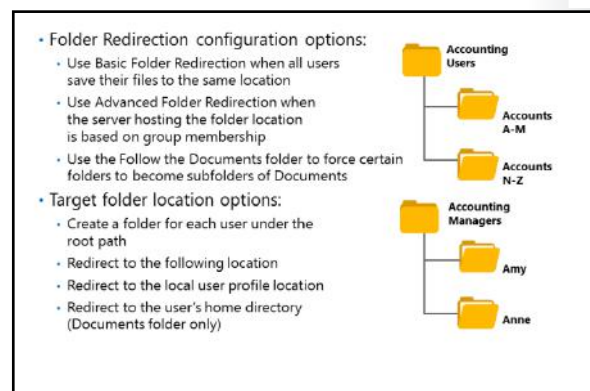
There are many advantages to Folder Redirection:

- Users who sign in to multiple computers can access their data providing they can access the network share.
- Offline folders allow users to access their data even if they disconnect from the local area network (LAN).
- You can easily back up data that is stored on servers.
- Redirecting data from the profile greatly reduces roaming profile sizes.
- In case of client machine replacement, there is less data to transfer.

### Settings for configuring Folder Redirection

In a GPO, the following settings are available for Folder Redirection:

- **None.** **None** is the default setting. With this setting, Folder Redirection is not enabled.
- **Basic.** The **Basic** setting is for:
  - Users who redirect their folders to a common area.
  - Users who need data to be private.
- **Advanced.** You can use the **Advanced** setting to specify different network locations for different Active Directory security groups.



- **Follow the Documents folder.** **Follow the Documents folder** is available only for the **Pictures**, **Music**, and **Videos** folders. This setting makes the affected folder a subfolder of the **Documents** folder.


### Target folder locations for Basic and Advanced settings

If you choose **Basic** or **Advanced** settings, you can choose from the following options:

- **Create a folder for each user under the root path.** This option creates a folder in the form `\\server\share\User account name\Folder name`. For example, if you want to store users' desktop settings in a shared folder called **Documents** on a server named **LON-DC1**, you would define the root path as `\\LON-DC1\Documents`. Each user has a unique path for the redirected folder to ensure that data remains private. By default, that user is granted exclusive rights to the folder. In the case of the **Documents** folder, the current contents of the folder move to the new location.
- Redirect to the following location. This option uses an explicit path for the redirection location. It causes multiple users to share the same path for the redirected folder. By default, that user is granted exclusive rights to the folder. In the case of the **Documents** folder, the current contents of the folder move to the new location.
- Redirect to the local user profile location. This option moves the location of the folder to the local user profile under the **Users** folder.
- Redirect to the user's home directory. This option is available only for the **Documents** folder.

### Removing Folder Redirection

If you decide to remove Folder Redirection, you also have to consider what to do with the data in the redirected folders. The default is to leave the data in the redirected folder. This might be the correct decision, but then you have to figure out a way to make the data available to the users again. The solution could be to create a mapped drive pointing to the redirected folder.

 **Note:** After you initially create and apply a GPO that delivers Folder Redirection settings, users require two sign-ins before redirection takes effect. Using the **Advanced** setting in Folder Redirection could require three sign-ins. This is because users will sign in with cached credentials. This is applicable only if **Fast Logon Optimization** is turned on, which is the default setting for Windows 7 and newer. To allow Folder Redirection settings to take effect with just one sign-in, the **Always wait for the network at computer startup and logon** setting has to be enabled. However, enabling this policy setting will degrade the overall user sign-in experience because it will take longer to sign in.

**Question:** Users in the same department often sign in to different computers. They need access to their **Documents** folders. They also need data to be private. What Folder Redirection setting would you choose?

## Security settings for redirected folders

You must create and configure permissions manually on a shared network folder to store redirected folders by using the permissions listed in the tables in this topic. If the users' redirected folders do not exist, Folder Redirection can create them.

Folder permissions are managed as follows:

- If you let Folder Redirection create the users' redirected folders, the correct subfolder permissions are set automatically.
- If you manually create folders, you must know the correct permissions to use.

NTFS permissions for root folder	
<b>Creator/Owner</b>	<b>Full control – subfolders and files only</b>
Administrator	None
Security group of users that save data on the share	List Folder/Read Data, Create Folders/Append Data-This Folder Only
Local System	Full control
Share permissions for root folder	
<b>Creator/Owner</b>	<b>Full control – subfolders and files only</b>
Security group of users that save data on the share	Full control
NTFS permissions for each user's redirected folder	
<b>Creator/Owner</b>	<b>Full control – subfolders and files only</b>
%Username%	Full control, owner of folder
Administrators	None
Local System	Full control

The tables below illustrate these permissions.

### NTFS file system permissions for root folder

Creator/Owner	Full Control – subfolders and files only
Administrator	None
Security group of users that save data on the share	List Folder/Read Data, Create Folders/Append Data-This Folder Only
System	Full Control

### Share permissions for root folder

Creator/Owner	Full Control – subfolders and files only
Security group of users that save data on the share	Full Control

### NTFS permissions for each user's redirected folder

Creator/Owner	Full Control – subfolders and files only
%Username%	Full Control, owner of folder
Administrators	Full Control
System	Full Control

## Demonstration: Configuring Folder Redirection

This demonstration shows how to:

- Create a shared folder for Folder Redirection.
- Create a GPO to redirect the Documents folder.
- Test Folder Redirection.

## Demonstration Steps

### Create a shared folder

1. On **LON-DC1**, create a folder named **C:\Redir**.
2. Share the folder with **Everyone**, and with **Read/Write** permission.

### Create a GPO to redirect the Documents folder

1. Open the **GPMC**.
2. Create a GPO named **Folder Redirection**, and then link it to the **Adatum** domain.
3. Edit the **Folder Redirection** GPO.
4. Configure the **Documents** folder properties to use the **Basic-Redirect everyone's folder to the same location** setting.
5. Ensure that the **Target folder location** is set to **Create a folder for each user under the root path**.
6. Specify the root path as **\\LON-DC1\Redir**.
7. Close all open windows on **LON-DC1**.

### Test Folder Redirection

1. Sign in to **LON-CL1** as **Adatum\Administrator** with password **Pa\$\$w0rd**.
2. Check the properties of the **Documents** folder. The path should now be **\\LON-DC1\Redir\Administrator**.
3. Sign out of **LON-CL1**.

## Managing software with Group Policy

Windows Server 2016 includes a feature called **Software Installation and Maintenance**, which AD DS, Group Policy, and the Windows Installer service use to install, maintain, and remove software from your organization's computers.

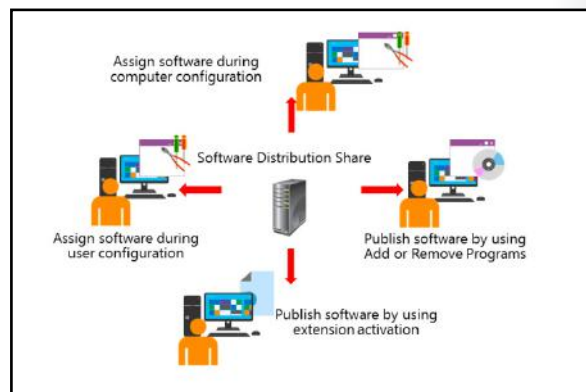
### How Group Policy software installation helps to address the software lifecycle

The software lifecycle consists of four phases: preparation, deployment, maintenance, and removal. You can use Group Policy to manage all phases, except for preparation. You can apply Group Policy settings to users or computers in a site, domain, or organizational unit (OU) to install, upgrade, or remove software automatically.

By applying Group Policy settings to software, you can manage the phases of software deployment without deploying software onto each computer individually. Using Group Policy to manage the software lifecycle has some advantages and some disadvantages, which are important to consider.

The advantages of using Group Policy to manage the software lifecycle are:


- Group Policy software installation is available as part of Group Policy and AD DS. Thus, using Group Policy does not incur any additional costs for your organization, and is always available to implement because it is already installed and ready for use.



- Group Policy software installation does not require client software, agent software, or additional management software. Instead, IT administrators can use familiar tools such as the GPMC and Group Policy Management Editor to manage the software lifecycle.
- Group Policy software installation is quick and easy to use. This allows for both faster software distribution and reduced IT training costs.

The disadvantages of using Group Policy to manage the software lifecycle are:

- Group Policy software installation has a minimal feature set. This minimal feature set limits the ability to control aspects of the distribution such as the day and time of installation, the order of installation when deploying multiple applications, and the restart process, such as reboot suppression or reboot windows.
- Group Policy software installation does not have any reporting. Thus, you cannot easily gather information such as how many computers have the distributed software, which computers installation failed on, or which computers do not have the distributed software. This could lead to a scenario in which you deploy an update to an application and the update attempts to install on computers that no longer have the application to be updated.
- Group Policy software installation is limited Windows Installer package deployments. Before being able to deploy the software by using Group Policy, IT administrators must convert any non-.msi installation programs into .msi packages.

 **Note:** For larger organizations, particularly organizations that have more than 500 computers, and for any organization with specific software distribution requirements, Microsoft System Center Configuration Manager provides enterprise-level features and control. Most large organizations will benefit from using Microsoft System Center Configuration Manager (Configuration Manager) instead of Group Policy software installation, because of the enterprise-level features and control that Configuration Manager provides.

Two deployment methods are available for delivering software to clients. Administrators can either install software for users or computers in advance by assigning the software, or give users the option to install the software when they require it by publishing the software in AD DS. Both the **User Configuration** and the **Computer Configuration** nodes of a GPO have a **Software Settings** node. You can add software to a GPO by adding a new package to the **Software Installation** node, and then specifying whether to assign or publish it.

You also can choose to apply advanced deployment for a package. Use this option to apply a customization file to a package for custom deployment—for example, if you use the Office Customization tool to create a setup customization file to deploy Microsoft Office.

### Assigning software

When you assign software to a user, the user's **Start** menu advertises the software when the user signs in. Installation does not begin until the user double-clicks either the application's icon or a file that is associated with the application.

Assigning software has the following characteristics:

- Users do not share assigned applications. When you assign software to a user, an application that you install for one user through Group Policy might not be available to other users. Assigning software to a user is preferred when the software is used by a subset of users, or when the software has licensing costs associated with it and you do not want to purchase licenses that are not necessary.

- When you assign an application to a computer, the application installs the next time that the computer starts. The application will be available to all users of the computer. Assigning software to a computer is preferred when you need to have the software installed on a specific set of computers or on all computers in an environment, regardless of which users use the computers. This is a common situation when using agent software, such as monitoring agents, security-related agents, or management agents.

### Publishing software

The **Programs\Programs and Features** shortcut in Control Panel advertises a published application to the user. Users can install the application by using the **Install a program from the network** shortcut, or extension activation can install the application. Extension activation will initiate the program installation when a user clicks on a file type that is associated with the program.

Publishing software has the following characteristics:

- Control Panel does not advertise applications to users who do not have permission to install them.
- You cannot publish applications to computers.

### Managing software updates

Software vendors release software updates to address (usually) minor fixes, such as performance updates or feature enhancements that do not warrant a complete application reinstallation. Microsoft releases some software updates as .msp files.

Major updates that provide new functionality require users to upgrade a software package to a newer version. You can open the GPO that deploys a software package, modify the software installation settings, and then use the **Upgrades** tab to upgrade a package. When you perform upgrades by using Group Policy, you will notice the following characteristics:

- You might redeploy a package if the original Windows Installer file has been modified.
- Upgrades will often remove the old version of an application and install a newer version. These upgrades usually maintain application settings.
- You can remove software packages if they were delivered originally by using Group Policy. This is useful if you are replacing a line-of-business (LOB) application with a different application. Removal can be mandatory or optional.

### Group Policy settings for applying scripts

You can use Group Policy scripts to perform a number of tasks. There might be actions that you need to perform every time a computer starts up or shuts down, or when users sign in or sign out. For example, you can use scripts to:

- Clean up desktops when users sign out and shut down computers.
- Delete the contents of temporary directories.
- Map drives or printers.
- Set environment variables.
- Assign scripts to the computer to run in the security context of the Local System account.
- Assign scripts to the user who is signing in to run in that user's security context.

- You can use scripts to perform many tasks, such as clearing page files, mapping drives, and clearing temp folders for users
- Scripts languages include VBScript, Jscript, Windows PowerShell, and command/batch files
- You can assign Group Policy script settings to assign:
  - For computers:
    - Startup scripts
    - Shutdown scripts
  - For users:
    - Logon scripts
    - Logoff scripts



Other Group Policy settings control aspects of how scripts run. For example, when assigning multiple scripts, you can control whether they run synchronously or asynchronously.

You can write scripts in any scripting language that the Windows client operating system can interpret, such as Microsoft Visual Basic, Scripting Edition (VBScript); JScript; or simple command or batch files.



**Note:** In all Windows operating systems since Windows Server 2008 R2 and Windows 7, the UI in the Local Group Policy Editor for Logon, Logoff, Startup, and Shutdown scripts provides an additional tab for Windows PowerShell command-line interface scripts. You can deploy your Windows PowerShell script by adding it to this tab. The operating systems can run Windows PowerShell scripts through Group Policy.

Scripts are stored in shared folders on the network. You need to make sure that the client has access to that network location. If clients cannot access the network location, the scripts fail to run. Although any network location stores scripts, as a best practice, use the Netlogon share because all users and computers that authenticate to AD DS have access to this location.

For many of these settings, using Group Policy preferences is a better alternative than configuring them in Windows images, or by using logon scripts. Group Policy preferences is covered in more detail later in this module.

## Demonstration: Configuring scripts with GPOs

This demonstration shows how to:

- Create a logon script to display a message.
- Create and link a GPO to use the script.
- Sign in to a client computer and test the results.

### Demonstration Steps

#### Create a logon script to display a message

1. On **LON-DC1**, start **Notepad**, type the following command, and then press Enter:

```
Msgbox "This is the script"
```

2. Save the file as **logon.vbs**.
3. Copy the file to the Clipboard.

#### Create and link a GPO to use the script

1. Use the **Group Policy Management Console** to create a new GPO named **User Logon Script**, and then link it to the **Adatum.com** domain.
2. Edit the GPO to configure a user logon script.
3. Paste the **Logon.vbs** script folder.
4. Add the **Logon.vbs** script to the logon scripts.

**Sign in to a client computer and test the results**

1. On **LON-CL1**, sign in as **Adatum\Administrator** with password **Pa\$\$word**.
2. Refresh the Group Policy settings on the client computer.
3. Sign in as **Adatum\Connie** with password **Pa\$\$word**.
4. Verify that the message dialog box displays. Note that this could take up to ten minutes to display. If the message does not appear, restart **LON-CL1** and repeat step one through three.
5. Sign out of **LON-CL1**.

**Check Your Knowledge**

Question	
Which of the following folders can you redirect by using Folder Redirection? (Select all that apply.)	
Select the correct answer.	
<input type="checkbox"/>	Documents
<input type="checkbox"/>	Favorites
<input type="checkbox"/>	AppData (Roaming)
<input type="checkbox"/>	AppData (Local)
<input type="checkbox"/>	Program Files

**Categorize Activity**

Categorize each item below.

Items	
1	Logon Scripts
2	Startup Scripts
3	Assign Software
4	Logoff Scripts
5	Shutdown Scripts
6	Folder Redirection
7	Publish Software

Category 1	Category 2	Category 3
User Configuration	Computer Configuration	User Configuration and Computer Configuration

## Lesson 3

# Configuring Group Policy preferences

Some organizations still use scripts that run when users sign in. These scripts typically deliver settings such as mapped drivers, printers, and registry changes.

Windows Server 2008 and newer operating systems include Group Policy preferences. You can configure settings such as mapped drives to deliver through Group Policy. Additionally, you can configure preferences by installing the Remote Server Administration Tools (RSAT) on a client computer that is running Windows 7 or later. This allows you to deliver many common settings by using Group Policy.

### Lesson Objectives

After completing this lesson, you will be able to:

- Describe Group Policy preferences.
- Compare Group Policy preferences and GPO settings.
- Describe features of Group Policy preferences.
- Configure Group Policy preferences.

### What are Group Policy preferences?

Group Policy preferences include more than 20 Group Policy extensions that expand the range of configurable settings within a GPO. You now can use Group Policy preferences to apply a number of settings that previously applied to scripts, such as drive mappings and shared printers.

Windows operating systems later than Windows Server 2008 and Windows Vista Service Pack 2 (SP2) and newer operating systems natively support Group Policy preferences.

Examples of the Group Policy extensions in Group Policy preferences are:

- Folder Options
- Drive Maps
- Registry
- Shortcuts
- Printers
- Scheduled Tasks
- Services
- Start Menu

Configuring Group Policy preferences does not require any special tools or software installation. Group Policy preferences are native parts of GPMC in Windows Server 2008 and newer, and they apply in the same manner as Group Policy settings by default. Preferences have two distinct sections: Windows Settings and Control Panel Settings.

Group Policy preferences extensions expand the range of configurable settings within a GPO:

- Enables you to manage settings that were previously not manageable by using Group Policy
- Are supported natively on Windows Server 2008 and newer and Windows Vista SP2 and newer
- Can be created, deleted, replaced, or updated
- Categories include mapped drives, shortcuts, registry changes, power options, schedules tasks, and Internet Explorer settings

When you configure a new preference, you can perform the following four basic actions for the user or computer:

- **Create.** Create a new preference setting.
- **Delete.** Remove an existing preference setting.
- **Replace.** Delete and recreate a preference setting. The result is that Group Policy preferences replace all existing settings and files associated with the preference item.
- **Update.** Modify an existing preference setting.

## Comparing Group Policy preferences and Group Policy settings

Group Policy preferences are similar to Group Policy settings in that they apply configurations to the user or computer. However, there are several differences in the way that you can configure and apply them. One of these differences is that preferences are not enforced, although you can configure them to reapply automatically.

The following list is of other differences between Group Policy settings and Group Policy preferences:

- Preferences are not enforced.
- Group Policy settings effectively disable the user interface for any settings that the policy manages. Preferences do not do this.
- Group Policy settings can apply at regular intervals. However, you can configure preferences to apply once only, or at the same intervals as Group Policy settings.
- End users can change any preference setting that applies through Group Policy, but Group Policy settings prevent users from changing them.
- In some cases, you can configure the same settings through a policy setting and a preference item. If conflicting preference and Group Policy settings configure and apply to the same object, the value of the policy setting always applies.

Group Policy settings	Group Policy preferences
Strictly enforce policy settings by writing the settings to areas of the registry that standard users cannot modify	Are written to the normal locations in the registry that the application or operating system feature uses to store the setting
Typically disable the user interface for settings that Group Policy is managing	Do not cause the application or operating system feature to disable the user interface for settings they configure
Refresh policy settings at a regular interval	Refresh preferences by using the same interval as Group Policy settings by default, but can be configured to apply only once



**Note:** While the Group Policy setting effectively disables the user interface for a given setting, if the user has the ability to edit the registry, the user can alter the setting.

## Features of Group Policy preferences

After you create a Group Policy preference, you must configure its properties. Different preferences will require different input information. For example, shortcut preferences require target paths, whereas environment variables require variable types and values. Preferences also provide a number of features in the common properties to assist in deployment.

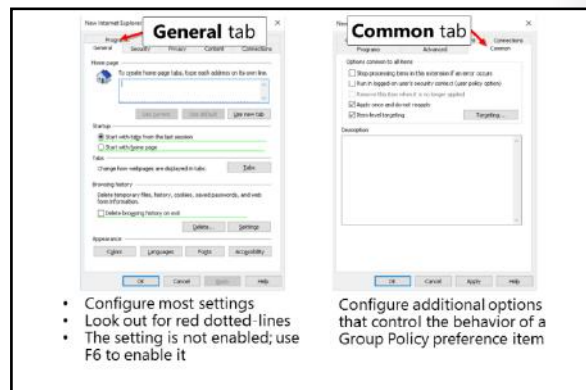
### General tab

You usually configure the basic settings of a preference in the **General** tab. Here, the first step is to specify the action for the preference: **Create**, **Delete**, **Replace**, or **Update**. Different settings will be available depending on the initial action selected. For example, when creating a drive mapping, you must provide a Universal Naming Convention (UNC) path and an option for the drive letter that you want to assign.

### Common tab

Common options are consistent for all preferences. You can use the **Common** tab to control the behavior of the preference as follows:

- **Stop processing items in this extension if an error occurs.** If an error occurs while processing a preference, no other preferences in this GPO will process.
- **Run in logged-on user's security context.** Preferences can run as the System account or the signed-in user. This setting forces preference items to run in the signed-in user context instead of the System account, and is useful when you configure mapped drives and shared printers where you want the user's credentials to connect to the resource.
- **Remove this item when it is no longer applied.** Unlike policy settings, preferences are not removed when the GPO that delivered it is removed. This setting will change that behavior. If you select this option, the action changes to **Replace**. Be careful when you use this option though, because Group Policy preferences changes the registry in the normal location, and unforeseen issues could occur if you use this option.
- **Apply once and do not reapply.** Normally, preferences refresh at the same interval as Group Policy settings. This setting changes that behavior to apply the setting only once for a user or computer.
- **Use Item-level targeting.** One of the most powerful features of preferences is preference item-level targeting. You can use this feature to specify criteria so that you can determine exactly which users or computers will receive a preference. Criteria includes, but is not limited to:
  - Computer name
  - IP address range
  - Operating system
  - Security group
  - User
  - Windows Management Instrumentation (WMI) queries



## Enabling and disabling settings in Group Policy preferences

Not all settings that you can configure in Group Policy preferences are enabled by default. For example, if you want to configure the Internet Explorer home page using Group Policy preferences, the setting will not work by default. When you configure the setting, you can see a dotted red line, whereas on the same tab the **Delete browsing history on exit** setting has a green solid line. This means that the setting is enabled.

You can enable and disable settings on a tab by using the **F5**, **F6**, **F7**, and **F8** keys. The keys enable and disable the settings as follows:

- F5 enables all settings on a tab.
- F6 enables the selected setting.
- F7 disables the selected setting.
- F8 disables all settings on a tab.

Notice that check boxes and options have green circles or red circles to show whether the setting is enabled or not.

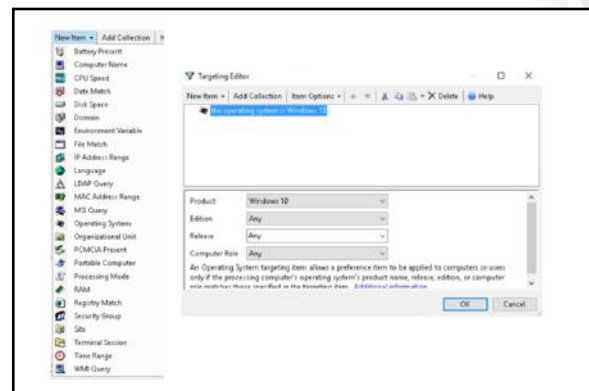
## Item-level targeting options

*Item-level targeting* is a feature that allows Group Policy preferences settings to apply to computers or user objects only when the computers or user objects match defined criteria. This makes advanced targeting control possible and allows Group Policy administrators to pinpoint exactly where and when a setting should apply. Item-level targeting offers the following capabilities:

- Target 27 different categories. Item-level targeting can use 27 different categories for targeting computers and user objects. This allows for precision targeting.
- Combine different categories together by using AND or OR Boolean logic. Instead of using a single category for targeting, you can use multiple categories.
- Refresh item-level targeting during the Group Policy background refresh. This means that configuring computer and user objects by using item-level targeting is a dynamic way to manage the user objects and computer objects.

The following categories are available in item-level targeting:

- Battery Present
- Computer Name
- CPU Speed
- Date Match
- Disk Space
- Domain
- Environment Variable



- File Match
- IP Address Range
- Language
- LDAP Query
- MAC Address Range
- MSI Query
- Network Connection
- Operating System
- Organizational Unit
- PCMCIA Present
- Portable Computer
- Processing Mode
- RAM
- Registry Match
- Security Group
- Site
- Terminal Session
- Time Range
- User
- WMI Query

### Scenarios to configure using item-level targeting

By using the different categories with Boolean logical expressions, you can create precise item-level targeting for each Group Policy preferences setting that you configure.

The following list are some of the scenarios that you could use item-level targeting for:

- Restrict drive mappings to an Active Directory security group. You can go a step further by restricting drive mappings with sensitive content to a specific IP address range.
- Restrict drive mappings to computers with only a specific file (or program) present on the computer. For example, there is no need to map a drive to where an application stores data if the application is not present on the computer.
- Configure different power plans for portable and desktop computers. You can go a step further and base the power plan on time of day, so client computers go into standby mode after shorter times during non-work hours.
- Deploy printers only to portable computers when the users are members of a specific group. You can go a step further by deploying one group of printers to computers that meet certain criteria, such as if they are: portable, being used by a member of a specific group, and in a specific IP subnet. You then could deploy another set of printers when the IP subnet changes.
- Copy Microsoft Office templates based on the language of the operating system installed on the computer.



- Create a shortcut based on whether the user is a member of a specific group, and the computer has a specific name (for example, W10-001), the time criteria meets a specific time (for example, is between 8AM and 5PM), and the user is connected to a Terminal Server from a client computer with an IP address between a specified range (for example, 10.5.5.10 and 10.5.5.15).

## Demonstration: Configuring Group Policy preferences

This demonstration shows how to:

- Create a printer with Group Policy preferences.
- Target the preference.
- Create a power plan with Group Policy preferences.
- Target the preference.
- Test the preferences.

### Demonstration Steps

#### Create a printer with Group Policy preferences

1. On **LON-DC1**, add a new local printer named and shared as **Brother** using the **Brother Color Leg Type1 Class Driver** driver.
2. Start the **GPMC**.
3. In the GPMC, create a new GPO named **GP Prefs**, and link the GPO to the domain.
4. Edit the GPO and go to **User Configuration\Preferences\Control Panel Settings\Printers**.
5. Create a Shared Printer using the **\\LON-DC1\Brother** printer.

#### Target the preference

- Target the preference for IP addresses in the **172.16.0.50 – 172.16.0.99** range.

#### Configure a power plan with Group Policy preferences

1. Navigate to **Computer Configuration\Preferences\Control Panel Settings\Power Options**.
2. Create a new power plan named **Adatum Power Plan** and make it the active power plan.

#### Target the preference

- Target this preference for computers that are running **Windows 10**.

#### Test the preferences

1. Switch to **LON-CL1**, and then if necessary, refresh the group policies by using the following command at the command prompt:

```
gpupdate /force
```

2. Sign in, and then verify the presence of both the **Brother on LON-DC1** printer and the **Adatum Power Plan**.

**Check Your Knowledge**

Question	
Which Group Policy preferences settings can you use to configure a user's Internet Explorer experience? (Select all that apply)	
Select the correct answer.	
<input type="checkbox"/>	Internet Explorer
<input type="checkbox"/>	Shortcuts
<input type="checkbox"/>	Registry
<input type="checkbox"/>	Power Options
<input type="checkbox"/>	Folder Options

Verify the correctness of the statement by placing a mark in the column to the right.

Statement	Answer
You can use item-level targeting to limit Group Policy preferences depending on which AD DS forest the user belongs to.	

**Question:** In what scenarios have you used Group Policy preferences and item-level targeting?

## Lab: Managing user settings with Group Policy

### Scenario

A. Datum Corporation has implemented Microsoft Office 2016 and you want to use Group Policy to configure settings for some Office 2016 apps. The IT department uses logon scripts to provide users with drive mapping to shared folders. However, maintaining these scripts is an ongoing problem, because they are large and complex. Your manager has asked that you implement drive mapping by using Group Policy preferences to remove logon scripts.

Your manager also has asked that you place a desktop shortcut to the Notepad app for all users who belong to the IT Security group. Additionally, you must add a new computer administrator's security group as a local administrator on all servers.

To help minimize profile sizes, you also need to configure Folder Redirection to redirect several profile folders to each user's home drive. Finally, you have to complete the GPO design to manage user desktops and server security.

### Objectives

After completing this lab, you will be able to:

- Use administrative templates to manage user settings.
- Implement settings by using Group Policy preferences.
- Configure Folder Redirection.

### Lab Setup

Estimated Time: 45 minutes

Virtual machines: **20742A-LON-DC1**, **20742A-LON-DC2**, and **20742A-LON-CL1**

User name: **Adatum\Administrator**

Password: **Pa\$\$w0rd**

For this lab, you will use the available virtual machine environment. Before you begin the lab, you must complete the following steps:

1. On the host computer, start **Hyper-V Manager**.
2. In Microsoft Hyper-V Manager, click **20742A-LON-DC1**, and in the **Actions** pane, click **Start**.
3. In the **Actions** pane, click **Connect**. Wait until the virtual machine starts.
4. Sign in by using the following credentials:
  - User name: **Administrator**
  - Password: **Pa\$\$w0rd**
  - Domain: **Adatum**
5. Repeat steps 2-4 for **20742A-LON-DC2**.
6. Repeat steps two through four for **20742A-LON-CL1**.

## Exercise 1: Using administrative templates to manage user settings

### Scenario

As a part of implementing Group Policy to configure settings for the Office 2016 apps, you now need to import custom administrative templates for Office 2016 and configure settings.

The main tasks for this exercise are as follows:

1. Import administrative templates for Microsoft Office 2016.
2. Configure Office 2016 settings.
3. Apply and verify settings on the client computer.

#### ► Task 1: Import administrative templates for Microsoft Office 2016

1. On **LON-DC1**, double-click the **E:\LabFiles\Mod06\ admintemplates\_x64\_4390-1000\_en-us.exe** file and extract the files to the Desktop.
2. Copy all files and subfolders from the **C:\Users\Administrator\Desktop\admx** directory to **C:\Windows\PolicyDefinitions**.

#### ► Task 2: Configure Office 2016 settings

1. On **LON-DC1**, from **Server Manager**, start **Group Policy Management**.
2. Create a new GPO named **Office 2016 settings**.
3. Edit the GPO.
4. Locate the **User Configuration\Policies\Administrative Templates\Microsoft Excel 2016** node.
5. In **Excel Options\Customize Ribbon**, enable the **Display Developer tab in the Ribbon** setting.
6. In **Excel Options\Save**, enable the **Default file location** setting, and set the Default file location to **%userprofile%\Desktop**.
7. Close the Group Policy Management Editor.
8. Link the **Office 2016** settings to the **Adatum.com** domain.

#### ► Task 3: Apply and verify settings on the client computer

1. Switch to **LON-CL1** and refresh Group Policy.
2. Start **Microsoft Excel 2016**.
3. Create a blank workbook.
4. Verify that the **Developer** tab displays on the ribbon.
5. If the **Developer** tab is not displayed on the ribbon, perform the following steps:
  - a. Restart **LON-CL1**.
  - b. Sign in as **Adatum\Administrator** with the password **Pa\$\$w0rd**.
  - c. Perform steps 2-4 again.
6. Save the file and verify that the default file location is the Desktop for the user.
7. Close **Excel 2016**.

**Results:** After completing this exercise, you should have successfully extended administrative templates with templates for Office 2016 and configured some Office settings by using Group Policy.

## Exercise 2: Implementing settings by using Group Policy preferences

### Scenario

You now have to implement drive mapping by using Group Policy preferences to remove logon scripts that A. Datum uses currently to provide users with drive mapping to shared folders. You also need to place a desktop shortcut to the Notepad app for all users who belong to the IT Security group.

The main tasks for this exercise are as follows:

1. Set up the current environment.
2. Test mapped drive for Branch Office 1 users.
3. Create a Preferences GPO with the required Group Policy preferences.
4. Test the preferences.

#### ► Task 1: Set up the current environment

1. Switch to **LON-DC1**.
2. On **LON-DC1**, open **File Explorer**, and then go to **E:\Labfiles\Mod06**.
3. Run the **Mod06-1.ps1** Windows PowerShell script.
4. Copy the **BranchScript.cmd** file to the clipboard.
5. Switch to **Group Policy Management**.
6. Edit the **Branch1** GPO to configure a user logon script.
7. Paste the **BranchScript.cmd** script into the scripts folder.
8. Add the **BranchScript.cmd** script to the logon scripts GPO setting.

#### ► Task 2: Test mapped drive for Branch Office 1 users

1. Switch to **LON-CL1**.
2. Restart the computer.
3. When the computer has restarted, sign in as **Adatum\Abbi** with password **Pa\$\$w0rd**.
4. Open **File Explorer** and verify that drive **S** displays.
5. If the S drive is not available, perform these steps:
  - a. Refresh Group Policy.
  - b. Restart **LON-CL1**.
  - c. Sign in as **Adatum\Abbi** with password **Pa\$\$w0rd**.
  - d. The S drive should now display in File Explorer.

#### ► Task 3: Create a Preferences GPO with the required Group Policy preferences

1. Switch to **LON-DC1**.
2. On **LON-DC1**, open **Active Directory Users and Computers**.
3. In the **IT** OU, create a new global security group named **Computer Administrators**.
4. In the GPMC, on the **Branch Office 1 OU**, delete the link for the **Branch1** GPO.
5. Create a new GPO named **Preferences**, and link it to the domain.
6. Go to **User Configuration\Preferences\Windows Settings\Shortcuts**.

7. Create a new shortcut to Notepad.exe with the following settings:
  - o Name: **Notepad**
  - o Action: **Create**
  - o Location: **All Users Desktop**
  - o Target path: **C:\Windows\System32\Notepad.exe**
8. On the **Common** tab, clear the **Run in logged-on user's security context (user policy option)** check box.
9. Target the preference for members of the **IT Security** group.
10. Go to **User Configuration\Preferences\Windows Settings\Drive Map**.
11. Create a new mapped drive with the following settings:
  - o Action: **Update**
  - o Location: **\\LON-DC1\Branch1**
  - o Reconnect: **Selected**
  - o Label: **Drive for Branch Office 1**
  - o Use: **S**
12. On the **Common** tab, select the **Run in logged-on user's security context (user policy option)** check box.
13. Target the preference for users in the **Branch Office 1** OU.
14. Go to **Computer Configuration\Preferences\Control Panel Settings\Local Users and Groups**.
15. Update the local Administrators group using the following settings:
  - o Action: **Update**
  - o Name: **Administrators**
  - o Add new local group member: **Computer Administrators**
16. On the **Common** tab, clear the **Run in logged-on user's security context (user policy option)** check box.
17. Target the preference for computers that are running the **Windows Server 2016 Technical Preview 5** operating system.
18. Close all open windows except **Group Policy Management** and **Server Manager**.

► **Task 4: Test the preferences**

1. Switch to and restart **LON-CL1**.
2. Sign in as **Adatum\Abbi** with the password **Pa\$\$w0rd**.
3. Open **File Explorer**, and verify that drive **S** displays.

 **Note:** The drive label now is **Drive for Branch Office 1**, which verifies that the drive is mapped through Group Policy preferences.

4. On the desktop, verify a shortcut for Notepad displays.

5. If the shortcut for Notepad is not available, perform these steps:
  - a. Refresh Group Policy.
  - b. Restart **LON-CL1**.
  - c. Sign in as **Adatum\Abbi** with password **Pa\$\$w0rd**.
  - d. The shortcut for Notepad should now display on the desktop.
6. Open **Computer Management**.
7. In **Computer Management**, browse to the **System Tools\Local Users and Groups\Groups** node.
8. Verify that the **Computer Administrators** group is not a member of the **Administrators** group, because the preferences setting only applies to servers.
9. Sign out of **LON-CL1**.

**Results:** After completing this exercise, you should have successfully removed the logon scripts, configured preference settings, and then assigned them by using GPOs.

## Exercise 3: Configuring Folder Redirection

### Scenario

To help minimize profile sizes, you decide to configure Folder Redirection for the branch office users, to redirect several profile folders to each user's home drive.

The main tasks for this exercise are as follows:

1. Create a shared folder to store the redirected folders.
2. Create a new GPO and link it to the Branch Office 1 organizational unit (OU).
3. Edit the Folder Redirection settings in the policy.
4. Test the Folder Redirection settings.

#### ► Task 1: Create a shared folder to store the redirected folders

- On **LON-DC1**, open **File Explorer**, create a new folder by using the following properties, and then share it with **Specific people**:
  - Path: **C:\Branch1Redirect**
  - Share name: **Branch1Redirect**
  - Permissions: **Everyone, Read/Write**

#### ► Task 2: Create a new GPO and link it to the Branch Office 1 organizational unit (OU)

- On **LON-DC1**, open **Group Policy Management**, and then create and link a new GPO named **Folder Redirection** to the **Branch Office 1** OU.

#### ► Task 3: Edit the Folder Redirection settings in the policy

1. Open the **Folder Redirection** GPO for editing.
2. Under **User Configuration**, browse to **Policies\Windows Settings\Folder Redirection**.
3. Configure the **Documents** folder properties to use the **Basic-Redirect everyone's folder to the same location** setting.

4. Ensure that the **Target folder** location is set to **Create a folder for each user under the root path**.
5. Specify the root path as **\\LON-DC1\Branch1Redirect**.
6. Configure the **Pictures** and **Music** folders to follow the **Documents** folder.
7. Close all open windows on **LON-DC1**.

► **Task 4: Test the Folder Redirection settings**

1. Switch to **LON-CL1**.
2. Sign in as **Adatum\Abbi** with the password **Pa\$\$w0rd**.
3. Open the **Command Prompt** window, type the following command to refresh Group Policy, and then press Enter:

```
gpupdate /force
```

4. Sign out, and then sign back in to **LON-CL1** as **Adatum\Abbi** with the password **Pa\$\$w0rd**.
5. Open **File Explorer**, and verify that in the **Documents** properties dialog box, the location is **\\LON-DC1\Branch1Redirect\Abbi**.
6. In the **Documents** folder, verify that the two subfolders, **Music** and **Pictures** exist.



**Note:** This verifies that **Music** and **Pictures** are redirected as well.

7. Sign out of **LON-CL1**.

**Results:** After completing this exercise, you should have successfully configured Folder Redirection to a shared folder on the **LON-DC1** server.

## Exercise 4: Planning Group Policy (optional)

### Scenario

You are tasked with planning a GPO model for the current infrastructure to manage security for the user desktops and servers. You need to finalize the delegation model for administrative tasks and determine the administrators that will have rights on the client computers.

A. Datum management also wants you to configure Windows Update settings, and restrict administrative tools for regular user accounts. Additionally, one of the security requirements is that the company have a compliance warning related to misuse of corporate computers.

As the administrator of A. Datum, you are tasked with translating the business requirements into GPO settings. You must then design and implement the GPOs at the appropriate levels of the OU design.

In this exercise, you will design the GPO strategy that meets the business and organizational requirements for A. Datum.



## Supporting Documentation

### Beth Burke

From: Huong Tang [Huong@adatum.com]  
 Sent: 2<sup>nd</sup> July 11:43  
 To: [Beth@adatum.com](mailto:Beth@adatum.com)  
 Subject: GPO Design

Hello Beth,

As we've discussed in our meeting yesterday, we need to strengthen the security of servers and configure the users' desktops according to the first initial design.

I've included the notes of our meeting in the attached proposal document. Please read the document.

Also, it would be great if you could send me the updated proposal document later this week.

Thank you very much,

Huong

A. Datum GPO Strategy Proposal	
Document Reference Number: BS00918/1	
Document Author	Beth Burke
Date	2 <sup>nd</sup> July
<p><b>Requirements Overview</b></p> <p>Design a GPO strategy that meets the following requirements:</p> <ul style="list-style-type: none"> <li>• All of the organization's computers should have a core group of GPO settings that must be applied. These settings should include:             <ul style="list-style-type: none"> <li>○ Configuring the local administrator accounts.</li> <li>○ Configuring update settings.</li> <li>○ Restricting certain options, such as access to the registry editor.</li> </ul> <p>These settings should not apply to administrator desktops.</p> </li> <li>• Each office should have a core group of settings that apply to their workstations. As of now, you need to implement the following:             <ul style="list-style-type: none"> <li>○ Display a security warning prior to computer sign-in stating that only A. Datum employees can use the computers. This setting needs to be applied to each location, and to display automatically in other languages for foreign locations.</li> </ul> </li> <li>• All users must have a default set of mapped drives assigned to them. You should base the mapped drive on the department membership.</li> <li>• The central IT administrators in London must be able to manage all GPOs and settings in the organization. Administrators in each office should be able to manage only GPOs that apply to that office.</li> </ul>	
<p><b>Summary of Information</b></p> <p>The supporting OU structure includes the following:</p> <ul style="list-style-type: none"> <li>• Users are currently grouped by department in a top-level OU.</li> <li>• Clients are in the top-level Clients OU, which is separated by location on the next level.</li> </ul>	

**A. Datum GPO Strategy Proposal**

**Proposals**

- Which of the requirements will necessitate creating one or more GPOs?
- Can you fulfill any of the requirements without creating GPOs?
- Are there any exceptions to the default GPO application that you must consider?
- List the GPOs that you must create to fulfill the lab scenario's requirements. Provide the following information in the table provided:
  - Name of the GPO
  - The requirements that the GPO fulfills
  - The configuration settings (user policies, computer policies, user preferences, or computer preferences) that the GPO will contain
  - The container (domain, OU, site) to which the GPO will be linked

Name	Requirements fulfilled	Configuration settings	Applies to

- List other configuration tasks that you must perform within the Group Policy Management Console to fulfill the scenario requirements.

The main tasks for this exercise are as follows:

1. Read the supporting documentation.
2. Update the proposal document with your planned course of action.
3. Examine the suggested proposals in the Lab Answer Key.
4. Discuss your proposed solution with the class, as guided by your instructor.
5. Prepare for the next module.

► **Task 1: Read the supporting documentation**

- Read the documentation provided.

► **Task 2: Update the proposal document with your planned course of action**

- Answer the questions in the proposals section of the A. Datum GPO Strategy Proposal document.

► **Task 3: Examine the suggested proposals in the Lab Answer Key**

- Compare your proposals with the ones in the Lab Answer Key.

► **Task 4: Discuss your proposed solution with the class, as guided by your instructor**

- Be prepared to discuss your proposals with the class.

**Results:** After completing this exercise, you should have successfully designed a GPO strategy.

► **Task 5: Prepare for the next module**

When you finish the lab, revert the virtual machines to their initial state. To do this, perform the following steps:

1. On the host computer, start **Hyper-V Manager**.
2. In the **Virtual Machines** list, right-click **20742A-LON-DC1**, and then click **Revert**.
3. In the **Revert Virtual Machine** dialog box, click **Revert**.
4. Repeat steps two and three for **20742A-LON-DC2** and **20742A-LON-CL1**.

**Question:** Which options can you use to separate users' redirected folders to different servers?

**Question:** Can you name two methods that you could use to assign a GPO to selected objects within an OU?

**Question:** You have created Group Policy preferences to configure new power options. How can you make sure that they apply only to laptop computers?

## Module Review and Takeaways

### Best Practices

Best Practices Related to Group Policy Management:

- When configuring settings in GPOs, include comments on GPO settings.
- Use a central store for Administrative templates.
- Use Group Policy preferences to configure settings that are not available in Group Policy settings.

### Common Issues and Troubleshooting Tips

Common Issue	Troubleshooting Tip
You have configured Folder Redirection for an OU, but none of the users' folders are redirecting to the network location. When you look in the root folder, you observe that a subdirectory named for each user has been created, but they are empty.	
You have a mixture of Windows 7 and Windows 10 computers. After configuring several settings in the Administrative templates of a GPO, users with Windows 7 operating systems report that some settings apply and others do not.	
Group Policy preferences do not apply.	

### Review Questions

**Question:** Why do some Group Policy settings take two sign-ins before taking effect?

**Question:** What is the benefit of having a central store?

**Question:** What is the main difference between Group Policy settings and Group Policy preferences?

# Module 7

## Securing Active Directory Domain Services

### Contents:

Module Overview	7-1
<b>Lesson 1:</b> Securing domain controllers	7-2
<b>Lesson 2:</b> Implementing account security	7-15
<b>Lesson 3:</b> Implementing audit authentication	7-34
<b>Lesson 4:</b> Configuring managed service accounts	7-38
<b>Lab:</b> Securing AD DS	7-45
Module Review and Takeaways	7-55

## Module Overview

In your organization's information technology (IT) infrastructure, securing Active Directory Domain Services (AD DS) domain controllers is a critical task. Domain controllers provide access to many different resources, and they contain information about users and their passwords. If a single domain controller is compromised, any objects in the same Active Directory domain or in any trusted domain are at risk of being compromised, too.

The Windows Server 2016 operating system provides features and apps that you can use to help secure your network against security threats. The operating system provides measures to secure domain controllers by minimizing their attack surface and determining their domain-controller placements. The operating system also determines the AD DS roles that are used for administration, design, and implements password security, in addition to auditing when attacks occur. You also can use domain controllers to deploy security measures to other clients and servers in your Windows-based infrastructure.

AD DS administrators must understand the threats to domain controllers and the methods that they can use to secure AD DS and its domain controllers.

### Objectives

After completing this module, you will be able to:

- Secure domain controllers.
- Implement account security.
- Implement audit authentication.
- Configure managed service accounts (MSAs).

# Lesson 1

## Securing domain controllers

Your network's domain controllers are the core of your AD DS infrastructure. They contain all of your user-account information, and without them, users cannot sign in to the network or access the resources that they need to perform their jobs. When user accounts are compromised, other accounts in the same domain and any trusted domain also might be compromised. Therefore, securing your domain controllers is a critical component in securing your entire IT infrastructure.

### Lesson Objectives

After completing this lesson, you will be able to:

- Describe security risks that can affect domain controllers.
- Explain how to modify the security settings of domain controllers.
- Implement secure authentication.
- Secure physical access to domain controllers.
- Describe read-only domain controllers (RODCs).
- Deploy an RODC.
- Plan and configure RODC password replication policy.
- Configure a password replication policy.
- Describe role separation for RODC local administrators.

### Security risks that can affect domain controllers

Before you define any security measures, you need to determine against which threats you need to protect your network. You need to define your organization's security boundaries, and you must identify from where hackers or attackers might try to compromise your security. For example, you will need to secure your network against attacks from outside your company. You also might have regions, departments, or groups where you cannot trust your organization's employees in the same way as you trust employees in a strictly controlled environment, such as your main office.

Do you have administrative groups that you cannot trust? Do you have locations or departments that require a higher level of security? All of these factors will have an impact on your security planning.

To secure your Active Directory domain and domain controllers, you need to address security in terms of the following risks:

- **Network security.** An attacker must gain access to your network to get further information. Therefore, you should ensure that network boundaries, such as firewalls and exposed services, are highly protected. Also, you should ensure that your wireless networks are secured properly and do not allow untrusted devices to connect to your internal network. Use certificates for wireless connections and implement Network Access Protection (NAP) to secure network access.

- Domain controllers are prime targets for attacks and the most important resources to secure
- Security risks include:
  - Network security
  - Authentication attacks
  - Elevation of privilege
  - DoS attack
  - Operating system, service, or application attacks
  - Operational risks
  - Physical security threats

- Authentication attacks. Access to authentication credentials, such as user names and passwords, is the primary target for anyone who tries to access your network and data. Active Directory domain controllers store all information about all users and their passwords, and they need sufficient security to protect this information.
- Elevation of privilege. While regular, user credentials can access certain information, domain administrators or other administrative groups have elevated privileges, giving those accounts control over data. In many cases, administrators can grant themselves additional access to resources. Additionally, they can configure security measures. If attackers can elevate the credentials they use by putting their accounts into elevated groups in the same or trusted domains, they can lower security and potentially bypass auditing or security safeguards.
- Denial of service (DoS) attack. A malicious user or users do not launch DoS attacks to access data, but rather to disable services, systems, or whole infrastructures. Certain security measures, such as account lockout policies, might be useful in protecting your network against some threats, but they also provide an easily accessible DoS attack surface.
- Operating system, service, or app attacks. Network operating systems, in addition to services and apps that support communication over networks, are vulnerable to security attacks. These systems provide communication over a network, and attackers will try to trick the expected communications to make these services do something differently than what was intended.
- Operational risks. It is important to maintain any organization's infrastructure properly. Any kind of software that operates over networks could be a potential target for attackers. To tighten security, software and hardware vendors release updates regularly. Administrators need to keep their systems up-to-date and remove or disable any unused user and computer accounts that are likely to have unsecure passwords. Any permissions that are granted need to be verified and monitored regularly to ensure that they do not leave a network vulnerable.
- Physical security threats. It is important for Active Directory domain controllers to be physically secure. If someone gets physical access to a server, it is easier to disable security safeguards and run malicious software locally to retrieve all passwords in a domain.

## Modifying the security settings of domain controllers

An Active Directory domain usually includes multiple domain controllers. To ensure that all security settings apply consistently to all domain controllers, you should configure security settings for Active Directory domain controllers centrally. To do this, use the Default Domain Controllers Group Policy Object (GPO), or create a new, custom GPO that is linked to the Domain Controllers organizational unit (OU). You create all domain-controller computer accounts in this OU, and you should not move them out of this OU, because they will fall out of the Default Domain Controllers Policy scope.

- Use a GPO to apply the same security settings to all domain controllers
- Consider custom GPOs that link to the Domain Controllers OU
- Security options include:
  - Account policies, such as passwords and account lockout
  - Local policies, such as auditing, user rights, and security options
  - Event log configuration
  - Restricted groups
  - Secure system services
  - Windows Firewall with advanced security
  - Public key policies
  - Advanced auditing

Some organizations prefer to use a different GPO than the Default Domain Controllers Policy. When configuring security settings, it is possible to apply settings that might be too secure. For example, you could configure policies that lock out some administrative groups or policies that prevent anyone from accessing the domain. While it is simple to unlink or disable a custom GPO, you should not disable or

unlink the Default Domain Controllers Policy. For this reason, we recommend that you create a custom GPO and link it to the Domain Controllers OU instead of modifying the Default Domain Controllers Policy.

### Default Domain Policy vs. Default Domain Controllers Policy

There are two default GPOs, the Default Domain Policy and the Default Domain Controllers Policy, and it is essential to understand the differences between the two:

- **Default Domain Policy GPO.** This GPO links to the domain, and it applies to all users and computers, including client computers, domain controllers, and servers in the domain. You should use this policy and others that link to a domain carefully. This policy should contain only settings that are explicitly intended to apply to all objects in an organization.
- **Default Domain Controllers GPO.** This GPO links to the Domain Controllers OU, and it applies to all domain controllers in the domain. This is the GPO in which you configure most security settings that pertain to domain controllers.

### Security settings in the GPO

The following are some of the most important security settings that you can configure in a GPO. You can find the **Security Settings** in any GPO under **Computer Configuration\Policies\Windows Settings**:

- **Account Policies.** Under this node, you can configure the Password Policy, Account Lockout Policy, and Kerberos Policy. These settings only apply to the local user accounts of the computers to which the policy applies, unless you configure the settings in the Default Domain Policy. Only the Account Policies that you configure in the Default Domain Policy apply to all domain accounts.
- **Local Policies.** This node contains three of the most important nodes for security configuration:
  - **Audit Policy.** These settings configure legacy-auditing policies that apply to all Windows operating-system versions. However, if you have Windows Server 2008 R2 and Windows 7 or newer deployed in your network, we recommend that you use Advanced Audit Policy Configuration instead of these auditing policies.
  - **User Rights Assignment.** These settings configure many security settings that apply to user rights. For example, you can specify who can access the computer from the network, who can sign in locally or through Remote Desktop Services (RDS), and who is able to change the time or shut down the computer. For domain controllers, you also can specify who is able to synchronize directory services data.
  - **Security Options.** These settings contain important security settings, including options for managing default accounts, such as the Guest and Administrator accounts, and these options also pertain to managing devices, domain controllers, domain-member security protocols, logon security settings, network access, and security settings, among others.
- **Event Log.** Under this node, you can configure settings such as event log size, retention method, and retention duration for the default Application, Security, and System event logs. It is important to have all Security logs on domain controllers configured identically. If you configure the Security log on one domain controller to keep logs for six days, and another retains logs for only three days, you will receive inconsistent results, depending on the domain controller on which you perform the search.
- **Restricted Groups.** Under this node, you can define two properties for security-sensitive groups (or restricted groups). For each group that you add here, you can define **Members** and **Member of** attributes. For groups that you configure as restricted, you cannot change membership by using other tools, such as **Active Directory Users and Computers**.
- **System Services.** Under this node, you can define startup behavior and security permissions for system services by using GPOs. This enables you to disable all services that are not required for a specific server role, such as a domain controller.



- **Windows Firewall with Advanced Security.** This setting allows you to administer Windows Firewall with advanced security centrally. By using a GPO to configure Windows Firewall settings, you can ensure that all servers that provide the same services, such as domain controllers, have a consistent Windows Firewall configuration.
- **Public Key Policies.** Under this node, you configure settings that rely on a public key infrastructure (PKI), such as the Encrypting File System (EFS) and its recovery key, BitLocker Drive Encryption, Automatic Certificate Request Settings (autoenrollment), and Trusted Root Certification Authorities, among others.
- **Advanced Audit Policy Configuration.** The settings under this node enable a more extensive policy configuration than the Audit Policy under the Local Policies node. When targeting Windows Server 2008 R2 or newer, or Windows 7 computers or newer, we recommend that you use the new Advanced Audit Policy Configuration settings.

## Implementing secure authentication

Having a secure authentication process is one of the most important security components of your domain environment, and you should consider the following factors when implementing secure authentication:

- Secure user accounts and passwords. It is very important to secure user accounts and passwords. You do this by configuring and utilizing technical components, such as configuring password and account policies, and also by educating your users about how to create and use complex and lengthy passwords. If your apps support lengthy passwords, teach users how to use passphrases to replace passwords.
- Secure groups with elevated permissions. Every organization has groups with elevated permissions. These groups include the Domain Admins, Schema Admins, and Enterprise Admins groups. Implementing secure management processes for these groups is important. For example, you might limit who knows the passwords for members of these groups, and ensure that all administrators have special administrative accounts and that they sign in only with those accounts when performing administrative tasks. For these groups, you can also use the Restricted Groups setting in Group Policy, which a later section of this module details.
- Audit critical object changes. To track any changes to critical administrative groups, such as built-in accounts, built-in groups, and especially groups with elevated permissions, configure your auditing policy to track all changes made to these groups. If possible, ensure that only members of an auditing team have access to the audited events, which prevents administrators from deleting events.
- Deploy secure authentication. Two-factor authentication is the key to achieve heightened security, beyond regular user-name and password credentials. It is common to use smart cards to secure authentication or implement multi-factor authentication with mobile phones. Smart cards have a stored certificate that acts as a user's credentials for signing in, rather than a user name and password. To authenticate by using a smart card, you must possess the smart card, and you must have the personal identification number (PIN) or password to unlock the private key. The combination of the public key, known to the domain controller, and the private key on the smart card, enables the

Consider the following factors when implementing secure authentication:

- Secure user accounts and passwords
- Secure groups with elevated permissions
- Audit critical object changes
- Deploy secure authentication, such as smart cards or multi-factor authentication
- Secure network activity
- Establish deprovisioning and cleanup processes
- Secure client computers

domain controller to authenticate the user. You also can enforce the use of smart cards if users want to access additional apps and across RDS. If you use smart phones as a second factor for authentication, you can require users to use the application, text message, or phone to prove their identity.

- Secure network activity. Securing your network is necessary when trying to achieve a secure client/server infrastructure. If your organization supports wireless networks, ensure that all networks with access to your organization's servers are secure, preferably by using certificates. If required, provide public or guest networks to allow customers, partners, or other nonemployees to have Internet access, rather than allowing them access to the corporate network. For your wired networks, consider device health attestation to prevent unknown devices from connecting to your network. For critical servers that host highly confidential information, consider enforcing Internet Protocol security (IPsec) signatures or encryption to secure network communication.
- Establish deprovisioning and cleanup processes. Basically, *provisioning* empowers a new employee by creating their account, group memberships, mailbox, and other components that they need to work in your organization. Although provisioning is important, you should remember that the often-forgotten *deprovisioning* is even more important. You must define and establish processes for employees who resign voluntarily, and more important, involuntarily. Also, consider other reasons an employee might take leave, such as parental leave or sabbatical leave. Define what type of access, if any, is necessary. Additionally, you should decide whether to deactivate accounts, delete accounts, or remove accounts from certain groups, such as general distribution lists or critical human resources (HR) apps, and decide whether to allow or prevent access by users who are outside your organization's network.

A cleanup process also is necessary for domain members, such as for client computers, because they also are allowed to authenticate against the domain, and a malicious user may utilize their credentials to compromise a network. Furthermore, ensure that there are no client computers or users that were created, but which have not been used to connect to the domain. This is because their passwords are default, well-known passwords, which a malicious user might discover and utilize.

- Secure client computers. If you want to secure your AD DS and Active Directory domain controllers, you must secure your client computers. Client computers cache the last 10 logons, by default. Therefore, if a client computer is lost, you need to have a process by which you track accounts that signed in within the password-change interval, and you need to know how to reset passwords after a loss is reported. You also need to protect your internal network from client computers that connect from wired or wireless networks from homes, hotels, or airports. To protect client computers, ensure that client computers have all security updates installed, that they have current virus protection and a host-based firewall, and consider using drive encryption such as BitLocker drive encryption.

## Securing physical access to domain controllers

The physical security of domain controllers is critically important. Domain controllers contain all of the credentials in your organization's Active Directory domain. If attackers achieve physical access to your domain controllers, they can bypass almost any safeguards that you have. They then can access most passwords quickly, and they can use this information to attack your network.

Therefore, you should do the following steps to further secure your Active Directory domain controllers, including that you:

When securing physical access to your domain controllers, consider the following:

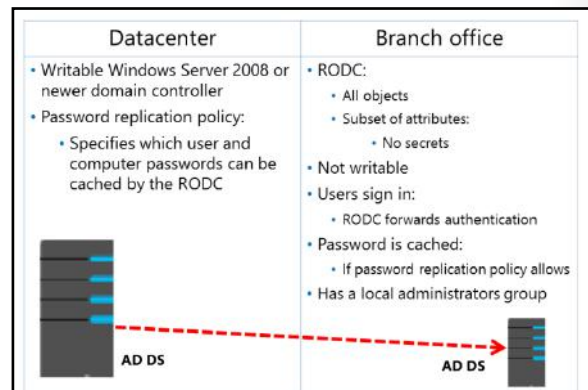
- Only deploy domain controllers where physical security is ensured
- Use RODCs
- Use BitLocker on domain controller disk volumes
- Monitor hot-swap disk systems because they can lead to domain controller theft
- Protect virtual disks; virtual machine admins must be highly trusted
- Store backups in secure locations

- Only deploy domain controllers where you can ensure physical security. If your server locations do not have dedicated rooms with access control, do not put a domain controller in that environment.
- Use RODCs, where possible. You can use RODCs as domain controllers in locations with less physical security because, by default, RODCs do not store secrets such as account passwords. A later section of this lesson details RODCs.
- Use BitLocker drive encryption. To provide an extra level of security, consider encrypting domain-controller hard drives by using BitLocker. This prevents attackers from accessing the data on server hard drives if they are removed from the servers. Windows Server 2016 supports using BitLocker on volumes that store AD DS databases. However, it does not support the use of EFS to protect AD DS database files.
- Monitor hot-swap disk systems. Usually, servers deploy with *hot-swap* disk systems, which enable you to change a drive, without server interruption, when a hardware failure occurs. If you have Redundant Array of Independent Disks (RAID) Level 1 mirroring in your servers, you should ensure that you have monitoring in place, so you are aware if any disks are removed or exchanged. Otherwise, it is simple to remove, and possibly replace, a drive from your domain controller. If someone possesses your domain controller's hard drive, he or she has the same ability to exploit the system as they would if they had the whole domain controller.
- Protect virtual disks. Many organizations deploy domain controllers as virtual machines. The virtual disks used by virtual machines must be as secure as physical disks, and the administrators of your virtual infrastructure must be as trusted as your Domain Admins. Sometimes, running a dedicated virtual infrastructure for critical components such as domain controllers addresses these risks.
- Store backups in secure locations. Your domain-controller backups contain all of the same information as domain controllers. Make sure that backups are stored in secure locations, which only trusted administrators can access.

## What are RODCs?

Branch offices present a unique challenge for an organization's IT staff. Branch offices usually are smaller sites in which no datacenter exists. Additionally, branch offices might not have a secure facility in which to house servers, and there might be few, if any, local IT staff to support the servers. If a wide area network (WAN) link separates a branch office from your hub site, depending on the number of users and the services that are available in the branch office, you must decide whether to place a domain controller in the branch office. AD DS in Windows

Server 2008 and newer versions support a new type of domain controller, a *read-only domain controller* or *RODC*, which deploys in this type of environment.



### Reasons for deploying RODCs

If you do not deploy a domain controller in a branch office, you must use a WAN link to direct authentication and service-ticket activities to the hub site. When a user first tries to access a specific service, the user's client requests a service ticket from a domain controller. Users typically connect to multiple services during a workday, so service-ticket activity happens regularly. Authentication and service ticket activity over a WAN link between a branch office and a hub site can result in slow or unreliable performance.

If you place a domain controller in a branch office, authentication occurs more efficiently. However, there are several potentially significant concerns, which include:

- A domain controller maintains a copy of all object's attributes in its domain, including secure information, such as user passwords. If a hacker accesses or steals a domain controller, or its hard drive or backup drive, a determined malicious user could identify valid user names and passwords. At that point, your entire domain is compromised, and you would have to reset passwords for every user and computer account in the domain. Server security at branch offices often is not ideal, so a branch-office domain controller poses a considerable security risk.
- Changes to the Active Directory database on a branch-office domain controller replicate to the hub site and to the environment's other domain controllers. Therefore, corruption to a branch-office domain controller poses a risk to the integrity of the organization's AD DS. For example, a branch office administrator who performs a restoration of the domain controller from an outdated backup could cause significant repercussions for the entire domain.
- A branch-office domain controller might require maintenance, such as the installation of new device drivers. To perform maintenance on a standard domain controller, you must sign in as a member of the Administrators group, which means you effectively are an administrator of the domain. It might not be appropriate to grant that level of capability to a branch-office support team.

These concerns can leave organizations with a difficult decision. For this reason, Microsoft introduced the RODC, which addresses the branch-office scenario. An RODC is a domain controller that maintains a copy of all objects and attributes in the domain, except for secure information such as password-related properties. If you do not configure caching, an RODC receives sign in requests from branch office users and forwards them to a domain controller in the hub site for authentication.

You can configure a password replication policy for an RODC that specifies the user and computer accounts for which passwords might be cached on the RODC. If any user signs in by using an RODC, the RODC requests that user's credentials from a full domain controller. When the user is a member of the password replication policy that applies to an RODC, the RODC can retrieve the password, and the full domain controller allows the replication of the secret. This means that the next time the user requests authentication from the same RODC, the RODC can perform the task locally. While users who are included in the password replication policy sign in, the RODC builds its cache of credentials so that it can perform authentication locally for those users. Normally, you add users and computers to the password replication policy who are in the same physical site as the RODC.

Because RODCs maintain only a subset of user credentials, security exposure is limited if an RODC is compromised or stolen. If an RODC is compromised, only the user and computer accounts that the RODC cached must have their passwords reset.

The RODC replication process also enhances security. An RODC replicates changes to AD DS from writable domain controllers, but it does not replicate any data to other domain controllers. This eliminates the exposure of Active Directory services to corruption because of changes made to a compromised branch-office domain controller. Finally, RODCs have the equivalent of a local Administrators group. You can give one or more local support personnel the ability to maintain an RODC fully without granting them the equivalent Domain Admins rights.

### **RODC limitations and considerations**

To reduce security risks and administrative costs, some domain controller options that are available for writable domain controllers are not available on RODCs. Before you decide to deploy an RODC, you should be aware of the following limitations and considerations:

- RODCs cannot be operations master role holders. Operations master role holders must be able to write information to the Active Directory database. Because of the read-only nature of the RODC's Active Directory database, it cannot act as an operations master role holder.
- RODCs cannot be bridgehead servers. Bridgehead servers specifically replicate changes from other sites. RODCs perform only inbound replication, so they cannot act as a bridgehead server for a site.
- You should have only one RODC per site, per domain. If you have multiple RODCs, the behavior of caching is inconsistent because shared secrets are only cached if a user signs in to that specific RODC. It is likely that one RODC has the shared secrets and another RODC in the same site does not have them at all.
- RODCs cannot authenticate across trusts when a WAN connection is not available. If your users and computers are in different domains, they cannot perform logons when the branch site uses RODCs and is disconnected from the hub site.
- Because AD DS changes cannot be written directly to an RODC, no replication changes originate at an RODC. This means that any changes or corruption that a hacker might make at branch locations cannot replicate from the RODC to the forest. This also reduces the workload of the hub's bridgehead servers and the effort required to monitor replication. RODC's unidirectional replication applies to both AD DS and Distributed File System (DFS) replication.
- RODCs cannot support any app properly that needs to update AD DS interactively, such as Microsoft Exchange Server. If you are going to deploy Exchange Server or similar apps at a site, you also should deploy a writable domain controller. Further, if you deploy Exchange Server at a site, you also should have a physically secure location for your servers.

- You can install the Domain Name System (DNS) server service on RODCs. RODCs can replicate all app directory partitions that DNS uses, including ForestDnsZones and DomainDnsZones. If you install a DNS server on an RODC, clients can query it for name resolution just as they would query any other DNS server. Similar to the AD DS information on an RODC, the DNS zone information on an RODC is read-only, and therefore, it does not support client updates directly. When client computers try to register a resource record in a DNS zone hosted on an RODC, the RODC returns the name of a full domain controller that contains a writable copy of that zone to the client. The client uses the full domain controller to register the record.

## Deploying an RODC

Before deploying an RODC in your Windows Server 2016-based AD DS, you must:

- Run **ADPrep /RODCPrep** if you have upgraded your domain from Windows Server 2003 or older versions.
- Ensure that you have a sufficient number of domain controllers to support your RODCs. RODCs need Windows Server 2008 or newer writable domain controllers as replication partners.
- Note that if you are using Windows Server 2012 or newer as writable domain controllers, you do not have additional prerequisites for RODCs.

- Prerequisites:
  - ADPrep /RODCPrep**
  - Sufficient Windows Server 2008 or newer replication partners for the RODCs
- For a one-step deployment, perform either of the following steps:
  - In Server Manager, open Add Roles and Features, and then use Active Directory Domain Services Configuration Wizard
  - Windows PowerShell: **Install-ADDSDomainController-ReadOnlyReplica**
- For a two-step deployment, perform the following steps:
  - Pre-staging: Create the account by using Active Directory Administrative Center or **Add-ADDSDomainControllerAccount**
  - Delegated promotion: Join the RODC as delegated admin: Server Manager or **Install-ADDSDomainController-ReadOnlyReplica**

After completing the preparatory steps, you can install an RODC. An RODC can be a full or Server Core installation of Windows Server 2016. You can perform an RODC installation in one step or in two steps by prestaging the account.

### Installing an RODC in one step

You can use the **Active Directory Domain Services Configuration Wizard**, even remotely, in **Server Manager** to create an RODC. On the **Additional Domain Controller Options** page of the wizard, you only have to click **RODC**.

Alternatively, you can use the **Install-ADDSDomainController** cmdlet with the **-ReadOnlyReplica** switch to install an RODC.

On a Server Core installation of Windows Server 2016, we recommend you to use **Server Manager** remotely or to use the **Install-ADDSDomainController** Windows PowerShell command-line interface cmdlet remotely by using the **Invoke-Command** cmdlet.

### Installing an RODC in two steps: prestaging and delegated promotion

You can complete the installation of an RODC in two stages; a different individual performs each stage. The first stage of the installation creates an account for an RODC in AD DS. The second stage of the installation attaches the actual server that will be the RODC to the account that was created for it previously. You can delegate the ability to attach the server to a non-administrative group or a user, such as a delegated branch office administrator.

During the first stage, the **Active Directory Domain Services Configuration Wizard** records all of the data about the RODC, such as its domain-controller account name and the site in which it will be placed. The distributed Active Directory database stores this information. A member of the Domain Admins group must perform this stage of the installation.

The administrator who creates the RODC account also can specify which users or groups can complete the next stage of the installation. Any user or group in the branch office who was delegated the right to complete the installation can perform the next stage. This stage does not require any membership in built-in groups, such as the Domain Admins group. If the user who creates the RODC account does not specify any delegate to complete the installation and administer the RODC, only a member of the Domain Admins or Enterprise Admins groups can complete the installation.

You can perform a staged installation of an RODC by using several approaches. You can precreate an RODC account by using **Active Directory Administrative Center**, which is appropriate for a small number of accounts. You also can use the **Add-ADDSTReadOnlyDomainControllerAccount** cmdlet with appropriate switches.

## Planning and configuring an RODC password replication policy

A password replication policy determines which users' or computers' credentials that a specific RODC caches. If a password replication policy allows an RODC to cache a user's credentials, the RODC can process that user's authentication and service-ticket activities. If an RODC cannot cache a user's credentials, the RODC refers the authentication and service-ticket activities to a writable domain controller.

Two multivalued attributes of the RODC's computer account determine the password replication policy of an RODC. These attributes are the *allowed list* and the *denied list*. If a user's account is on the allowed list, the RODC caches the user's credentials. You can include groups on the allowed list, in which case, the RODC caches all users who belong to the group. If a user is on both the allowed list and the denied list, the user's credentials are not cached—the denied list takes precedence.

- A password replication policy determines which users' or computer's credentials that a specific RODC caches
- You can configure these credentials by using a:
  - Domain-wide password replication policy
  - RODC-specific password replication policy
  - RODC filtered attribute set

### Domain-wide password replication policy

To facilitate the management of your password replication policy, Windows Server 2008 or newer operating systems create two domain local security groups in the Users container within AD DS:

- **Allowed RODC Password Replication Group.** Members of this group are included in the allowed list of each new RODC. By default, the group has no members. Therefore, by default, a new RODC does not cache any user's credentials. You should add users for whom you want all domain RODCs to cache credentials to the Allowed RODC Password Replication Group.
- **Denied RODC Password Replication Group.** Members of this group are included in the denied list of each new RODC. You should add users whose credentials you want to ensure are never cached by domain RODCs to the Denied RODC Password Replication Group. By default, this group contains security-sensitive accounts that are members of groups including Domain Admins, Enterprise Admins, and Group Policy Creator Owners.



**Note:** Users are not the only generators of authentication and service ticket activity. Computers in a branch office also require such activity. To improve system performance and to ensure that computers can establish a secure channel with a domain controller in a branch office, also allow the branch RODC to cache computer credentials. During a WAN outage, be aware that users are only able to sign in when both the computer and the users credentials are cached.

### RODC-specific password replication policy

These two groups allow you to manage password replication policy on all RODCs. However, to best support a branch-office scenario, you need to allow the RODC in each branch office to cache user and computer credentials in that specific location. Therefore, while you can use the global denied list, you should configure a specific allowed list for each RODC.

### RODC filtered attribute set

Some apps that use AD DS as a data store might use credential-like data, such as passwords, credentials, and encryption keys, which you do not want to store on an RODC, in case it becomes compromised. For these apps, you can configure a schema attribute set that will not replicate to an RODC. This set of attributes is the RODC filtered attribute set. Attributes that you define in the RODC filtered attribute set cannot replicate to any RODCs in the forest. You cannot add system-critical attributes to the RODC filtered attribute set. An attribute is system-critical if the following require it to function properly:

- AD DS
- Local Security Authority
- Security Accounts Manager
- Microsoft-specific Security Support Provider Interfaces, such as Kerberos version 5 protocol

If you have apps that you want to use the RODC filtered attribute set, you have to verify with the app vendor if they support it. While write-requests to an RODC receive referrals to a full domain controller, apps that ask an RODC for an attribute in the RODC filtered attribute set receive it as empty. RODC knows about the attribute but never receives a value for it. The app must be aware of this feature and know to request a writable domain controller when reading the RODC filtered attribute set.

## Demonstration: Configuring a password replication policy

In this demonstration, you will see how to:

- Stage a delegated installation of an RODC.
- View an RODC's password replication policy.
- Configure an RODC-specific password replication policy.
- Verify the resultant password policy.

### Demonstration Steps

#### Stage a delegated installation of an RODC

1. On **LON-DC1**, from **Server Manager**, open **Active Directory Sites and Services**, create a new site named **Munich**, and then assign it to the **DEFAULTIPSITELINK**.
2. Start **Active Directory Administrative Center**, and then navigate to the **Domain Controllers** OU.



3. Precreate an RODC account with the name **MUC-RODC1**, which also should be a **DNS server** and a **Global catalog**.
4. Delegate **Bill Norman** to install and administer the RODC.
5. Finish the precreation of the RODC account.

### View an RODC's password replication policy

1. In **Active Directory Administrative Center**, in the **Domain Controllers** OU, open the properties of the **MUC-RODC1** computer account.
2. In the **Extensions** section, select the **Password Replication Policy** tab, and then note its settings.

### Configure an RODC-specific password replication policy

1. Switch to **Server Manager**, and from the **Tools** menu, start **Active Directory Users and Computers**.
2. Navigate to the **Users** container, and then create a new group named **Munich Allowed RODC Password Replication Group**.
3. Add **Ana Cantrell** to the new group.
4. Switch to **Active Directory Administrative Center** and then open the properties of **MUC-RODC1**.
5. In the **Extensions** section, on the **Password Replication Policy** tab, configure the **Munich Allowed RODC Password Replication Group** to allow password replication, and then close the properties of **MUC-RODC1**.

### Verify the resultant password policy

1. In **Active Directory Administrative Center**, open the properties of **MUC-RODC1**, and then in the **Extensions** section, on the **Password Replication Policy** tab, click **Advanced**.
2. Note that this dialog box displays all accounts whose passwords are stored in the RODC.
3. Select **Accounts that have been authenticated to this Read-only Domain Controller**, and then note that this page only shows accounts that have the requisite permissions and that the RODC has authenticated.
4. Select the **Resultant Policy** tab, and then add **Ana Cantrell**. Note that Ana has a **Resultant Setting** of **Allow**.
5. Close all open dialog boxes.

## Separating RODC local administration

RODCs in branch offices might require maintenance, such as updates to device drivers. Additionally, small branch offices might combine the RODC role with a file-server role on a single system. In this scenario, it will be important to back up the system. RODCs support local administration by using the *administrator role separation* feature. With this feature, you can delegate any domain user or security group as a RODC's local administrator, without granting that user or group rights to the domain or other domain controllers. Therefore, a delegated

- Administrator role separation allows performance of local administrative tasks on the RODC for nondomain administrators
- Each RODC maintains a local Security Accounts Manager database of groups for specific administrative purposes
- Configure the local administrator by:
  - Adding the user or group when precreating or installing the RODC
  - Adding a user or group on the Managed By tab on the RODC account properties

administrator can sign in to an RODC to perform maintenance work, such as upgrading a driver on the server. However, the delegated administrator cannot sign in to any other domain controller or perform any other administrative task in the domain.

Each RODC maintains a local database of groups for specific administrative purposes. You can add a domain user account to these local roles to allow support of a specific RODC.

You can configure the delegated administrators for an RODC when you precreate an RODC computer account or when you install the RODC. You can add a user or group on the **Delegation of RODC Installation and Administration** page in the **Active Directory Domain Services Installation Wizard**. You also can add the user or group account on the **Managed By** tab of the RODC account properties in **Active Directory Users and Computers**.

**Question:** How can you provide extra security for hard drives in domain controllers?

## Lesson 2

# Implementing account security

As an administrator, you must make sure that user accounts in your environment conform to the security standards set by your organization. To achieve this, Windows Server 2016 allows you to use account policies to configure security-related settings for user accounts. Additionally, with Windows Server 2016, you can configure additional security with protected groups, authentication policies, and authentication policy silos. This lesson explains the settings that are available for account security and the methods to configure those settings.

### Lesson Objectives

After completing this lesson, you will be able to:

- Describe account security in Windows Server 2016.
- Describe password policies.
- Describe account lockout policies.
- Describe Kerberos policies.
- Configure domain account policies.
- Describe how to protect groups in AD DS.
- Describe fine-grained password and lockout policies.
- Describe Password Settings objects (PSOs).
- Configure a fine-grained password policy.
- Describe PSO precedence and resultant PSO.
- Explain account-security options in Windows Server 2016.
- Configure user account policies.
- Describe how to enhance password authentication with Windows Hello and the Microsoft Azure Multi-Factor Authentication (MFA) service.

### Account security in Windows Server 2016

In any authentication-based network, it is critically important to secure account credentials, such as usernames and passwords. To achieve account security, Windows Server 2016 provides multiple options, including:

- Password policies to configure multiple requirements, such as password age, length, and complexity, which users' passwords must meet.
- Account lockout policies that enable you to configure that an account must lock when the wrong passwords are entered.

Account security features in Windows Server 2016 include:

- Password policies
- Account lockout policies
- Fine-grained password policies
- Protected users
- Authentication policies
- Authentication policy silos

- Fine-grained password policies that provide the ability to specify different password policies and account lockout policies for different groups of users, such as executives, administrators, service accounts, or regular users.
- Protected users, which enables you to specify critical accounts that should be additionally secured.
- Authentication policies and authentication policy silos that provide you the ability to use claim-based rules to specify which users are able to sign in to which computers.
- Kerberos policies that determine Kerberos-related settings, such as ticket lifetimes and enforcement.

This lesson explains these options in further detail.

## Password policies

Account policies in AD DS define the default settings for security-related attributes that are assigned to user objects. In AD DS, account policies classify into three different groups of settings: password policy, account lockout, and Kerberos policy. You can configure password policy and account lockout settings in the local policy settings for an individual Windows Server 2016 server, or you can configure all three groups of settings for the entire domain by using the Group Policy Management Console in AD DS. When local policy settings and Group Policy settings conflict, Group Policy settings override local policy settings.

Set password requirements by using the following settings:

- Enforce password history
- Maximum password age
- Minimum password age
- Minimum password length
- Password complexity requirements:
  - Does not contain name or user name
  - Must have at least six characters
  - Contains characters from three of the following four groups groups: uppercase, lowercase, numeric, and special characters

In Group Policy Management within AD DS, most policy settings can apply at different levels within the AD DS structure: domain, site, or OU. However, account policies for domain accounts can apply only at one level in AD DS—to the entire domain. Therefore, only one set of account policy settings can apply to an AD DS domain.

The password policy is one of the most important policies when securing your AD DS user accounts. Use the password policy to configure the properties of the passwords that users might choose. You use these settings to ensure that users cannot use simple passwords, which provide insufficient protection against password attacks.

You define the password policy by using the following settings:

- **Enforce password history.** This is the number of unique, new passwords that must be associated with a user account before an old password can be reused. The default setting is 24 previous passwords. When you use this setting with the minimum password age setting, the enforced password history setting prevents constant reuse of the same password.
- **Maximum password age.** This is the number of days that a user can utilize a password before they must change it. Regularly changing passwords helps prevent the compromise of passwords. However, you must balance this security consideration against the logistical considerations that result from requiring users to change passwords too often. The default setting of 42 days is appropriate for most organizations.

- **Minimum password age.** This is the number of days that a password must be used before the user can change it. The default value is one day, which is appropriate if you also enforced password history. You can restrict the constant use of the same password if you use this setting with the enforced password history setting.
- **Minimum password length.** This is the minimum number of characters that a user's password must contain. The default value is seven. This default is a widely used minimum, but you should consider increasing the password length to at least 10 characters to enhance security.
- **Complexity requirements.** Windows Server includes a default password filter that is enabled by default, and you should not disable it. The filter requires that a password have the following characteristics:
  - Does not contain your name or your username
  - Contains at least six characters
  - Contains characters from three of the following four groups:
    - Uppercase letters [A–Z]
    - Lowercase letters [a–z]
    - Numerals [0–9]
    - Special, non-alphanumeric characters, such as !@#)(\*&^%

## Account lockout policies

In addition to password policies, most organizations configure account lockout policies. While password policies specify that users need to use secure passwords, account lockout policies enable you to define whether accounts should be locked if there are too many sign-in attempts with invalid passwords.

You can define thresholds for an account lockout, the duration of the lockout, and a way to unlock accounts. Thresholds for an account lockout stipulate that accounts become inoperable after a certain number of failed sign-in attempts during a certain time period. Account lockout policies help detect and prevent brute-force attacks on account passwords. The following settings are available:

- Account lockout policies define whether accounts should be locked automatically after several failed attempts to sign in
- To configure these policy settings, you must consider:
  - Account lockout duration
  - Account lockout threshold
  - Reset account lockout counter after
- Account lockout policies provide a level of security but also provide an opportunity for DoS attacks

- **Account lockout duration.** Defines the number of minutes that a locked account remains locked. After the specified number of minutes, the account unlocks automatically. To specify that an administrator must unlock the account, set the value to 0. Consider using fine-grained password policies to require administrators to unlock high-security accounts, and then configuring this setting to 30 minutes for normal users.
- **Account lockout threshold.** Determines the number of failed sign-in attempts that are allowed before a user account is locked out. A value of 0 means that the account is never locked out. You should set this value high enough to allow for mistyped passwords, but low enough to ensure the failure of brute force attempts to guess a password. Common values for this setting range from three through five.

- **Reset account lockout counter after.** Determines how many minutes must elapse after a failed sign-in attempt before the sign-in counter is reset to 0. This setting applies when a user has typed in a password incorrectly, but the user has not exceeded the account lockout threshold. Consider setting this value to 30 minutes.

Most organizations implement account lockout policies to prevent attackers from using password-guessing techniques to gain access to a network. Although this approach provides a level of security, it also exposes your organization to a DoS attack because attackers can run scripts to guess user passwords and lock out all user accounts. This prevents the correct person from being able to access his or her account. If you choose not to implement account lockout policies, it is critical that you monitor failed sign-in attempts in real time to prevent attackers from taking advantage of this configuration.

## Kerberos policies

You deploy Kerberos policy settings for the entire domain from the Default Domain Policy. This policy is for domain user and computer accounts, and determines Kerberos-related settings such as ticket lifetimes and enforcement. Kerberos policies do not exist in the Local Computer Policy.

The Kerberos Policy configuration options contain settings for the Kerberos v5 authentication protocol ticket-granting ticket (TGT), the session ticket lifetimes, and time-stamp settings. For most organizations, the default settings are appropriate. You will find the Kerberos policy in the Group

Policy Object Editor in the **Account Policy** section of the **Computer Configuration** node, **Security Settings** page, under the **Password and Account Lockout** policies.

*Kerberos* is an authentication protocol that issues identity tickets, which allow entities to prove who they are to other entities in a secure manner. Kerberos has several unique advantages as an authentication protocol. It has the ability to provide delegated authentication by allowing Windows operating system services to impersonate a client computer when accessing resources for it. Kerberos provides single sign-on for domain users and computers by issuing TGTs that they can trade for session tickets to access specific server sessions. Kerberos has expansive interoperability with other networking components because Kerberos is part of the TCP/IP suite of nonproprietary protocols. Kerberos provides a more efficient authentication with servers because you use Kerberos session tickets presented by user-level services for approved access to server resources. Finally, Kerberos delivers mutual authentication because the server presents its credentials back to the user-level services.

### Kerberos policy

You can use the Kerberos policy in a GPO to enforce user sign in restrictions and to define thresholds for maximum service and user ticket lifetime, maximum user ticket renewal lifetime, and the maximum time computer clocks can be out of synchronization. The following settings are available:

- **Enforce user logon restrictions.** Determines if the Kerberos v5 Key Distribution Center (KDC) will validate every session ticket request against the user account's user rights policy. This can add extra security, but it is not required. Choosing to enforce user logon restrictions can slow down services' access to network resources. This setting is enabled by default.


• Kerberos policy settings determine timing for Kerberos tickets and other events

Setting	Default
Enforce user logon restrictions	Enabled
Maximum lifetime for service ticket	600 minutes
Maximum lifetime for user ticket	10 hours
Maximum lifetime for user ticket renewal	7 days
Maximum tolerance for computer clock synchronization	5 minutes

• Kerberos claims and compound authentication for DAC requires Windows Server 2012 or newer domain controllers

- **Maximum lifetime for service ticket.** Defines the maximum time a service ticket is valid for authenticating client access to a particular service. If the service ticket expires before the client requests the server connection, the server will respond with an error and the client redirects requests back to the KDC to receive a new service ticket. This maximum lifetime must be at least 10 minutes but not greater than the maximum lifetime for a user ticket. By default, the maximum service ticket lifetime is 600 minutes, or 10 hours.
- **Maximum lifetime for user ticket.** Sets the amount of time a user account's TGT is valid. The default is 10 hours.
- **Maximum lifetime for user ticket renewal.** Sets the amount of time, in days, for which the user account's TGT can be renewed. The default is seven days.
- **Maximum tolerance for computer clock synchronization.** Determines the amount of time that client computers' clocks can be out of sync with the domain controller. The primary domain controller (PDC) emulator operation master role on a domain determines the correct time for the entire domain. The domain replication packets of TGT and service tickets are time stamped and the times on the various tickets and packets are verified between correspondent computers. However, it is possible for any two computers to be out of sync on their clocks. Administrators can set the amount of time by which the clocks can be out of sync. The default for this setting is five minutes.

You can create access control based on claims and compound authentication by deploying Dynamic Access Control (DAC). You must ensure that you have sufficient Windows Server 2008 or newer domain controllers available that use these new authorization types. The **KDC administrative template policy** setting allows you to configure a domain controller to support claims and compound authentication for DAC and Kerberos armoring. Additionally, Windows Server 2012 or newer domain controller is required for Kerberos clients running the Windows 10, Windows 8.1, or Windows 8 operating systems to support claims and compound authentication by using Kerberos authentication.

 **Note:** Devices that are running Windows 8 and newer operating systems will fail authentication if they cannot find a domain controller that is running Windows Server 2012 or newer. You must ensure that there are sufficient domain controllers that are running Windows Server 2012 or newer for any account, referral, and resource domains that are supported.

## Demonstration: Configuring domain account policies

In this demonstration, you will see how to configure a domain-based password policy and an account lockout policy.

### Demonstration Steps

#### Configure a domain-based password policy

1. On **LON-DC1**, from **Server Manager**, open the **Group Policy Management** console.
2. Edit the Default Domain Policy, and then configure the following account password policy settings:
  - Password history: **20 passwords**
  - Maximum password age: **45 days**
  - Minimum password age: **1 day**
  - Password length: **10 characters**
  - Complexity enabled: **Yes**

## Configure an account lockout policy

1. In the **Group Policy Management Editor** window, configure the following account lockout policy settings for the Default Domain Policy:
  - o Account lockout duration: **30 minutes**
  - o Account lockout threshold: **5 attempts**
  - o Reset account lockout counter after: **15 minutes**
2. Close the **Group Policy Management Editor** window and the **Group Policy Management Console**.

## Protecting groups in AD DS

In most AD DS deployments, some security groups are considered as security critical. Windows Server 2016 provides the Restricted Groups feature and the Protected Users security groups feature to provide additional protection for these groups.

### Restricted groups

For security-critical local groups on servers or workstations, you can use the Restricted Groups functionality available in Group Policy to control membership in these groups and membership of these groups.

Restricted Groups allow you to select a local security group and define two attributes: **Members** and **Member of**.

When defining the **Members** attribute, you specify who should and should not belong to the restricted group being configured. When you configure the **Members** attribute, any current member of a restricted group that is not listed as member is removed automatically, with the exception of the administrator in the Administrators group. Additionally, any user that is listed as member, who is not currently a member of the restricted group, is added automatically.

When you use the **Member of** attribute of a restricted group, make sure that the restricted group is a member of groups that are listed in the **Member Of** text box. You cannot use this attribute to remove the restricted group from any other group.

To configure Restricted Groups, open Group Policy Management Editor and navigate to the **Computer Configuration\Policies\Windows Settings\Security Settings** node.

An example of when you might want to use Restricted Groups is if you want to control membership in the local Administrator group on your organization's workstations.



**Note:** You cannot use this feature to manage domain groups in AD DS. You must use the Restricted Groups feature only with local groups on client or server computers.

- **Restricted groups:**
  - You can control membership for local groups on workstations and servers by using the following attributes:
    - Members
    - Member of
  - You cannot use these with domain groups
- **Protected Users group:**
  - Provides additional protection against the compromise of credentials during authentication processes
  - Members of this group automatically have nonconfigurable protection applied to their accounts



## Protected Users security groups

Windows Server 2012 R2 introduced the Protected Users security group, which generates nonconfigurable protection on:

- Devices and computers that are running Windows Server 2012 R2 and Windows 8.1 or newer operating systems.
- Domain controllers in domains with a primary domain controller that are running Windows Server 2012 R2 or newer.

This substantially reduces the memory footprint of credentials when users sign in to computers on the network from an uncompromised computer. Consider the following points when using Protected Users groups:

- The Protected Users group membership cannot authenticate by using NTLM, Digest authentication, or Credential Security Support Provider (an authentication mechanism also known as *CredSSP*). On devices running Windows 8.1 and newer, passwords are not cached, so the device that uses any one of these Security Support Providers (SSPs) will fail to authenticate to a domain when the account is part of the Protected User group.
- The Kerberos protocol will not use the weaker Data Encryption Standard (DES) or RC4 encryption types in the preauthentication process. Therefore, you must configure the domain to support at least the Advanced Encryption Standard (AES) cipher suite.
- You cannot delegate the user's account with Kerberos constrained or unconstrained delegation. This can cause former connections to other systems to fail if the user is in the Protected Users group.
- The default **Kerberos TGTs lifetime** setting of four hours is configurable by using **Authentication Policies and Silos**, which you can access through the **Active Directory Administrative Center**. This means that the user must authenticate again after four hours.

## Fine-grained password and lockout policies

Starting with Windows Server 2008, administrators can define more than one password policy in a single domain by implementing fine-grained password policies. These give you individual control over user password requirements, and you can have different password requirements for different users or groups. This is beneficial for enforcing more restrictive password settings for administrators, service accounts, or users with highly critical business functions.

To support the fine-grained password policy feature, AD DS in Windows Server 2008 and newer include two object types:

- Password Settings Container. Windows Server creates this container by default, and you can view it in the domain's system container. The container stores the PSOs that you create and link to global security groups or to users.
- PSOs. Members of the Domain Admins group create PSOs and then define specific password and account lockout settings to link to a specific security group or user.

- You can use fine-grained password policies to specify multiple password policies within a single domain
- Fine-grained password policies:
  - Apply only to user objects, **InetOrgPerson** objects, or global security groups
  - Do not apply directly to an OU
  - Do not interfere with custom password filters that you might use in the same domain

Fine-grained password policies only apply to user objects, **InetOrgPerson** objects, or global security groups. By linking a PSO to a user or a group, you are modifying an attribute called **msDS-PSOApplied**, which is empty by default. This approach now treats password and account lockout settings not as domain-wide requirements, but as attributes of a specific user or a group. For example, to configure a strict password policy for administrative accounts, create a global security group, add the administrative user accounts as members, and then link a PSO to the group. Applying fine-grained password policies to a group in this manner is more manageable than applying policies to each individual user account. If you create a new service account, you simply add it to a group, and the PSO manages the account.

By default, only members of the Domain Admins group can create and apply fine-grained password policies. However, you also can delegate the ability to set these policies to other users on a domain-by-domain basis.

### Applying fine-grained password policies

You cannot apply a fine-grained password policy directly to an OU. To apply a fine-grained password policy to OU users, you can use a *shadow group*. A shadow group is a global security group that maps logically to an OU and enforces a fine-grained password policy. You can add an OU's users as members of the newly created shadow group, and then you can apply the fine-grained password policy to this shadow group. If you move a user from one OU to another, you must update the membership of the corresponding shadow groups.

The settings that fine-grained password policies manage are identical to those in the **Password Policy** and **Accounts Policy** nodes of a GPO. However, you neither implement fine-grained password policies as part of Group Policy nor are they applied as part of a GPO. Instead, the PSO is a separate class of object in AD DS that maintains the settings for fine-grained password policy. Additionally, fine-grained password policies do not interfere with custom password settings or filters that you might have implemented.

You can create one or more PSOs in your domain. Each contains a complete set of password and lockout policy settings, and each allows the same configuration options that are available in domain-based password and lockout settings. You apply a PSO by linking it to one or more global security groups or users.

To use a fine-grained password policy, your domain functional level must be at least Windows Server 2008, which means that all of your domain controllers in the domain must be running at least Windows Server 2008. To meet this condition, you must raise the domain functional level to at least Windows Server 2008.

To confirm and modify the domain functional level, use the following procedure:

1. Open **Active Directory Domains and Trusts**.
2. In the console tree, expand **Active Directory Domains and Trusts**, and then expand the tree until you can see the domain.
3. Right-click the domain, and then click **Raise domain functional level**.

## Tools for creating PSOs

PSOs are the key components to implementing fine-grained password policies.

The following table highlights some settings that a PSO can contain.

Windows Server 2012 and newer operating systems provide two tools for configuring PSOs:

- Windows PowerShell cmdlets:
  - **New-ADFineGrainedPasswordPolicy**
  - **Add-FineGrainedPasswordPolicySubject**
- Active Directory Administrative Center

Setting	Value	Description
<b>Password settings</b>		
<b>Name</b>	String	Name of the PSO. Make sure to implement a naming strategy for PSOs.
<b>ComplexityEnabled</b>	True or False	Defines if the PSO enforces the use of complex passwords.
<b>MinPasswordLength</b>	Integer	Minimum length of the password.
<b>MaxPasswordAge</b>	Time: <i>dd.hh:mm:ss</i>	Maximum amount of days before users will need to change their passwords.
<b>MinPasswordAge</b>	Time: <i>dd.hh:mm:ss</i>	Minimum amount of time before users are able to change their passwords. You use this often with <b>PasswordHistoryCount</b> to prevent users from changing their passwords multiple times right away to reuse their old passwords.
<b>PasswordHistoryCount</b>	Integer	Number of passwords that cannot be reused.
<b>ReversibleEncryptionEnabled</b>	True or False	Defines if reversible encryption is allowed. You must set it to False unless you have specific reasons to allow reversible encryption.
<b>Account lockout settings</b>		
<b>LockoutThreshold</b>	Integer	Number of wrong password logons that lead to a locked account.
<b>LockoutObservationWindow</b>	Time: <i>hh:mm:ss</i>	Time period during which the number of wrong passwords will lock the account.
<b>LockoutDuration</b>	Time: <i>hh:mm:ss</i>	Duration after which the account will unlock automatically. If not configured, an administrator needs to unlock the account.

Setting	Value	Description
<b>General settings</b>		
<b>Precedence</b>	Integer	Number that defines the priority of the PSO. If different PSOs apply to the same user, the precedence defines which one will apply.
<b>PSOApplied</b>	Multivalue list of distinguished names	Distinguished names of the users or global security groups to which the PSO should apply.
<b>ProtectedFromAccidentalDeletion</b>	True or False	Defines whether the PSO should be protected from accidental deletion.

You can create and apply PSOs in the Windows Server 2012 and newer environment by using either of the following tools:

- Windows PowerShell
- **Active Directory Administrative Center**

### Configuring PSOs by using Windows PowerShell

In Windows Server 2012 and newer, you can use the following cmdlets in the Active Directory module for Windows PowerShell to create and manage PSOs in your domain.

- **New-ADFineGrainedPasswordPolicy.** This cmdlet creates a new PSO and defines its parameters. For example, the following command creates a new PSO named **TestPwd** and then specifies its settings:

```
New-ADFineGrainedPasswordPolicy TestPswd -ComplexityEnabled:$true -
LockoutDuration:"00:30:00" -LockoutObservationWindow:"00:30:00" -LockoutThreshold:"0"
-MaxPassDuration:"42.00:00:00" -MinPassDuration:"1.00:00:00" -MinPasswordLength:"7" -
PasswordHistoryCount:"24" -Precedence:"1" -ReversibleEncryptionEnabled:$false -
ProtectedFromAccidentalDeletion:$true
```

- **Add-FineGrainedPasswordPolicySubject.** This cmdlet enables you to link a user or group to an existing PSO. For example, the following command links the **TestPwd** PSO to the AD DS group named **Marketing**:

```
Add-ADFineGrainedPasswordPolicySubject TestPswd -Subjects Marketing
```

### Configuring PSOs by using Active Directory Administrative Center

The **Active Directory Administrative Center** provides a GUI for creating and managing PSOs. To manage PSOs in the **Active Directory Administrative Center**, follow this procedure:

1. Open **Active Directory Administrative Center**.
2. Click **Manage**, click **Add Navigation Nodes**, in the **Add Navigation Node** dialog box, select the appropriate target domain, and then click **OK**.
3. In the **Active Directory Administrative Center** navigation pane, open the **System** container, and then click **Password Settings Container**.
4. In the **Tasks** pane, click **New**, and then click **Password Settings**.
5. Configure the settings for the new PSO.

6. Under **Directly Applies To**, click **Add**, type **Marketing**, and then click **OK**.

This associates the **Password Policy** object with the members of the global group that you created for the test environment.

7. Click **OK** to submit the creation of the PSO.



**Note:** The **Active Directory Administrative Center** interface for PSO management uses the Windows PowerShell cmdlets mentioned previously to carry out the creation and management of PSOs.

## Demonstration: Configuring a fine-grained password policy

In this demonstration, you will see how to configure and apply a fine-grained password policy.

### Demonstration Steps

1. On **LON-DC1**, open **Active Directory Administrative Center**.
2. Change the group scope for the **Managers** group to **Global**.



**Note:** Ensure that you open the **Properties** dialog box for the Managers group, and not the Managers OU.

3. In **Active Directory Administrative Center**, configure a fine-grained password policy for the **Adatum\Managers** group with the following settings:
  - o Name: **ManagersPSO**
  - o Precedence: **10**
  - o Password length: **15 characters**
  - o Password history: **20 passwords**
  - o Complexity enabled: **Yes**
  - o Minimum password age: **1 day**
  - o Maximum password age: **30 days**
  - o Number of failed logon attempts allowed: **3 attempts**
  - o Reset failed logon attempts count after: **30 minutes**
  - o Select **Until an administrator manually unlocks the account**
4. Close the **Active Directory Administrative Center**.

## PSO precedence and resultant PSO


You can link more than one PSO to a user or a security group. This happens when a user is a member of multiple security groups that might each already have an assigned PSO or when you assign multiple PSOs directly to a user object. In either case, only one PSO can be the effective password policy. If you assign multiple PSOs to a user or a group, the **msDS-PasswordSettingsPrecedence** attribute helps determine the resultant PSO. A PSO with a lower value takes precedence over a PSO with a higher value.

- If multiple PSOs apply to a user:
  - The PSOs that you directly apply take precedence rather than the PSOs that you apply by using group memberships
  - The PSO with the lowest precedence wins
  - If two PSOs have the same precedence, the smallest objectGUID wins
- To evaluate a user object to see which PSO has been applied, you can use the **msDS-ResultantPSO** Active Directory attribute
- To view the effective PSO that AD DS applies to a user:
  1. Open Active Directory Users and Computers, and on the **View** menu, ensure that **Advanced Features** is enabled
  2. Open the properties of a user account
  3. On the **Attribute Editor** tab, view the **msDS-ResultantPSO** attribute if you have configured the **Show Constructed Attributes** option under the **Filter** options

The following process describes how AD DS determines the resultant PSO if you link multiple PSOs to a user or a group:

1. Any PSO that you link directly to a user object is the resultant PSO. If you link multiple PSOs directly to the user object, the PSO with the lowest **msDS-PasswordSettingsPrecedence** value is the resultant PSO. If two PSOs have the same precedence, the PSO with the mathematically smallest objectGUID is the resultant PSO.
2. If you do not link any PSOs directly to the user object, AD DS compares the PSOs for all global security groups that contain the user object. The PSO with the lowest **msDS-PasswordSettingsPrecedence** value is the resultant PSO. If you apply multiple PSOs to the same user, and they have the same **msDS-PasswordSettingsPrecedence** value, AD DS applies the PSO with the mathematically smallest objectGUID.
3. If you do not link any PSOs to the user object, either directly or indirectly through group membership, AD DS applies the Default Domain Policy.

All user objects contain a new attribute called **msDS-ResultantPSO**. You can use this attribute to determine the distinguished name of the PSO that AD DS applies to the user object. If you do not link a PSO to the user object, this attribute does not contain any value and the Default Domain Policy GPO contains the effective password policy. To view the effective PSO that AD DS applies to a user, open **Active Directory Users and Computers**, and on the **View** menu, ensure that **Advanced Features** is enabled. You then should open the properties of a user account, and you can view the **msDS-ResultantPSO** attribute on the **Attribute Editor** tab if you have configured the **Show Constructed Attributes** option under the **Filter** options.

 **Note:** While you must define PSOs from a highly privileged group such as Domain Admins, you should train help-desk administrators to evaluate the effective PSOs for a user. This helps administrators answer user's questions when they do not understand which password settings apply.

## Account-security options in Windows Server 2016

Secure accounts achieve a secure AD DS forest and domain infrastructure. By default, every account that signs in to a domain-joined client or server is cached locally on that computer. The computer maintains, by default, the last 10 user profiles and their associated credentials. This is risky, for example, in the following situations:

- Consider an administrative account that is used for troubleshooting or supporting users by signing in locally to a regular user's device. The user account profile and its credentials are stored in the system. If the owner of the system has higher local rights, he or she can use tools to retrieve the administrative credentials, and then use them to access other information on the network.
- Certain user accounts and computers contain highly critical information of your organization. Therefore, ensure that only authorized users can sign in to their workstations, and make sure that other users cannot access the same computers.

You should configure highly trusted service accounts for authorization only on a certain set of computers.

To provide administrators with the ability to address these risks and requirements, Windows Server 2016 and Windows Server 2012 R2 include new functionalities for credential protection and management:

- Protected Users
- Authentication policies
- Authentication policy silos

### Protected Users

The Protected Users security group prevents highly sensitive accounts from being locally cached on domain member computers. It requires domain-controller authentication for those accounts for every sign in that occurs.

Protected Users is a new group that you can use to configure highly sensitive accounts and you can find it in the Users container in AD DS. To enable Protected Users, an administrator simply adds the highly trusted accounts to the Protected Users security group. This Protected Users feature does not require Windows Server 2012 R2 domain controllers. However, this group is created only when a Windows Server 2012 R2 or newer domain controller receives the PDC emulator operations master role. For further use of this feature, it is not necessary that the PDC emulator operations master remain on the Windows Server 2012 R2 domain controller, and it is not necessary to maintain the domain controller. However, because the domain controller can only be promoted when the schema has been extended, the schema extension for Windows Server 2012 R2 or newer needs to be in place even if the feature does not require it.

The Protected Users feature is a client-side feature that protects domain accounts on domain member computers. Protected Users depend on the domain member's operating system and is available on the following operating systems:

- Windows 8.1 or newer
- Windows Server 2012 R2 or newer

- **Protected Users group:**
  - Protects users in the Protected Users group
  - Prevents locally cached user profiles and credentials
  - Requires Kerberos authentication, limits TGT to four hours
  - No offline sign in
  - Windows 8.1, Windows 10, Windows Server 2012 R2 and Windows Server 2016 domain members only
- **Authentication policies:**
  - Configured as authentication policy object in AD DS, applied to user, service, or computer accounts
  - Custom TGT
  - Uses claims (DAC) for custom conditions
- **Authentication policy silos:**
  - AD DS object
  - Centrally apply authentication policies to multiple objects
  - Additional claim allows administrators to configure file access per silo

Older operating systems will not support this feature and will not prevent the accounts in the Protected Users group from being cached locally. To ensure that accounts within the Protected Users group are not compromised on older operating systems, use the other methods such as the **Deny log on locally** security setting where appropriate.

Protected Users who sign in to a domain member computer that has a supported operating system will be prevented from using the following protocols:

- Default credential delegation, or Credential Security Support Provider (CredSSP)
- Digest authentication
- NTLM

When all domain controllers of the sign-in domain are based on Windows Server 2012 R2, and the domain functional level is raised to Windows Server 2012 R2, additional security is provided. Because of this additional security, users cannot:

- Use DES or RC4 encryption in Kerberos preauthentication.
- Be delegated with unconstrained or constrained delegation.
- Renew their Kerberos TGT without contact with the domain controller.

The following applies when a user is a member of the Protected Users security group:

- The user must be able to use authentication based on AES encryption. Therefore, all domain controllers must be at a Windows Server 2008 level or newer.
- The password of any account in the Protected Users group must have been changed against a Windows Server 2008 or newer domain controller to ensure that the password was encrypted by using AES.
- On supported domain members, such as Windows 10 and Windows Server 2016, the credentials of the user will not be cached.
- The user will only be able to sign in to domain members that are able to authenticate against a domain controller. Offline sign in will not work for these accounts. The startup of services that use an account that is a member of the Protected Users group will fail when the domain member is offline.
- The maximum lifetime of the issued Kerberos TGT and the maximum lifetime for ticket renewal are limited to 240 minutes (four hours). While administrators configure all other accounts by using the domain policy settings, which are 10 hours by default for the ticket and seven days for renewal, four hours are hard-coded for Protected Users.

Protected Users is a security setting that is global within the domain. This setting does not allow you to protect certain users only on certain devices. Therefore, use Protected Users carefully and test it before relying on the Protected Users feature.

### Authentication policies

With authentication policies, you can configure more-restrictive Kerberos settings for specific user or service accounts. Additionally, you can use DAC claims to define conditions that need to be met by users, service accounts, and/or devices during sign in.

Authentication policies implement by using a new object class with the name **authentication policy** in AD DS.




To implement authentication policies, you need to ensure that you meet the following prerequisites, including that:


- All domain controllers in the domain must be based on Windows Server 2012 R2 or newer.
- The domain functional level must be Windows Server 2016 or Windows Server 2012 R2.
- Domain controllers must be configured to support DAC.
- Windows 10, Windows 8.1, Windows 8, Windows Server 2016, Windows Server 2012 R2, or Windows Server 2012 domain members must be configured to support DAC, including Kerberos compound claims (device claims).

When configuring an authentication policy in the **Active Directory Administrative Center**, you can configure the following settings:

- Display name of the authentication policy.
- Description.
- If the policy should be enforced (default), or if you want to validate the policy by audit policy restrictions only.
- Accounts to which the policy should apply. Accounts are in the authentication policy settings; however, be aware that you configure this on the account, unlike authentication policy silos, where the accounts are configured within the silo.
- For user, service, and computer accounts, you can define the following settings separately:
  - The TGT lifetime of the account.
  - Access control conditions using DAC claims that define which users or services are able to run on which devices.

You can configure these settings to user accounts either within the user properties window in the **Active Directory Administrative Center**, or by configuring them in the authentication policy properties window. Regardless of where you configure these settings, they are written to the authentication policy. After you configure these settings, you will sign in to a device, or you will receive the message that "Your account is configured to prevent you from using this PC." In either case, an event is logged.

 **Note:** While older operating systems had options to restrict users from signing in to specific devices, they were easy to circumvent. Authentication policies and authentication-policy silos that are built on Kerberos (instead of names only), and DAC claims, provide a secure method to ensure that only certain users can sign in to certain devices.

 **Note:** Authentication policies do not prevent users from signing in by using NTLM. When a domain member is fully able to communicate by using Kerberos, it is likely that the rules configured in the authentication policy work as expected. However, there might be scenarios where NTLM is used. To prevent this, consider combining Protected Users and account policies.

## Authentication policy silos

Authentication policy silos enable administrators to configure users, service accounts, and computers within the same security scope to apply the same authentication policy. Authentication policies enable administrators to select a separate authentication policy for each security principal type: user, service, or computer accounts. The system then adds an additional claim to a silo's principals, which enables file-server administrators to restrict access to certain files for security principals of specific authentication policy silos.

The prerequisites of authentication policy silos are the same as the prerequisites of authentication policies. You should use them as an alternative means to assign user, service, or computer accounts to use certain authentication policies. By using Active Directory delegation, you are able to assign different roles to create authentication policies and then assign those policies to security principals by using authentication policy silos.

Like authentication policies, you can configure authentication policy silos to be enforced or in auditing mode. Authentication policies are enforced by default, while authentication policy silos are configured in auditing mode. Additionally, authentication policy silos have a higher precedence than authentication policies.

Furthermore, authentication policy silos do provide a claim and an administrator can use it to ensure that certain files or certain file structures can only be accessed when users or computers have been validated by an authentication policy silo.



**Additional Reading:** For more information on credentials protection and management, refer to: <http://aka.ms/R5bfd>

## Configuring user account policies

There are several options available for configuring user account policies when you are administering an AD DS environment.

### Local policy settings with Secpol.msc

Each individual Windows Server 2016 computer has its own set of account policies, which apply to accounts created and managed on the local computer. To configure these policy settings, open the **Local Security Policy Console** by running **secpol.msc** at the command prompt. You can locate the password policy and account policy settings within the **Local Security Policy Console** by expanding **Security Settings**, and then expanding **Account Policies**.

- Local Security Policy account settings:
  - Configure with **secpol.msc**
  - Apply to local user accounts
- Group Policy account settings:
  - Configure with the Group Policy Management console
  - Apply to all accounts in AD DS and local accounts on computers joined to the domain
  - Can apply only once in a domain and in only one GPO
  - Take precedence over Local Security Policy settings

### Group Policy with Group Policy management

In the AD DS domain environment, you configure domain-wide account policy settings within the Group Policy Management Editor. To find the settings' domain-wide account policy settings, expand the **Computer Configuration** node, expand the **Policies** node, expand the **Windows Settings** node, expand the **Security Settings** node, and then expand the **Account Policies** node.

The settings found within the **Account Policies** node are the same settings found in the Local Security Policy, with the addition of the Kerberos Policy settings that apply to domain authentication.

The Group Policy account policy settings exist in the template of every GPO that you create in the Group Policy Management Console. However, you can apply an account policy only once in a domain and in only one GPO. This is the Default Domain Policy, and it links to the root of the AD DS domain. Therefore, the account policy settings in the Default Domain Policy apply to every computer that is joined to the domain.



**Note:** If settings conflict between the account policy settings in the Local Security Policy and the account policy settings in the Default Domain Policy GPO, the Default Domain Policy settings take precedence.

When you initially install a Windows operating system, such as Windows 8.1, Windows 10, or Windows Server 2016, the computer will have a password policy with settings configured and established by default, but the account lockout policy does not have any settings configured. When you install a domain, the Default Domain Policy that is created contains all three policies. You can make changes to any of the policies, including configuring the settings in the account lockout policy. However, you need to consider the implications carefully before doing so.

In most cases, your organization will already have established domains and computer systems that have these settings configured. Most organizations also have numerous written security policies that dictate standards for password and account lockout policies. In these cases, you cannot make changes without approval or without addressing the written security policies.

## Enhancing password authentication with Windows Hello and MFA

As user identities become more critical, it is necessary to develop new technologies to protect identities, and to protect the process of identity verification or authentication. In the new version of operating systems, and in cloud services, Microsoft provides enhanced authentication technologies that combine multiple factors.

### Windows Hello and Microsoft Passport

To enhance security on the client side, and to additionally secure authentication process, Microsoft implemented Microsoft Passport and Windows Hello technologies in the Windows 10 operating system. These technologies allow you to use additional or different methods of authentication, instead of the traditional combination of a username and password.

Windows Hello is the biometric technology that allows users to sign in to Windows by using their fingerprints, facial recognition, or iris scan. Many business laptops today have built-in fingerprint readers, and Windows Hello supports most of the existing fingerprint-reader hardware. Additionally, on some mobile devices, such as Microsoft Lumia 950, an iris-scan camera is available, and it uses Windows Hello to recognize a user and allow them to sign in.

Windows Hello technology enables you to use alternative and more secure methods to sign in to your computer or mobile device. Additionally, because Windows Hello is an extensible technology, it will be compatible with new hardware that has not yet reached the market.

To enhance security of the authentication process, you can use:

- Windows Hello:
  - For biometric-based sign in to Windows
- Microsoft Passport:
  - To leverage Windows Hello and TPM
- Azure Multi-Factor Authentication:
  - To enhance account security by adding second factor of verification
  - Can be used in cloud or for on-premises applications



Microsoft Passport is a technology that complements Windows Hello. Microsoft Passport provides a two-factor authentication by combining biometrics data from Windows Hello with encryption keys taken from the device. Microsoft Passport also lets you establish a PIN that you can use to sign in to a Windows 10 device, instead of using a password. Using a PIN instead of a password is more secure, as the PIN is bound to the device that you use. For each device that you use, you can establish a different PIN, but still be signed in with a same user account.

Microsoft Passport is a technology that uses trusted platform module (TPM) chips intensively. TPM provides the ability to store authentication keys securely. When the user authenticates to Windows Hello, by using the biometrics mechanism, Microsoft Passport takes the authentication data and uses it to have the TPM chip generate a set of public and private keys.

On each Windows 10 device (mobile, desktop, and laptop), you can configure more than one authentication method. For example, you can configure a PIN and also utilize your fingerprint to sign in to your Windows 10 computer. Furthermore upon each sign in, you can decide which method you will use. Similarly, on your mobile Windows 10 device, such as Lumia 950, you can use a PIN or an iris scan to unlock the device.

Windows Hello is the technology that you can also use to authenticate to your application, not just to the operating system. Developers can use Windows Hello to enhance security on their applications that require authentication.

### **Microsoft Azure Multi-Factor Authentication**

The purpose of Multi-Factor Authentication (MFA) is to increase security. Traditionally, standard authentication requires knowledge of sign-in credentials, which typically consist of a user name and an associated password. Multi-Factor Authentication adds an extra verification that relies on either having access to a device that is presumably in the possession of the rightful owner or having physical characteristics of that person, as in the case of biometrics. This additional requirement makes it considerably more difficult for an unauthorized individual to compromise the authentication process.

Multi-Factor Authentication is integrated into Azure Active Directory (Azure AD). It allows the use of a phone as the physical device that provides the means of confirming a user's identity. The process of implementing Multi-Factor Authentication for an Azure AD user account starts when a user with the global administrator role enables the account for Multi-Factor Authentication from the Azure portal. At the next sign-in attempt, the user is prompted to set up authentication by selecting one of the following options:

- Mobile phone. Requires the user to provide a mobile phone number. Verification can be a text message or in the form of a phone call—at the end of which, the user must press the pound key (#).
- Office phone. Requires the specification of the OFFICE PHONE entry of the user's contact information in Azure AD. An administrator must preconfigure this entry, and the user cannot modify or provide this entry at verification time.
- Mobile app. Requires that the user has a smartphone on which the user must install and configure the mobile phone app.

As part of the verification process, a user also can generate application passwords, because Multi-Factor Authentication is limited to authenticating access to applications and services from a browser. Effectively, it does not apply to traditional desktop applications or modern applications such as Outlook, Skype for Business, or mobile apps for email. A user then can use their configuration settings to assign randomly generated application passwords to individual applications.

However, application passwords can be vulnerable to attacks. Therefore, as an administrator, you can prevent all directory users from creating application passwords. You also can invalidate all application passwords for an individual user if the computer or device where the applications are installed is compromised.

After the verification process is complete, the Multi-Factor Authentication status for the user changes from enabled to enforced. The same verification process repeats during every subsequent authentication attempt. The additional security verification option appears in the Access Panel, reflecting the status change. From the Access Panel, you can choose and configure a different verification mechanism and generate application passwords. Generating application passwords is especially important, because without assigned application passwords, desktop applications and modern applications that rely on authenticated access to Azure AD will fail to connect to Azure Cloud Services.

You can use Multi-Factor Authentication to protect on-premises resources by using the Azure Multi-Factor Authentication Server. Multi-Factor Authentication Server integrates with Internet Information Services (IIS) authentication to secure Microsoft IIS web applications, Remote Authentication Dial-in User Service (RADIUS) authentication, Lightweight Directory Access Protocol (LDAP) authentication, and Windows authentication.

Before you can use the Multi-Factor Authentication Server, you must download and activate it. The download is available through a link on the Multi-Factor Authentication management portal. The Azure Multi-Factor Authentication Users Portal is an Internet Information Services (IIS) website at which users can enroll for Azure Multi-Factor Authentication and manage their Multi-Factor Authentication accounts.

User enrollment and self-management involves users completing their enrollment, such as by selecting an authentication method if the administrator has not prespecified this.

**Question:** Which technology allows you to use biometric functionality to sign in to Windows devices?

## Lesson 3

# Implementing audit authentication

Auditing is an important security component. Windows Server 2016 domain controllers and other servers log security-related events to the Security log, where you can monitor and identify issues that might warrant further investigation. Auditing can log successful activities to provide documentation of changes. It also can log failed and potentially malicious attempts to access enterprise resources. Auditing involves up to three management steps: configuring an audit policy, configuring auditing settings on objects, and viewing events in the Security log. In this lesson, you will learn how to configure auditing to address several common scenarios.

### Lesson Objectives

After completing this lesson, you will be able to:

- Describe account logon and logon events.
- Configure authentication-related audit policies.
- Describe scope audit policies.
- View logon events.

### Account logon and logon events

Before configuring auditing, you first need to understand the difference between two similarly named policy settings: **Audit account logon events** and **Audit logon events**.

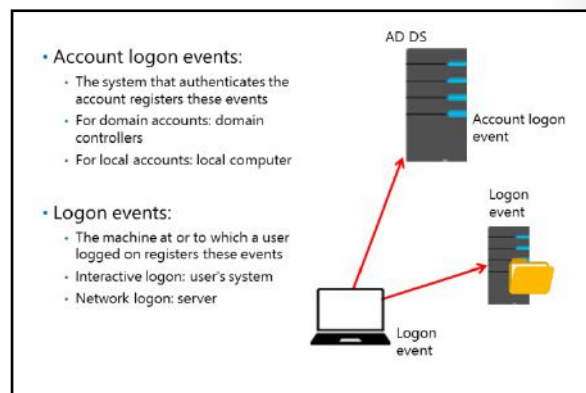
When a user signs in to any computer in the domain by using a domain user account, a domain controller authenticates this attempt. This generates an account logon event on the domain controller.

The computer to which the user signs in, for example, the user's laptop, generates a logon event. The computer did not authenticate the user against the account, but rather passed the account to a domain controller for validation. However, the computer did allow the user to sign in interactively to the computer. Therefore, the event is a logon event.

When a user connects to a folder on a server in the domain, that server authorizes the user for a type of logon called a network logon. Again, the server does not authenticate the user. Instead, it relies on the ticket that the domain controller gives to the user. However, the user connection generates a logon event on the server.

### Advanced audit policies

In previous Windows Server versions, such as Windows Server 2008, there are only nine auditing categories. Administrators can configure each category to perform auditing and to monitor the success, failure, or both success and failure, of specific tasks and events. These events are fairly broad in scope, and can be triggered by a variety of similar actions, some of which can generate a large number of event log entries.



In Windows Server 2012 and Windows Server 2016, the number of auditable events expanded from nine to 53, which enables administrators to be more selective in the number and types of events to audit.

These new, advanced audit policies allow administrators to connect business rules and audit policies. This gives administrators much more control over the logon process, and they can obtain information about very specific events that happen during the logon or logoff process.

For an account logon event, you now can define four different audit settings:

- **Credential validation.** Audits events that validation tests generate on user-account logon credentials.
- **Kerberos service ticket operations.** Audits events that Kerberos service-ticket requests generate.
- **Other account logon events.** Audits events that are generated by responses to credential requests that are not credential validation or Kerberos tickets requests.
- **Kerberos authentication service.** Audits events that Kerberos authentication TGT requests generate.

You can audit the following logon and logoff events:


- **Logon.** Audits events that are generated by user account logon attempts on a computer.
- **Logoff.** Audits events that closing a logon session generates. These events occur on the accessed computer, and for an interactive logon, the security audit event is generated on the computer to which the user account logged on.
- **Account lockout.** Audits events that are generated by a failed attempt to sign in to an account that is locked out.
- **IPsec main mode.** Audits events that are generated by the Internet Key Exchange (IKE) protocol and Authenticated Internet Protocol (AuthIP) during main mode negotiations.
- **IPsec quick mode.** Audits events that IKE and AuthIP generate during quick-mode negotiations.
- **IPsec extended mode.** Audits events that IKE and AuthIP generate during extended-mode negotiations.
- **Special logon.** Audits events that special logons generate.
- **Other logon and logoff events.** Audits of other events that are related to logon and logoff, and which are not included in the **Logon** and **Logoff** settings.
- **Network Policy Server.** Audits events that are generated by RADIUS, Internet Authentication Service, and NAP user access requests. These requests can be Grant, Deny, Discard, Quarantine, Lock, and Unlock.

### Basic audit policies vs. advanced audit policies

The basic security audit-policy settings are in **Security Settings\Local Policies\Audit Policy**, and the advanced security audit policy settings are in **Security Settings\Advanced Audit Policy Configuration\Audit Policies**. Although the basic and advanced security audit-policy settings appear to overlap, they are recorded and applied differently.

The new set of advanced audit policies enables administrators to be more selective in the number and types of events to audit. For example, where a basic audit policy provides a single setting for account logon, advanced audit policy provides four. Enabling the single basic account logon setting is the equivalent of setting all four advanced account logon settings. In comparison, setting a single advanced audit policy setting does not generate audit events for activities for which you have no interest. For example, if you enable success auditing for the basic **Audit account logon events** policy setting, only success events will be logged for all account logon-related behaviors. In comparison, you can configure

success auditing for one advanced account logon setting, failure auditing for a second advanced account logon setting, success and failure auditing for a third advanced account logon setting, or no auditing, depending on the needs of your organization.

 **Note:** Using both the basic and advanced settings can cause unexpected results. Therefore, do not combine the two sets of audit policy settings. If you use **Advanced Audit Policy Configuration** settings, you should enable the **Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings** policy setting under **Local Policies\Security Options**. This will prevent conflicts between similar settings by forcing basic security auditing to be ignored.

## Demonstration: Configuring authentication-related audit policies

In this demonstration, you will see how to configure authentication-related audit policies.

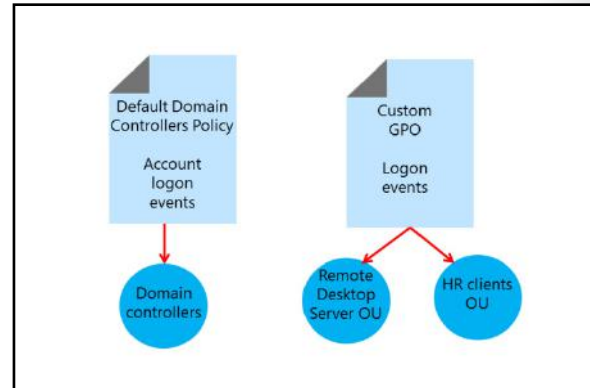
### Demonstration Steps

1. On **LON-DC1**, from **Server Manager**, open the **Group Policy Management Console**.
2. Navigate to the **Default Domain Controllers Policy**, and then edit the policy.
3. In the **Group Policy Management Editor** window, navigate to **Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Audit Policy**.
4. Explain the nine legacy policy categories shown in the details pane.
5. Navigate to **Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies**.
6. View the ten main categories under advanced audit policies, and then click **Account Logon** and **Logon/Logoff** to view the available subcategories.
7. Under **Account Logon**, open the properties of the **Audit Kerberos Authentication Service** policy.
8. Note that you can enable the policy to log a Success or Failure event. Enable the policy and select **Success** and **Failure**.
9. Click the **Explain** tab to view the detailed information about the event, the default logging settings, and the predicted auditing volume.
10. Apply the changed policy, and then click **OK** to close the policy setting.



## Scoping audit policies

As with all policy settings, you should define the scope carefully for the GPOs that apply your audit policies, so that the settings affect the correct systems. For example, if you want to audit attempts by users to connect to remote desktop servers in your enterprise, you can configure logon event auditing in a GPO that is linked to the OU that contains your remote-desktop servers. However, on the other hand, if you want to audit desktop logons by users in your Human Resources department, you can configure logon-event auditing in a GPO that is linked to the OU that contains Human Resources computer objects. Remember that a domain user who signs in to a client computer or connects to a server will generate a logon event—not an account logon event—on that system.



Only domain controllers generate account-logon events for domain users. Remember that an account-logon event occurs on the domain controller that authenticates a domain user, regardless of where that user logs on. If you want to audit logons to domain accounts, you should ensure account logon event auditing to affect all domain controllers. The Default Domain Controllers GPO that is created when you install your first domain controller is an ideal GPO in which to configure account logon audit policies.

## Demonstration: Viewing logon events

In this demonstration, you will see how to view logon events.

### Demonstration Steps

1. On **LON-DC1**, run **gpupdate /force**.
2. Sign out.
3. Attempt to sign in as **Adatum\Aidan** with password as **123456**.
4. Sign in as **Adatum\Administrator** with password as **Pa\$\$w0rd**.
5. From **Server Manager**, in the **Tools** menu, open **Event Viewer**.
6. Navigate to the **Security** log.
7. Show the **Audit Failure** event with the Event ID 4771, and then show the **Audit Success** event with the Event ID 4768.

Verify the correctness of the statement by placing a mark in the column to the right.

Statement	Answer
When a user signs in to a domain controller, a logon event is generated.	

## Lesson 4

# Configuring managed service accounts

Creating user accounts to provide authentication for applications, system services, and background processes is a common practice in the Windows environment. Historically, you would create accounts and name them for use by a specific service. Windows Server 2016 supports AD DS account-like objects, known as *managed service accounts* (MSAs), which make service accounts easier to manage and which pose less of a security risk to your environment.

This lesson will introduce you to MSAs and the new functionality related to MSAs introduced in Windows Server 2016.

### Lesson Objectives

After completing this lesson, you will be able to:

- Describe service accounts.
- Identify the challenges of using standard user accounts for services.
- Describe MSAs.
- Describe group MSAs.
- Configure group MSAs.
- Describe Kerberos delegation and service principal names (SPNs).

### Overview of service accounts

In the Windows operating system, applications sometimes require administrative access to local and network resources. In the past, it was common to give these applications administrative account permissions to the resources. For example, a Microsoft SQL Server needs to manage its databases and it might need local administrative access to do this. In a distributed SQL Server environment, with multiple SQL Servers each hosting numerous databases, it may need administrative access to all of them. For that reason, an administrator needs to create an

account for SQL Server that belongs to the Domain Admins group, or at least the computers' local Administrators group, with a password that is configured to not ever expire. Administrators need to remember to periodically change the password manually on every server service under which it runs. This type of account introduces possible security issues and, if compromised, can endanger an entire domain.

- Sometimes, applications require resource access:
  - For this purpose, you can create domain or local accounts to manage such access. However, this might compromise security
- Use the following service accounts instead:
  - Local System:
    - Most privileged, still vulnerable if compromised
  - Local Service:
    - Least privileged, may not have enough permissions to access all required resources
  - Network Service:
    - Can access network resources with proper credentials

Therefore, because of the possible security issues, you could consider running the program or service by using a built-in local account. Windows operating systems have three built-in local accounts to allow program and service access of resources. These accounts are tied to the individual computer rather than a user account, as follows:

- **Local System.** Has extensive privileges on the local system and acts as the computer on the network. It is a very high-privileged built-in account. The name of the account is NT AUTHORITY\SYSTEM.
- **Local Service.** Has the same level of access to resources and objects as members of the local Users group. This limited access helps protect the system if individual services or processes are compromised. Services running as the Local Service account will access network resources as a null session without any credentials. The name of the account is NT AUTHORITY\LOCAL SERVICE.
- **Network Service.** Has more access to resources and objects than members of the Users group have, such as the Local Service account. Services that run as the Network Service account access network resources by using the credentials of the computer account. The name of the account is NT AUTHORITY\NETWORK SERVICE.

You should be aware that using the Local System account still might compromise security, considering the high-level privileges under which it operates. Therefore, you should take extra care when using this account for program access. Alternatively, the Local Service account may not have enough privileges to access all the resources required by the program. If the program needs resources on other computers, you could use the Network Service account. However, you must add the machine account to a group in the domain or individually on the other computers. In all cases, you should make a thorough security analysis to ensure you consider all aspects of using the service accounts.

## Challenges of using service accounts

Many programs such as SQL Server or IIS contain services that you install on the server that hosts the program. These services typically run at server startup or are triggered by other events. Services often run in the background and do not require any user interaction.

For a service to start up and authenticate, you use a service account. A service account may be an account that is local to the computer, such as the built-in Local System, Local Service, or Network Service accounts. You also can configure a service account to use a domain-based account located in AD DS.

- Extra administration effort to manage the service account password
- Difficulty in determining where a domain-based account is used as a service account
- Extra administration effort to manage the SPN

- To help centralize administration and to meet program requirements, many organizations choose to use a domain-based account to run program services. Although this does provide some benefit over using a local account, there are a number of associated challenges, such as the following: Extra administration effort may be necessary to manage the service account password securely. This includes tasks such as changing the password and resolving situations that cause an account lockout. Service accounts also typically are configured to have passwords that do not expire, which may go against your organization's security policies.

- Difficulty in determining where a domain-based account is used as a service account. You may use a standard user account for multiple services on various servers throughout the environment. A simple task, such as changing the password, may cause authentication issues for some applications. It is important to know where and how to use a standard user account when it is associated with a program service.
- Extra administration effort may be necessary to manage the service principal name (SPN). Using a standard user account may require manual administration of the SPN. If the logon account of the service changes, the computer name is changed. Alternatively, if a DNS host name property is modified, you may need to modify the SPN registrations manually to reflect the change. A misconfigured SPN causes authentication problems with the program service.

Windows Server 2016 supports an AD DS object, named a *Managed Service Account (MSA)*, which you use to facilitate service-account management. The subsequent topics provide information on the requirements and use of MSAs in Windows Server 2016.

## Overview of managed service accounts

An MSA is an AD DS object class that enables simplified password and SPN management for service accounts. The MSA was introduced in Windows 7 and Windows Server 2008 R2.

Many network-based programs use an account to run services or provide authentication. For example, a program on a local computer might use the Local Service, Network Service, or Local System accounts. These service accounts may work fine. However, these typically are shared among multiple programs and services, which makes it difficult to manage for a specific program. Furthermore, you cannot manage these local service accounts at the domain level.

Alternatively, it is quite common that a program might use a standard domain account that you configure specifically for the program. However, the main drawback is that you need to manage passwords manually, which increases administration effort. A managed service account can provide a program with its own unique account, while eliminating the need for an administrator to administer the account's credentials manually.

### How an MSA works?

MSAs are stored in AD DS as **msDS-ManagedServiceAccount** objects. This class inherits structural aspects from the Computer class, which it inherits from the User class. This enables an MSA to fulfill User-like functions, such as providing authentication and security context for a running service. It also enables an MSA to use the same password-update mechanism that Computer objects in AD DS use, which is a process that requires no user intervention.

MSAs provide the following benefits to simplify administration:


- Automatic password management. An MSA maintains its own password, including password changes, automatically.
- Simplified SPN management. SPN management happens automatically if you configure your domain at the Windows Server 2008 R2 domain functional level or higher.

- Use MSAs to automate password and SPN management for service accounts that services and applications use
- Requires a Windows Server 2008 R2 or newer installed with:
  - .NET Framework 3.5.x
  - Active Directory module for Windows PowerShell
- Recommended to run with AD DS configured at the Windows Server 2008 R2 functional level or higher

MSAs are stored in the **CN=Managed Service Accounts, DC=<domain>, DC=<com>** container. You can view this by enabling the **Advanced Features** option on the **View** menu within **Active Directory Users and Computers**. This container is visible by default in the **Active Directory Administrative Center**.

### Requirements for using MSAs

To use an MSA, the server that runs the service or program must be running Windows Server 2008 R2 or a newer operating system. You also must ensure that Microsoft .NET Framework 3.5.x and the Active Directory module for Windows PowerShell are both installed on the server.

 **Note:** You cannot share a standard MSA between multiple computers or that you use in server clusters where the service is replicated between nodes. Additionally, you cannot use MSAs for unattended scheduled tasks.

To simplify and provide full automatic password and SPN management, we strongly recommend that the AD DS domain be at the Windows Server 2008 R2 functional level or higher. However, if you have a domain controller that is running Windows Server 2008, you can update the Active Directory schema to Windows Server 2008 R2 to support this feature. The only disadvantage is that the domain administrator must configure SPN data manually for the MSAs.

### Using MSAs on Windows Server 2016 Domain Controllers

In Windows Server 2016, you create MSAs as the new group managed service account object type by default. However, on a Windows Server 2016 domain controller, you accommodate this by creating a key distribution services (KDS) root key for the domain. To create the root key, you must run the following cmdlet from the Active Directory module for Windows PowerShell:

```
Add-KDSRootKey -EffectiveTime ((Get-Date).AddHours(-10))
```

The next topic discusses group MSAs in more detail, including providing further explanation of how you can create a KDS root key and the **Add-KDSRootKey** cmdlet.

### What are group MSAs?

You use group MSAs to extend the capabilities of standard MSAs to more than one server in your domain. In server-farm scenarios with Network Load Balancing (NLB) clusters or IIS servers, you often need to run system or program services under the same service account. Standard MSAs cannot provide MSA functionality to services that are running on more than one server. However, by using group MSAs, you can configure multiple servers to use the same MSA and still retain the benefits that MSAs provide, like automatic password maintenance and simplified SPN management.


- Group MSAs extend the capability of standard MSAs by:
  - Enabling MSAs for use on more than one computer in the domain
  - Storing MSA authentication information on domain controllers
- To support group MSA, your environment:
  - Must have at least one Windows Server 2012 or newer domain controller
  - Must have a KDS root key created for the domain

## Requirements for group MSAs

Your environment must meet the following requirements if you want to support group MSA functionality, including that:

- At least one domain controller must be running Windows Server 2012 or newer to store managed password information.
- Client computers using group MSAs must have Windows 8 or newer, and server-based computers must have Windows Server 2012 or newer.
- You must create a KDS root key on one of the domain's domain controllers. To create the KDS root key, you must run the following command from the Active Directory Module for Windows PowerShell on a Windows Server 2016 domain controller:

```
Add-KdsRootKey -EffectiveImmediately
```

 **Note:** The **-EffectiveImmediately** switch uses the current time to establish the timestamp that marks the key as valid. However, when using the **-EffectiveImmediately** switch, the actual effective time is set to 10 hours later than the current time. This 10-hour difference is to allow for AD DS replication to replicate changes to other domain controllers in the domain. For testing purposes, you can bypass this functionality by setting the **-EffectiveTime** parameter to 10 hours before the current time by running the following command:

```
Add-KdsRootKey -EffectiveTime ((get-date).addhours(-10))
```

## Group MSA functionality

Group MSAs enable managed service account functionality across multiple servers by delegating the management of MSA password information to Windows Server 2016 domain controllers. By doing this, the management of passwords is no longer dependent on the relationship between a single server and AD DS, but is controlled entirely by AD DS.

The group managed service account object contains a list of principals, either computers or AD DS groups, which are allowed to retrieve group MSA password information from AD DS. The principals then can use the Managed Service Account group for authentication for services.

You create group MSAs by using the same cmdlets that you used for creating the standard MSA from the Active Directory Module for Windows PowerShell. That is, the cmdlets used for managed service account management create group MSAs by default.

On a Windows Server 2016 domain controller, create a new MSA by using the **New-ADServiceAccount** cmdlet with the **-PrincipalsAllowedToRetrieveManagedPassword** parameter. This parameter accepts one or more comma-separated computer accounts or AD DS groups that are permitted to obtain password information for the group MSA that is stored in AD DS on Windows Server 2016 domain controllers.

For example, the following cmdlet creates a new group MSA called SQLFarm, and enables the LON-SQL1, LON-SQL2, and LON-SQL3 hosts to use the group MSA:

```
New-ADServiceAccount -Name LondonSQLFarm -PrincipalsAllowedToRetrieveManagedPassword LON-SQL1, LON-SQL2, LON-SQL3
```

After you add a computer to use the **PrincipalsAllowedToRetrieveManagedPassword** parameter, you can assign the group MSA to services by using the same assignment process as standard MSAs.

## Using AD DS groups to manage group MSAs

You can use AD DS security groups to identify group MSAs. When you use an AD DS group for the **PrincipalsAllowedToRetrieveManagedPassword** parameter, any computers that are members of that group will be allowed to retrieve the password and utilize group MSA functionality. When you use an AD DS group as the principal allowed to retrieve a managed password, any accounts that are members of the group will also have the same capability.

## Demonstration: Configuring group MSAs

In this demonstration, you will see how to configure group MSAs.

### Demonstration Steps

#### Create the KDS root key for the domain

1. On **LON-DC1**, from **Server Manager**, open the **Active Directory Module for Windows PowerShell** console.
2. Use the **Add-KdsRootKey -EffectiveTime ((get-date).addhours(-10))** cmdlet to create the domain KDS root key.

#### Create and associate an MSA

1. Use the **New-ADServiceAccount** cmdlet to create an MSA.
2. Use the **Add-ADComputerServiceAccount** cmdlet to associate the MSA with **LON-SVR1**.
3. Use the **Get-ADServiceAccount** cmdlet to view the newly-created MSA and confirm proper configuration.

#### Install an MSA

1. On **LON-SVR1**, open the **Active Directory Module for Windows PowerShell** console.
2. Use the **Install-ADServiceAccount** cmdlet to install the MSA on **LON-SVR1**.
3. Open **Server Manager**, and start the **Services** console.
4. Open the **Properties** pages for the Data Sharing Service, and then select the **Log On** tab.
5. Configure the Data Sharing Service to use **Adatum\SampleApp\_SVR1\$**.
6. Clear the password for both the **Password** and **Confirm password** boxes.

## SPNs and Kerberos delegation

In some scenarios, a program for a service might need to make a connection to another server's services on behalf of the client. For example, when a client uses a front-end server that makes a connection to a back-end server, this connection requires authentication. Kerberos uses authentication delegation for such scenarios. The requesting service, which in this example is the client, requests that the KDC authorize a second service to act on its behalf. The second service then can delegate authentication to a third service. However, in Windows Server 2008 and newer, Microsoft has added the constrained delegation model to limit the scope of services that can be delegated this way, particularly third-tier services and beyond. This model provides a safer form of delegation for services to use.

- Kerberos delegation of authentication:
  - Services can delegate service tickets issued to them by the KDC to another service
- Constrained delegation:
  - Allows administrators to define which services can use service tickets issued to other services
- SPNs help identify services uniquely
- Windows Server 2016 allows:
  - Constrained delegation across domains
  - Service administrators to configure constrained delegation

When you use constrained delegation, you can configure service account delegation to specific sets of service accounts. You can configure a particular service account to be trusted for delegation to a specific instance of a service running on a specific computer or a set of specific instances of services running on specified computers.

An SPN is a unique identifier for each instance of a service running on a computer. When using Kerberos authentication, a defined SPN for a service allows clients to identify that instance of the service on the network. The SPN is registered in AD DS and is associated with the account of the service that the SPN specifies. When a service needs to authenticate to another service, it uses that service's SPN to distinguish it from other services on that computer. A service can use constrained delegation if it can obtain a Kerberos service ticket for itself on behalf of the user being delegated, in this case, another service. When using constrained delegation, the user can obtain the service ticket directly by authenticating through curb roles or the service can obtain the service ticket on behalf of the user.

One problem with this model is that when a domain administrator configured the service for constrained delegation, the service administrator did not know which front-end service was being delegated to the resource services they owned. In Windows Server 2016, this is overcome by also allowing the service administrator to configure a service's constrained delegation. This means that the back-end service administrator to allow or deny access by front-end services.

Windows Server 2012 and Windows Server 2016 implement new extensions for constrained delegation. For example, the Service for User to Proxy, known as *S4U2proxy* extension allows a service to use its Kerberos service ticket for a user to obtain a service ticket from the KDC to a back-end service. A service administrator can configure constrained delegation on the back-end service's account, even in another domain. You can configure front-end services, such as Microsoft Office Outlook on the Web and Microsoft SharePoint Server, for constrained delegation to back-end servers on other domains. This enhances your ability to support service solutions across domains by using your existing Kerberos authentication mechanisms.

**Question:** How are group MSAs different from standard MSAs?



## Lab: Securing AD DS

### Scenario

The security team at A. Datum Corporation has been examining possible security issues in the organization, focusing on AD DS. The security team is particularly concerned with AD DS authentication and security of branch-office domain controllers.

You must help improve security and monitoring of authentication against the enterprise's AD DS domain. Additionally, management at A. Datum has instituted a password policy, and you must enforce it for all user accounts and develop a more-stringent password policy for security-sensitive administrative accounts. It also is important that you implement an appropriate audit trail to help monitor authentication attempts within AD DS.

The second part of your assignment includes deploying and configuring RODCs to support AD DS authentication within a branch office. Lastly, you should evaluate the usage of a group MSA by deploying it to the test server.

### Objectives

After completing this lab, you will be able to:

- Implement security policies for accounts, passwords, and administrative groups.
- Deploy and configure an RODC.
- Create and associate a group MSA.

### Lab Setup

Estimated Time: 60 minutes

Virtual machines: **20742A-LON-DC1**, **20742A-LON-DC2**, **20742A-LON-SVR1**

User name: **Adatum\Administrator**

Password: **Pa\$\$w0rd**

For this lab, you will use the available virtual machine environment. Before you begin the lab, you must complete the following steps:

1. On the host computer, start **Hyper-V Manager**.
2. In Hyper-V Manager, click **20742A-LON-DC1**, and then in the **Actions** pane, click **Start**.
3. In the **Actions** pane, click **Connect**. Wait until the virtual machine starts.
4. Sign in by using the following credentials:
  - User name: **Adatum\Administrator**
  - Password: **Pa\$\$w0rd**
5. Repeat steps two through four for **20742A-LON-DC2** and **20742A-LON-SVR1**.

## Exercise 1: Implementing security policies for accounts, passwords, and administrative groups

### Scenario

A. Datum management has indicated that it is important that all management processes are as secure as possible, to help prevent a security breach. The company's security and management teams have identified its business requirements with respect to account logons and password security. In this exercise, you will define and implement the Group Policy settings to meet the company's requirements.

### Supporting documentation

#### A. Datum GPO strategy proposal

##### Requirements overview

A. Datum has identified the following requirements regarding account logon and password policies:

- All users must use a password that is at least eight characters long. For IT administrators, the minimum length must be 10 characters.
- Passwords for all users must be complex and stored securely.
- All users, except IT administrators, must change their password every 60 days or less.
- IT administrators must change their password every 30 days or less.
- If users enter the wrong password more than five times within 20 minutes, their accounts must be locked. For normal users, accounts are unlocked automatically after one hour.
- For IT administrators, accounts must be locked after three incorrect password attempts. IT administrator accounts are never unlocked automatically. An administrator must unlock the account. IT administrator accounts include all members of the IT group and the Domain Admins group.
- No users should be able to use at least 10 of their previous passwords.
- The membership list for the local Administrators group on all member servers must be limited to only the local Administrator account, the Domain Admins group, and the IT group.
- The Domain Admins group must include only the Administrator account.
- The Enterprise Admins and Schema Admins groups must be empty during normal operations. Users must be added explicitly to these groups only when they need to perform tasks that require this level of administrative rights.
- Other built-in groups, such as Account Operators and Server Operators, should contain no members. If users are added to one of these groups, they should be removed from the group automatically.
- All changes made to user objects and security groups in AD DS must be audited.

##### Proposals

List the settings that you must configure to meet A. Datum's requirements regarding password policies and account lockout.

Setting	Configuration for all users	Configuration for IT administrators
Enforce password history		
Maximum password age		
Minimum password age		
Minimum password length		

Passwords must meet complexity requirements		
Store password using reversible encryption		
Account lockout duration		
Account lockout threshold		
Reset account lockout counter after		

1. How can you configure that IT administrators have different password and account lockout settings than regular users?
2. How can you identify IT administrators in terms of more restricted password and account lockout settings?
3. How can you meet the requirement to limit the membership list for the local Administrators groups on all member servers to only the local Administrator account, the Domain Admins group, and the IT group?
4. How can you meet the requirement that the Domain Admins group must include only the Administrator account and that the Enterprise Admins and Schema Admins groups must be empty during normal operations?
5. How can you meet the requirement that other built-in groups, such as Account Operators and Server Operators, must not contain members?
6. How can you meet the requirement that you must audit all changes to AD DS?

The main tasks for this exercise are as follows:

1. Identify the required settings.
2. Configure password settings for all users.
3. Configure a PSO for IT administrators.
4. Implement administrative security policies.
5. Implement administrative auditing.

► **Task 1: Identify the required settings**

1. Read the documentation provided.
2. Fill in the table of settings according to the requirements of A. Datum Corporation.
3. Answer the additional questions from the proposals document.

**► Task 2: Configure password settings for all users**

1. On **LON-DC1**, from **Server Manager**, open the **Group Policy Management Console**.
2. Navigate to the **Default Domain Policy**, and then click **Edit**.
3. In the **Group Policy Management Editor** window, navigate to **Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies**, and then select **Password Policy**.
4. Configure the following policy settings:
  - Enforce password history: **10 passwords remembered**
  - Maximum password age: **60 days**
  - Minimum password age: **1 days**
  - Password must meet complexity requirements: **Enabled**
  - Password length: **8 characters**
  - Store passwords using reversible encryption: **Disabled**
5. Select **Account Lockout Policy**, and then define and configure the following policy settings:
  - Account lockout duration: **60 minutes**
  - Accept the suggested value change
  - Account lockout threshold: **5 invalid logon attempts**
  - Reset account lockout counter after: **20 minutes**
6. Close the **Group Policy Management Editor** window and the **Group Policy Management Console**.

**► Task 3: Configure a PSO for IT administrators**

1. On **LON-DC1**, from **Server Manager**, open **Active Directory Administrative Center**.
2. Navigate to **Adatum (local)\System>Password Settings Container**.
3. Create a new PSO with the following parameters:
  - Name: **Adatum Administrators Password Settings**
  - Precedence: **10**
  - Enforce minimum password length: **Selected, 10 characters minimum password length**
  - Enforce password history: **Selected, 10 passwords remembered**
  - Password must meet complexity requirements: **Selected**
  - Store password using reversible encryption: **Not selected**

Password age options:

- Enforce minimum password age: **Selected**
- User cannot change the password within (days): **1**
- Enforce maximum password age: **Selected**
- User must change the password after (days): **30**

Account lockout options:

- Enforce account lockout policy: **Selected**

- Number of failed logon attempts allowed: **3**
  - Reset failed logon attempts count after (mins): **20**
  - Account will be locked out: **Until an administrator manually unlocks the account**
4. In the **Directly Applies To** section, configure the PSO to apply to the **IT** group.
  5. IT will not work because it is not a global group. Open Windows PowerShell, and then verify the IT group's scope with the following command:

```
Get-ADGroup IT
```

6. Modify the group's scope by using the following command:

```
Set-ADGroup IT -GroupScope Global
```

7. In the **Directly Applies To** section, configure the PSO to apply to the following groups:
  - **IT**
  - **Domain Admins**
8. Create the PSO.
9. In **Active Directory Administrative Center**, switch to the **Overview** page, and in the **Global Search** box, search for **Abbi Skinner**. Use the **View resultant password settings** to verify that the **Adatum Administrative Password Settings** PSO applies to **Abbi**; he is in the IT group.
10. Repeat step nine to verify the user **Adam Hobbs**. He is not in an IT group, and the Default Domain Policies settings apply to him.
11. Close **Active Directory Administrative Center** and **Windows PowerShell**.

#### ► Task 4: Implement administrative security policies

1. On **LON-DC1**, open **Active Directory Administrative Center** and create a top-level OU named **Adatum Servers**.
2. Move **LON-SVR1** and **LON-SVR2** to the **Adatum Servers** OU.
3. Open the **Group Policy Management Console**, and then create and link a policy named **Restricted Administrators on Member Servers** to the **Adatum Servers** OU.
4. Edit the GPO to restrict the local Administrators group to the **Administrator** account, the **Domain Admins** group, and the **IT** group.
5. Switch to **LON-SVR1** and refresh Group Policy.
6. Verify that the policy has applied to **LON-SVR1** and has restricted the local Administrators group.
7. Switch back to **LON-DC1**.
8. Edit the **Default Domain Controllers Policy**.
9. Configure the GPO with **Restricted Groups**. Add the groups **Account Operators** and **Server Operators**, and configure both to contain no members.
10. Close the **Group Policy Management Console**.

► **Task 5: Implement administrative auditing**

1. On **LON-DC1**, from **Server Manager**, start the **Group Policy Management Console**.
2. Navigate to and edit the **Default Domain Controllers Policy**.
3. Configure the Default Domain Controllers Policy to enable **Success** auditing of **Audit Directory Service Changes** under **Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\DS Access**.
4. In the Default Domain Controllers Policy, enable **Success** auditing of **Audit Security Group Membership** under **Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Management**.
5. In the Default Domain Controllers Policy, enable the policy **Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings** under **Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options**.
6. At a command prompt, type **gpupdate /force**, and then press Enter.
7. Open **Active Directory Users and Computers** and enable the **Advanced Features** view. In the **Adatum.com** properties dialog box, under **Advanced Security Settings**, in **Auditing**, locate the **Success** auditing entry for **Everyone** with **Special** access, which applies to **This object only**.
8. Open and change the auditing entry to apply to **This object and all descendent objects**.
9. In **Active Directory Users and Computers**, add the user **Abbi** to the **Domain Admins** group.
10. Locate the user **Ada Russel** in the **Marketing** OU, and then change her city from **London** to **Birmingham**.
11. Open **Event Viewer**, go into the **Security** log, and then open the most recent **Event ID 4728**. In the properties, note that **ADATUM\Administrator** has added **ADATUM\Abbi** to the **Domain Admins** groups.
12. In **Event Viewer**, open the most recent **Event ID 5136**, and note that **ADATUM\Administrator** has modified the user object **cn=Ada Russel** and deleted the value **London**.
13. Move and open the next event in the **Event Properties** details page, and notice that **ADATUM\Administrator** has modified **Ada Russel** and added the value **Birmingham**.
14. Close all open windows except for **Server Manager**.

**Results:** After this exercise, you should have identified and configured the security policies for A. Datum.

## Exercise 2: Deploying and configuring an RODC

### Scenario

In this exercise, you will configure the server **LON-SVR1** as an RODC in the distant branch office. To avoid travel costs, you decide to do the conversion remotely, working with a desktop-support technician and the branch's only IT staff member. This user already has installed a Windows Server 2016 computer named **LON-SVR1**. You will stage a delegated installation of an RODC so that this administrative user can complete the installation. After the deployment is complete, you will configure a domain-wide password replication policy and the password replication policy specific to **LON-SVR1**.

The main tasks for this exercise are as follows:

1. Stage a delegated installation of an RODC.
2. Run the Active Directory Domain Services Installation Wizard on an RODC to complete the deployment process.
3. Configure the domain-wide password replication policy.
4. Create a group to manage password replication to the branch office RODC.
5. Evaluate the resultant password replication policy.

### ► Task 1: Stage a delegated installation of an RODC

#### Preparation

To prestage an RODC account, the computer name must not be in use in the domain. Therefore, you first need to remove **LON-SVR1** from the domain by performing the following steps:

1. Remove **LON-SVR1** from the domain, add it to the **MUNICH** workgroup, and then restart the server.
2. Sign in as:
  - User name: **Administrator**
  - Password: **Pa\$\$w0rd**
3. Switch to **LON-DC2**.
4. From **Server Manager**, start **Active Directory Users and Computers**, navigate to the **Adatum Servers** OU, and then delete **LON-SVR1**. Confirm the deletion.

#### Stage a delegated installation of an RODC


1. In **Active Directory Sites and Services**, create a new site named **Munich**, and then assign it to **DEFAULTIPSITELINK**.
2. Start **Active Directory Administrative Center**, and then navigate to the **Domain Controllers** OU.
3. Precreate an RODC account with the name **LON-SVR1**, which also should be a **DNS Server** and a **Global Catalog**.
4. Delegate **Nestor Fiore** to install and administer the RODC.
5. Finish the precreation of the RODC account.

► **Task 2: Run the Active Directory Domain Services Installation Wizard on an RODC to complete the deployment process**

1. Switch to **LON-SVR1**. From **Server Manager**, start the **Add Roles and Features Wizard**.
2. Use the wizard to install **Active Directory Domain Services** on **LON-SVR1**. Accept the installation of features and management tools.
3. When the installation is finished, click in the notification area of **Server Manager** to promote this server to a domain controller.
4. Configure to add the server as a domain controller to an existing domain. Click **Change**, and provide the following credentials:
  - User name: **Adatum\Nestor**
  - Password: **Pa\$\$w0rd**
5. Select **Adatum.com** as the domain, and then proceed.
6. Notice that the **Active Directory Domain Services Installation Wizard** finds the precreated account. Accept all further defaults in the wizard to use that account, and then configure AD DS.

► **Task 3: Configure the domain-wide password replication policy**

1. Switch to **LON-DC2**. From **Server Manager**, start **Active Directory Administrative Center**.
2. Make the IT group, found in the IT OU, a member of the **Denied RODC Password Replication Policy Group**.

 **Note:** The members of the IT group have elevated permissions, so storing their password on a RODC would be a security risk. Therefore, you add the IT group to the global Deny List, which applies to every RODC in the domain.

► **Task 4: Create a group to manage password replication to the branch office RODC**

1. Switch to **Server Manager**, and from the **Tools** menu, start **Active Directory Users and Computers**.
2. Navigate to the **Users** container, and then create a new group named **Munich Allowed RODC Password Replication Group**.
3. Add **Ana Cantrell** to the new group.
4. In **Active Directory Administrative Center**, from the **Domain Controllers** OU, view the properties for **LON-SVR1**.
5. In the **Extensions** section, on the **Password Replication Policy** tab, configure the **Munich Allowed RODC Password Replication Group** to allow password replication. Close the properties for **LON-SVR1**.

► **Task 5: Evaluate the resultant password replication policy**

1. In **Active Directory Administrative Center**, open the properties of **LON-SVR1**, and then in the **Extensions** section, on the **Password Replication Policy** tab, click **Advanced**. Note that this dialog box shows all accounts whose passwords are stored in the RODC.
2. Select **Accounts that have been authenticated to this Read-only Domain Controller**, and then note that this only shows accounts that have the permissions and already have been authenticated by this RODC.



3. Click the **Resultant Policy** tab, and then add **Ana Cantrell**. Notice that Ana Cantrell has a resultant policy of **Allow**.
4. Close all open dialog boxes.

**Results:** After this exercise, you should have deployed and configured an RODC.

## Exercise 3: Creating and associating a group MSA

### Scenario

You need to configure a group MSA to support a new web-based application that is being deployed. Using a group MSA will help maintain the password security requirements for the account.

The main tasks for this exercise are as follows:

1. Create and associate an MSA.
2. Install a group MSA.
3. Prepare for the next module.

#### ► Task 1: Create and associate an MSA

1. On **LON-DC1**, open the **Active Directory Module for Windows PowerShell** console.
2. Create the KDS root key by using the **Add-KdsRootKey** cmdlet. Make the effective time minus 10 hours, so the key will be effective immediately.
3. Create the new service account named **Webservice** for the host **LON-DC1**.
4. Associate the **Webservice** MSA with **LON-DC1**.
5. Verify the group MSA was created by using the **Get-ADServiceAccount** cmdlet.

#### ► Task 2: Install a group MSA

1. On **LON-DC1**, install the Webservice service account using the following command:

```
Install-ADServiceAccount -Identity Webservice
```

2. From the **Tools** menu in **Server Manager**, open **Internet Information Services (IIS) Manager**.
3. Expand **LON-DC1 (Adatum\Administrator)**, and then click **Application Pools**.
4. In the **DefaultAppPool** actions pane, in the **Advanced Settings** dialog box, configure the **DefaultAppPool** to use the **Webservice\$** account as the identity. Note that you can click the **ellipses (...)** by the identity name to add the **Webservice\$** account as a custom account.
5. Stop and then start the application pool.

**Results:** After completing this exercise, you should have configured an MSA.

**► Task 3: Prepare for the next module**

When you finish the lab, revert the virtual machines to their initial state. To do this, perform the following steps:

1. On the host computer, start **Hyper-V Manager**.
2. In the **Virtual Machines** list, right-click **20742A-LON-DC1**, and then click **Revert**.
3. In the **Revert Virtual Machine** dialog box, click **Revert**.
4. Repeat steps two and three for **20742A-LON-DC2** and **20742A-LON-SVR1**.

**Question:** In the lab, you configured the password settings for all users within the Default Domain Policy, and you configured the password settings for Administrators within a PSO. What other options were available to help you accomplish the solution?

**Question:** In the lab, you were using precedence for the administrative PSO with a value of 10. What is the reason for this?

## Module Review and Takeaways

### Review Questions

**Question:** Why is physical security so important, especially for AD DS domain controllers?

**Question:** You need to implement auditing policies for domain authentication and changes to directory services. What is the best way to implement these auditing settings?

**Question:** Your organization requires you to maintain a highly reliable and secure AD DS infrastructure. It also requires that users can access corporate email from the Internet by using Outlook Web Access. You are considering implementing account-lockout settings. What must you consider?

### Common Issues and Troubleshooting Tips

Common Issue	Troubleshooting Tip
You have configured advanced auditing policy settings, but they do not apply.	
You have configured auditing of account logon or directory services changes. Now you are testing them, but you cannot find the events in your server's event log.	

### Tools

The following table lists the tools that this module references.

Tool	Use for	Where to find it
<b>Active Directory Users and Computers</b>	Managing objects within AD DS, such as users, groups, and computers.	<b>Server Manager</b>
<b>Active Directory Administrative Center</b>	Managing objects within AD DS, such as users, groups, and computers.	<b>Server Manager</b>
Group Policy Management	Managing, reporting, backup, and restoration of GPOs.	<b>Server Manager</b>
Gpupdate.exe	Manually updating the GPOs of local machines.	Command-line

**MCT USE ONLY. STUDENT USE PROHIBITED**

# Module 8

## Deploying and managing AD CS

### Contents:

Module Overview	8-1
Lesson 1: Deploying CAs	8-2
Lesson 2: Administering CAs	8-11
Lesson 3: Troubleshooting and maintaining CAs	8-21
Lab: Deploying and configuring a two-tier CA hierarchy	8-28
Module Review and Takeaways	8-32

## Module Overview

The public key infrastructure (PKI) consists of several components, such as certification authority (CA), that help you secure corporate communications and transactions. You can use CAs to manage, distribute, and validate the digital certificates that you use to secure information. You can install Active Directory Certificate Services (AD CS) as a root CA or a subordinate CA in your organization. In this module, you will learn about deploying and managing CAs.

### Objectives

After completing this module, you will be able to:

- Deploy CAs.
- Administer CAs.
- Troubleshoot and maintain CAs.

## Lesson 1

# Deploying CAs

To use certificates in your Active Directory Domain Services (AD DS) infrastructure, you have to use externally provided certificates or deploy and configure at least one CA. The first CA that you deploy is a root CA. After you install the root CA, you can install a subordinate CA to apply policy restrictions and issue certificates. You also can use a CAPolicy.inf file to automate root CA installations and to provide additional configuration settings that are not available with standard GUI-based installations. In this lesson, you will learn about deploying CAs in the Windows Server 2016 operating system environment.

### Lesson Objectives

After completing this lesson, you will be able to:

- Describe AD CS.
- Describe the options for implementing CA hierarchies.
- Describe the differences between standalone and enterprise CAs.
- Describe the considerations for deploying a root CA.
- Deploy an enterprise root CA.
- Describe the considerations for deploying a subordinate CA.
- Explain how to use the CAPolicy.inf file for installing a CA.

### What is AD CS?

AD CS is an identity technology within Windows Server 2016 that allows you to implement PKI, so that you can easily issue and manage certificates to meet your organization's requirements.

#### Overview of PKI

PKI is the combination of software, encryption technologies, processes, and services that enables an organization to secure its communications and business transactions. PKI relies on the exchange of digital certificates between authenticated users and trusted resources. You use certificates to secure data and manage identification credentials from users and computers both within and outside your organization.

You can design a PKI solution by using AD CS to meet the following security and technical requirements of your organization:

- Confidentiality. PKI gives you the ability to encrypt stored and transmitted data. For example, you can use a PKI-enabled Encrypting File System (EFS) to encrypt and secure data. You also can maintain the confidentiality of transmitted data on public networks by using PKI-enabled Internet Protocol security (IPsec).

- Allows you to implement a PKI for your organization
  - Issue and manage certificates
- AD CS role services in Windows Server 2016
  - CAs
  - CA Web Enrollment
  - Online Responder
  - Network Device Enrollment Service
  - Certificate Enrollment Web Service
  - Certificate Enrollment Policy Web Service

- **Integrity.** You can use certificates to digitally sign data. A digital signature will identify whether any data was modified while communicating information. For example, a digitally signed email message will ensure that the message's content was not modified while in transit. Additionally, in a PKI, the issuing CA digitally signs certificates that are issued to users and computers, which proves the integrity of the issued certificates.
- **Authenticity.** A PKI provides several authenticity mechanisms. Authentication data passes through hash algorithms, such as Secure Hash Algorithm 2 (SHA-2) to produce a message digest. The message digest then is digitally signed by using the sender's private key from the certificate to prove that the sender produced the message digest.
- **Non-repudiation.** When data is digitally signed with an author's certificate, the digital signature provides both proof of the integrity of the signed data and proof of the data's origin. The integrity and origin of the data at any time, and the owner of the certificate that digitally signed the data cannot refute it.
- **Availability.** You can install multiple CAs in your CA hierarchy to issue certificates. If one CA is not available in a CA hierarchy, other CAs can continue to issue certificates.

### **AD CS in Windows Server 2016**

Windows Server 2016 deploys all PKI-related components as role services of the AD CS server role. Each role service is responsible for a specific portion of the certificate infrastructure while working together to form a complete solution.

The role services of the AD CS role in Windows Server 2016 are as follows:

- **Certification Authority.** The main purposes of CAs are to issue certificates, revoke certificates, and publish authority information access (AIA) and revocation information. When you install the first CA, it establishes the PKI in your organization. You can have one or more CAs in one network, but only one CA can be at the highest point in the CA hierarchy. The root CA is the CA located at the highest point in the hierarchy. However, you can have more than one CA hierarchy, which allows you to have more than one root CA. After a root CA issues a certificate for itself, subordinate CAs lower in the hierarchy receive certificates from the root CA.
- **Certification Authority Web Enrollment.** This component provides a method to issue and renew certificates for users, computers, and devices that are not joined to the domain, are not connected directly to the network, or are for users of operating systems other than Windows.
- **Online Responder.** You can use this component to configure and manage Online Certificate Status Protocol (OCSP) validation and revocation checking. An Online Responder decodes revocation status requests for specific certificates, evaluates the status of those certificates, and returns a signed response containing the requested certificate status information. The certificate revocation data can come from a CA on a computer that is running Windows Server 2003 or later.
- **Network Device Enrollment Service (NDES).** With this component, routers, switches, and other network devices can obtain certificates from AD CS.
- **Certificate Enrollment Web Service (CES).** This component works as a proxy client between the computer (running Windows 7 or higher) and the CA. Windows Server 2008 R2 introduced this component, and it requires that the Active Directory forest is at least at the Windows Server 2008 R2 level. It enables users, computers, or applications to connect to a CA by using web services to perform the following actions:
  - Request, renew, and install issued certificates.
  - Retrieve certificate revocation lists (CRLs).
  - Download a root certificate.

- Enroll over the Internet or across forests.
- Renew certificates automatically for computers that are part of untrusted AD DS domains, or are not joined to a domain.
- Certificate Enrollment Policy Web Service. This component enables users to obtain certificate enrollment policy information. Combined with CES, it enables policy-based certificate enrollment when the client computer is not a member of a domain, or when a domain member is not connected to the domain.

The AD CS server role, in addition to all related role services, can run on Windows Server 2016 with a full desktop experience or a Server Core installation. However, AD CS roles cannot run on Nano Server. You can deploy the AD CS role services in Windows Server 2016 by using Server Manager or Windows PowerShell command-line interface cmdlets. Additionally, you can deploy the role services while working locally at the computer or remotely over the network.

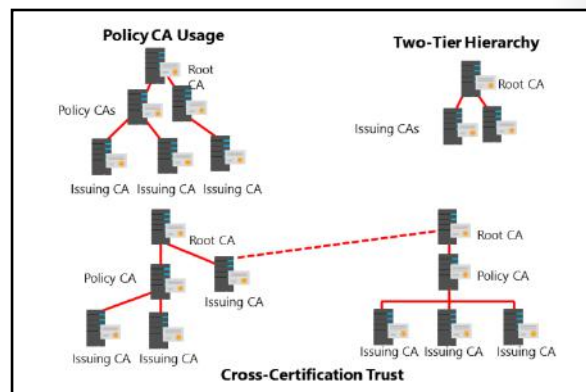
AD CS in Windows Server 2016 now has increased support for Trusted Platform Module (TPM) key attestation. Although client support has existed for TPM-protected private keys since Windows 8, AD CS in Windows Server 2012 R2 could only perform TPM key attestation by using the Microsoft Platform Crypto Provider. AD CS now allows you to use the Microsoft Smart Card Key Storage Provider (KSP) for TPM key attestation so that devices that are not-domain joined can enroll for certificates attesting to a TPM-protected private key by using NDES enrollment.

## Options for implementing CA hierarchies

When you decide to implement AD CS in your organization, one of the first decisions you must make is how to design your CA hierarchy. CA hierarchy determines the core design of your internal PKI and determines the purpose of each CA in the hierarchy. Each CA hierarchy usually includes two or more CAs. Usually, the second CA and all others after that are deployed with a specific purpose. Only the root CA is mandatory.



**Note:** It is not mandatory to have a multi-level CA hierarchy deployed to use PKI and certificates. For smaller and simpler environments, you can have a CA hierarchy with just one CA deployed. This CA usually is deployed as an enterprise root CA. In addition, you may choose to not deploy an internal CA at all and use externally provided certificates.



If you decide to implement a CA hierarchy and have deployed a root CA already, you must decide which roles to assign CAs on the second and third tiers. In general, we do not recommend building a CA hierarchy deeper than three levels, unless it is in a complex and distributed environment.

Most commonly, CA hierarchies have two levels, with the root CA at the top level and the subordinate issuing CA on the second level. The root CA usually is taken offline while the subordinate CA issues and manages certificates for all clients. However, in some more complex scenarios, you also can deploy other types of CA hierarchies.



In general, CA hierarchies fall into one of following categories:

- CA hierarchies with a policy CA. Policy CAs are types of subordinate CAs that are located directly below the root CA in a CA hierarchy. You use policy CAs to issue CA certificates to subordinate CAs that are located directly below the policy CA in the hierarchy. The role of a policy CA is to describe the policies and procedures that an organization implements to secure its PKI, the processes that validate the identity of certificate holders, and the processes that enforce the procedures that manage certificates. A policy CA issues certificates only to other CAs. The CAs that receive these certificates must uphold and enforce the policies that the policy CA defined. It is not mandatory to use policy CAs unless different divisions, sectors, or locations of your organization require different issuance policies and procedures. However, if your organization requires different issuance policies and procedures, you must add policy CAs to the hierarchy to define each unique policy. For example, an organization can implement one policy CA for all certificates that it issues internally to employees and another policy CA for all certificates that it issues to users who are not employees.
- CA hierarchies with cross-certification trust. In this scenario, two independent CA hierarchies interoperate when a CA in one hierarchy issues a cross-certified CA certificate to a CA in another hierarchy. When you do this, you establish mutual trust between different CA hierarchies.
- CAs with a two-tier hierarchy. In a two-tier hierarchy, there is a root CA and at least one subordinate CA. In this scenario, the subordinate CA is responsible for policies and for issuing certificates to requestors.

### Standalone vs. enterprise CAs

In Windows Server 2016 AD CS, you can deploy two types of CAs: standalone and enterprise CAs. These types are not about hierarchy, but about functionality and configuration storage. The most important difference between these two CA types is AD DS integration and dependency. A standalone CA can work without AD DS and does not depend on it in any way. An enterprise CA requires AD DS, but it also provides several benefits, including autoenrollment. The autoenrollment feature allows users and domain-joined devices to enroll automatically for certificates if you have enabled automatic certificate enrollment through Group Policy.

Standalone CAs	Enterprise CAs
Must be used if any CA (root/intermediate/policy) is offline because a standalone CA is not joined to an AD DS domain	Requires the use of AD DS and stores information in AD DS
Users must provide identifying information and specify the type of certificate	Can use Group Policy to propagate certificates to the trusted root CA certificate store Publishes user certificates and CRLs to AD DS
Does not support certificate templates	Issues certificates based on a certificate template
All certificate requests are kept pending until administrator approval	Supports autoenrollment for issuing certificates

The following table details the most significant differences between standalone and enterprise CAs.

Characteristic	Standalone CA	Enterprise CA
Typical usage	You typically use a standalone CA for offline CAs, but you also can use it for a CA that consistently is available on the network.	You typically use an enterprise CA to issue certificates to users, computers, and services, and you cannot use it as an offline CA.
AD DS dependencies	A standalone CA does not depend on AD DS, and you can deploy it in environments other than AD DS.	An enterprise CA requires AD DS, which you use as a configuration and registration database. An enterprise CA also provides a publication point for certificates issued to users and computers.

Characteristic	Standalone CA	Enterprise CA
Certificate request methods	Users can request certificates only from a standalone CA by using a manual procedure or web enrollment.	Users can request certificates from an enterprise CA by using the following methods: <ul style="list-style-type: none"> <li>• Manual enrollment</li> <li>• Web enrollment</li> <li>• Autoenrollment</li> <li>• Enrollment on behalf</li> <li>• Web services</li> </ul>
Certificate issuance methods	A certificate administrator must approve all requests manually.	Requests can be issued or denied automatically based on issuance-requirements settings.

Most commonly, you deploy the root CA, which is the first CA that deployed, is deployed as a standalone CA, and it is taken offline after it issues a certificate for itself and for a subordinate CA.

## Considerations for deploying a root CA

Before you deploy a root CA, you should decide several aspects. First, you should decide whether you need to deploy an offline root CA. Based on that decision, you also need to decide if you are going to deploy a standalone root CA or an enterprise root CA.

Usually, if you deploy a single-layer CA hierarchy, which means that you deploy only a single CA, it is most common to choose an enterprise root CA. However, if you deploy a two-layer hierarchy with a subordinate CA, the most common scenario is to deploy a standalone root CA. This makes the root CA more secure and allows it to be taken offline except for when it needs to issue certificates for new subordinate CAs.

The next factor to consider is the operating system installation type. Both the Desktop Experience and the Server Core installation scenarios support AD CS. Server Core installation provides a smaller attack surface and less administrative overhead, and therefore, you should consider it for AD CS in an enterprise environment. In Windows Server 2016, you also can use Windows PowerShell to deploy and manage the AD CS role.

You should be aware that you cannot change computer names, domain name, or computer domain memberships after you deploy a CA of any type on that computer. Therefore, it is important to determine these attributes before installing a CA.

- Computer name and domain membership cannot change
- When you plan private key configuration, consider the following:
  - CSP
  - Key character length with a default of 2,048
  - The hash algorithm that is used to sign certificates issued by a CA
- When you plan a root CA, consider the following:
  - Name and configuration
  - Certificate database and log location
  - Validity period

The following table details additional considerations.

Consideration	Description
A cryptographic service provider (CSP) that is used to generate a new key	<ul style="list-style-type: none"> <li>The default CSP is the RSA#Microsoft Software Key Storage Provider.</li> <li>Any provider whose name contains a number sign (#) is a Cryptography Next Generation (CNG) provider.</li> </ul>
The key character length	The default key length for the Microsoft Strong Cryptographic Provider is 2,048 characters. This is the minimum recommended value for a root CA, although it is a best practice to choose a 4,096-bit key.
The hash algorithm that is used to sign certificates issued by a CA	The default hash algorithm is SHA-256. In previous versions of Windows Server, the default hash algorithm is SHA-1. While Windows Server 2016 AD CS still supports SHA-1, you should avoid it unless you specifically need to support older versions of Windows. SHA-1 is no longer considered secure, and many web browsers will stop supporting it by 2017.
The validity period for certificates issued by a CA	Templates define the default value for certificates. You can choose various validity periods on various certificate templates.
The status of the root server (online or offline)	You should deploy the root server as an offline standalone CA, if possible. This enhances security and safeguards the root certificate because it is not available to attack over the network.

If you decide to deploy an offline, standalone root CA, there are some specific considerations that you should keep in mind:

- Before you issue a subordinate certificate from the root CA, make sure that you provide at least one certificate revocation list distribution point (CDP) and AIA location that will be available to all clients. This is because, by default, a standalone root CA has the CDP and AIA located on itself. Therefore, when you take the root CA off the network, a revocation check will fail because the CDP and AIA locations will be inaccessible. When you define these locations, you should copy CRL and AIA information manually to that location.
- Set a validity period for CRLs that the root CA publishes to a long period of time, for example, one year. This means that you will have to turn on root CA once per year to publish a new CRL, and then copy it to a location that is available to clients. If you fail to do so, after the CRL on the root CA expires, revocation check for all certificates also will fail.
- Use Group Policy to publish the root CA certificate to a trusted root CA store on all server and client machines. You must do this manually because a standalone CA cannot do it automatically, unlike an enterprise CA. You also can publish the root CA certificate to AD DS by using the certutil command-line tool.

## Demonstration: Deploying an enterprise root CA

### Demonstration Steps

#### Deploy an enterprise root CA

1. In **Server Manager**, add the **Active Directory Certificate Services** role.
2. Select the **Certification Authority** role service.
3. After the installation completes successfully, click the text **Configure Active Directory Certificate Services on the destination server**.
4. Select to install an Enterprise Root CA.
5. Set the Key length to **4096**.
6. Name the CA **AdatumRootCA**.

### Considerations for deploying a subordinate CA

You can use a subordinate CA to implement policy restrictions for PKI and to issue certificates to clients. After installing a root CA for the organization, you can install one or more subordinate CAs.

When you use a subordinate CA to issue certificates to users or computers that have an account in an AD DS environment, you can install the subordinate CA as an enterprise CA. Then, you can use the data from the client accounts in AD DS to issue and manage certificates, and to publish certificates to AD DS. To complete this procedure, however, you must be a member of the local Administrators group or have equivalent permissions. If the subordinate CA is an enterprise CA, you also need to be a member of the Domain Admins group or have equivalent permissions. From a security perspective, a recommended scenario would be to have an offline, standalone root CA and an enterprise subordinate CA.

- Computer name and domain membership cannot change
- When you plan private key configuration, consider the following:
  - CSP
  - Key character length with a default of 2,048
  - The hash algorithm that is used to sign certificates issued by a CA
- When you plan a root CA, consider the following:
  - Name and configuration
  - Certificate database and log location
  - Validity period

A subordinate CA usually is deployed to achieve some of the following functionalities:

- **Usage.** You can issue certificates for a number of purposes, such as Secure/Multipurpose Internet Mail Extensions (S/MIME), EFS, or remote access. The issuing policy for these different uses might be distinct, and separation provides a basis for administering these policies.
- **Organizational divisions.** You might have different policies for issuing certificates that depend on an entity's role in the organization. You can create subordinate CAs to separate and administer these policies.
- **Geographic divisions.** Organizations often have entities at multiple physical sites. Limited network connectivity between these sites might require individual subordinate CAs for many or all sites.
- **Load balancing.** If you use your PKI to issue and manage a large number of certificates and have only one CA, it can result in considerable network load for that single CA. Using multiple subordinate CAs to issue the same kind of certificates divides the network load between CAs.
- **Backup and fault tolerance.** Multiple CAs increase the possibility that your network has operational CAs available to respond to user requests.

## How to use the CAPolicy.inf file for installing a CA

You can use the CAPolicy.inf file if you want to deploy a root or subordinate CA, and you want to define some values and parameters during or after installation. The CAPolicy.inf file is a plain text file that contains various settings that you can use when you install the AD CS role, or when you renew the CA certificate. The CAPolicy.inf file is not required to install AD CS, but without it, default settings are applied. In many cases, the default settings are insufficient for more complex deployments. You can use the CAPolicy.inf file to configure CAs in more complex deployments.

- The CAPolicy.inf file is stored in the %Windir% folder of the root or subordinate CA
- The CAPolicy.inf file defines the following:
  - Certification practice statement
  - Object identifier
  - CRL publication intervals
  - CA renewal settings
  - Key size
  - Certificate validity period
  - CDP and AIA paths

Each CAPolicy.inf file is divided into sections and has a simple structure, described as follows:

- A *section* is an area in the .inf file that contains a logical group of keys. A section always appears in brackets in the .inf file.
- A *key* is the parameter that is to the left of the equal (=) sign.
- A *value* is the parameter that is to the right of the equal (=) sign.

For example, if you want to specify an AIA point in the CAPolicy.inf file, you will use following syntax:

```
[AuthorityInformationAccess]
URL=http://pki.adatum.com/CertData/adatumCA.crt
```

In this example, AuthorityInformationAccess is a section, URL is the key, and <http://pki.adatum.com/CertData/adatumCA.crt> is the value.

You also can specify some CA server settings in the CAPolicy.inf file. One example of the section that specifies these settings is:

```
[certsrv_server]
RenewalKeyLength=2048
RenewalValidityPeriod=Years
RenewalValidityPeriodUnits=5
CRLPeriod=Days
CRLPeriodUnits=2
CRLDeltaPeriod=Hours
CRLDeltaPeriodUnits=4
ClockSkewMinutes=20
LoadDefaultTemplates=True
AlternateSignatureAlgorithm=0
ForceUTF8=0
EnableKeyCounting=0
```



**Note:** All parameters from the previous examples are optional.

You also can use the CAPolicy.inf file when installing AD CS to define the following:

- Certification practice statement. Describes the practices that the CA uses to issue certificates. This includes the types of certificates issued, information about issuing, renewing, and recovering certificates, and other details about the CA's configuration.
- Object identifier. Identifies a specific object or attribute.

- CRL publication intervals. Defines the interval between publications for the base CRL.
- CA renewal settings. You can define renewal settings as follows:
  - Key size. Defines the length of the key pair used during a root CA renewal.
  - Certificate validity period. Defines the validity period for a root CA certificate.
  - CDP and AIA paths. Provides the path used for root CA installations and renewals.

After you have created your CAPolicy.inf file, you must copy it into the %SystemRoot% folder of your server (for example, C:\Windows) before you install the AD CS role, or before you renew the CA certificate.



**Note:** The CAPolicy.inf file is processed for both the root and subordinate CA installations and renewals.

### Check Your Knowledge

Question	
Which of the following options describe the advantages of deploying an enterprise CA instead of a standalone CA?	
Select the correct answer.	
<input type="checkbox"/>	Provides multiple ways in which users and devices can receive certificates.
<input type="checkbox"/>	Does not require AD DS.
<input type="checkbox"/>	Certificate requests can be issued or denied automatically based on policy.
<input type="checkbox"/>	Can be taken offline to prevent compromise.
<input type="checkbox"/>	Can use templates to issue certificates based on data in AD DS.

### Check Your Knowledge

Question	
Which of the following options are reasons for which you might deploy multiple subordinate CAs?	
Select the correct answer.	
<input type="checkbox"/>	You want to segment certificate issuance based on unique usage policies.
<input type="checkbox"/>	You have multiple domains in your AD DS environment and each domain requires its own subordinate CA.
<input type="checkbox"/>	You want to segment certificate issuance based on organizational division or geographic region.
<input type="checkbox"/>	You want multiple subordinate CAs for high availability and load balancing of requests.
<input type="checkbox"/>	You need to publish multiple certificate templates and each template requires its own subordinate CA.

## Lesson 2

# Administering CAs

After you design and deploy a CA hierarchy, you must configure various options for CAs. You must have efficient methods for the CA hierarchy management, and for configuring security options, auditing, and monitoring. AD CS provides several methods for CA hierarchy management. In this lesson, you will learn how to administer and manage CA hierarchy and CAs.

### Lesson Objectives

After completing this lesson, you will be able to:

- Explain how to manage CAs.
- Describe how to configure CA security.
- Describe how to configure security roles for CA administration.
- Describe how to configure CA policy and exit modules.
- Describe how to configure CDP and AIA locations.
- Configure CA properties.

### Managing CAs

After you deploy a CA, there are several tasks that you should perform to configure it, and later, to manage it properly. A CA is a very important service, so you should manage it carefully.

After a CA hierarchy is deployed, you should verify the CA security configuration to ensure which users and groups are allowed to perform administrative tasks on that CA. Additionally, it is important that you configure logging and monitoring options for a CA, so you have all important tasks and activities logged.

You can configure the most common CA management options if you use the CA management console. However, you also can use Windows PowerShell and the certutil command-line utility to manage various advanced CA options and to perform some tasks that are not available in a graphical console.

- For managing CA hierarchy, you can use:
  - CA management console
  - Windows PowerShell
  - Certutil command-line utility
- Certutil provides an interface for advanced CA and PKI configuration and management
- PKI options are manageable through Group Policy, if you use the following:
  - Credential roaming
  - Autoenrollment of certificates
  - Certificate path validation
  - Certificate distribution

### Windows PowerShell cmdlets for deploying and administering a CA

Windows Server 2016 provides several Windows PowerShell cmdlets for AD CS deployment and administration. In Windows Server 2016, the **ADCSDeployment** and **ADCSAdministration** Windows PowerShell modules are available to deploy and administer CAs. If you have already installed the AD CS binaries, you can import the modules for use in Windows PowerShell by running the following commands:

```
Import-Module ADCSDeployment
Import-Module ADCSAdministration
```

If you want to see all of the cmdlets available for CA deployment and administration, you can run the following command in Windows PowerShell:

```
Get-Command -Module ADCS*
```

The following list describes some cmdlets for CA administration:

- **Add-CATemplate.** Adds a certificate template to the CA.
- **Add-CACrIDistributionPoint.** Adds a CDP Uniform Resource Identifier (URI) where the CA publishes certification revocations.
- **Add-CAAuthorityInformationAccess.** Configures AIA or OCSP URI on a CA.
- **Get-CATemplate.** Gets the list of templates set on the CA for issuance of certificates.
- **Get-CACrIDistributionPoint.** Gets all the locations set on the CDP extension of the CA properties.
- **Get-CAAuthorityInformationAccess.** Gets the AIA and OCSP URI information set on the AIA extension of the CA properties.
- **Remove-CATemplate.** Removes the templates from the CA that were set for issuance of certificates.
- **Remove-CACrIDistributionPoint.** Removes the URI for the CDP from the CA.
- **Remove-CAAuthorityInformationAccess.** Removes AIA or OCSP URI from the AIA extension set on the CA.



**Additional Reading:** For more information, refer to:

- "AD CS Deployment Cmdlets in Windows PowerShell" at: <http://aka.ms/Giih2g>
- "AD CS Administration Cmdlets in Windows PowerShell" at: <http://aka.ms/Dekm5i>

### Using certutil to administer a CA

While Windows PowerShell does not provide full AD CS management, certutil provides full management capability. Certutil.exe is a command-line utility that is installed as part of AD CS. Certutil.exe can display CA configuration information, configure AD CS, back up and restore CA components, and verify certificates, key pairs, and certificate chains.

For common CA configuration and management tasks, you do not have to use certutil. However, for more advanced tasks, certutil may be your only choice.

For example, if you want to review all configuration settings for the CA, you can do it by issuing the following commands:

```
Certutil -dump
Certutil -getreg
Certutil -getreg CA
```

This command provides much more information about your CA configuration. This includes the type of information that is set by CAPolicy.inf, or after the installation by running post-configuration scripts. You cannot access all the information by using the CA Admin console only.

To view the contents of the AIA container in AD DS for a domain named adatum.com, run the following command:

```
certutil -viewstore "ldap:///CN=AIA,CN=Public Key
Services,CN=Services,CN=Configuration,DC=adatum,DC=com?
cACertificate?base?objectclass=certificationAuthority"
```



## Managing PKI with Group Policy

After your PKI is in place, you will need to turn to Group Policy to automate distribution and to set configuration options. You can use Group Policy for the followings areas related to AD CS:

- Credential roaming. Credential roaming enables users to maintain their certificates with AD DS across multiple computers. This removes the requirement to manage multiple client certificates and private keys across multiple client workstations for a single user.
- Autoenrollment of certificates. Autoenrollment simplifies the issuance of certificates by enabling client computers to request and renew certificates automatically. Autoenrollment requires an enterprise CA and the use of Group Policy to enable the computers and users in your AD DS environment for autoenrollment.
- Certificate path validation. With certificate path validation, you can manage certificates used for code signing, deploying subordinate CA certificates, blocking certificates that are not trusted, and configuring retrieval settings for certificates and CRLs.
- Certificate distribution. Typically, you use Group Policy for the automated distribution of certificates or to specify settings related to enrollment.

## Configuring CA security

To manage and configure security on the CA, you can use the **Security** tab to view the properties of a CA in the Certification Authority (certsrv.msc) console. You can set the following security permissions on a CA:

- Read. Security principals assigned with this permission can locate this CA in AD DS or access it by using the web console or web services if you deployed the CA as a standalone CA.
- Issue and Manage Certificates. Security principals assigned with this permission can approve or deny certificate requests that are in a pending state. They also can revoke an issued certificate, specify a revocation reason, and perform an un-revoke. The security principals can also read all issued certificates and export them to files.
- Manage CA. Security principals assigned with this permission can manage and configure all options on the CA. They cannot manage certificates by default but can grant themselves the right.
- Request Certificates. Security principals assigned this permission can perform certificate requests against this CA. However, this does not mean that they can enroll for a certificate. The certificate template controls the enrollment permissions.

- You can assign the following permissions on a CA object:
  - Read
  - Issue and Manage Certificates
  - Manage CA
  - Request Certificates
- Security principals with the Issue and Manage Certificates permission can be restricted to a specific template
  - Certificate Managers tab on the CA object properties

In addition to defining security permissions on the access control list (ACL) of the CA object, you also can use the **Certificate Managers** tab on the CA properties to restrict further security principals containing the **Issue and Manage Certificates** permission.

For example, if you want to delegate the **Issue and Manage Certificates** permission for a specific template, you would:

1. Grant the security principal the **Issue and Manage Certificates** right on the **Security** tab of the CA properties.
2. On the **Certificate Managers** tab of the CA properties, select **Restrict certificate managers**.
3. Select the security principal you wish to restrict, and modify the templates you want the security principal to manage.

By using the **Certificate Managers** tab of the CA properties, you can delegate rights to a specific certificate template without giving a security principal the **Issue and Manage Certificates** right on all templates published on the CA.

## Security roles for CA administration


Role-based administration in AD CS provides the ability to delegate the predefined permissions available on a CA to groups you create in either AD DS (for enterprise CAs) or the local Security Account Manager database (for standalone CAs that are not domain-joined). Although you can assign CA permissions to a specific user object, we recommend as a best practice that you only delegate permissions to a group. Delegating to a group reduces the administrative effort required and provides transparency of what permissions you have assigned.

- Role-based administration:
  - Grant predefined CA permissions to a security group
  - Must be manually configured; roles are not automatically created
- Typical roles for AD CS might be:
  - CA Administrator
  - Certificate Manager
  - Backup Operator
  - Auditor
  - Enrollee
- Roles may be unique to each AD CS deployment

Each role you create should only be able to perform a predetermined task or series of tasks that you assign to a security group. The following table shows the details of roles and groups typically involved in the role-based administration of an AD CS deployment.

Role/group	Permissions	Description
CA Administrator	Manage CA Issue and Manage Certificates	Assigned in the CA console. Users in this role can configure all aspects of the CA and assign other roles as necessary.
Certificate Manager	Issue and Manage Certificates	Assigned in the CA console.
Backup Operator	Back up files and directories Restore files and directories	This role is an operating system role, which the membership in the local <b>Backup Operators</b> security group defines.
Auditor	Manage auditing and security log	This role is an operating system role, which the local security policy on the CA defines.

Role/group	Permissions	Description
Enrollees	Request Certificates (defined on the CA object) Enroll (defined on the certificate template)	This role is a CA role, which allows assigned users the ability to see the CA and request certificates. It does not imply that assigned users have permissions to enroll because that permission is assigned on a certificate template. By default, the <b>Authenticated Users</b> security principal has <b>Request Certificates</b> permissions on a CA. However, you might have more specific roles, which assign enrollment permissions for each unique template required by your organization.

 **Note:** The local **Administrators** group on a CA has the **Manage CA** and **Issue and Manage Certificates** permissions by default. On enterprise CAs, these permissions also extend to the **Domain Admins** and **Enterprise Admins** groups. On standalone CAs joined to a domain, members of the **Domain Admins** group also have full administrative rights on the CA.

### Create security roles for AD CS administration

You should be aware that AD CS does not create the roles and groups listed in the above table automatically when you install AD CS. The roles listed above are representative of a typical AD CS deployment where you desire role-based administration. Role-based administration might be unique to each AD CS deployment. Therefore, you should plan and create only the roles needed for your organization. Read the following scenario and think about how you would configure role-based administration to meet the requirements.

Scenario: You are the AD CS administrator for A. Datum. You have deployed a standalone root CA that is domain joined and two enterprise subordinate CAs. One subordinate CA will issue user certificates, and the other subordinate CA will issue computer certificates. You want to set up role-based administration so that you have the following roles:

- A role that has the **Manage CA** and **Issue and Manage Certificates** rights on all CAs in the hierarchy.
- A role that has the **Manage CA** and **Issue and Manage Certificates** rights on subordinate CAs only.
- A role that has the **Issue and Manage Certificates** rights for the **User** certificate template.
- A role that has the **Issue and Manage Certificates** rights for the **Computer** certificate template.

You would configure role based AD CS administration by following the steps below.

1. Create a security group in AD DS, which aligns to each role you want to assign in AD CS. Based on the requirements above, you would create the following groups for each required role.
  - Enterprise PKI Admins
  - Subordinate CA Admins
  - User Certificate Managers
  - Computer Certificate Managers
2. On each CA in the hierarchy, you assign the **Enterprise PKI Admins** group the **Manage CA** and **Issue and Manage Certificates** permission in the Certification Authority console.

3. On each subordinate CA, you assign the **Subordinate CA Admins** group the **Manage CA and Issue and Manage Certificates** permission in the Certification Authority console.
4. On the subordinate CA that will issue user certificates, you assign the **User Certificate Managers** group the **Issue and Manage Certificates** permission in the Certification Authority console. On the **Certificate Managers** tab of the CA properties, you restrict the **User Certificate Managers** group to the **User** certificate template.
5. On the subordinate CA that will issue computer certificates, you assign the **Computer Certificate Managers** group the **Issue and Manage Certificates** permission in the Certification Authority console. On the **Certificate Managers** tab of the CA properties, you restrict the **Computer Certificate Managers** group to the **Computer** certificate template.

## Configuring CA policy and exit modules

More advanced deployments of CA hierarchies, or scenarios where a CA with another PKI-related service, require that you configure and manage *policy* and *exit modules* on your CA. Policy and exit modules exist on every CA, standalone or enterprise. Each CA has default policy and exit modules, and in most scenarios, you will not have to configure these modules. You can manage both policy and exit modules if you use the CA administrator console. For more complex configuration, however, you must use the certutil command-line tool.

- The policy module determines the action that is performed after the certificate request is received
- The exit module determines what happens with a certificate after it is issued
- Each CA is configured with default policy and exit modules
- MIM 2016 Certificate Management deploys custom policy and exit modules
- The exit module can send email or publish a certificate to a file system
- You have to use certutil to specify these settings, as they are not available in the CA the administrator console

### What is a policy module?

A policy module determines the action that the CA performs after it receives the certificate request. You can configure a default policy module to put every certificate request in a pending state until an administrator approves or denies it. The behavior of the default policy module is to issue a certificate if the settings in the certificate template allow it. However, you can install a custom policy module to do other tasks when the CA receives the certificate request.

For example, if you install Microsoft Identity Manager (MIM) 2016 Certificate Management in your internal PKI, you will have to deploy the MIM Certificate Management policy module on your CA that issues certificates. MIM 2016 can manage certificate issuance through workflows. The MIM Certificate Management policy module forwards each request for a certificate managed by MIM 2016 Certificate Management to MIM 2016 Certificate Management when a CA receives a request. After the MIM workflow processes the request, it issues the certificate or denies the request. The MIM Certificate Management policy module also specifies the signature certificate thumbprint for an agent that passed certificate requests from users to a CA. Each request that the CA signs with a thumbprint specified in the MIM Certificate Management policy module is passed to the MIM workflow before it issues the certificate. This is one example of using the custom policy module, but there also are other third-party applications that might use custom policy modules.

### What is an exit module?

Unlike the policy module, the exit module determines what happens with a certificate after the CA issues it. The most common actions are to send an email or publish a certificate to a file system. These actions are possible even with a default exit module on each CA.

However, you also can deploy a custom policy module. To use the same example as the policy module, if you deploy MIM 2016 Certification Management in your environment, you also will have to deploy a custom exit module to your CA. The exit module forwards data about each issued certificate to a Microsoft SQL Server specified in the exit module. If you write information about the issued certificates to a computer that is running SQL Server, MIM Certificate Management can view and monitor issued certificates without direct interaction with the CA database. A CA can use multiple exit modules simultaneously, unlike the policy module, where you can have only one active policy module at a time.


For example, if you want to send an email to a specific address each time the CA issues a certificate, you have to use certutil to specify these settings because they are not available in the CA administrator console.

First, you should specify the Simple Mail Transfer Protocol (SMTP) server that is used to send emails, which you can do by running following certutil command:

```
certutil -setreg exit\smtp\<smtpServerName>
```

You have to enter the fully qualified domain name of your email server instead of the `<smtpServerName>` variable. After this you have to specify the event and email address to which the notification is sent by typing the following command:

```
certutil -setreg exit\smtp\CRLIssued\To<E-mailString>
```

 **Note:** The exit module on the CA that is configured to send emails on an event does not use SMTP authentication. If your SMTP server requires authentication, you have to configure it on the CA side by typing the following command:

```
certutil -setreg exit\smtp\SMTPAuthenticate 1  
certutil -setsmtpinfo<UserName>
```

The `<UserName>` specifies the user name of a valid account on the SMTP server. You will be prompted to provide the password for this user name.

Besides sending notification emails when the CA issues a certificate, you also can configure an exit module to send notifications of the following events:

- Certificate request in pending state.
- Certificate request denied.
- Certificate revoked.
- CRL is issued.
- CA service startup.
- CA service shutdown.

If you want to configure an exit module to publish certificates to the file system, you can use the CA admin console to open the properties of the exit module. After you enable the **Allow certificates to be published to the file system** option and restart the CA, certificates issued from that CA are copied into the .cer file in the C:\Windows\System32\CertEnroll folder on the CA. However, for this to happen, the certificate requestors must include a **certfile:true** attribute in their request.

If you deploy custom exit modules, their configuration might be possible through the CA admin console or with some other utility.


## Configuring CDPs and AIA locations

To ensure a properly functioning PKI environment, you must configure the Authority Information Access (AIA) and CRL Distribution Point (CDP) certificate extensions for each CA. This will ensure that it encounters minimal failures when applications or services attempt to validate the trust chain or revocation status of a certificate.

- AIA addresses are the URLs that tell a certificate verifier the location of the CA certificate. AIA addresses are necessary so that applications and services using a certificate can establish both the validity of the CA and a trust chain to a CA that the verifier explicitly trusts (if it does not explicitly trust the CA which directly issued the certificate).
- CDP addresses are the URLs that tell a certificate verifier the location of the Certificate Revocation List (CRL) maintained by the CA. CDP addresses are necessary so that applications and services using a certificate can establish the revocation status of a certificate.

- The AIA specifies where to retrieve the CA's certificate
- The CDP specifies from where the CRL for a CA can be retrieved
- Publication locations for AIA and CDP:
  - AD DS (LDAP)
  - Web servers (HTTP)
  - FTP servers
  - File servers
- Ensure that you properly configure CRL and AIA locations for offline and standalone CAs
- Ensure that the CRL for an offline root CA does not expire


Each certificate that you issue from your CA contains the AIA and CDP URLs that you configured on the CA at the time the CA issued the certificate. The AIA and CDP extensions must each contain at least one accessible URL or the verifier may assume that the certificate is not valid, rendering the certificate unable for use.

 **Note:** The URLs for AIA and CDP locations can be HTTP, File Transfer Protocol (FTP), Lightweight Directory Access Protocol (LDAP), or FILE addresses.


### AIA and CDP publishing considerations


If you are using an enterprise CA, the AIA and CDP extension values are automatically configured so that the CA certificate and CRL is available in the AD DS configuration partition replicated to all domain controllers in the AD DS forest. However, if you want to deploy an offline or standalone CA, or you will use certificates issued by your CA outside of your AD DS environment, there are other things you must consider.

- Offline or standalone CAs. Because offline and standalone CAs do not integrate with AD DS, you will need to ensure AIA and CDP accessibility manually by publishing the offline or standalone CA certificate and CRL to AD DS by using the certutil command. This provides the same benefit as an enterprise CA and makes AIA and CDP URLs accessible to AD DS clients throughout the forest, but you must manually publish the information and manually configure the CA extensions with the correct LDAP URL.

 **Note:** Besides configuring CDP and AIA publication points, you also should make sure that the CRL is valid. An online CA will automatically renew the CRL periodically, but an offline CA will not. If the offline CA CRL expires, revocation checks will fail. To prevent failure, make sure that you configure the validity period for the offline CA CRL to be long enough, and set a reminder to turn that CA on and issue a new CRL before the old one expires.

- Clients that are not domain joined. Internal clients that are not domain joined will not be able to access the AIA or CDP LDAP URLs, which reference the AD DS configuration partition. In this case, you should place the CA certificate and CRL on an internally accessible web server and configure a valid HTTP URL for the AIA and CDP extensions. You may also choose to use FTP or FILE URLs, but we recommend that you use only HTTP in this scenario for maximum interoperability and flexibility.
- External clients. Clients that are external to your network (including domain clients on an external network) will also not be able to access the AIA or CDP LDAP URLs, which reference your internal AD DS environment. In addition, they might not be able to access internal HTTP URLs without a VPN or DirectAccess connection. If external clients need to validate certificates issued by your internal CA, you might need to take the following actions:
  - Publish the internal HTTP URLs externally by using the Windows Server 2016 Web Application Proxy service of the Remote Access role. You can optionally use a third-party reverse proxy solution. If the internal and external URLs do not match, you will need to configure an additional AIA/CDP HTTP URL on the CA.
  - External clients not belonging to your AD DS domain will need to have your CA certificate manually imported into the Trusted Root Certification Authorities or Intermediate Certification Authorities stores. This might be necessary as the external client will not otherwise trust certificates that were issued by your internal CA.

 **Note:** The order in which you list the CDP and AIA URLs is important because the certificate-chaining engine searches the URLs sequentially. If your certificates are mostly used internally in an AD DS environment, place the LDAP URL first in the list. Order any other URLs based on the likelihood the URL will be available to internal or external clients.

 **Note:** If you decommission the AIA or CDP URLs present on the issued certificates (by removing them from the CA), you should ensure that all certificates containing a decommissioned URL have either expired, been revoked, or contain an additional URL which is still valid and accessible.

## Demonstration: Configuring CA properties

### Demonstration Steps

1. On **LON-SVR1**, open the **Certification Authority** console, and then open the **Properties** for **AdatumRootCA**.
2. View the **Certification Authority** certificate.
3. Review the settings for the active policy module.
4. Review the settings for the exit module.
5. Review the values provided on the **Extension** tab.
6. Review the **Security** settings of the CA.
7. Review the **Certificate Managers** settings.

**Check Your Knowledge**

Question	
<b>Which of the following options are true statements regarding role-based administration of your AD CS deployment?</b>	
Select the correct answer.	
<input type="checkbox"/>	AD CS automatically creates three built-in roles and groups for CA Administrator, Certificate Manager, and Enrollee.
<input type="checkbox"/>	You can grant AD CS role groups one or more of the following CA permissions: Manage CA, Issue and Manage Certificates, Read, Request Certificates.
<input type="checkbox"/>	You can limit the Issue and Manage Certificates CA permission to a specific template or set of templates.
<input type="checkbox"/>	You can create custom AD CS role groups based upon the specific needs of your organization.
<input type="checkbox"/>	The Authenticated Users security principal can enroll for any certificate published on a CA.

**Check Your Knowledge**

Question	
<b>Which of the following are true statements regarding the AIA and CDP extensions of a CA?</b>	
Select the correct answer.	
<input type="checkbox"/>	Each extension requires a minimum of two valid and accessible URLs for certificate validation to function properly.
<input type="checkbox"/>	You can manually publish offline and standalone CA certificates and CRLs into an AD DS environment.
<input type="checkbox"/>	The order in which you specify AIA and CDP URLs is not important as the certificate-chaining engine automatically orders locations based on the fastest connection.
<input type="checkbox"/>	To facilitate certificate validation for external clients, you should publish external AIA and CDP URLs using HTTP through a Windows Server 2016 Web Application Proxy.
<input type="checkbox"/>	If you are using an enterprise CA, internal certificate validation will work without any additional configuration.



## Lesson 3

# Troubleshooting and maintaining CAs

Troubleshooting and maintaining CA hierarchies is a very important part of an internal PKI deployment. You must use the available techniques, tools, and methods to maintain and troubleshoot your whole PKI effectively and proactively. AD CS provides several tools that you can use to maintain and troubleshoot a CA hierarchy. In this lesson, you will learn how to troubleshoot and maintain CAs.

### Lesson Objectives

After completing this lesson, you will be able to:

- Explain how to troubleshoot CAs.
- Explain how to renew a CA certificate.
- Describe how to move a root CA to another computer.
- Describe how to monitor CA operations.
- Describe how to back up and recover a CA.

### Troubleshooting CAs

Troubleshooting AD CS begins with the built-in tools that give administrators a detailed view into the current conditions of the AD CS role services.

The following list describes a few tools that you can use:

- Certificates snap-in. Use this snap-in to view and manage certificate stores for a computer, user, or service.
- PKIView tool. Use this tool to monitor multiple CA, CRL, and AIA locations, and to manage AD CS objects that it publishes to AD DS.
- CA snap-in. Use this snap-in to administer a CA, and to revoke and enroll a certificate. The CA snap-in also allows you to manage the certificate templates available on a CA.
- Certutil.exe. Use this command-line tool to display CA configuration information, configure AD CS, back up and restore CA components, and verify certificates, key pairs, and certificate chains.
- Certificate Templates snap-in. Use this snap-in to analyze and manage the certificate templates in AD DS, and to configure their permissions.
- Windows PowerShell. You can use the ADCSDeployment, ADCSAdministration, and PKI modules in Windows PowerShell as a replacement or a complement to the tools listed above. By taking advantage of the functionality in the available Windows PowerShell modules, you can write scripts to test automatically or verify your AD CS configuration.
- The Group Policy Management Console and gpresult.exe tools can help you verify the correct application of Group Policy Objects (GPOs), which configure autoenrollment or other PKI-related settings.

- Tools for managing CAs:
  - Certificates snap-in
  - PKIView tool
  - CA snap-in
  - Certutil.exe
  - Certificate Templates snap-in
- Common AD CS issues:
  - Client autoenrollment issues
  - Unavailable enterprise CA option
  - Error accessing CA webpages
  - Enrollment agent restriction

## AD CS common issues

The following list describes common AD CS issues that you might encounter:

- Users or computers do not enroll automatically for certificates as expected.
  - Because you enable autoenrollment through Group Policy, you should verify that the GPOs that enable autoenrollment for the user and computer are applying autoenrollment correctly and that the user or computer is not in an organizational unit (OU) where policy inheritance has been blocked or overridden by another GPO. Both the user and computer must be enabled separately, although both settings can reside in the same GPO.
  - You should verify that AD CS is publishing the certificate template to an enterprise CA, which can be accessed by the computer or user.
  - You should verify that the computer or user have the **Request Certificates** permission on the CA and **Autoenroll** permission on the certificate template in question.
  - You should verify that the requested certificate template does not require information that cannot be supplied automatically by AD DS.
- Cannot configure autoenrollment permissions on a template. For you to configure autoenrollment against a certificate, the template must be version 2 or later. Version 2 templates can only be added to a CA running Windows Server 2008 Enterprise or later.
- Unavailable enterprise CA option. This issue occurs when a user who is not a member of the Enterprise Admins or Domain Admins group installs a CA; as such, the CA might not be installed as an enterprise CA. In this case, the enterprise CA option is unavailable, and information about the CA cannot automatically publish to AD DS.
- Error accessing CA web enrollment pages. This error occurs while accessing CA webpages. In this case, you should ensure that the user is a member of the Administrators or Power Users group on the client computer.
- Enrollment agent restriction. This restriction occurs when an enrollment agent cannot enroll on behalf of a user for a specific certificate template. This might occur because of the restrictions configured on the enrollment agent or the lack of enrollment permissions on the certificate template.

## Troubleshooting validation issues

All certificates have a validity period. After the validity period expires, the certificate is no longer an acceptable credential. Client computers might not be able to connect to resources that require certificates if any certificate validation problems occur. AD CS services can stop, or fail to run, if there are problems of availability, validity, and chain validation for the CA certificate. You can use the PKIView utility to verify that the AIA and CRL CDP locations and certificates are valid. In addition, you can use the CA snap-in to install new certificates.

## Renewing a CA certificate

A CA also has its own certificate. A root CA issues a certificate for itself, a self-signed certificate, while subordinate CAs get their certificates from a root CA. Every CA certificate has a validity period. Usually, when deploying a root CA, IT administrators choose to set the validity period of the root CA certificate for five years or more. You need to renew a CA certificate when the validity period is close to the expiration date. A CA with an expired certificate cannot work, therefore, you should not let the CA certificate expire.

- The CA certificate needs to be renewed when the validity period of the CA certificate is close to its expiration date
- The CA will never issue a certificate that has a longer validity time than its own certificate
- Considerations for renewing a root CA certificate:
  - Key length
  - Validity period
- Considerations for renewing a certificate for an issuing CA:
  - New key pair
  - Smaller CRLs
- Procedure for CA certificate renewal

The validity period of the CA certificate is important also for the certificates that the CA issues. A CA will never issue a certificate that has a longer validity time than its own certificate. This is useful if you choose not to renew the CA in the event that you want to decommission it. For example, when the CA certificate reaches the end of its lifetime, all of the certificates that the now-expired CA has issued can no longer be used as valid security credentials.

This can have a side effect. When the CA certificate lifetime comes close to expiration, it will start to reduce the lifetime of certificates that it issues. For example, assume that your issuing CA has a certificate with five years of validity time, and it issues certificates with a two-year lifetime. For the first three years of its lifetime, no problems will arise. However, after three years, this CA will issue certificates with less than a two-year validity period.

### Renewing root CA certificates

A root CA usually has the certificate with a long validity period. Unlike a subordinate CA, which by default can have a maximum of a five-year validity time, you can set a much longer validity time for a root CA certificate during setup. You, also, should select a longer key length for the root CA public and private key pair. If you use a long key length, which makes the key more secure against brute force attack, you increase the length of time that the CA can use the same private key. In general, create a root CA that has a shorter validity period than the estimated lifetime of the key.

With this in mind, a reasonable strategy is to create a 4,096-bit RSA key during a root CA setup, which reduces the need for frequent renewal. Given the current state of computer technology, a 4,096-bit private key is secure from a brute force attack for an estimated 15–20 years. If you choose a 4,096-bit key during the root CA setup, you then can create a root certificate using the 4,096-bit key that is valid for five years. Afterward, you should renew the CA's certificate every four years, one year before the expiration of the validity period, each time with a certificate validity of five years. Every time you renew the CA certificate, we recommend that you assess whether the same key, given current computer technology and other security considerations, can be used with confidence for the next five years.

### Renewing subordinate CA certificates

For a subordinate CA that issues certificates to end users and devices, the recommended strategy might be to renew the CA certificate regularly with a new key 6–12 months before the end of the CA's validity period. This makes an attack on any one key less valuable because any compromised key would have a relatively limited lifetime.

CRL management is another advantage of renewing a subordinate CA by using a new key. When you renew a CA with a new key, it begins to publish a separate CRL for the revoked certificates it has issued. The CA continues to publish the CRL for certificates signed with the old key as long as the validity period of these certificates is valid. However, this can reduce the size of a single CRL greatly, and it will reduce the

size of the CRL that the certificate verifier has to download when presented with a certificate from an issuing CA.

You can complete the procedure for CA certificate renewal from the CA admin console. You must stop a CA service before you start the renewal procedure. When you start to renew a CA certificate procedure from the CA admin console, you will have to choose if you want to generate a new key set or reuse the existing one. The renewal procedure starts after you choose which key to use. If you choose the root CA, it will renew its certificate after the renewal procedure. For subordinate CAs, you must submit a renewal request to the parent CA, similar to when you first issued the certificate.

## Moving a root CA to another computer

As discussed in the previous topic, CAs are designed and configured to work for many years, during which time you might want to upgrade the hardware and operating system that supports the CA. Such scenarios usually require that you move a CA from one computer to another.

A CA is unlike some other services that you simply can install on a new computer and continue to work. When you move a CA from one computer to another, it is very important that you keep the identity of the CA during this process so that it can continue to work on the new hardware or operating system with the same identity.

- To move a CA from one computer to another, you have to perform backup and restore:
- To back up a computer, follow this procedure:
  - Record the names of the certificate templates
  - Back up a CA in the CA admin console
  - Export the registry subkey
  - Uninstall the CA role
  - Confirm the %SystemRoot% folder locations
  - Remove the old CA from the domain
- To restore, follow this procedure:
  - Install AD CS
  - Use the existing private key
  - Restore the registry file
  - Restore the CA database and settings
  - Restore the certificate templates

In general, the procedure for moving a CA can be divided into two phases:

- CA backup
- CA restore

### Performing a CA backup before a move

You should have a CA backup even if you are not moving a CA to another computer. A CA backup is different from ordinary backup scenarios. To perform a CA backup before moving a CA to another computer, you should perform the following procedure:

1. If you are backing up an enterprise CA, click the **Certificate Templates** item in the CA console, and then record the names of the certificate templates that are listed. These templates are in AD DS, so you do not have to back them up. You must note which templates you have published on the CA that you are moving because you will have to add them manually after you move the CA.
2. In the CA snap-in, right-click the **CA name**, click **All Tasks**, and then click **Backup CA** to start the Certification Authority Backup Wizard. In the backup wizard, you have to select the option to make the backup of the CA a private key, CA certificate, certificate database, and certificate database log. You also have to provide an appropriate location for the backup content. You should protect a CA private key with a password for security reasons.
3. After the backup is complete, you should open Registry Editor.
4. Locate and export the following registry subkey, located at:

**HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration.**



**Note:** We recommend that you save this registry key to a file in the same folder with the CA backup from the previous step.

5. Uninstall the CA from the old server, and then rename the old server or permanently disconnect it from the network.

Before you begin the restore procedure, confirm that the `%SystemRoot%` folder of the target server matches the `%SystemRoot%` folder of the server from which you took the backup. In addition, the location of the CA restore must match the location of the CA backup. For example, if you back up the CA from the `D:\Winnt\System32\Certlog` folder, you must restore the backup to the `D:\Winnt\System32\Certlog` folder. After you restore the backup, you can move the CA database files to a different location.

### Performing a CA restore on a new computer

After you successfully finalize the backup procedure, you have to restore the CA on another computer. The new CA should have the same name as the old CA. To restore the CA, perform the following procedure:

1. Install AD CS on the target computer. Select to install either **Stand-alone** or **Enterprise**, depending on the type of CA that you are moving. When you come to the **Set Up Private Key** page, click **Use existing private key**. Then choose to select a certificate and use its associated private key. This will provide you with the ability to use an existing certificate from an old CA.
2. On the **Select Existing Certificate** page, click **Import**, type the path of the .p12 file in the backup folder, type the password that you chose in the previous procedure to protect the backup file, and then click **OK**. When prompted for **Public and Private Key Pair**, verify that **Use existing keys** is selected. This is very important because you want to keep the same root CA certificate.
3. When prompted on the **Certificate Database** page, specify the same location for the certificate database and certificate database log as on the previous CA computer. After you select all these options, wait for the CA setup to finish.
4. After the setup is complete, open the Services snap-in to stop the AD CS service. You do that to restore settings from the old CA.
5. Locate the registry file that you saved in the backup procedure, and then double-click it to import the registry settings.
6. After you restore the registry settings, open the CA management console, right-click the **CA name**, click **All Tasks**, and then click **Restore CA**. This will start the Certification Authority Restore Wizard. In the wizard, select the **Private key and CA certificate** and the **Certificate database and certificate database log** check boxes. This specifies that you want to restore these objects from backup. Next, provide a backup folder location and verify the settings for the restore. The **Issued Log** and **Pending Requests** settings should be displayed.
7. When the restore process completes, choose to restart the AD CS service.
8. If you restored an enterprise CA, restore the certificate templates from AD DS that you recorded in the previous procedure.

## Monitoring CA operations

Because the CA is a critical service for each enabled PKI, it is very important that you establish techniques for monitoring and maintaining each CA object, in addition to certificates, CRLs, and other PKI-related objects. When you install AD CS and the CA role, you can use some of the tools for management, monitoring, and auditing.

### PKIView console

Windows Server 2016 includes the PKIView console, which is a management tool, when you install the AD CS role. It provides a summary view of the status of the enterprise PKI. The PKIView console also enables you to view multiple CAs and their current health state, but you cannot view standalone CAs. You can use PKIView to access AD DS PKI-related containers and to manage their content, including certificate templates. You can start the PKIView console when you type **pkiview.msc** at the command prompt or in Windows PowerShell.

PKIView shows all of the CAs and their health state as indicated by a small icon. The following are the available health states:

- CA health state evaluation (question mark)
- CA has no problems (green indicator)
- CA has a noncritical problem (yellow indicator)
- CA has a critical problem (red indicator)
- CA is offline (red cross over CA indicator)

PKIView also shows a quick health summary of the following areas by indicating their status options are OK or Unable to Download:

- CA certificates
- AIA locations
- CRLs and delta CRLs
- CDPs
- OCSP locations

PKIView evaluates the CDP or AIA state for each location defined on each CA. For example, you easily can see if any CDP or AIA locations are not accessible, or if any of the locations contain an expired CRL. PKIView also is able to evaluate the state of the Online Responder, if you have deployed that role service.

### Auditing CA events

Besides monitoring and reviewing the whole CA hierarchy with the PKIView console, you also can use auditing options on the CA level in the Certification Authority console to monitor events that happen on each CA. To access the auditing options, you have to open the **CA Properties** window and go to the **Auditing** tab. You can configure this tab to monitor the following events:

- Backup and restore of the CA database
- Change of the CA configuration
- Change of the CA security settings

- For monitoring and maintenance of a CA hierarchy, you can use PKIView and CA auditing
- With PKIView, you can:
  - Access and manage AD DS PKI-related containers
  - Monitor CAs and their health state
  - Check the status of CA certificates
  - Check the status of AIA locations
  - Check the status of CRLs
  - Check the status of CDPs
  - Evaluate the state of the Online Responder
- CA auditing provides logging for various events that happen on the CA

- Management of certificate requests
- Certificates revoke and CRL publish
- Store and retrieve archived keys
- Start and stop of the AD CS service

The Certification Authority console does not configure any of these options by default, which means that it does not enable auditing on CA automatically. If you want to start logging events from the CA, you have to enable one or more options manually.

### Check Your Knowledge

Question	
<b>Which of the following issues could prevent autoenrollment from correctly working in AD CS?</b>	
Select the correct answer.	
<input type="checkbox"/>	The computer that you expect to autoenroll for a certificate is in an AD DS OU where policy inheritance is blocked.
<input type="checkbox"/>	The user that you expect to autoenroll for a certificate is in an AD DS OU where the necessary Group Policy setting is not linked or inherited.
<input type="checkbox"/>	The CA is a standalone CA.
<input type="checkbox"/>	The certificate template is not published on a CA.
<input type="checkbox"/>	The AIA URL is configured incorrectly on the extensions tab of the CA.

### Check Your Knowledge

Question	
<b>Which of the following are true statements regarding the PKIView tool?</b>	
Select the correct answer.	
<input type="checkbox"/>	PKIView shows all of your enterprise CAs and their current health state.
<input type="checkbox"/>	You can use PKIView to manually add standalone CAs.
<input type="checkbox"/>	You can use PKIView to configure autoenrollment for users and computers.
<input type="checkbox"/>	PKIView evaluates the CDP or AIA state for each location defined on each CA.
<input type="checkbox"/>	PKIView can evaluate the status of the AD CS Online Responder role service.

## Lab: Deploying and configuring a two-tier CA hierarchy

### Scenario

A. Datum Corporation has expanded, therefore, its security requirements also have increased. The Security department is particularly interested in enabling secure access to critical websites, and in providing additional security for features. To address these and other security requirements, A. Datum has decided to implement a PKI by using the AD CS role in Windows Server 2016. As a senior network administrator at A. Datum, you are responsible for implementing the AD CS deployment.

### Objectives

After completing this lab, you will be able to:

- Deployed an offline root CA.
- Deploy an enterprise subordinate CA.

### Lab Setup

Estimated Time: 60 minutes

Virtual machines: **20742A-LON-DC1**, **20742A-LON-DC2**, **20742A-LON-SVR1**, **20742A-CA-SVR1**

User name: **Adatum\Administrator**

Password: **Pa\$\$w0rd**

For this lab, you will use the available virtual machine environment. Before you begin the lab, you must complete the following steps:

1. On the host computer, start **Hyper-V Manager**.
2. In Hyper-V Manager, click **20742A-LON-DC1**, and in the **Actions** pane, click **Start**.
3. In the **Actions** pane, click **Connect**. Wait until the virtual machine starts.
4. Sign in by using the following credentials:
  - o User name: **Adatum\Administrator**
  - o Password: **Pa\$\$w0rd**
5. Repeat steps 2 through 4 for **20742A-LON-DC2** and **20742A-LON-SVR1**.
6. Repeat steps 2 through 3 for **20742A-CA-SVR1**. Do not sign in to **20742A-CA-SVR1** until directed to do so.



## Exercise 1: Deploying an offline root CA

### Scenario

A. Datum wants to use certificates for various purposes. You need to install the appropriate CA infrastructure. Because A. Datum uses Windows Server 2016 AD DS, you decided to implement the AD CS role. When you reviewed the available designs, you decided to implement a standalone root CA. This CA will be taken offline after it issues a certificate for a subordinate CA. After installation, you must make sure that you configured the CDP and AIA locations correctly. You also must make sure that you have a Domain Name System (DNS) record for the offline root CA so that it is accessible from the network.

The main tasks for this exercise are as follows:

1. Create file and printer sharing exceptions.
2. Install and configure AD CS on CA-SVR1.
3. Create a Domain Name System (DNS) record for an offline root CA.

#### ► Task 1: Create file and printer sharing exceptions

1. Sign in to **CA-SVR1** as **Administrator** with password **Pa\$\$w0rd**.
2. On **CA-SVR1**, from the Network and Sharing Center, turn on file and printer sharing on guest and public networks.
3. On **LON-SVR1**, from the Network and Sharing Center, turn on file and printer sharing on the guest/public network.

#### ► Task 2: Install and configure AD CS on CA-SVR1

1. Switch to **CA-SVR1** and start **Server Manager**.
2. Use the **Add Roles and Features Wizard** to install the **Active Directory Certificate Services** role.
3. After installation completes successfully, click the text **Configure Active Directory Certificate Services on the destination server**.
4. Configure the AD CS role as a stand-alone root CA with the name **AdatumRootCA**.
5. Set the key length to **4096**, and then accept all other values as default.
6. On **CA-SVR1**, open the **Certification Authority** console.
7. Open the **Properties** dialog box for **AdatumRootCA**.
8. Configure the new locations for the CDP to be **http://lon-svr1.adatum.com/CertData /<CaName><CRLNameSuffix><DeltaCRLAllowed>.crl**.
9. Select the following options
  - **Include in the CDP extension of issued certificates**
  - **Include in CRLs. Clients use this to find Delta CRL locations**
10. Configure new locations for AIA to be on **http://lon-svr1.adatum.com/CertData /<ServerDNSName>\_<CaName><CertificateName>.crt**.
11. Select the **Include in the AIA extension of issued certificates** check box.
12. Publish the CRL on **CA-SVR1**.
13. Export the root CA certificate, and then copy the .cer file to **\\lon-svr1\C\$**.
14. Copy the contents of folder **C:\Windows\System32\CertSrv\CertEnroll** to **\\lon-svr1\C\$**.

► **Task 3: Create a Domain Name System (DNS) record for an offline root CA**

1. On **LON-DC1**, from **Server Manager**, open the DNS Manager console.
2. Create a host record for **CA-SVR1** in the **Adatum.com** forward lookup zone.
3. Use IP address **172.16.0.40** for the **CA-SVR1** host record.

**Results:** After completing this exercise, you should have successfully installed and configured the standalone root certification authority (CA) role on **CA-SVR1** server. In addition, you should have created an appropriate DNS record in Active Directory Domain Services (AD DS) so that other servers can connect to **CA-SVR1**.

## Exercise 2: Deploying an enterprise subordinate CA

### Scenario

After deploying the standalone root CA, the next step is to deploy an enterprise subordinate CA. A. Datum wants to use an enterprise subordinate CA to utilize AD DS integration. In addition, because the root CA is a standalone CA, you want to publish its certificate to all clients.

The main tasks for this exercise are as follows:

1. Install and configure AD CS on LON-SVR1.
2. Install a subordinate CA certificate.
3. Publish a root CA certificate through Group Policy.
4. Prepare for the next module.

► **Task 1: Install and configure AD CS on LON-SVR1**

1. On **LON-SVR1**, from **Server Manager**, install the **Active Directory Certificate Services** role. Include the **Certification Authority** and **Certification Authority Web Enrollment** role services.
2. After installation is successful, click the **Configure Active Directory Certificate Services on the destination server** text.
3. Select the **Certification Authority** and **Certification Authority Web Enrollment** role services.
4. Configure **LON-SVR1** to be an **Enterprise CA**.
5. Configure the CA Type to be a **Subordinate CA**.
6. For the CA Name, type **Adatum-IssuingCA**.
7. Save the request file to the local drive.

► **Task 2: Install a subordinate CA certificate**

1. On **LON-SVR1**, install the **C:\RootCA.cer** certificate to the Trusted Root Certification Authority store.
2. Go to **Local Disk (C:)**, and then copy the **AdatumRootCA.crl** and **CA-SVR1\_AdatumRootCA.crt** files to **C:\inetpub\wwwroot\CertData**.
3. Copy the **LON-SVR1.Adatum.com\_Adatum-LON-SVR1-CA.req** request file to **\\CA-SVR1\C\$**.
4. Switch to **CA-SVR1**.
5. From the **Certification Authority** console on **CA-SVR1**, submit a new certificate request by using the .req file that you copied in step 3.

6. Issue the certificate, and then export it to .p7b format with a complete chain. Save the file to **\\lon-svr1\C\$\SubCA.p7b**.
7. Switch to **LON-SVR1**.
8. Install the subordinate CA certificate on **LON-SVR1** by using the **Certification Authority** console.
9. Start the service. Ensure that the AD CS service starts successfully.
10. Switch to **CA-SVR1**, and then shut down the server.

► **Task 3: Publish a root CA certificate through Group Policy**

1. On **LON-DC1**, from **Server Manager**, open the **Group Policy Management Console**.
2. Edit the Default Domain Policy.
3. Publish the **RootCA.cer** file from **\\lon-svr1\C\$** to the Trusted Root Certification Authorities store, which is located in **Computer Configuration\Policies\Windows Settings\Security Settings\Public Key Policies**.

**Results:** After completing this exercise, you should have successfully deployed and configured an enterprise subordinate CA. You also should have a subordinate CA certificate issued by a root CA installed on **LON-SVR1**. To establish trust between the root CA and domain-joined clients, you will use Group Policy to deploy a root CA certificate.

► **Task 4: Prepare for the next module**

1. On the host computer, start **Hyper-V Manager**.
2. In the **Virtual Machines** list, right-click **20742A-LON-DC1**, and then click **Revert**.
3. In the **Revert Virtual Machine** dialog box, click **Revert**.
4. Repeat steps 2 and 3 for **20742A-LON-SVR1**, **20742A-LON-DC2**, and **20742A-CA-SVR1**.

**Question:** Why is it not recommended to install only an enterprise root CA?

**Question:** What are some reasons that an organization would use an enterprise root CA?

## Module Review and Takeaways

### Review Questions

**Question:** What are some reasons that an organization would use a PKI?

**Question:** Why would you deploy a custom policy and exit modules?

### Best Practice

- When deploying a CA infrastructure, deploy a standalone (not domain-joined) root CA and an enterprise subordinate CA (issuing CA). After the enterprise subordinate CA receives a certificate from the root CA, take the root CA offline.
- Review the validation time of root CA certificate revocation lists (CRLs).
- Provide more than one location for AIA and CRL.

### Common Issues and Troubleshooting Tips

Common Issue	Troubleshooting Tip
The location of the CA certificate that is specified in the AIA extension is not configured to include the certificate name suffix. Clients might not be able to locate the correct version of the issuing CA's certificate to build a certificate chain, and certificate validation might fail.	
The CA is not configured to include CDP locations in the extensions of issued certificates. Clients might not be able to locate a CRL to check the revocation status of a certificate, and certificate validation might fail.	

### Tools

- CA admin console
- Certutil command-line utility
- Windows PowerShell command-line interface
- PKIView.msc
- Server Manager

# Module 9

## Deploying and managing certificates

### Contents:

Module Overview	9-1
Lesson 1: Deploying and managing certificate templates	9-2
Lesson 2: Managing certificate deployment, revocation, and recovery	9-8
Lesson 3: Using certificates in a business environment	9-18
Lesson 4: Implementing and managing smart cards	9-27
Lab: Deploying and using certificates	9-33
Module Review and Takeaways	9-40

## Module Overview

After designing and deploying the certification authority (CA) hierarchy, it is very important to design certificate templates properly, to define certificate usage, and to implement backup and recovery techniques for certificates.

In this module, you will learn how to deploy and manage certificates, to configure certificate templates, and to manage the enrollment process. Also, you will learn about using certificates in business environments and about deploying and managing smart cards.

### Objectives

After completing this module, you will be able to:

- Deploy and manage certificate templates.
- Manage certificates deployment, revocation, and recovery.
- Use certificates in a business environment.
- Implement and manage smart cards.

## Lesson 1

# Deploying and managing certificate templates

Certificate templates define how a certificate is requested and used, such as for file encryption or email signing. You configure templates on the CA, and they are stored in the Active Directory Domain Services (AD DS) database. There are several different versions of templates that correlate to the operating system on the CA. The Windows Server 2012 operating system introduces version 4 templates, and it still supports all three previous template versions.

The two types of certificate categories are: certificate templates for users and certificate templates for computers. You can use both the user and computer templates for multiple purposes. You can assign permissions to certificate templates to define who can manage them and who can perform enrollment or autoenrollment. You also can update certificate templates by modifying the original certificate template, copying a template, or superseding existing certificate templates. In this lesson, you will learn how to manage and deploy certificate templates.

### Lesson Objectives

After completing this lesson, you will be able to:

- Describe certificates and certificate templates.
- Describe certificate template versions in Windows Server 2016.
- Describe how to configure certificate template permissions.
- Describe how to configure certificate template settings.
- Describe options for updating a certificate template.
- Modify and enable a certificate template.

### What are certificates and certificate templates?

A *certificate* is a small file that contains several pieces of information about its owner. This data can include the owner's email address, the owner's name, the certificate usage type, the validity period, and the URLs for authority information access (AIA) and certificate revocation list distribution point (CDP) locations. A certificate also contains the *key pair*, which is the private key and its related public key. These keys are used in processes of validating identities, digital signatures, and encryption. The key pair that is generated with each certificate works under the following conditions:

- When content is encrypted with the public key, it can be decrypted only with the private key.
- When content is encrypted with the private key, it can be decrypted only with the public key.
- There is no other key that is involved in the relationship between the keys from a single key pair.
- The private key cannot be derived in a reasonable amount of time from a public key, and vice versa.

A certificate contains information about users, devices, usage, validity, and a key pair

A certificate template defines:

- The format and contents of a certificate
- The process for creating and submitting a valid certificate request
- The security principals that are allowed to read, enroll, or use autoenrollment for a certificate that will be based on the template
- The permissions that are required to modify a certificate template

During the enrollment process, the client generates the private key, while the CA generates a corresponding public key. Certificates provide a mechanism for gaining confidence in the relationship between a public key and the entity that owns the corresponding private key.

You can think of a certificate as being similar to a driver's license. A driver's license is accepted by numerous businesses as a form of identification because the community accepts the license issuer (a government institution) as trustworthy. Because businesses understand the process by which someone can obtain a driver's license, they trust that the issuer has verified the identity of the individual to whom the license was issued. Therefore, the driver's license can be accepted as a valid form of identification. A certificate trust is established in a similar way.

### Certificate Templates

Certificate templates allow administrators to customize the distribution method of certificates, define certificate purposes, and mandate the type of usage that is allowed by a certificate. Administrators can create templates and then can deploy them quickly to an enterprise by using built-in graphical user interface (GUI) or command-line management utilities.

Associated with each certificate template is its discretionary access control list (DACL), which defines what security principals have permissions to read and configure the template and what security principals can enroll or use autoenrollment for certificates based on the template. Certificate templates and their permissions are defined in AD DS and are valid within the forest. If more than one enterprise CA is running in the AD DS forest, permission changes will affect all CAs.

When you define a certificate template, the definition of the certificate template must be available to all CAs in the forest. You accomplish this when you store the certificate template information in the configuration-naming context of AD DS. The replication of this information depends on the AD DS replication schedule, and the certificate template might not be available to all CAs until replication completes. Storage and replication occur automatically.

### Certificate template versions in Windows Server 2016

The CA in Windows Server 2016 Active Directory Certificate Services (AD CS) supports four versions of certificate templates. Aside from corresponding with Windows Server operating system versions, certificate template versions also have some functional differences, including:

- Version 1 templates. The only modification allowed to version 1 templates is the ability to change the permissions to read, write, allow, or disallow enrollment of the certificate template. When you install a CA, version 1 certificate templates are created by default.
- Version 2 templates. You can customize several settings in version 2 templates. The default installation of AD CS provides several preconfigured version 2 templates. You also can create version 2 templates based on the requirements of your organization. Alternatively, you can duplicate a version 1 certificate template to create a new version 2 template. You then can modify and secure the newly created version 2 certificate template. Templates must be a minimum of version 2 to support autoenrollment.

<ul style="list-style-type: none"> <li>• Version 1               <ul style="list-style-type: none"> <li>• Created by default when CA is installed</li> <li>• Cannot be modified (except for permissions) or removed</li> <li>• Can be duplicated to create version 2 or version 3 templates.</li> </ul> </li> <li>• Version 2               <ul style="list-style-type: none"> <li>• Allows customization of most settings in the template</li> <li>• Supports autoenrollment.</li> </ul> </li> <li>• Version 3               <ul style="list-style-type: none"> <li>• Supports advanced Suite B cryptographic settings</li> <li>• Includes advanced options for encryption, digital signatures, key exchange, and hashing</li> </ul> </li> <li>• Version 4               <ul style="list-style-type: none"> <li>• Supports both CSPs and key storage providers</li> <li>• Supports renewal with the same key</li> </ul> </li> </ul>
--

- Version 3 templates. Version 3 certificate templates support Cryptography Next Generation (CNG). CNG provides support for Suite B cryptographic algorithms such as elliptic curve cryptography. You can duplicate default version 1 and version 2 templates to bring them up to version 3. When you use the version 3 certificate templates, you can use CNG encryption and hash algorithms for certificate requests, issued certificates, and protection of private keys for key exchange and key archival scenarios.
- Version 4 templates. Version 4 certificate templates are available only to Windows Server 2012, Windows 8, and later operating systems. To help administrators separate which operating system versions support what features, the **Compatibility** tab was added to the certificate template **Properties** tab. It marks options as unavailable in the certificate template properties, depending on the selected operating system versions of a certificate client and CA. Version 4 certificate templates also support both cryptographic service providers (CSPs) and key storage providers. They also can be configured to require renewal with the same key.

## Configuring certificate template permissions

To configure certificate template permissions, you need to define the DACL on the **Security** tab for each certificate template. The permissions that are assigned to a certificate template will define which users or groups can read or modify a certificate template and who can enroll or use autoenrollment for the certificate based on that certificate template.

You can assign the following permissions to certificate templates:

- Full Control. The Full Control permission allows a security principal to modify all attributes of a certificate template, which includes permissions for the certificate template itself. It also includes permission to modify the security descriptor of the certificate template.
- Read. The Read permission allows a user or computer to view the certificate template when enrolling for certificates. The certificate server requires Read permission to find certificate templates in AD DS.
- Write. The Write permission allows a user or computer to modify the attributes of a certificate template.
- Enroll. The Enroll permission allows a user or computer to enroll for a certificate based on the certificate template. However, to enroll for a certificate, you also must have Read permissions for the certificate template.
- Autoenroll. The Autoenroll permission allows a user or computer to receive a certificate through the autoenrollment process. However, the Autoenroll permission requires the user or computer also to have both Read and Enroll permissions for a certificate template.

As a best practice, you should assign certificate template permissions to global or universal groups only. This is because the certificate template objects are stored in the configuration-naming context in AD DS. Avoid assigning certificate template permissions to individual users or computer accounts.

Permission	Description
Full Control	Allows a designated user, group, or computer to modify all attributes—including ownership and permissions
Read	Allows a designated user, group, or computer to read the certificate in AD DS when enrolling
Write	Allows a designated user, group, or computer to modify all attributes except permissions
Enroll	Allows a designated user, group, or computer to enroll for the certificate template
Autoenroll	Allows a designated user, group, or computer to receive a certificate through the autoenrollment process



As a best practice, keep the read permission allocated to the **Authenticated Users** group. Read permissions enable all users and computers to view the certificate templates in AD DS. This permission assignment also enables the CA, which runs under the System context of a computer account, to view the certificate templates when assigning certificates. This permission, however, does not grant Enroll rights, so it is safe to have it configured this way.


## Configuring certificate template settings

Besides configuring security settings for certificate templates, you also can configure several other settings for each template. Be aware, however, that the number of configurable options depends on the certificate template version. For example, version 1 certificate templates do not allow modification of any settings except for security, while you can use certificate templates from later versions to configure most of the available options.

Windows Server 2016, like previous versions of Windows Server, provides several default certificate templates for purposes that include code-signing for digitally signing software, Encrypting File System (EFS) for encrypting data, and the ability for users to sign in with a smart card. To customize a template for your organization, you can duplicate the template and then modify the certificate configuration.

To configure templates, you must:

- Determine the format and content of a certificate based on the certificate's intended use.
- Determine the process for creating and submitting a valid certificate request.
- Determine which CSP is supported.
- Set the key length.
- Set the validity period.
- Determine the enrollment process or enrollment requirements.

 **Note:** Certificate usage might relate to users or computers based on the types of security implementations that are required to use the public key infrastructure (PKI).

You also can define a certificate's purpose in certificate settings. Certificate templates can be:

- **Single purpose.** A single-purpose certificate serves one purpose, such as allowing users to sign in with a smart card. Organizations use single-purpose certificates in cases where the certificate configuration differs from other certificates that are being deployed. For example, if all users receive a certificate for smart card sign in but only a couple of groups will receive a certificate for EFS, then organizations generally will keep these certificates and templates separate to ensure that users only receive the required certificates.

For each certificate template, you can customize several settings, such as validity time, purpose, CSP, private key exportability, and issuance requirements

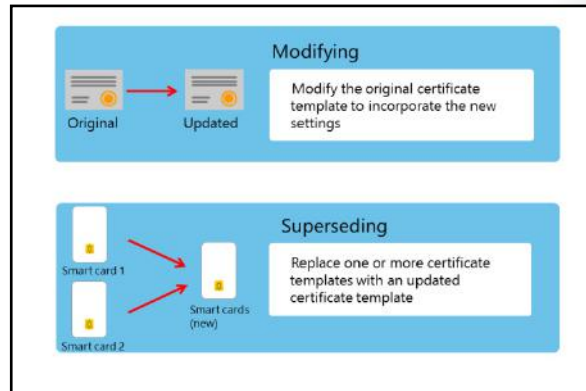
Category	Example of single purpose	Example of multipurpose
Users	• Basic EFS	• Administrator
	• Authenticated session	• User
	• Smart card sign in	• Smart card user
Computers	• Web server	• Computer
	• IPsec	• Domain controller

- **Multipurpose.** A multipurpose certificate serves more than one, often unrelated, purpose at the same time. While some templates, such as the User template, serve multiple purposes by default, organizations often will modify templates to serve additional purposes. For example, if a company intends to issue certificates for three purposes, those purposes can combine into a single certificate template to ease administrative efforts and maintenance.

## Options for updating a certificate template

The CA hierarchy in most organizations has one certificate template for each job function. For example, there might be a certificate template for file encryption and another for code signing. Additionally, a few templates might cover functions for most of the common groups of subjects.

As an IT administrator, you might need to modify an existing certificate template because of incorrectly configured settings or other issues in the original certificate template. You also might need to merge multiple existing certificate templates into a single template.



You can update a certificate template either by modifying the template or by superseding the existing template:

- **Modifying the original certificate template.** To modify a certificate template of version 2, 3, or 4, you need to make changes and then apply them to that template. After this, any certificate issued by a CA based on that certificate template will include your modifications.
- **Superseding existing certificate templates.** The CA hierarchy of an organization might have multiple certificate templates that provide the same or similar functionality. In such a scenario, you can supersede or replace multiple certificate templates by using a single certificate template. You can make this replacement in the **Certificate Templates** console by designating that a new certificate template supersedes, or replaces, the existing certificate templates. After this, all users who have certificates issued based on superseded templates will be issued certificates based on the new template.

## Demonstration: Modifying and enabling a certificate template

In this demonstration, you will see how to modify and enable a certificate template.

### Demonstration Steps

1. On **LON-DC1**, from **Server Manager**, open **Certification Authority**.
2. In the **Certification Authority**, open the **Certificate Templates** console.
3. Review the list of available templates.
4. Open the **IPsec** certificate template properties, and then review the available settings.
5. Duplicate the **Exchange User** certificate template. Name it **Exchange User Test1**, and then configure it to supersede the **Exchange User** template.

6. Allow **Authenticated Users** to enroll and autoenroll for the **Exchange User Test1** template.
7. Issue the **Exchange User Test1** template on **LON-DC1**.

### Check Your Knowledge

Question	
Which of the following statements are true regarding version 2 certificate templates in AD CS? (Choose all that apply.)	
Select the correct answer.	
<input type="checkbox"/>	Version 2 templates support autoenrollment.
<input type="checkbox"/>	You can only modify the Security tab on a version 2 template.
<input type="checkbox"/>	You can upgrade to a version 2 template by duplicating a version 1 template.
<input type="checkbox"/>	Version 2 templates are only supported on Windows Server 2008 and Windows Vista or later operating systems.
<input type="checkbox"/>	Version 2 templates are only supported on Windows Server 2012 and Windows 8 or later operating systems.

### Check Your Knowledge

Question	
You are the AD CS administrator for A. Datum Corporation. Several users in your AD DS environment have autoenrolled for a user certificate. You want to shorten the validity period of the user certificate and need to ensure that users get a new certificate immediately without experiencing any break in validity of the existing certificate. Which of the following actions should you take? (Choose all that apply.)	
Select the correct answer.	
<input type="checkbox"/>	Duplicate the existing template and provide a new template name. Modify the validity period of the new template.
<input type="checkbox"/>	Modify the validity period of the existing template.
<input type="checkbox"/>	Modify the autoenrollment settings of the existing template.
<input type="checkbox"/>	Revoke all user certificates issued from the existing template.
<input type="checkbox"/>	Modify the new template so that it supersedes the existing template. Publish the new template.

## Lesson 2

# Managing certificate deployment, revocation, and recovery

One of the steps in deploying a PKI in your organization will be to define methods for certificate distribution and enrollment. In addition, during the certificate management process, there are times that you might need to revoke certificates. Reasons for revoking certificates can include a key becoming compromised or someone leaving the organization. You need to ensure that network clients can determine which certificates are revoked before accepting authentication requests. During the certificate lifecycle, certificate or key recovery is one of the most important management tasks. If you lose your public and private keys, you can use a key archival and recovery agent for data recovery. You can also use automatic or manual key archival and key recovery methods to ensure that you can access data in the event that your keys are lost.

### Lesson Objectives

After completing this lesson, you will be able to:

- Describe certificate enrollment methods.
- Describe certificate autoenrollment.
- Explain what an enrollment agent is.
- Describe how certificate revocation works.
- Describe key archival and recovery.
- Describe how to configure automatic key archival.
- Configure a CA for key archival.

### Certificate enrollment methods

In Windows Server 2016, you can use several methods to enroll for a user or computer certificate. Which method you choose depends on your specific scenario. For example, you can use autoenrollment to mass deploy certificates to a large number of users or computers. However, you may choose to use manual enrollment for certificates that are dedicated to specific security principals. The following list describes the different enrollment methods and specifies when to use them:

- **Autoenrollment.** When you use this method, the administrator defines the permissions and the configuration of a certificate template. These definitions help the requestor to request, retrieve, and renew certificates automatically without end-user interaction. This method is commonly used for AD DS domain computers. The certificate must be configured for autoenrollment through Group Policy. This method is discussed in more detail in the next topic.

Method	Use
Autoenrollment	<ul style="list-style-type: none"> <li>• To automate the request, retrieval, and storage of certificates for domain-based computers</li> </ul>
Manual enrollment	<ul style="list-style-type: none"> <li>• To request certificates by using the <b>Certificates</b> console or <b>Certreq.exe</b> when the requestor cannot communicate directly with the CA</li> </ul>
CA Web enrollment	<ul style="list-style-type: none"> <li>• To request certificates from a website that is located on a CA</li> <li>• To issue certificates when autoenrollment is not available</li> </ul>
Enroll on behalf	<ul style="list-style-type: none"> <li>• To provide IT staff with the right to request certificates on behalf of another user (Enrollment Agent)</li> </ul>

- **Manual enrollment.** By using this method, the private key and a certificate request are generated on a device, such as a web service or a computer. The certificate request then is transported to the CA to generate the requested certificate. The certificate then is transported back to the device for installation. Use this method when the requestor cannot communicate directly with the CA or if the device does not support autoenrollment. This method is used when buying a public certificate. You can use this method through the Certificates snap-in or the Certreq.exe tool.
- **CA Web enrollment.** By using this method, you can enable a website CA so that users can obtain certificates. To use CA Web enrollment, you must install Internet Information Services (IIS) and the CA Web Enrollment role on the CA. To obtain a certificate, the requestor signs in to the website, selects the appropriate certificate template, and then submits a request. The certificate issues automatically if the user has the appropriate permissions to enroll for the certificate. Use the CA Web Enrollment method to issue certificates when you cannot use autoenrollment. This can happen in the case of an advanced certificate request.
- **Enrollment on behalf.** To use this method, you must first create an Enrollment Agent. An *Enrollment Agent* is a user account used to request certificates on behalf of another user account. A specific certificate template is applied to an Enrollment Agent which grants the necessary rights. You would use this method, for example, if you need to allow a manager to preload the logon certificates of new employees onto smart cards.


## Overview of certificate autoenrollment

In situations where it may be inefficient to use manual enrollment, you can configure certificate templates so that the requestor is able to enroll for and renew certificates automatically without end-user interaction.

One example where manual enrollment would be inefficient would be when you need to issue a certificate to every user and computer in your organization. A common and more efficient method would be to use *autoenrollment*. This method provides an automated way to deploy certificates to users and computers within your AD DS organization. It is important to note, however, that you cannot use autoenrollment with a standalone CA. You must have an enterprise CA available to use autoenrollment.

- A certificate template is configured for Allow, Enroll, and Autoenroll permissions for users who receive the certificates
- The CA is configured to issue the template
- An AD DS Group Policy Object (GPO) should be created to enable autoenrollment
- The GPO should be linked to the appropriate site, domain, or Organizational Unit (OU)
- The user or computer receives the certificates during the next Group Policy refresh interval

The Autoenroll permission is not available on version 1 certificate templates. Because of this, you must duplicate a certificate template and then configure the permissions to allow Read, Enroll, and Autoenroll permissions for users or computers who will receive the certificates. Domain-based Group Policy can then activate and manage autoenrollment through computer-based and user-based policies.

 **Note:** By default, computer-based Group Policy is applied at startup and user-based Group Policy is processed at user sign in. Group Policy also refreshes approximately every 90 minutes on domain members. The Group Policy setting to enable autoenrollment for computers and users is named **Certificate Services Client - Auto-Enrollment**. This setting must be enabled for both the computer and user object. If you only enable autoenrollment through computer-based policy, the autoenrollment process is not invoked for users who sign in to the computer.

An internal timer triggers autoenrollment every eight hours after the last autoenrollment activation. However, a certificate is not issued each time a timer is triggered. If the user or computer has already enrolled for certificates assigned using autoenrollment, no action is taken. If the certificate template requires user interaction to process the enrollment request, a pop-up window displays approximately 60 seconds after the user signs in.

To configure and enable autoenrollment for certificates in a domain environment, you must:

- Have membership in either the Domain Admins or Enterprise Admins group.
- Configure a certificate template with the Autoenroll permission.
- Configure an autoenrollment policy and apply it to the domain users and computers requiring autoenrollment.

### What is Credential Roaming?

*Credential Roaming* is a feature that enables users to access their credentials remotely. Credential Roaming makes it possible for a user who signs in to any domain-joined computer running Windows Server to seamlessly and silently have all of their credentials (certificates and private keys) available on the local machine for applications and services. In addition, the integrity of these credentials is maintained under any conditions, such as when certificates are updated, or when users sign in to more than one computer at a time. This avoids the scenario in which a user is enrolled automatically for a certificate on each new machine to which he or she signs in.

Credential roaming triggers in few scenarios: any time a private key or certificate in the user's local certificate store changes, whenever the user locks or unlocks the computer, and whenever Group Policy refreshes. All certificate-related communication between components on the local computer, and between the local computer and AD DS, is signed and encrypted. Windows 7 and newer operating systems support Credential Roaming.

### What is an enrollment agent?

On a Windows Server 2016 CA, you can configure certificate enrollment so that designated users can enroll on behalf of other users in your organization. The designated users are referred to as an *Enrollment Agent*, which is a user account used to request certificates on behalf of another user account. To enable enrollment on behalf of another user, the enrollment agent must possess a certificate based on the **Enrollment Agent** template. Unlike a certificate manager, an enrollment agent can only process the enrollment request and cannot approve pending requests or revoke issued certificates.

- An *Enrollment Agent* is a user account used to request certificates on behalf of another user account.
- An enrollment agent must possess a certificate based on the **Enrollment Agent** template.
- Enrollment agents are typically members of corporate or IT security departments
- The scope of an enrollment agent can be limited to:
  - Specific users or security groups
  - Specific certificate templates




**Note:** Since a user who possesses an Enrollment Agent certificate can impersonate other users, the **Enrollment Agent** template should be secured appropriately. As a best practice, we recommend that the Enrollment Agent template should only be published on a CA whenever it is necessary to designate an enrollment agent for your organization. After the enrollment agent has received the necessary certificate, you should remove the Enrollment Agent template from any CAs where it was published.


Windows Server 2016 includes three certificate templates that enable different types of enrollment agents:

- Enrollment Agent. Used to request certificates on behalf of another subject.
- Enrollment Agent (Computer). Used to request certificates on behalf of another computer subject.
- Exchange Enrollment Agent (Offline Request). Used to request certificates on behalf of another subject and supply the subject name in the request. The Network Device Enrollment Service (NDES) uses this template for its enrollment agent certificate.

Typically, one or more authorized individuals within an organization are designated as enrollment agents. Enrollment agents typically are members of corporate security, IT security, or Help desk teams, because these individuals are already trusted to safeguard valuable resources. In some organizations, such as banks that have many branches, help desk and security workers might not be conveniently located to perform this task. In this case, designating a branch manager or another trusted employee to act as an enrollment agent may be required to enable smart card credentials to be issued in multiple locations.

When you create an enrollment agent, you can restrict the agent's ability to enroll for certificates on behalf of others by limiting their scope to a specific security group and specific certificate templates. For example, you might want to implement a restriction that the enrollment agent can only perform smart card logon certificate enrollment for users belonging to a specific departmental security group. Prior to Windows Server 2008 Enterprise, it was not possible to restrict the scope of an AD CS enrollment agent. As a result, every user with an Enrollment Agent certificate was able to enroll any user in an organization for any certificate template. However, with more recent versions of AD CS, the scope of the enrollment agent can be limited to specific groups and certificate templates. For each certificate template, you can select the users or security groups which an enrollment agent can enroll on behalf of.

 **Note:** You cannot restrict an enrollment agent based on specific AD DS organizational units or containers. Enrollment on behalf of other users can only be restricted to specific users or security groups in AD DS.

 **Note:** Restricting the scope of an enrollment agent can affect the performance of the CA. To optimize performance and security, you should minimize the number of accounts designated as enrollment agents by modifying the access control list on the Enrollment Agent template.

## How does certificate revocation work?

*Revocation* is the process in which you disable the validity of one or more certificates. By initiating the revocation process, you actually publish a certificate thumbprint in the corresponding certificate revocation list (CRL). This announces that a specific certificate is no longer valid.

An overview of the certificate revocation lifecycle is outlined as follows:

1. A certificate is revoked from the CA Microsoft Management Console (MMC) snap-in. Specify a reason code and a date and time during revocation. This is optional but recommended.

The following are steps to revoke a certificate:

1. A certificate is revoked
2. A CRL is published
3. A client computer verifies certificate validity and revocation

2. The CRL publishes by using the CA console, or the scheduled revocation list is published automatically based on the configured value. CRLs can publish in AD DS, in a shared folder location, or on a website.
3. When client computers running Windows are presented with a certificate, they use a process to verify the revocation status by querying the issuing CA and CDP location. This process determines whether the certificate is revoked and then presents the information to the application that requested the verification. The client computer running Windows uses one of the CRL locations specified in the certificate to check its validity.

Windows operating systems include CryptoAPI, which is responsible for the certificate revocation and status-checking processes. CryptoAPI uses the following phases in the certificate-checking process:

- **Certificate discovery.** Certificate discovery collects CA certificates, AIA information in issued certificates, and details of the certificate enrollment process.
- **Path validation.** *Path validation* is the process of verifying the certificate through the CA chain, or *path*, until the root CA certificate is reached.
- **Revocation checking.** Each certificate in the certificate chain is verified to ensure that none of the certificates are revoked.
- **Network retrieval and caching.** Network retrieval is performed by using Online Certificate Status Protocol (OCSP). CryptoAPI is responsible for checking the local cache first for revocation information, and if there is no match, making a call by using OCSP, which is based on the URL that is provided by the issued certificate.

### What is an Online Responder service?

You also can use an *Online Responder service*, which is a more effective way to check certificate revocation status. By using the OCSP, an Online Responder service provides clients with an efficient way to determine the revocation status of a certificate. OCSP submits certificate status requests by using HTTP.

Clients access CRLs to determine the revocation status of a certificate. CRLs might be large, and clients might use a large amount of time to search through these CRLs. An Online Responder service can search these CRLs dynamically for the clients, and respond to the client about the status of the requested certificate. You can use a single Online Responder to determine revocation status information for certificates that are issued by a single CA or by multiple CAs. You also can use more than one Online Responder to distribute CA revocation information.


You should install an Online Responder and a CA on different computers. You must configure the CAs to include the URL of the Online Responder in the AIA extension of issued certificates. The OCSP client uses this URL to validate the certificate status. You also must issue the **OCSP Response Signing** certificate template, so the Online Responder also can enroll that certificate.



## Overview of key archival and recovery

Keeping the certificate and the corresponding key pair secure can be critical in some scenarios. For example, if you use a certificate to perform content encryption of emails or documents, and you lose your public and private keys, you will not be able to access any data that is encrypted by using the certificate's public key. This data can include EFS-encrypted data and Secure /Multipurpose Internet Mail Extensions-protected emails. Therefore, archival and recovery of public and private keys are important. You can archive or back up your private key by exporting a certificate with a private key and storing it in a secure location, such as an alternative media source, or some cloud-based storage. However, this approach requires that each user back up his or her private key, which usually is not a reliable backup method. Another method is to centralize private key archival on the CA.


- Private keys can get lost when:
  - A user profile is deleted
  - An operating system is reinstalled
  - A disk is corrupted
  - A computer is lost or stolen
- It is critical that you archive private keys for certificates that are used for encryption
- The KRA is needed for key recovery
- Key archival must be configured on the CA and on the certificate template
- Key recovery is a two-phase process:
  1. Key retrieval
  2. Key recovery
- The KRA certificate must be protected

 **Note:** In regular operations, the CA does not have access to a user's private key, as it is generated on the client side. Because of this, you must enable the archival of private keys explicitly on each certificate template where you want to have this functionality.

### Conditions for losing keys

You might lose key pairs because of the following conditions:

- A user profile is deleted or corrupted. A CSP encrypts a private key and stores the encrypted private key in the local file system and registry in the user profile folder. Deletion or corruption of the profile results in the loss of the private key material.
- An operating system is reinstalled. When you reinstall the operating system, the previous installations of the user profiles are lost, including the private key material. In this scenario, the computer's certificates also are lost.
- A disk is corrupted. If a hard disk becomes corrupted and the user profile is unavailable, the private key material is lost automatically, in addition to the installed computer certificates.
- A computer is lost or stolen. If a user's computer is lost or stolen, the user profile with the private key material is unavailable.

 **Note:** Losing a key pair (certificate) is not always critical. For example, if you lose a certificate used for digital signing or logging, you simply can issue a new one, and no data will be affected. However, losing a certificate that was used for data encryption will result in the inability to access data—for that reason, archival and recovery is critical.

### Key archival and recovery agents

To use private key archival, you must enable this functionality on both the CA and specific certificate templates, such as EFS. This functionality is not enabled by default on the CA or on any certificate template. To be able to archive private keys from certificates, you also must define a Key Recovery Agent (KRA).



**Note:** Key archival on the CA works from the moment that you fully configure it. It does not apply, however, to the certificates that were issued before this functionality was enabled.

You use key archival and KRAs for data recovery in scenarios where the private key is lost. The KRA is a user with the KRA certificate issued who is able to decrypt private keys stored in an AD CS database. When key archival is enabled on the CA and on certificate templates, each private key is encrypted with a KRA's public key and then stored in the CA database. As a result, a KRA's private key must be used to decrypt the private key on any user. KRAs are designated to users who are able to retrieve the original certificate, private key, and public key that were used to encrypt the data.



**Note:** Do not confuse the KRA with the Data Recovery Agent. The Data Recovery Agent is able to decrypt data directly that is encrypted with EFS when the originating user's private key is not available. Alternatively, the KRA does not decrypt any data directly: it just decrypts archived private keys. Data Recovery Agent functionality is discussed later in this module.

To become a KRA, you must enroll a certificate that is based on the KRA template. After this certificate is issued to the designated user, a public key from the KRA's certificate is imported on the CA, and key archival is enabled. From that moment, each certificate that is issued based on a template where key archival is enabled will have its private key stored in the CA database and encrypted with the KRA's public key.

During the key recovery process, the certificate manager or CA administrator retrieves the encrypted file that contains the certificate and private key from the CA database. Next, a KRA uses its private key to decrypt the private key from the encrypted file and then returns the certificate and private key to the user.



**Note:** Key recovery is a two-phase process. First, the encrypted key is retrieved from the CA database. Next, the KRA decrypts the key and certificate. For security reasons, we recommend that different people perform these two phases. By default, the KRA does not have permission to retrieve encrypted keys from a CA database.

### Security for key archival

When you have a configured CA to issue a KRA certificate, any user with Read and Enroll permission on the KRA certificate template can enroll and become a KRA. Members of the Domain Admins and Enterprise Admins groups receive permissions by default. However, you must ensure that:

- Only trusted users are allowed to enroll for this certificate.
- The KRA's private key is stored in a secure manner.
- The server where the keys are archived is in a separate, physically secure location.

After the KRA certificate is issued, we recommend that you remove this template from the CA. Also, we recommend that you import the KRA certificate only when a key recovery procedure must be performed.

## Understanding key archival and recovery

Key recovery implies that the private key portion of a public-private key pair might be archived and recovered. Private key recovery does not recover any data or messages. It merely enables a user to retrieve lost or damaged keys or for an administrator to assume the role of a user for data access or data recovery purposes. In many applications, data recovery cannot occur without first performing key recovery. The key recovery procedure is as follows:

1. A user requests a certificate from a CA and provides a copy of the private key as part of the request. The CA, which processes the request, archives the encrypted private key in the CA database and issues a certificate to the requesting user.
2. An application such as EFS can use the issued certificate to encrypt sensitive files.
3. If, at some point, the private key is lost or damaged, the user can contact the organization's certificate manager to recover the private key. The certificate manager, with the help of the KRA, recovers the private key, stores it in a protected file format, and then sends it back to the user.
4. After the user stores the recovered private key in the user's local keys store, an application such as EFS once again can use the key to decrypt previously encrypted files or to encrypt new ones.

## Configuring automatic key archival

Before you can use key archival, you must perform several configuration steps. The key archival feature is not enabled by default, and you must configure both the CA and applicable certificate templates for key archival and key recovery.

The following steps describe the automatic key archival procedure:

1. Configure the KRA certificate template. By default, only members of the Enterprise Admins or Domain Admins groups can request a KRA certificate. If you want to authorize other users to enroll for a KRA certificate, you must specify it on the access control list of the KRA template.
2. Designated key recovery agents enroll for a KRA certificate. Users who have been designated as a key recovery agent must enroll for a KRA certificate from the CA. After all necessary KRA certificates have been issued, the KRA certificate template should be removed from the CA.
3. Enable key recovery agents on the CA.
  - a. Sign in as the administrator of the server or as the CA administrator if role separation is enabled.
  - b. In the CA console, right-click the CA name, and then click **Properties**. To enable key archival, on the **Recovery Agents** tab, click **Archive the key**.
  - c. By default, the CA uses one KRA. However, you must first select the KRA certificate for the CA to begin archival by clicking **Add**.

### Steps to configure automatic key archival:

1. Configure the KRA certificate template
2. Designated key recovery agents enroll for a KRA certificate
3. Enable key recovery agents on the CA
4. Configure necessary certificate templates for key archival

- d. The system finds valid KRA certificates that have been issued, and then displays the available KRA certificates. These generally publish to AD DS by an enterprise CA during enrollment. KRA certificates are stored under the KRA container in the Public Key Services branch of the configuration partition in AD DS. Because a CA may issue multiple KRA certificates, each KRA certificate will be added to the multivalued user attribute of the CA object.
  - e. Select one certificate, and then click **OK**. Ensure that you have selected the intended certificate.
  - f. After you have added one or more KRA certificates, click **OK**. The CA service will restart, and only the KRA certificates process at service start.
4. Configure necessary certificate templates for key archival:
    - a. In the **Certificate Templates** console, right-click the certificate template that you wish to enable for key archival, and then click **Properties**.
    - b. To always enforce key archival for the CA, in the **Properties** dialog box, on the **Request Handling** tab, select the **Archive subject's encryption private key** check box. In Windows Server 2008 or later CAs, select **Use advanced symmetric algorithm to send the key to the CA**.

## Demonstration: Configuring a CA for key archival

### Demonstration Steps

1. On **LON-DC1**, open the **Certification Authority** console from **Server Manager**. Right-click the **Certificates Templates** folder, and then click **Manage**.
2. In the **Certificates Templates** console, open the **Key Recovery Agent certificate properties** dialog box.
3. On the **Issuance Requirements** tab, clear the **CA certificate manager approval** check box.
4. On the **Security** tab, notice that only the Domain Admins and Enterprise Admins groups have the Enroll permission.
5. Right-click the **Certificates Templates** folder, and then issue the **Key Recovery Agent** template.
6. Open the **Microsoft Management Console** that includes the **Certificates** snap-in for the current user.
7. Use **Certificate Enrollment Wizard** to request a new certificate and to enroll the KRA certificate.
8. Refresh the console window, and then view the KRA in the personal store.
9. On **LON-DC1**, in the **Certification Authority** console, open the **AdatumCA Properties** dialog box.
10. On the **Recovery Agents** tab, click **Archive the key**, and then add the **Administrator** certificate by using the **Key Recovery Agent Selection** dialog box.
11. Restart **AD CS** when prompted.

**Check Your Knowledge**

Question	
When you revoke a certificate, where is the thumbprint of the certificate published?	
Select the correct answer.	
<input type="checkbox"/>	CRL distribution point (CDP)
<input type="checkbox"/>	Authority information access (AIA)
<input type="checkbox"/>	Certificate revocation list (CRL)
<input type="checkbox"/>	AD DS
<input type="checkbox"/>	The Online Responder service

**Check Your Knowledge**

Question	
Which of the following actions must you take to configure key archival on an AD CS CA? (Choose all that apply.)	
Select the correct answer.	
<input type="checkbox"/>	Configure the KRA certificate template.
<input type="checkbox"/>	Enroll a designated user for a KRA certificate.
<input type="checkbox"/>	Publish the KRA public key by using Group Policy.
<input type="checkbox"/>	Configure a recovery agent on the CA.
<input type="checkbox"/>	Configure desired certificate templates for key archival.

## Lesson 3

# Using certificates in a business environment

Certificates are used very often in today's electronic communications. Each time you open an HTTPS URL, a certificate enables encryption. Also, certificates are used to sign content digitally, encrypt it, and to authenticate a user or a device. In this lesson, you will learn about some of the most common ways to use certificates in business environments.

### Lesson Objectives

After completing this lesson, you will be able to:


- Describe how to use certificates for Secure Sockets Layer (SSL).
- Describe how to use certificates for digital signatures.
- Sign a document digitally.
- Describe how to use certificates for content encryption.
- Encrypt a file with EFS.
- Describe how to use certificates for authentication.

### Using certificates for SSL

Most websites that process sensitive data are protected with *SSL* security technology. *SSL* establishes a secure, encrypted link between a server and a client. Most commonly, the connection is between a web server and a browser or email client on a client computer. *SSL* commonly is referred to as a security protocol because it specifies algorithms for encryption and the necessary variables for the connection encryption. The purpose of securing a connection with *SSL* is to protect data, such as credit card numbers, sign in credentials, and other critical data, while the data transfers between a client and a server.

- The purpose of securing a connection with *SSL* is to protect data during communication
- For *SSL*, a certificate must be installed on the server
- Be aware of trust issues
- *SSL* works in the following steps:
  1. The user types an *HTTPS* URL
  2. The web server sends its *SSL* certificate
  3. The client performs a check of the server certificate
  4. The client generates a symmetric encryption key
  5. The client encrypts this key with the server's public key
  6. The server uses its private key to decrypt the encrypted symmetric key

To establish a connection protected by *SSL*, the certificate must be installed on the server. Your internal CA or a public CA can issue a certificate for *SSL*. For websites available on the Internet, it is common to have a certificate issued by a public CA so that your server certificate is trusted widely by most browsers. However, you also can use a certificate issued by your local CA. Both types of certificates can secure a connection, but most browsers that connect to the website where the certificate is installed cannot trust an internally issued certificate. Being untrusted will not prevent a certificate from securing a connection, but it will present a warning message when the browser connects to your website. Most companies want to avoid this, so most secure websites on the Internet use public certificates. Internet browsers come with a preinstalled list of trusted CAs, and they store it in the trusted root CA store.

 **Note:** Buying a public *SSL* certificate does not guarantee that all clients will trust the certificate automatically. Make sure that you choose a certificate vendor that is trusted globally and has its CA certificates present in clients' preinstalled trusted root CA stores.

## Securing a connection with an SSL certificate

Each certificate has a key pair associated with it after it is issued. The key pair consists of a public key and a private key. These keys work together in an encryption process. Data that is encrypted with a public key can be decrypted only with a corresponding private key, and vice versa. Each key pair is unique. Besides having a key pair, each certificate also has its subject name that specifies the identity of the server or website where the certificate is installed.

When a web browser connects to a secure website, the client and server establish an SSL connection. The SSL connection establishes during the SSL *handshake*. This handshake process occurs as described below:

1. The user types or clicks an HTTPS URL in a web browser.
2. The web browser software connects to a website and requests for the server to identify itself.
3. The web server sends its SSL certificate. With the certificate, the server also distributes its public key to the client.
4. The client performs a check of the server certificate. It checks the subject name and compares it with the URL that it used to access the server. Also, it checks if the certificate is issued by any of the CAs in the trusted root CA store, and it checks the CRL distribution point (CDP) locations to verify if the certificate is revoked.
5. If all checks pass, the client generates a symmetric encryption key. The client and server use a symmetric key for decrypting data because the public and private key pairs are not very efficient in encrypting and decrypting large amounts of data. The client generates a symmetric key and then encrypts this key with the server's public key. After that, the client sends the encrypted symmetric key to the server.
6. The server uses its private key to decrypt the encrypted symmetric key. Now both server and client have a symmetric key and secure data transfer can begin.

During this process, the server proves its identity to the client by presenting its SSL certificate. If the server name in the certificate matches the URL that the client requested, and if a trusted CA issued the certificate, then the client trusts that the server has a valid identity. Also, the client has checked the validity of the certificate by checking its lifetime and CDP location for the CRLs. This means that establishing an SSL session is not just about encryption; it also provides authentication from the server to the client.



**Note:** Client authentication is not part of the classic SSL handshake. This means that a client does not have to provide its identity to the server. However, you also can configure your website to require client authentication. The client also can use a certificate to authenticate itself to the server.


## Configuring an SSL certificate on a server

To use SSL to protect communication between a server and a client, you must install the certificate on the server. You can install it in several ways. However, before you install the certificate on the server, you must define the name or names that the certificate supports. For example, if you want to protect your website on the URL [www.adatum.com](http://www.adatum.com), then you need to issue the certificate with the common name [www.adatum.com](http://www.adatum.com).



**Note:** A certificate can be issued only for a domain name, not for a full URL. For example, a certificate with the common name [www.adatum.com](http://www.adatum.com) also will protect the URL [www.adatum.com/sales](http://www.adatum.com/sales) or similar.

In some scenarios, you need to have more than one domain name on the same server. A typical example for this is Microsoft Exchange Server. A certificate installed on the server must support its public name, for example, mail.adatum.com and autodiscover.adatum.com. Because both names are associated with the same website and you cannot assign more than one certificate to a single website, you must use a certificate that supports multiple names, also known as *subject alternative names*. This means that you have one certificate with more than one name. These certificates can be issued from both an internal CA on Windows Server 2016 and from public CAs.

 **Note:** Instead of having one certificate with multiple names on the same domain, you also can issue a wild card certificate with a common name, for example, \*.adatum.com. This certificate will be valid for all names with domain suffix adatum.com. If you choose to utilize a wild card certificate, you should take extra precautions to secure the associated private key. If the private key were to be compromised, it could be used to decrypt sensitive traffic with a legitimate host or to impersonate a trusted host in the domain.

To issue an SSL certificate from an internal CA, you can use following approaches:

- Use the CA console on the server to make a certificate request to the CA. By using this approach, you can specify any additional attributes for the certificate, such as the certificate template or the subject alternative name. However, after the certificate installs, you must assign it to the appropriate website manually.
- Use the IIS console. In the IIS console, you make a certificate request directly to the CA. However, when you use this approach, you are not able to choose a certificate template—it looks for a web server template by default—and you cannot specify a subject alternative name. This is, however, the simplest way to install a certificate on the website.
- Use CA Web enrollment. This approach is appropriate if you want to issue a certificate to a server that is not a member of your domain. For this type of enrollment, you must first make a certificate request (.req) file and then submit that request on the CA Web enrollment page. There, you also can specify the certificate template and add subject alternative names, if needed.

If you are buying a publicly trusted SSL certificate, the procedure is somewhat different. After you choose a certificate vendor, you will first have to go through an administrative procedure to prove the identity of your company and domain name ownership. After that is done, you have to create a Certificate Signing request (CSR) on your server. This CSR creates the private key and a CSR data file, which basically is a certificate request. You then send the CSR to the certificate issuer. The CA uses the CSR data file to create a public key to match your private key without compromising the key itself. The CA never recognizes the private key in this or any previous scenario for certificate issuing, except when key archival is configured—but even then, the key is encrypted.



## Using certificates for digital signatures

Besides protecting communications, certificates also can protect content and verify the identity of the content author. When you receive a message with confidential content, it is important to know that you can be sure about two things. First, you can be sure that the message was not modified in transit. Second, you can be sure that the identity of the author is verifiable.

You can use certificates to protect and verify content and to verify the identity of an author. It is a common scenario for a user to sign a document digitally.

- Digital signatures ensure that:
  - Content is not modified during transport
  - The identity of the author is verifiable
- Digital signatures work in the following steps:
  1. When an author digitally signs a document or a message, the operating system on his or her computer creates a message cryptographic digest
  2. The cryptographic digest is then encrypted by using the author's private key and added to the end of the document or message
  3. The recipient uses the author's public key to decrypt the cryptographic digest and compare it to the cryptographic digest created on the recipient's computer
- Users need to have a certificate that is based on a **User** template to use digital signatures

### Digital signatures

When a person digitally signs a document in an application, such as in email, a Microsoft Word document, or similar, he or she confirms that the document is *authentic*. In this context, authentic means that it is known who created a document and that the document has not been altered in any way since the person created and signed it.

A public key infrastructure (PKI) can achieve this level of security. Compared to the web server from the previous topic, a user also can have a certificate with a public and private key pair. This certificate is used in the process of digital signing.

When an author digitally signs a document or a message, the operating system on his or her computer creates a message cryptographic digest that ranges from a 128-bit to a 256-bit number. It is generated by running the entire message through a hash algorithm. This number then is encrypted by using the author's private key, and it is added to the end of the document or message.

When the document or message reaches the recipient, it will go through same hash algorithm as when it was digitally signed. Also, the recipient uses the author's public key to decrypt the digest that is added to the message. After it is decrypted, it is compared to the digest that the recipient has generated. If they are the same, the document or the message was not altered during transport. Also, if the recipient is able to decrypt the digest by using the author's public key, then this means that the digest was encrypted by using author's private key, and that confirms the author's identity. At the end, the recipient also verifies the certificate that was used to prove the author's identity. During this check, the validity period, CRL, subject name, and certificate chain trust also are verified.

### Implementing digital signatures

To implement digital signatures in internal communications, you need to issue certificates based on the **User** template. You must issue certificates to all users who use digital signatures. You can issue the certificate without any user intervention if you use autoenrollment. Also, users must use an application that supports content signing. For example, you can use digital signatures by default in Microsoft Word and Microsoft Outlook.

Digital signatures are ready to use after the application issues and configures the certificate. However, if you want to send digitally signed content outside of your organization, you can experience CA trust issues. In this scenario, a recipient is not in the same AD DS domain as the author, so it does not trust the CA that issued the certificate for the digital signature. Although this kind of digital signature will still be valid from a content protection perspective, an application being used will probably generate a warning on the recipient side.

If you need to send digitally signed content to recipients outside of your organization, we recommend that you buy certificates from a public, globally trusted CA.

## Demonstration: Signing a document digitally

In this demonstration, you will see how to sign a document digitally.

### Demonstration Steps

1. On **LON-CL1**, open the **Windows PowerShell** command-line interface, and then run **mmc.exe**.
2. Add the **Certificates** snap-in, and then choose **My user account**.
3. Start **Request New Certificate Wizard**, and then enroll for a **User** certificate.
4. Open Word 2016. Type some text in a blank document, and then save the document.
5. Click **Insert** on the ribbon, and then insert the signature line.
6. Fill the signature fields with your data.
7. Right-click the signature line, and then choose to sign the document.
8. Choose the certificate.
9. Sign the document.
10. Make sure that the document cannot be edited anymore.

## Using certificates for content encryption

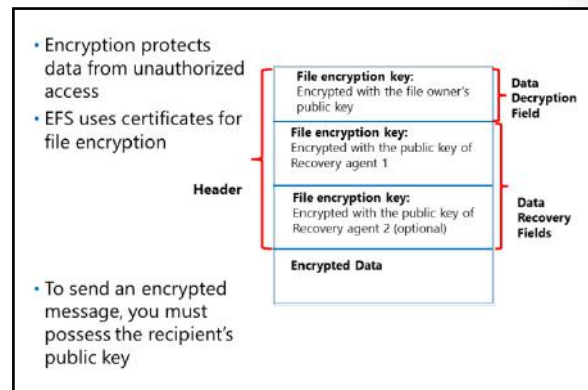
While digital signatures can verify an author's identity and ensure content consistency, they cannot protect the content itself. For example, if someone intercepts a digitally signed message, they can still read its content; although, the attempt to alter the content is detected because the digital signature check will fail.

If you want to protect the content of the document so that it cannot be read, you must use encryption.

Microsoft Windows operating systems support file-based encryption called Encrypting File System (EFS). Also, Outlook supports the encryption of email messages.

### EFS

To encrypt a file by using EFS, you must have an EFS certificate issued. Like other certificates, this certificate also provides a private and public key pair. However, these keys are not used directly to encrypt or decrypt content. The reason for this is the inefficiency of the algorithms that use *asymmetric encryption*, where one key is used for encryption and another for decryption. These algorithms are much slower than algorithms that use the same key for both encryption and decryption, called *symmetric encryption*. EFS uses a hybrid approach to overcome this problem.




When a user selects the option to encrypt a file, the local computer generates a symmetric key, which is also known as a file encryption key, and uses that key to encrypt the file. After the file is encrypted, the system uses the user's public key to encrypt the symmetric key and then store it in the file header.

When the user who originally encrypted the file wants to decrypt the file and access its content, the local computer accesses the user's private key and first decrypts the symmetric key from the file header, which also is called the Data Decryption Field (DDF). After that, the symmetric key is used to decrypt the content.


This works fine if the file's owner is the only person who accesses the encrypted file. However, there are scenarios in which you would want to share encrypted files with other users, and it might be inconvenient or unacceptable to decrypt the file before sharing it with other people. Also, if the user who originally encrypted the file loses his or her private key, then the file might be inaccessible to anyone.

To resolve this, a Data Recovery Field (DRF) is defined for each file encrypted with EFS. When you configure EFS to be used locally or in an AD DS domain, the Data Recovery Agent (DRA) role is defined by default and assigned to the local or domain administrator. The DRA is actually a certificate with a key pair that can be used to decrypt files in case the private key of the originating user is not accessible for some reason.

When a user encrypts the file with EFS, his or her public key is used to encrypt the symmetric key, and that encrypted key is then stored to the DDF in the file header. At the same time, the public key of the DRA is used to encrypt the symmetric key once more. The symmetric key is encrypted with a public key of the DRA and is then stored to the DDF in the file header. If there is more than one DRA defined, then the symmetric key is encrypted with each DRA public key. Then, if the user who originally encrypted the file does not have a private key available for any reason, the DRA can use its private key to decrypt the symmetric key from the DRF and then decrypt the file.

 **Note:** As an alternative to the DRA, you also can use the Key Recovery Agent (KRA) to retrieve a user's private key from a CA database, if key archival is enabled for the EFS certificate template on the CA.

When a user wants to share an encrypted file with other users, a similar approach is taken as when DRA is used. When EFS sharing is selected, the file's owner must select a certificate from each user who shares the file. These certificates can be published to AD DS and taken from there. When the certificate is selected, the public key of the destination user is taken, and the symmetric key is encrypted and added to the file header. At this point, the other user also can access the EFS encrypted content, because they can use their private keys to decrypt the symmetric key.

 **Note:** A data recovery certificate also can be defined for BitLocker Drive Encryption. Although a BitLocker Data Recovery Agent certificate template is not predefined in AD CS, you can copy the KRA template and then add new application policies for BitLocker encryption and data recovery using the following object identifiers:

- BitLocker Drive Encryption = 1.3.6.1.4.1.311.67.1.1
- BitLocker Data Recovery Agent = 1.3.6.1.4.1.311.67.1.2

After you enroll a user for this certificate, you can define a recovery agent at the domain level if you use Group Policy settings in the following path: **Computer Configuration\Windows Settings\Security\Public Key Policies\BitLocker Drive Encryption**. We recommend that you use BitLocker for full drive encryption.

## Email encryption

Besides using EFS to encrypt files, and BitLocker to encrypt drives, you can also use certificates to encrypt emails. Email encryption, however, is a bit more complicated than a digital signature. Although you can send digitally signed emails to anyone, you cannot do the same with an encrypted email. To be able to send an encrypted email to someone with a PKI, you must possess the recipient's public key from his or her key pair. In the AD DS environment, where Exchange Server is used as an email system, you can publish the public keys of all mailbox users to a global address list (GAL). When you do that, applications such as Outlook can grab a recipient's public key easily from the GAL, if you are sending encrypted email. When you send an encrypted email to an internal user, your email application takes the recipient public key from GAL, encrypts the email with it, and then sends the email. After the email is received, the recipient uses his or her private key from the certificate to decrypt the content of the email.

However, sending an encrypted email to external users is more complicated. While the public keys of internal users can publish to AD DS or the GAL, you cannot do the same with external users. To send encrypted email to an external user, you first must get his or her public key. You can get the key if the external user sends it to you in a .cer file, which you can import in your local address book. Also, if an external user sends you one digitally signed email, then you will get his or her public key, which you also can import to your local address book. After the public key imports to your address book, you can use it to send encrypted emails to external users.



**Note:** If you want to provide authenticity, content consistency, and protection, then you can send a message that is both digitally signed and encrypted.

## Demonstration: Encrypting a file with EFS

In this demonstration, you will see how to encrypt a file with EFS.

### Demonstration Steps

1. Open the advanced properties of the Word document that you created in the previous demonstration.
2. Choose **Encrypt the file only**.
3. Move the file to the **C:\Users\Public\Public Documents** folder.
4. Sign out of **LON-CL1**.
5. Sign in as **Adatum\Aidan**.
6. Try to access the encrypted document in the **C:\Users\Public\Public Documents** folder.

## Using certificates for authentication

Besides using certificates for digital signing and encryption, they often are used for user and device authentication. Also, certificates commonly are used for network access authentication because they provide strong security for authenticating users and computers, and they eliminate the need for less secure password-based authentication methods.

For example, you can use certificates on computers that are allowed to access your network by using virtual private network (VPN) connections. This enables you to authenticate devices and users. A user can authenticate with a user name and password, while a device authenticates with a certificate. Devices that do not have your organization's certificate will not be allowed to connect, even if a user is authorized. This approach improves security.

You can use certificates for user and device authentication and also in network and application access scenarios such as:

- L2TP/IPsec VPN
- EAP-TLS
- PEAP
- NAP with IPsec
- Outlook Web App
- Mobile device authentication

Two authentication methods for network access use certificates: Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) and Protected Extensible Authentication Protocol (PEAP). Both methods always use certificates for server authentication. Depending on the authentication type configured with the authentication method, certificates might be used for user and client device authentication. You must use certificate-based authentication for VPN connections based on Layer Two Tunneling Protocol (L2TP) over Internet Protocol security (IPsec).

Certificates are also used to authenticate clients when Network Access Protection (NAP) is implemented with IPsec. In this scenario, Health Registration Authority issues a certificate to a computer that satisfies the health policy for establishing an IPsec connection.

IIS in Windows Server 2016 also supports certificate authentication for users. For example, you can configure Microsoft Outlook Web App to use certificate-based authentication.

Finally, you also can use certificates for mobile device authentication. Some types of mobile devices can install certificates and use them to authenticate a user or device to the network resource.

### Check Your Knowledge

Question	
Which of the following are true statements regarding the use of certificates in a business environment? (Choose all that apply.)	
Select the correct answer.	
<input type="checkbox"/>	Certificates can be used to encrypt HTTP traffic between a web server and browser.
<input type="checkbox"/>	Certificates can be used to digitally sign documents.
<input type="checkbox"/>	Digitally signed documents are invalidated if the contents are modified.
<input type="checkbox"/>	To send encrypted e-mail to an external recipient who is not part of your internal PKI, you must use an encryption certificate issued by a public CA.
<input type="checkbox"/>	Files encrypted using Encrypting File System (EFS) can only be read by the individual who first encrypted the file.

**Check Your Knowledge**

Question	
<p>You are the AD CS administrator for A. Datum. You want to enable your AD DS users to perform digital signature and encryption using certificates from your internal PKI. Which of the following steps are required?</p>	
Select the correct answer.	
<input type="checkbox"/>	Enable a key recovery agent.
<input type="checkbox"/>	Enable a data recovery agent.
<input type="checkbox"/>	Publish the User certificate template and configure the desired groups of users for autoenrollment.
<input type="checkbox"/>	Enable EFS on AD DS domain computers by using Group Policy.
<input type="checkbox"/>	Upgrade all AD DS domain computers to Windows Server 2016 or Windows 10.

## Lesson 4

# Implementing and managing smart cards

Smart card authentication is a common approach in scenarios where you want to have multifactor authentication to enhance security. Also, they are used to store certificates for digital signatures and encryption. To implement a smart card infrastructure, you must understand how they work and how to configure certificates for smart cards. This lesson describes the implementation and management of a smart card infrastructure.

### Lesson Objectives

After completing this lesson, you will be able to:

- Describe a smart card.
- Describe how smart card authentication works.
- Describe a virtual smart card.
- Describe how to enroll certificates for smart cards.
- Describe smart card management.

### What is a smart card?

The term *smart card* is used to describe a class of credit card–size or smaller devices with varying capabilities: stored-value cards, contactless cards, and integrated circuit (IC) cards. All of these cards differ in functionality and from the more familiar magnetic-stripe cards used as standard credit, debit, and automated teller machine (ATM) cards. The IC card is of most interest to the personal computer and to Windows operating systems because it can perform sophisticated operations such as digital signatures and key exchanges.

A smart card is essentially a miniature computer with limited storage and processing capabilities that is embedded in a plastic card, similar in size and form to a credit card. The circuitry in a smart card derives power from a smart card reader after the card is inserted into a reader. Data communication between a smart card and an application that is running on a computer is performed over a half-duplex serial interface that is managed by the smart card reader and its associated device driver. Smart card readers are available in a variety of form factors and can connect to a computer by using a Personal Computer Memory Card International Association (PCMCIA) or universal serial bus (USB) interface. Smart card readers often are built into laptop computers.

Smart cards provide enhanced security over passwords, as it is much more difficult for an unauthorized user to gain and maintain access to a system. Also, access to a smart card–protected system requires that a user have a valid card and know the Personal Identification Number (PIN) that provides access to that card. By default, only one copy of a smart card exists, so only one individual can use his or her sign in credentials at a time. In addition, users will notice quickly if their card is lost or stolen, especially when their card is also used for physical access to doors or other functions. This greatly reduces the risk of credential theft compared to passwords.

- A smart card is a miniature computer, with limited storage and processing capabilities, embedded in plastic card about the size of a credit card
- Smart cards:
  - Provide options for multifactor authentication
  - Provide enhanced security over passwords
- A valid smart card and PIN must be used together

## How does smart card authentication work?

The primary purpose of smart cards in Windows-based environments is to perform authentication. You can use smart cards to authenticate to an AD DS domain. Smart cards cannot be used for local sign in to computers that are not domain joined.

When signing in to AD DS, smart cards can be used in the following three ways:

- Interactive sign in to AD DS by using Kerberos protocol and a certificate.
- Client authentication by using a certificate that matches an account that is stored in AD DS.
- Remote sign in that uses a certificate with EAP-TLS to authenticate a remote user to an account stored in AD DS.

- Smart cards can be used for:
  - Interactive sign in to AD DS
  - Client authentication
  - Remote sign in
  - Offline sign in
- Interactive sign in steps:
  1. The sign-in request goes to the LSA, which is forwarded to the Kerberos package
  2. KDC verifies the certificate
  3. KDC verifies the digital signature on the authentication service
  4. KDC performs an AD DS query to locate the user account
  5. KDC generates a random encryption key to encrypt the TGT
  6. KDC signs the reply with its private key and sends it to the user

### Interactive sign in with smart cards

Interactive sign in is the most common scenario for smart card use. It begins when a user places the smart card into a smart card reader. This generates a similar process as when a user presses Ctrl+Alt+Delete. Windows operating systems will prompt the user for a smart card PIN. The smart card PIN is a way to authenticate a user to the smart card and not to a domain. After the PIN is entered and accepted, a public key from a certificate stored on the smart card is used to authenticate to the domain by using the Kerberos protocol and its associated Public Key Cryptography for Initial Authentication (PKINIT) in Kerberos extension.

After a user inputs a PIN, the operating system begins a sequence of actions to determine whether the user can be identified and authenticated based on the credential information that the user provided in the two-factor authentication process (PIN and smart card). This process is described in following steps:

1. The sign-in request first goes to the local security authority (LSA) that forwards it to the Kerberos authentication package running on the client. The Kerberos package sends an authentication service (AS) request to the Key Distribution Center (KDC), a service running on a domain controller to request authentication and a ticket-granting ticket (TGT). As part of the authentication service request, the client-side Kerberos package includes the user's certificate, retrieved from the smart card, in the preauthentication data fields of the AS request. An authenticator, which is included in the preauthentication data fields, is signed digitally by the user's private key so that the KDC can verify the AS request that is originated from the owner of the accompanying certificate.
2. Before KDC fulfills the authentication service request, it verifies the certificate from the perspective of its validity. It checks if a trusted root CA issued the certificate on the smart card, and it checks the whole certificate chain. It also checks CRL and AIA locations and verifies that the issuing CA is authorized to issue certificates whose name information can be used for authentication within the domain.
3. When a certificate is checked, the KDC proceeds to verify the digital signature on the authentication service request. This is done by using the public key of the user's certificate. Because the smart card stores both a user's private and public key, and the user must enter a PIN to access a private key and use it to sign requests, if the public key matches the private key in the signature, the request is legitimate. After this, the time stamp is checked on the authentication service request to verify that the request is not part of a replay attack.



4. When all these checks pass successfully, KDC performs an AD DS query to locate user account information. The user account is located based on a user principal name provided in the subject name of the certificate that is located on the smart card. The account information that the KDC retrieves from AD DS is then used to construct a TGT. The TGT includes the user's security identifier (SID), the SIDs for any domain groups to which the user belongs, and potentially the SIDs for any universal groups in which the user is a member, in a single or a multidomain environment.
5. After the TGT is built, KDC generates a random encryption key to encrypt the TGT. When it encrypts the TGT, KDC uses the user's public key to encrypt this random encryption key. This encrypted key is included in the preauthentication data field of the KDC's response to the user.
6. Then KDC signs the reply with its private key and sends it to the user. The user will perform the necessary checks on the KDC reply and then use its private key to first decrypt the random key from the preauthentication data field. After the client gets the key, it uses it to decrypt the TGT. Once in possession of the TGT, the standard Kerberos protocol is used to request tickets from the ticket-granting service for other domain resources.

### Offline sign in with smart cards

If a user uses a laptop computer and a smart card for authentication, it is common that he or she will need to sign in to the computer even when it is not connected to a network. This is similar to when a user uses an offline sign in with a user name and password from an AD DS domain. When a user signs in to an offline computer with a user name and password from an AD DS domain, the operating system retrieves the hash of the domain password that is stored in the LSA and compares it with the password hash that was provided during sign in.

However, if the user signs in with a smart card, a different procedure takes place. The operating system then uses the user's private key from the smart card to decrypt supplemental credentials that were encrypted originally by using the user's public key.

### What is a virtual smart card?

Although smart cards have many benefits, the implementation of a smart card infrastructure sometimes is expensive. To implement smart cards, companies must buy hardware, including the smart cards and smart card readers. In some cases, this cost prevents the deployment of multifactor authentication.

To address these issues, Windows Server 2012 AD CS introduced a technology that provides the security of smart cards while reducing material and support costs. *Virtual smart cards* (VSC) are a combination of hardware, software, and firmware that implement the same interface as a physical smart card but are not necessarily restricted to the same physical form factor. VSCs may be implemented entirely in software, but they more commonly use the cryptographic capabilities of the trusted platform module (TPM) chip that is present on most computer motherboards produced in the last several years.

Because the chip is already in the computer, there is no cost to buy smart cards and smart card readers. Unlike traditional smart cards, where a user physically possesses the card, the TPM chip on the motherboard acts like a smart card that is always inserted. When you use this approach, you can achieve a similar outcome as a physical smart card–authentication method. Users must have their computer, which

- A smart card infrastructure might be expensive
- Windows Server 2012 AD CS introduced virtual smart cards
- Virtual smart cards use the capabilities of the TPM chip
- No cost for buying smart cards and smart card readers
- The computer acts like a smart card
- Private keys are protected by the cryptographic capabilities of the TPM

was set up with the VSC, and know a PIN that is necessary to access the certificates stored on the computer's TPM chip.

It is important to understand how VSCs protect private keys. Traditional smart cards have their own storage and cryptographic mechanisms for protecting private keys. In the VSC scenario, private keys are protected not by isolation of physical memory but rather by the cryptographic capabilities of the TPM. All sensitive information that is stored on a smart card is encrypted by using the TPM, and then the encrypted information is stored on the hard drive. Although private keys are stored on a hard drive in encrypted form, all cryptographic operations occur in the secure, isolated environment of the TPM. Private keys never leave this environment in an unencrypted form. If the hard drive of the computer is compromised in any way, private keys cannot be accessed because they are protected and encrypted by the TPM. To provide more security, you also can encrypt the drive with BitLocker. To deploy VSCs, you need a Windows Server 2012 or later version of AD CS and a Windows 8 or later client computer with an embedded TPM chip.

## Enrolling certificates for smart cards

You must define a method for enrolling smart card certificates as part of a plan to implement a smart card infrastructure. Unlike other certificates, which you can assign to users without any action on their part, smart card certificate enrollment requires some manual intervention from an administrator and an end user.

First, you must define a certificate template to use for smart cards. Windows Server 2016 AD CS comes with two predefined templates for smart card usage: **Smart Card Logon** and **Smart Card User**. The **Smart Card Logon** template is only for

authentication purposes, while the **Smart Card User** template provides a certificate that is also for digital signing and encryption. These are version 1 templates, which means that you cannot modify any of their options except DACL. Because of your limited options, we recommend that you copy one of these templates and make version 2 or higher templates so that you can modify additional options, such as the validity period, which CSP is used on smart cards, and other details.

After you configure a certificate template for smart card certificates, you have to enroll one or more users for the Enrollment Agent certificate. This is required because users usually are not allowed to self-enroll for smart card certificates. Mostly, administrators issue smart cards for users and set default PINs. After that, users can change their PIN so that only they know it.



**Note:** We recommend that you use restricted functionality for defining Enrollment Agents for smart cards.

After you define an Enrollment Agent and issue a certificate, you can issue a smart card. To issue a certificate for another user, follow this procedure:

1. Sign in to the enrollment station where you have a smart card reader installed. You must sign in with the user account that has the Enrollment Agent certificate issued.
2. Open the **Certificates** console, and then open the **My user account** store.

- Before you issue smart cards, define the method of enrolling smart card certificates
- Smart card certificate enrollment requires some manual intervention
- For smart card enrollment:
  - Define the certificate template for the smart cards
  - Enroll one or more users for the Enrollment Agent certificate
  - Configure the enrollment station
  - Start the **Enroll On Behalf Of** wizard
- Ensure that users change their personal PINs

3. Right-click **Personal store**, go to **All Tasks**, click **Advanced Operations**, and then click **Enroll On Behalf Of...**
4. You will be prompted to select your Enrollment Agent certificate.
5. Select the appropriate certificate template for the smart card.
6. Select the user for which you are issuing a smart card. Put an empty smart card into the reader device.
7. Type the PIN that you want to set on the smart card.
8. Wait until a certificate generates, and then save it to the smart card.
9. Give or send the smart card to the end user.



**Note:** We highly recommended that you suggest to users that they change their smart card PIN immediately after their first sign in.

If you want to manage smart card enrollment with more advanced options, you have to use a dedicated product such as Microsoft Identity Manager (MIM).

## Smart card management

You also should have a plan for smart card management if you implement a smart card infrastructure as the primary method for authentication and storage of a user's certificate. Managing smart cards includes the following tasks and procedures:

- Issuance
- Revocation
- Renewal
- Blocking and unblocking
- Duplication
- Suspension

### • Smart card management tasks:

- Issuance
- Revocation
- Renewal
- Blocking and unblocking
- Duplication
- Suspension

### • Use MIM to:

- Issue smart cards to users
- Store information in a SQL database
- Manage revocation, renewal, unblocking, suspension, and reinstatement procedures
- Provide users and administrators with a web-based, self-service smart card management interface
- Manage smart card printing with appropriate hardware
- Implement workflows for each management task

You can perform some of these procedures and tasks with built-in Windows utilities, but utilities such as Cardutil or the **Certificates** console do not provide a large set of options.

Because of this, we recommend that you implement a dedicated solution for smart card and certificate management. MIM provides a powerful platform for centralized smart card management.

With MIM, you can move all of your smart card management tasks to one place, and you can implement workflows on each smart card management task.

MIM provides the following smart card and certificate management capabilities:

- Issue smart cards to users.
- Store information about all issued smart cards and other certificates in a SQL database.
- Manage smart card revocation, renewal, unblocking, suspension, and reinstatement procedures.
- Provide users and administrators with a web-based, self-service smart card management interface.

- Manage smart card printing with appropriate hardware.
- Implement workflows with one or more approvals for each management task.



**Note:** It is important to understand that MIM is a certificate management solution that does not provide any PKI capabilities. It extends the management functionality of an existing internal PKI, and it manages certificates on smart cards but also certificates of other kinds. To implement MIM certificate management, you must have built an internal CA hierarchy.

### Check Your Knowledge

Question	
Which of the following statements are true regarding smart cards?	
Select the correct answer.	
<input type="checkbox"/>	Smart cards provide an option for multifactor authentication.
<input type="checkbox"/>	Smart cards cannot be used for interactive sign in.
<input type="checkbox"/>	Smart cards contain a certificate and private key that can only be accessed by using a PIN.
<input type="checkbox"/>	Smart cards provide enhanced security beyond a password.
<input type="checkbox"/>	Smart cards can only be used for digital signature and encryption.

### Check Your Knowledge

Question	
When implementing a smart card infrastructure, which of the following processes should be part of your certificate management framework?	
Select the correct answer.	
<input type="checkbox"/>	Issuance
<input type="checkbox"/>	Revocation
<input type="checkbox"/>	Renewal
<input type="checkbox"/>	Blocking and unblocking
<input type="checkbox"/>	Suspension

## Lab: Deploying and using certificates

### Scenario

You are working as an administrator at A. Datum Corporation. As A. Datum expands, its security requirements are also increasing. The Security department particularly is interested in enabling secure access to critical websites and in providing additional security for features such as EFS, digital signatures, smart cards, and the DirectAccess feature in Windows 8.1 and Windows 10. The Security department especially wants to evaluate digital signatures in Microsoft Office documents. To address these and other security requirements, A. Datum has decided to use certificates that are issued by the AD CS role in Windows Server 2016.

As a senior network administrator at A. Datum, you are responsible for implementing certificate enrollment. You also will be developing the procedures and process for managing certificate templates and for deploying and revoking certificates.

### Objectives

After you complete this lab, you will be able to:

- Configure certificate templates.
- Configure certificate enrollment and usage.
- Configure and implement key recovery.

### Lab Setup

Estimated Time: **50 minutes**

Virtual machines: **20742A-LON-DC1**, **20742A-LON-SVR1**, **20742A-LON-SVR2**, and **20742A-LON-CL1**

User name: **Adatum\Administrator**

Password: **Pa\$\$w0rd**

For this lab, you will use the available virtual machine environment. Before you begin the lab, you must complete the following steps:

1. On the host computer, start **Hyper-V Manager**.
2. In Hyper-V Manager, click **20742A-LON-DC1**, and in the **Actions** pane, click **Start**.
3. In the **Actions** pane, click **Connect**. Wait until the virtual machine starts.
4. Sign in by using the following credentials:
  - User name: **Adatum\Administrator**
  - Password: **Pa\$\$w0rd**
5. Repeat steps 2 through 4 for **20742A-LON-SVR1**, **20742A-LON-SVR2**, and **20742A-LON-CL1**.

## Exercise 1: Configuring certificate templates

### Scenario

After deploying the CA infrastructure, the next step is to deploy the certificate templates that are required in the organization. First, A. Datum wants to implement a new web server certificate and to implement certificates for users.

The main tasks for this exercise are as follows:

1. Create a new template based on the Web Server template.
2. Create a new template for users that includes smart card sign in.
3. Configure the templates so that they can be issued.
4. Enroll the Web Server certificate on **LON-SVR2**.

#### ► Task 1: Create a new template based on the Web Server template

1. On **LON-DC1**, in **Server Manager**, click **Tools**, and then click **Certification Authority**.
2. In the **Certification Authority** console, open the **Certificate Templates** console.
3. Duplicate the **Web Server** template.
4. Create a new template, and then name it **Production Web Server**.
5. Configure validity for **3 years**.
6. Configure the private key as exportable.
7. Publish the CRL on **LON-DC1**.

#### ► Task 2: Create a new template for users that includes smart card sign in

1. On **LON-DC1**, open the **Certification Authority** console from **Server Manager**.
2. Open the **Certificate Templates** console, then duplicate the **User** certificate template.
3. Name the new template **Adatum User**.
4. On the **Subject Name** tab, clear both the **Include e-mail name in subject name** and the **E-mail name** check boxes.
5. Add **Smart Card Logon** to the application policies of the new certificate template.
6. Configure this new template to supersede the **User** template.
7. Allow **Authenticated Users** to **Read**, **Enroll**, and **Autoenroll** for this certificate.
8. Close the **Certificate Templates** console.

#### ► Task 3: Configure the templates so that they can be issued

- Issue the certificates based on the **Adatum User** and **Production Web Server** templates.

#### ► Task 4: Enroll the Web Server certificate on LON-SVR2

1. Switch to **LON-SVR2**.
2. Open Windows PowerShell, and then refresh Group Policy.
3. Open **Server Manager**, and then open **Internet Information Services (IIS) Manager**.

4. Enroll for a domain certificate by using the following settings:
  - o Common name: **lon-svr2adatum.com**
  - o Organization: **Adatum**
  - o Organizational unit: **IT**
  - o City/locality: **Seattle**
  - o State/province: **WA**
  - o Country/region: **US**
  - o Friendly name: **lon-svr2**
5. Create an HTTPS binding for the Default Web Site, and then associate it with the **lon-svr2** certificate.
6. Open Internet Explorer on **LON-CL1**, and then open **https://lon-svr2.adatum.com**. Ensure that the **Internet Information Services** page opens and that no certificate error displays.

**Results:** After completing this exercise, students will have configured certificate templates.

## Exercise 2: Enrolling and using certificates

### Scenario

The next step in implementing a PKI at A. Datum is configuring certificate enrollment. A. Datum wants to enable different options for distributing certificates. Users should be able to enroll automatically, and smart card users should get their smart cards from Enrollment Agents. Adatum has delegated Enrollment Agent rights for the Marketing department group to user Annie Conner.

The main tasks for this exercise are as follows:

1. Configure autoenrollment for users.
2. Verify autoenrollment.
3. Configure the enrollment agent for smart card certificates.
4. Use certificates for digital signing of a Microsoft Office document.

#### ► Task 1: Configure autoenrollment for users

1. On **LON-DC1**, open **Group Policy Management**.
2. Edit the **Default Domain Policy**.
3. Go to **User Configuration\Policies\Windows Settings\Security Settings**, and then click to highlight **Public Key Policies**.
4. Enable the **Certificate Services Client – Auto-Enrollment** option, and then enable **Renew expired certificates, update pending certificates, and remove revoked certificates** and **Update certificates that use certificate templates**.
5. Enable **Certificate Services Client – Certificate Enrollment Policy**.
6. Close the **Group Policy Management Editor** window and **Group Policy Management** console.

**► Task 2: Verify autoenrollment**

1. On **LON-CL1**, open **Windows PowerShell**, and then use **gpupdate /force** to refresh Group Policy.
2. Open **Microsoft Management Console**, and then add the **Certificates** snap-in focused on the user account.
3. Verify that you have been issued a certificate based on the **Adatum User** template.
4. Sign out of **LON-CL1**.

**► Task 3: Configure the enrollment agent for smart card certificates**

1. On **LON-DC1**, from the **Certification Authority** console, open the **Certificate Templates** console.
2. Allow **Annie Conner** to enroll for an **Enrollment Agent** certificate.
3. Publish the **Enrollment Agent** certificate template.
4. Sign in to **LON-CL1** as **Adatum\Annie** with the password **Pa\$\$w0rd**, and then enroll for an **Enrollment Agent** certificate.
5. Sign out of **LON-CL1**.
6. On **LON-DC1**, open the properties of **AdatumCA**, and then configure **Restricted Enrollment Agent** so that Annie can only issue certificates based on **Adatum User** for the security group **Marketing**.

**► Task 4: Use certificates for digital signing of a Microsoft Office document**

1. Sign in to **LON-CL1** as **Adatum\Administrator** with the password **Pa\$\$w0rd**.
2. Open Word 2016. Type some text in a new blank document, and then save the document.
3. Click **INSERT** in the ribbon, and then insert a signature line.
4. Fill the signature fields with your data.
5. Right-click the signature line, and then choose to sign the document.
6. Choose the certificate that you enrolled through autoenrollment.
7. Sign the document.
8. Make sure that the document cannot be edited anymore.
9. Sign out of **LON-CL1**.

**Results:** After completing this exercise, students will have implemented certificate enrollment.



## Exercise 3: Configuring and implementing key recovery

### Scenario

As a part of establishing a PKI, you want to configure and test procedures for private key recovery. You want to assign a KRA certificate for an administrator and to configure a CA and specific certificate templates to allow key archival. In addition, you want to test a procedure for key recovery.

The main tasks for this exercise are as follows:

1. Configure the certification authority (CA) to issue KRA certificates.
2. Acquire the KRA certificate.
3. Configure the CA to allow key recovery.
4. Configure a custom template for key archival.
5. Verify key archival functionality.
6. Prepare for the next module.

#### ► Task 1: Configure the certification authority (CA) to issue KRA certificates

1. On **LON-DC1**, in the **Certification Authority** console, right-click the **Certificates Templates** folder, and then click **Manage**.
2. In the **Certificates Templates** console, open the **Key Recovery Agent certificate properties** dialog box.
3. On the **Issuance Requirements** tab, clear the **CA certificate manager approval** check box.
4. On the **Security** tab, notice that only the Domain Admins and Enterprise Admins groups have the Enroll permission.
5. Right-click the **Certificates Templates** folder, and then issue the **Key Recovery Agent** template.

#### ► Task 2: Acquire the KRA certificate

1. Create the Microsoft Management Console that includes the **Certificates** snap-in for the current user.
2. Use **Certificate Enrollment Wizard** to request a new certificate and to enroll the KRA certificate.
3. Refresh the console window, and then view the KRA in the personal store.

#### ► Task 3: Configure the CA to allow key recovery

1. On **LON-DC1**, open the **Certification Authority** console from **Server Manager**. Then open the **AdatumCA Properties** dialog box.
2. On the **Recovery Agents** tab, click **Archive the key**, and then add the certificate by using the **Key Recovery Agent Selection** dialog box.
3. Restart **Certificate Services** when prompted.

#### ► Task 4: Configure a custom template for key archival

1. On **LON-DC1**, open the **Certificates Templates** console.
2. Duplicate the **User** template, and name it **Archive User**.
3. On the **Request Handling** tab, select the option for the **Archive subject's encryption private key**. By using the archive key option, the KRA can obtain the private key from the certificate store.

4. Click the **Subject Name** tab, and then clear the **E-mail name** and **Include E-mail name in subject name** check boxes.
5. Issue the **Archive User** template.

► **Task 5: Verify key archival functionality**

1. Sign in to **LON-CL1** as **Adatum\Aidan** with the password **Pa\$\$w0rd**.
2. Create the Microsoft Management Console that includes the **Certificates** snap-in.
3. Request and enroll a new certificate based on the **Archive User** template.
4. From the personal store, locate the **Archive User** certificate.
5. Delete the certificate for Aidan to simulate a lost key.
6. Switch to **LON-DC1**.
7. Open the **Certification Authority** console, expand **AdatumCA**, and then click the **Issued Certificates** store.
8. In the **Certification Authority** console, note the serial number of the certificate that has been issued for Aidan Delaney.
9. On **LON-DC1**, at a command prompt, type the following command, and then press Enter:

```
Certutil -getkey <serial number> outputblob
```



**Note:** Replace the serial number in the command above with the serial number that you wrote down. If you copy and paste the serial number, remove the spaces between the numbers.

10. Verify that the **Outputblob** file now displays in the **C:\Users\Administrator** folder.
11. To convert the **Outputblob** file into an importable **.pfx** file, at the command prompt, type the following command, and then press Enter:

```
Certutil-recoverkey outputblob aidan.pfx
```

12. Enter and confirm the password **Pa\$\$w0rd** for the certificate.
13. Verify the creation of the recovered key in the **C:\Users\Administrator** folder.
14. Switch to **LON-CL1**.
15. Open **File Explorer**, and then connect to **\\LON-DC1.adatum.com\c\$**. When prompted for credentials, use **Adatum\Administrator** with the password **Pa\$\$w0rd**. Copy and paste the **aidan.pfx** file from **\\LON-DC1.adatum.com\c\$\users\administrator** to **C:\Users\aidan** on **LON-CL1**.
16. On **LON-CL1**, import the **aidan.pfx** certificate.
17. Verify that the certificate displays in the personal store.

**Results:** After completing this exercise, students will have configured key recovery.

► **Task 6: Prepare for the next module**

When you finish the lab, revert the virtual machines to their initial state. To do this, complete the following steps:

1. On the host computer, start **Hyper-V Manager**.
2. In the **Virtual Machines** list, right-click **20742A-LON-DC1**, and then click **Revert**.
3. In the **Revert Virtual Machine** dialog box, click **Revert**.
4. Repeat steps 2 and 3 for **20742A-LON-CL1**, **20742A-LON-SVR1**, and **20742A-LON-SVR2**.

**Question:** What must you do to recover private keys?

**Question:** What is the benefit of using a restricted Enrollment Agent?

## Module Review and Takeaways

### Review Questions

**Question:** List the requirements to use autoenrollment for certificates.

**Question:** How do virtual smart cards work?

### Real-world Issues and Scenarios

Contoso, Ltd. wants to deploy a PKI to support and secure several services. It has decided to use Windows Server 2016 AD CS as a platform for PKI. Certificates will be used primarily for EFS, digital signing, and for web servers. Because documents that will be encrypted are important, it is crucial to have a disaster recovery strategy in case of key loss. In addition, clients that will access secure parts of the company website must not receive any warning in their browsers.

- What kind of deployment should Contoso choose?
- What kind of certificates should Contoso use for EFS and digital signing?
- What kind of certificates should Contoso use for a website?
- How will Contoso ensure that EFS-encrypted data is not lost if a user loses a certificate?

### Tools

- The **Certification Authority** console
- The **Certificate Templates** console
- The **Certificates** console
- **Certutil.exe**

### Best Practices

- When replacing old certificate templates, use superseding templates.
- Always archive certificates that are used for encryption purposes.
- Use autoenrollment for mass deployment of certificates.
- If you are using smart cards, make sure that users change their PINs regularly.
- If you are using smart cards, implement a smart card management solution.

### Common Issues and Troubleshooting Tips

Common Issue	Troubleshooting Tip
The certificate template is not visible during enrollment.	
Autoenrollment does not work.	
The user who encrypted a file cannot decrypt it.	

# Module 10

## Implementing and administering AD FS

### Contents:

Module Overview	10-1
Lesson 1: Overview of AD FS	10-2
Lesson 2: AD FS requirements and planning	10-11
Lesson 3: Deploying and configuring AD FS	10-23
Lesson 4: Web Application Proxy overview	10-38
Lab: Implementing AD FS	10-49
Module Review and Takeaways	10-60

## Module Overview

Active Directory Federation Services (AD FS) in the Windows Server 2016 operating system allows organizations to provide their users with the flexibility to sign in and authenticate to applications that exist on a local network, at a partner company, or in an online service. With AD FS, your organization can manage its own user accounts, and users have to remember only one set of credentials. Those credentials can provide access to a variety of applications, even when they reside at different locations.

### Objectives

After completing this module, you will be able to:

- Describe AD FS.
- Explain how to deploy AD FS.
- Explain how to implement AD FS for a single organization.
- Explain how to extend AD FS to external clients.
- Implement single sign-on (SSO) to support online services.

## Lesson 1

# Overview of AD FS

AD FS is the Microsoft implementation of an identity federation framework that allows organizations to establish federation trusts and share resources across organizational and Active Directory Domain Services (AD DS) boundaries. AD FS is compliant with common web services standards, thus allowing interoperability with identity federation solutions that other vendors provide. AD FS addresses a variety of business scenarios in which the typical authentication mechanisms used in an organization do not work.

This lesson provides an overview of the concepts and standards that AD FS implements and the business scenarios that AD FS can address.

### Lesson Objectives

After completing this lesson, you will be able to:


- Describe identity federation.
- Describe claims-based identity.
- Describe web services.
- Describe AD FS.
- Describe the new features in AD FS.
- Explain how AD FS enables SSO in a single organization.
- Explain how AD FS enables SSO in a business-to-business federation.

### What is identity federation?

Identity federation allows you to provide identification, authentication, and authorization across organizational and platform boundaries. You can implement identity federation either within a single organization to allow access to diverse web applications or between organizations that have an established trust relationship.

To establish an identity federation partnership, both partners agree to create a federated trust relationship. This federated trust is based on an ongoing business relationship, and it allows the organizations to implement business processes that the business relationship identifies.

- Allows identification, authentication, and authorization across organizational and platform boundaries
- Requires a federated trust relationship between two organizations or entities
- Allows organizations to retain control over who can access resources
- Allows organizations to retain control of their user and group accounts

 **Note:** A federated trust is not the same as a forest trust that organizations can configure between AD DS forests. In a federated trust, the AD FS servers in two organizations never have to communicate directly with each other. In addition, all communication in a federation deployment occur over HTTPS, so you do not need to open multiple ports on any firewalls to allow federation.

As part of the federated trust, each partner defines which of its resources are accessible to the other organization and how access to the resources is allowed. For example, to update a sales forecast, a sales representative might need to collect information from a supplier's database that is hosted on the supplier's network. The administrator of the domain for the sales representative is responsible for ensuring that the appropriate sales representatives are members of the group that requires access to the supplier's database. The administrator of the organization where the database is located is responsible for ensuring that the partner's employees have access only to the data that they require.

In an identity federation solution, user identities and their associated credentials are stored, owned, and managed by the organization where the users are located. As part of the identity federation trust, each organization also defines how user identities are shared in a security-enhanced manner to restrict access to resources. Each partner defines the services that it makes available to trusted partners and customers, and it defines which other organizations and users it trusts. Each partner also defines both what types of credentials and requests it accepts and its privacy policies to help ensure that private information is not accessible across the trust.

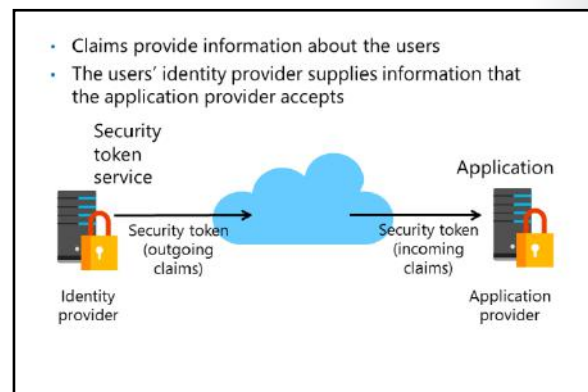
You can also use identity federation within a single organization. For example, an organization might plan to deploy several web-based applications that require authentication. By using AD FS, the organization can implement one authentication solution for all of the applications, making it easy for users in multiple internal domains or forests to access the application. The solution can also extend to external partners in the future, without requiring developers to change the application.

## What are claims-based identity and claims-based authentication?

In most organizations, users sign in to the network and are authenticated by an AD DS domain controller. A user who provides the right credentials to the domain controller is granted a security token. Applications that are running on servers in the same AD DS environment trust the security tokens that the AD DS domain controllers provide, because the servers can communicate with the same domain controllers where the users authenticate.

That type of authentication does not easily extend outside of AD DS forest boundaries. Although trusts based on the Kerberos V5 authentication protocol or on Integrated Windows Authentication (IWA) can be implemented between two AD DS forests, client computers and domain controllers on both sides of the trust must communicate with domain controllers in the other forest to make decisions about authentication and authorization. This communication requires network traffic that is sent on multiple ports, so these ports must be open on all firewalls between the domain controllers and the other computers. The problem becomes even more complicated when users must access resources that are hosted in cloud-based systems, such as Microsoft Azure or Microsoft Office 365.

Claims-based authentication provides a mechanism for separating user authentication and authorization from individual applications. With claims-based authentication, users can authenticate to a directory service that is located within their organization and be granted a claim based on that authentication. The claim is then presented to an application that is running in a different organization. The application allows user access to information or features based on the claims presented. All communication occurs over HTTPS.



The *claim* that is used in claims-based authentication is a statement about a user that is defined in one organization or technology and trusted in another. The claim can include a variety of information. For example, the claim can define the user's email address, the user principal name (UPN), and information about specific groups to which the user belongs. This information is collected from the identity store when the user successfully authenticates.

The organization that manages the application defines the types of claims that the application will accept. For example, the application might require the user's email address to verify identity and then use the group membership that is presented inside the claim to determine what level of access the user will have within the application.

## Overview of web services

For claims-based authentication to work, organizations must agree on the format for exchanging claims. Rather than have each business define this format, a set of specifications broadly identified as *web services* has been developed. Any organization that wants to implement a federated identity solution can use this set of specifications.

Web services comprise a set of specifications that are used for building connected applications and services and whose functionalities and interfaces are exposed to potential users through web technology standards, such as XML, Simple Object Access Protocol (SOAP), Web Services Description Language (WSDL), HTTP, and HTTPS. The goal of creating web applications by using web services is to simplify interoperability for applications across multiple development platforms, technologies, and networks.

To enhance interoperability, web services are defined by a set of industry standards:

- Most web services use XML to transmit data through HTTP and HTTPS. With XML, developers can create their own customized tags, thereby facilitating the definition, transmission, validation, and interpretation of data between applications and organizations.
- Web services expose useful functionality to web users through a standard web protocol. In most cases, web services use SOAP, which is the communication protocol for XML web services. SOAP is a specification that defines the XML format for messages, and it essentially describes what a valid XML document looks like.
- Web services provide a way to describe their interfaces in enough detail to allow a user to build a client application to communicate with a service. This description is usually provided in an XML document called a WSDL document. In other words, a WSDL file is an XML document that describes a set of SOAP messages and how those messages are exchanged.
- Web services are registered so that potential users can easily find them. This is done with Universal Description, Discovery, and Integration (UDDI). A UDDI directory entry is an XML file that describes a business and the services it offers.

- Web services comprise a standardized set of specifications used to build applications and services
- Web services typically:
  - Transmit data as XML
  - Use SOAP to define the XML message format
  - Use WSDL to define valid SOAP messages
  - Use UDDI to describe available web services
- SAML is a standard for exchanging identity claims



## Web Services Security specifications

Web services specifications include several components that are commonly known as WS-\* specifications. However, the most relevant specifications for an AD FS environment are the Web Services Security (WS-Security) specifications. WS-Security includes the following specifications:

- **WS-Security: SOAP Message Security and X.509 Certificate Token Profile.** WS-Security describes enhancements to SOAP messaging that provide quality of protection through message integrity, message confidentiality, and single-message authentication. WS-Security also provides a general-purpose, yet extensible, mechanism for associating security tokens with messages. Additionally, it provides a mechanism to encode binary security tokens—specifically, X.509 certificates and Kerberos tickets—in SOAP messages.
- **Web Services Trust (WS-Trust).** WS-Trust defines extensions that build on WS-Security to request and issue security tokens and to manage trust relationships.
- **Web Services Federation (WS-Federation).** WS-Federation defines mechanisms that WS-Security can use to allow attribute-based identity, authentication, and authorization federation across different trust realms.
- **WS-Federation Passive Requestor Profile (WS-F PRP).** This WS-Security extension describes how passive clients, such as web browsers, can acquire tokens from a federation server and how the clients can submit tokens to a federation server. The passive requestors of this profile are limited to the HTTP or HTTPS protocol.
- **WS-Federation Active Requestor Profile.** This WS-Security extension describes how active clients, such as SOAP-based mobile-device apps, can be authenticated and authorized, and how the clients can submit claims in a federation scenario.

## Security Assertion Markup Language

Security Assertion Markup Language (SAML) is an XML-based standard for exchanging claims between an identity provider and a service or application provider. SAML assumes that a user has been authenticated by an identity provider and that the identity provider has populated the appropriate claim information in the security token. When the identity provider authenticates the user, it passes a SAML assertion to the service provider. Based on this assertion, the service provider can make authorization and personalization decisions within an application. The communication between federation servers is based on an XML document that stores the X.509 certificate for token signing and the SAML 1.1 or SAML 2.0 token.

## What is AD FS?

AD FS is the Microsoft implementation of an identity federation solution that uses claims-based authentication. AD FS provides the mechanisms to implement both the identity provider and the service provider components in an identity federation deployment.

- AD FS is the Microsoft identity federation product that can use claims-based authentication
- AD FS has the following features:
  - SSO for web-based apps
  - Interoperability with web services on multiple platforms
  - Support for many clients, such as web browsers, mobile devices, and applications
  - Extensibility to support customized claims from third-party applications
  - The Delegation of account management to the user's organization

AD FS provides the following features:

- An enterprise claims provider for claims-based applications. You can configure an AD FS server as a claims provider, which means that the AD FS server can issue claims about authenticated users. This allows an organization to provide its users with access to claims-aware applications in another organization by using SSO.
- A federation service provider for identity federation across domains. This service offers federated web SSO across domains, thereby enhancing security and reducing overhead for IT administrators.

### **AD FS features**

The following are some of the key features of AD FS:

- **Web SSO.** Many organizations deploy AD DS. After authenticating to AD DS through IWA, users can access all other resources that they have permission to access within the AD DS forest boundaries. AD FS extends this capability to intranet or Internet-facing applications, enabling customers, partners, and suppliers to have a similar, streamlined user experience when they access an organization's web-based applications.
- **Web services interoperability.** AD FS is compatible with the web services specifications. AD FS employs the federation specification of WS-\* called WS-Federation. WS-Federation makes it possible for environments that do not use the Windows Identity Foundation (WIF) identity model to federate with environments that use the Windows operating system.
- **Passive and smart client support.** Because AD FS is based on the WS-\* architecture, it supports federated communications between any WS-enabled endpoints, including communications between servers and passive clients, such as browsers. AD FS in Windows Server 2016 allows access for SOAP-based smart clients, such as mobile phones, personal digital assistants, and desktop apps. AD FS implements WS-F PRP and some of the WS-Federation Active Requestor Profile standards for client support.
- **An extensible architecture.** AD FS provides an extensible architecture that supports various security token types, including SAML tokens and Kerberos authentication through Windows authentication, and the ability to perform custom claims transformations. For example, AD FS can convert one token type to another, or it can add custom business logic as a variable in an access request. Organizations can use this extensibility to modify AD FS to coexist with their existing security infrastructure and business policies.
- **Enhanced security.** AD FS also increases the security of federated solutions by delegating responsibility for account management to the organization closest to the user. Each individual organization in a federation continues to manage its own identities, and each is capable of the security-enhanced sharing and accepting of identities and credentials from other members' sources.

## What is new in AD FS in Windows Server 2016?

### New AD FS features introduced in Windows Server 2012

The AD FS version that ships with Windows Server 2012 includes several new features:

- Integration with the Windows Server 2012 operating system. In Windows Server 2012, AD FS is included as a server role that you can install by using Server Manager. When you install the server role, all the required operating system components automatically install.
- Integration with Dynamic Access Control. When you deploy Dynamic Access Control, you can configure user and device claims that are issued by AD DS domain controllers. AD FS can consume the AD DS claims that domain controllers issue. This means that AD FS can make authorization decisions based on both user accounts and computer accounts.
- Windows PowerShell command-line interface cmdlets for administering AD FS. Windows Server 2012 provides several new cmdlets that you can use to install and configure the AD FS server role.

- New AD FS features introduced in Windows Server 2012:
  - Integration with the Windows Server 2012 operating system
  - Integration with Dynamic Access Control
  - Windows PowerShell cmdlets for administering AD FS
- New AD FS features introduced in Windows Server 2016:
  - Support for any directory that is LDAP v3-compliant
  - New factors of authentication
  - Improvements in AD FS management
  - Conditional access

### New AD FS features introduced in Windows Server 2016

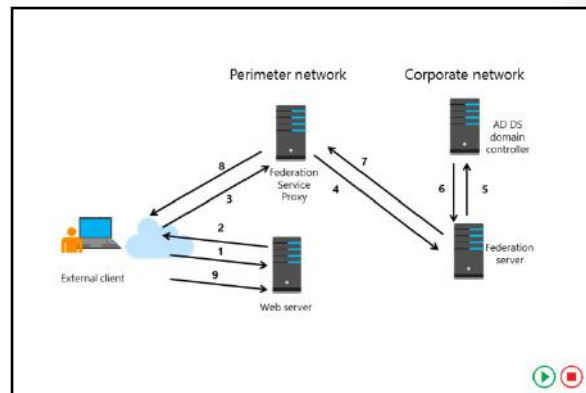
The AD FS version that ships with Windows Server 2016 includes the following new features:

- Support for any directory that is Lightweight Directory Access Protocol (LDAP) v3 compliant. This allows your users to:
  - Sign in to AD FS from any third-party directory that is LDAP v3 compliant.
  - Sign in from untrusted or partially trusted AD DS domains and forests.
- New factors of authentication. AD FS provides additional ways to authenticate users and devices. In addition to using AD DS and LDAP v3 directories, you can also configure Azure Multi-Factor Authentication as an authentication method.
- Improvements in AD FS management, including:
  - Application policies. In AD FS for Windows Server 2012 R2, you must use claims rules language to create custom AD FS policies. AD FS in Windows Server 2016 provides wizard-based management, making it easier to create custom policies.
  - Delegated service management. AD FS in Windows Server 2016 separates the AD FS server administrators from the AD FS service administrators. This means that the AD FS administrator is no longer required to be a local server administrator.
- Conditional access. AD FS in Windows Server 2016 provides improvements in device registration by working with Azure Active Directory (Azure AD) to restrict devices or require multiple factors of authentication, based on management or compliance status. For example, with conditional access, you can:
  - Allow access from only those of your users' devices that are managed or compliant with corporate standards.

- Restrict access to computers joined to the corporate domain, including managed devices and computers joined to the domain.
- Require Multi-Factor Authentication (MFA) for computers that are not joined to the domain and devices that are not compliant.

## How AD FS enables SSO in a single organization

For many organizations, configuring access to applications and services might not require an AD FS deployment. If all users are members of the same AD DS forest, and if all applications run on servers that are members of the same forest, you usually can use AD DS authentication to provide access to the application. However, several scenarios exist in which you can use AD FS to optimize the user experience by enabling SSO. In a single organization, you can use AD FS to enable SSO when:




- Your applications might not be running on Windows-based servers or on any servers that support AD DS authentication, or they might be running on servers that are running Windows Server and that are not joined to the domain. The applications might require SAML or web services for authentication and authorization.
- You have multiple domains and forests. This might be a result of mergers and acquisitions or because of security requirements. Users in multiple forests might require access to the same applications.
- Users from outside the office might require access to applications that are running on internal servers. External users might sign in to applications from computers that are not part of the internal domain.


You can use AD FS to enable SSO in these scenarios. If your organization has a single AD DS forest, you must deploy only a single federation server. This server can operate as the claims provider so that it authenticates user requests and issues the claims. The same server is also the relying party to provide authorization for application access.

The following steps describe the communication flow in this scenario:


1. The client computer, which is located outside of the network, accesses a web-based application on the web server. The client computer sends an HTTPS request to the web server.
2. The web server receives the request and identifies that the client computer does not have a claim.
3. The web server redirects the client computer to the Web Application Proxy. The client computer sends an HTTPS request to the Web Application Proxy. Depending on the scenario, the Web Application Proxy might prompt the user for authentication or use Windows authentication to collect the user's credentials.
4. The Web Application Proxy transmits the request and the credentials to the federation server.
5. The federation server uses AD DS to authenticate the user.
6. If the authentication succeeds, the federation server collects AD DS information about the user. That information is then used to generate the user's claims.

 **Note:** A relying party trust for the web application must exist in AD FS. If the same user tries to access a different web application, different user claims can be included in the security token, which is passed to the user and then to the web application.

7. If the authentication succeeds, the authentication information and other information is collected in a security token and passed back to the Web Application Proxy.

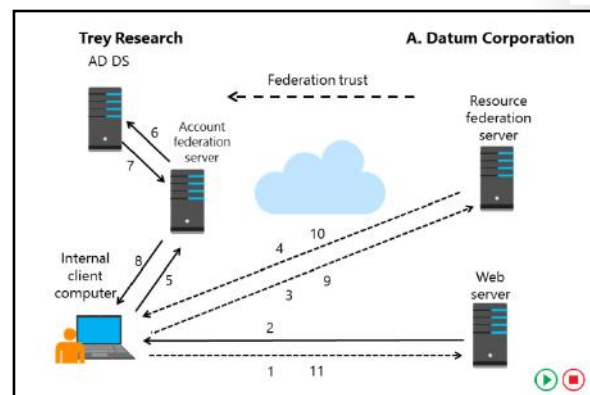
 **Note:** This security token is signed for the specific web application. Consequently, a relying party trust with this web application must exist in AD FS.

8. The Web Application Proxy passes the token to the client.
9. The client presents the token to the web server. The web resource:
  - a. Receives the request and validates the signed tokens.
  - b. Uses the claims in the user's token to provide access to the application.

 **Note:** The slide and the preceding description use the terms *Federation Service Proxy* and *Web Application Proxy* to describe AD FS role services. The federation server is responsible for issuing claims, and consuming the claims in this scenario. The Web Application Proxy is a proxy component that is recommended for deployments where users outside of the network need access to the AD FS environment. These components are covered in more detail in the next lesson.

## How AD FS enables SSO in a business-to-business federation

One of the most common scenarios for deploying AD FS is to provide SSO in a business-to-business federation. In this scenario, the organization that requires access to another organization's application or service can manage its own user accounts and define its own authentication mechanisms. The other organization can define which applications and services to expose to users outside of the organization and which claims it will accept to provide access to the application. To allow application or service sharing in this scenario, the organizations must establish a federation trust and then define the rules for exchange claims between them.



The slide for this topic is an animated slide that demonstrates the flow of traffic in a federated business-to-business scenario by using a claims-aware web application. In this scenario, users at Trey Research must access a web-based application at A. Datum Corporation. The AD FS authentication process for this scenario is as follows:

1. A user at Trey Research uses a web browser to establish an HTTPS connection to the web server at A. Datum Corporation.
2. The web application receives the request, and verifies that the user does not have a valid token stored in a cookie by the web browser. Because the user is not authenticated, the web application redirects the client to the federation server at A. Datum Corporation by using an HTTP 302 redirect message.
3. The client computer sends an HTTPS request to the federation server at A. Datum Corporation. The federation server determines the home realm for the user. In this case, the home realm is Trey Research.
4. The web server again redirects the client computer to the federation server in the user's home realm, which is Trey Research.
5. The client computer sends an HTTPS request to the Trey Research federation server.
6. If the user is already signed in to the domain, the federation server can take the user's Kerberos ticket and request authentication from AD DS on the user's behalf by using IWA. If the user is not signed in to the domain, the user is prompted for credentials.
7. The AD DS domain controller authenticates the user and sends the success message back to the federation server along with other information about the user that the federation server can use to generate the user's claims.
8. The federation server creates the claim for the user based on the rules defined for the federation partner. The federation server places the claims data in a digitally signed security token and then sends it to the client computer, which posts it back to the federation server at A. Datum Corporation.
9. The federation server at A. Datum Corporation validates that the security token came from a trusted federation partner.
10. The federation server at A. Datum Corporation creates and signs a new token, which it sends to the client computer. The client computer then sends the token back to the original URL that was requested.
11. The application on the web server receives the request and validates the signed tokens. The web server issues the client a session cookie, indicating that the authentication succeeded. The federation server issues a file-based persistent cookie, which is valid for 30 days by default. It eliminates the home-realm discovery step during the cookie's lifetime. The server then provides access to the application based on the claims that the user provides.

**Question:** Verify the correctness of the statement by placing a mark in the column to the right.

Statement	Answer
A federated trust is the same as a forest trust that organizations can configure between AD DS forests.	

## Lesson 2

# AD FS requirements and planning

After you understand how AD FS works, you can deploy the service. Before you deploy AD FS, you must understand the components that you must deploy and the prerequisites that you must meet, particularly with regard to certificates. This lesson provides an overview of deploying the AD FS server role in Windows Server 2016.

### Lesson Objectives

After completing this lesson, you will be able to:

- Describe the AD FS components.
- Describe the AD FS prerequisites.
- Describe the public key infrastructure (PKI) and certificate requirements for AD FS.
- Describe the AD FS federation server roles.
- Describe how to provide high availability for AD FS.
- Describe how to plan for capacity for AD FS.
- Describe how to plan an AD FS deployment for Microsoft online services.

### AD FS components

To understand the configuration process for AD FS, you must first understand all of the components that are part of AD FS. These components work together to provide a complete solution for claims-based authentication within an organization or between organizations.

Federation server	Relying parties
Federation server proxy and Web Application Proxy	Claims provider trust
Claims	Relying party trust
Claim rules	Certificates
Attribute store	Endpoints
Claims providers	

The following table lists the AD FS components.

Component	What it does
Federation server	The federation server issues, manages, and validates requests involving identity claims. All implementations of AD FS require at least one Federation Service for each participating party.
Federation server proxy and Web Application Proxy	The federation server proxy is an optional component that you usually deploy in a perimeter network. It does not add any functionality to the AD FS deployment, but it is deployed to provide a layer of security enhancement for connections from the Internet to the federation server. In Windows Server 2016, the federation server proxy functionality is part of Web Application Proxy.
Claims	A claim is a statement that is made by a trusted entity about an object such as a user. The claim can include the user's name, job title, or any other factor that might be used in an authentication scenario.
Claims rules	Claim rules determine how federation servers process claims. For example, a claims rule might state that an email address is accepted as a valid claim or that a group name from one organization is translated into an application-specific role in the other organization. The rules are usually processed in real time as claims are made.
Attribute store	AD FS uses an attribute store to look up claims values. AD DS is a common attribute store that is available by default, because the federation server role must be installed on a server joined to the domain.
Claims providers	The claims provider is the server that issues claims and authenticates users. A claims provider functions as one side of the AD FS authentication and authorization process. The claims provider manages user authentication and then issues the claims that the user presents to a relying party.
Relying parties	The relying party is the party where the application is located, and it functions as the other side of the AD FS authentication and authorization process. The relying party is a web service that consumes claims from the claims provider. The relying party server must have WIF installed or use the AD FS 1.0 claims-aware agent.
Claims provider trust	The claims provider trust contains the configuration data that defines the rules under which a client might request claims from a claims provider and subsequently submit them to a relying party. The trust consists of various identifiers such as names, groups, and rules.
Relying party trust	The relying party trust contains the AD FS configuration data that is used to provide claims about a user or client to a relying party. It consists of various identifiers, such as names, groups, and rules.
Certificates	AD FS uses digital certificates when communicating over Secure Sockets Layer (SSL) or as part of the token-issuing



Component	What it does
	process, the token-receiving process, and the metadata-publishing process. Digital certificates also are used for token signing.
Endpoints	Endpoints are Windows Communication Foundation mechanisms that enable access to AD FS technologies, including token issuance and metadata publishing. AD FS comes with built-in endpoints that are responsible for specific functionalities.

## AD FS requirements

Before you deploy AD FS, you must ensure that your internal network meets some basic prerequisites. The configuration of the following network services is critical for a successful AD FS deployment:

- Network connectivity. The following network connectivity is required:
  - The client computer must be able to communicate with the web application, the resource federation server or federation server proxy, and the account federation server or federation server proxy by using HTTPS.
  - The federation server proxies must be able to communicate with the federation servers in the same organization by using HTTPS.
  - The federation servers and internal client computers must be able to communicate with domain controllers for authentication.
- AD DS. AD DS is a critical piece of AD FS. The federation servers must be joined to an AD DS domain. However, the Web Application Proxy does not have to be joined to the domain.
- Attribute stores. AD FS uses an attribute store to build claims information. The attribute store contains information about users, which is extracted from the store by the AD FS server after the user has been authenticated.
- Domain Name System (DNS). Name resolution allows clients to find federation servers. Client computers must resolve DNS names for all the federation servers or AD FS farms to which they connect and the web applications that the client computer is trying to use. If a client computer is external to the network, the client computer must resolve the DNS name for the Web Application Proxy, not the internal federation server or AD FS farm. The Web Application Proxy must resolve the name of the internal federation server or farm. If internal users have to directly access the internal federation server, and if external users must connect through the federation server proxy, you must configure different DNS records in the internal and external DNS zones.

A successful AD FS deployment includes the following critical infrastructure:

- TCP/IP network connectivity
- AD DS
- Attribute stores
- DNS


## PKI and certificate requirements

AD FS allows computers to communicate in a security-enhanced manner, even though they might be in different locations. In this scenario, most of the communications between computers pass through the Internet. To help provide security for the network traffic, all communications are encrypted by using SSL. This factor means that it is important to correctly choose and assign SSL certificates to the AD FS servers. To provide SSL encryption, AD FS servers use certificates as service communication certificates, token-signing certificates, and token-decrypting certificates.

- The certificates used by AD FS:
  - Service communication certificates
  - Token-signing certificates
  - Token-decrypting certificates
- When choosing certificates, ensure that the service communication certificate is trusted by all federation partners and clients

### Service communication certificates

AD FS helps to secure all communication by using SSL, which requires a certificate. All computers that communicate with the AD FS server must trust the certificate used for service communication. If all of the computers and devices that contact your AD FS server are joined to the domain, you can consider using an internally generated certificate for AD FS. However, in most cases, at least some communication is between the AD FS server and external computers or partner organizations. In that case, you should use a certificate from a third-party certification authority (CA). You can use the certificate's snap-in and the **AD FS Management** console to manage all certificates.

 **Note:** If you change the service communication certificate after the initial configuration, you must change it on all nodes in the server farm and ensure that the AD FS service is granted read permission to the private key on the certificate on each node.

### Token-signing certificates

AD FS uses a token-signing certificate to sign every token that a federation server issues. This certificate is critical in an AD FS deployment because the token signature indicates which federation server issued the token. The claims provider uses this certificate to identify itself, and the relying party uses it to verify that the token came from a trusted federation partner.

The relying party also requires a token-signing certificate to sign the tokens that it prepares for AD FS-aware applications. For the destination applications to validate these tokens, the relying party's token-signing certificate must validate these tokens.


When you configure a federation server, the server assigns a self-signed certificate as the token-signing certificate. In most cases, you do not need to update this certificate with a certificate from a third-party CA. When AD FS creates a federation trust, it configures the trust of this certificate at the same time. You can configure multiple token-signing certificates on the federation server, but AD FS uses only the primary certificate.

### Token-decrypting certificates

AD FS uses token-decrypting certificates to encrypt the entire user token before transmitting the token across the network from the claims provider federation server to the relying party federation server. To provide this functionality, AD FS provides the public key from the relying party federation server certificate to the claims provider federation server. The certificate is sent without the private key. The claims provider server uses the public key from the certificate to encrypt the user token. When the claims provider server returns the token to the relying party federation server, it uses the private key from the

certificate to decrypt the token. This provides an extra layer of security enhancement when transmitting the certificates across an untrusted network, such as the Internet.


When you configure a federation server, the server assigns a self-signed certificate as the token-decrypting certificate. In most cases, you are not required to update this certificate with a certificate from a third-party CA. When AD FS creates a federation trust, it configures the trust of this certificate at the same time.

 **Note:** The federation server proxies require only an SSL certificate. The federation server uses this certificate to enable SSL communication for all client connections.

## Choosing a CA

AD FS federation servers can use self-signed certificates; certificates from an internal, private CA; or certificates that have been purchased from an external, public CA. In most AD FS deployments, the most important factor when choosing certificates is that they are trusted by all the parties involved. This means that if you configure an AD FS deployment that interacts with other organizations, you almost certainly will use a public CA for the SSL certificate on a federation server proxy, because the certificates issued by the public CA are automatically trusted by all partners.

If you deploy AD FS just for your organization, and all the servers and client computers are under your control, you can consider using a certificate from an internal, private CA. If you deploy an internal, enterprise CA in Windows Server 2016, you can use Group Policy to help ensure that all the computers in the organization automatically trust the certificates issued by the internal CA. Using an internal CA can significantly decrease the cost of certificates.


 **Note:** Deploying an internal CA by using Active Directory Certificate Services (AD CS) is a straightforward process, but it is critical that you carefully plan and implement the deployment.

## Federation server roles


In Windows Server 2016, the server roles for AD FS are:

- Claims provider. A claims provider is a federation server that provides users with signed tokens containing claims. Claims provider federation servers are deployed in organizations where user accounts are located. When a user requests a token, the claims provider federation server verifies user authentication by using AD DS, and then it collects information from an attribute store, such as AD DS or Active Directory Lightweight Directory Services (AD LDS), to populate the user claim with the attributes required by the partner organization. The server issues tokens in the SAML format. The claims provider federation server also helps to protect the contents of security tokens in transit by signing and optionally encrypting them.
- A claims provider federation server:
    - Authenticates internal users
    - Issues signed tokens containing user claims
  - A relying party federation server:
    - Consumes tokens from the claims provider
    - Issues tokens for application access
  - A Federation Service Proxy:
    - Gets deployed in a perimeter network
    - Provides a layer of security enhancement for internal federation servers

- **Relying party.** A relying party is a federation server that receives security tokens from a trusted claims provider. Relying party federation servers are deployed in organizations that provide application access to claims provider organizations. The relying party accepts and validates the claim, and then it issues new security tokens that the web server can use to provide appropriate access to the application.


 **Note:** A single AD FS server can operate as both a claims provider and a relying party, even with the same partner organizations. The AD FS server functions as a claims provider when it authenticates users and provides tokens for another organization, but it can also accept tokens from the same or different organizations in a relying party role.

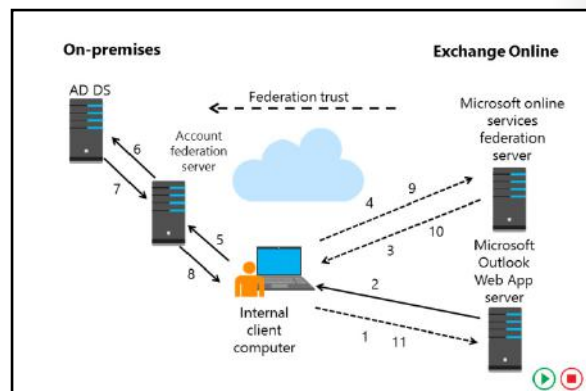
- **Web Application Proxy.** A Web Application Proxy provides an extra level of security enhancement for AD FS traffic that comes from the Internet to internal AD FS federation servers. A Federation Service Proxy can be deployed in both claims provider and relying-party organizations. On the claims provider side, the proxy collects the authentication information from client computers and passes it to the claims provider federation server for processing. The federation server issues a security token to the proxy, which sends it to the relying party proxy. The relying party federation server proxy accepts these tokens, and then passes them to the internal federation server. The relying party federation server issues a security token for the web application, and then it sends the token to the federation server proxy, which forwards the token to the client. The Web Application Proxy does not provide any tokens or create claims—it only forwards requests from clients to internal AD FS servers. All communication between the Web Application Proxy and the federation server uses HTTPS.

 **Note:** You cannot configure a Web Application Proxy as a claims provider or as a relying party. The claims provider and relying party must be members of an AD DS domain. You can configure the Web Application Proxy as a member of a workgroup or as a member of an extranet forest, and you can deploy it in a perimeter network.

## Planning an AD FS deployment for online services

You can use AD FS to provide an SSO experience to users across various cloud-based platforms. For example, after the users authenticate with AD DS credentials, they can then use those domain credentials to access Microsoft online services, such as Azure, Microsoft Intune, or Office 365.

 **Note:** AD FS can also provide SSO to other cloud-based providers. Because AD FS is based on open standards, it can interoperate with any compliant claims-based system.



A hybrid Microsoft Exchange deployment is an example of a cloud-based service that uses AD FS for authentication. In this type of deployment, an organization deploys some or all of its mailboxes in an Office 365 environment. However, the organization manages all of its user accounts in its on-premises AD DS environment. The deployment uses a directory synchronization tool to synchronize user account information from the on-premises environment to the Office 365 deployment.


When users try to sign in to their Office 365 mailboxes, they must authenticate by using their internal AD DS credentials. If users try to sign in directly to the Office 365 environment, they are redirected back to the internal AD FS deployment to authenticate before they are given access.

The following steps describe what happens when a user tries to access his or her online mailbox by using a web browser:

1. The user opens a web browser and sends an HTTPS request to the Office 365 Outlook Web App server.
2. The Outlook Web App server receives the request and verifies whether the user is part of a hybrid Exchange Server deployment. If this is the case, the server redirects the client computer to the Microsoft online services federation server.
3. The client computer sends an HTTPS request to the Microsoft online services federation server.
4. The client computer is redirected again to the on-premises federation server. The redirection to the user's home domain is based on the UPN suffix of the user.
5. The client computer sends an HTTPS request to the on-premises federation server.
6. If the user is already signed in to the domain, the on-premises federation server can take the user's Kerberos ticket and request authentication from AD DS on the user's behalf by using Windows authentication. If the user signs in from outside of the network or from a computer that is not a member of the internal domain, the user is prompted for credentials.
7. The AD DS domain controller authenticates the user and then sends the success message back to the federation server along with other information about the user that the federation server can use to generate the user's claims.
8. The federation server creates the claim for the user based on the rules defined during the AD FS server setup. The claims data is placed in a digitally signed security token. Then the data is sent to the client computer, which posts it back to the Microsoft online services federation server.
9. The Microsoft online services federation server validates that the security token came from a trusted federation partner. This trust is configured when you configure the hybrid Exchange Server environment.
10. The Microsoft online services federation server creates and signs a new token that it sends to the client computer, which then sends the token back to the Outlook Web App server.
11. The Outlook Web App server receives the request and validates the signed tokens. The server issues the client a session cookie indicating that it has successfully authenticated. The user is then granted access to his or her Exchange Server mailbox.

### Preparing for SSO integration with Microsoft online services

SSO, also referred to as *identity federation*, allows you to simplify your users' sign-in process when they access online services, such as Office 365 or Microsoft Intune. By using SSO, users can use their internal AD DS credentials to access these online services. When you configure AD FS to provide SSO for Microsoft online services, you create a federated trust between your organization's on-premises directory and the federated domain you specify in your Azure AD tenant.

 **Note:** For more information about Azure AD, see Lesson 1, "Overview of advanced AD DS deployments" in Module 3, "Advanced AD DS infrastructure management."

To deploy SSO integration with Microsoft online services, use the following high-level steps:

1. Prepare your environment for SSO:
  - a. Deploy AD DS in your on-premises environment.
  - b. Install the AD FS role.
  - c. Prepare AD DS. Depending on your domains, you might need to complete these tasks:
    - i. Verify that the UPNs are set and known by the users.
    - ii. Verify that the UPN domain suffix is under the domain that you choose to set up for SSO.



**Note:** Remember that the UPNs that you use for SSO must contain only letters, numbers, periods, dashes, and underscores.

- iii. Ensure that the domain you choose to federate is registered as a public domain with a domain registrar or within your own public DNS servers.



**Note:** If your AD DS domain name is not a public Internet domain, you must set a UPN to have a domain suffix that can be publicly registered. In this situation, we recommend that you use something familiar to your users, such as their email domain.

To prepare your Active Directory environment for SSO, you can run the Microsoft Deployment Readiness Tool. This tool inspects your Active Directory environment and provides a report that includes information about whether you are ready to set up SSO. If not, it lists the changes you need to make to prepare for SSO.



**Note:** To download the tool, go to “Microsoft Office 365 Deployment Readiness Tool” at: <http://aka.ms/D9vmqf>

2. Deploy federation services:
  - a. Deploy your AD FS server farm.
  - b. Configure extranet access:
    - i. Install the Web Application Proxy role.
    - ii. Configure the Web Application Proxy.
  - c. Establish a trust between AD FS and Azure AD:
    - i. Using Windows PowerShell and the Azure AD Module for Windows PowerShell, add the required domains with the **New-MSOLFederatedDomain** cmdlet.



**Note:** For additional guidance on these steps, refer to Checklist: “Use AD FS to implement and manage single sign-on” at: <http://aka.ms/U193rk>

3. Deploy directory synchronization:
  - a. Download and install Azure AD Connect to enable the synchronization of the domain in Azure.


4. Verify SSO:
  - a. On a computer that is joined to the domain, sign in to your Microsoft cloud service by using the same sign-in name that you use for your corporate credentials.
  - b. Click inside the **Password** box. If SSO is set up, the **Password** box will be shaded, and you will see the following message: **You are now required to sign in at your company.**
  - c. Click the **Sign in at your company** link. If you are able to sign in, SSO has been set up.

## Planning a highly available AD FS deployment

The availability of your AD FS environment is critical when services in Office 365 are enabled for federated authentication. For example, if your federation server is unavailable, all user authentication requests will fail, and users will not be able to access Office 365 services. Similarly, if your federation proxy is unavailable, external user authentication requests will not be passed to your federation server, and these users will not be able to access Office 365 services. Therefore, it is essential that the preparation for AD FS deployment include planning for the high availability of your AD FS federation servers and the AD FS federation proxy servers.

When planning the availability of your AD FS environment for federated authentication, you should consider the following categories:

- The federation server farm
- NLB
- The configuration database

 **Note:** AD FS availability affects only user authentication and does not affect Office 365 services. For example, if users are not able to access their email in Office 365, their mailboxes in Exchange Online will continue to receive email.

### Federation server farm

With Windows Server 2012 or earlier, you can deploy the AD FS federation server as a standalone server or in a federation server farm. However, we recommend that you always deploy more than one server in a federation server farm. Even if the farm initially consists only of one federation server, this deployment method provides you with the option of adding more federation servers later for load balancing or fault tolerance. However, if the AD FS federation server is deployed as a standalone server, you will not be able to add servers later.

With Windows Server 2012 R2 or later, you can deploy the AD FS federation server only in a federation server farm. Although this deployment method provides you with the option of adding more federation servers later, we recommend that you deploy more than one federation server in a farm for your production environments.

### NLB

You should use Network Load Balancing (NLB) or other forms of clustering to allocate a single IP address for multiple AD FS federation servers. With this deployment option, the failure of a single federation server should not affect the federation services for users. Similarly, you should also use NLB to provide an AD FS proxy array in the perimeter network to help ensure that external clients are not impacted by the failure of any AD FS proxy computer.



**Note:** Although the details are not covered in this course, you can also deploy a hardware load balancer instead of NLB to provide high availability to your federation servers and federation proxy servers.

## Configuration database

If you chose Windows Internal Database (WID) as your AD FS data storage, a copy of the configuration database exists on each server. However, if you chose Microsoft SQL Server as your AD FS data storage, you need to plan for a high availability SQL Server deployment. As opposed to WID, deploying an AD FS federation server farm with SQL Server does not enable high availability for the configuration database, by default. For example, if the server running SQL Server is unavailable, the AD FS federation server will be unable to connect to the configuration database, and the AD FS service will not start. For this reason, you should consider deploying AD FS with a SQL Server cluster or a SQL Server failover partner. Although you can enable the SQL Server cluster at any time, the SQL Server cluster failover partner can be enabled only during the AD FS deployment or afterward. This is because you use AD FS to configure the failover partner.



**Note:** For more information on the high availability solutions of SQL Server, refer to: "High Availability Solutions (SQL Server)" at: <http://aka.ms/lsr6m4>

## Capacity planning

Capacity planning for federation servers helps you to assess the hardware requirements for each federation server and the number of federation servers to deploy. Capacity planning also helps you estimate and prepare for growth in the size of the AD FS configuration database.

### Capacity Planning spreadsheet

The AD FS Capacity Planning spreadsheet includes calculator-like functionality that takes expected usage data about users in your organization and returns a recommended optimal number of federation servers for an AD FS production environment.

The AD FS Capacity Planning spreadsheet requires the following inputs:

- A value (40, 60, or 80 percent) that best represents the percentage of total users expected to send authentication requests to AD FS during peak usage periods
- A value (1 minute, 15 minutes, or 1 hour) that best represents the length of time the peak usage period is expected to last
- The total number of users that will require SSO access to the target claims-aware application, based on whether the users are:
  - Signing in to AD DS from a computer on the corporate network
  - Remotely signing in to AD DS from a computer
  - Signing in from another organization or from a SAML 2.0 identity provider


- Use the following when planning for the capacity of your federation servers:

- Capacity Planning spreadsheet requirements:
  - The percentage of total users expected to send authentication requests to AD FS during peak usage periods
  - The length of time the peak usage period is expected to last
  - The total number of users that will require SSO access

- Estimation table:


Number of users	Minimum number of servers
Fewer than 1,000	2 federation servers, 2 proxies
1,000 – 15,000	2 federation servers, 2 proxies
15,000 – 60,000	3–5 federation servers, 2 proxies
More than 60,000	5+ federation servers, 3+ proxies



 **Note:** For more information about The AD FS Capacity Planning spreadsheet or to download it, refer to: "Planning for AD FS Server Capacity" at: <http://aka.ms/M9f7aw>

### Estimation table

AD FS can scale to support tens of thousands of users, and it allows you to add more federation servers to a server farm as your company scales up. You can use the following table to help you estimate the minimum number of AD FS federation servers and Web Application Proxy servers or federation proxy servers that you will need to deploy. These estimations are based on the number of users who will require SSO access—including remote access—to the cloud service.

 **Note:** Unless otherwise noted, all of the federation servers should be deployed in a federation server farm with a WID store for the configuration database. Although fewer federation servers might be possible in some of the scenarios in the following table, an additional federation server is included to provide redundancy.

Number of users accessing Office 365 services	Minimum number of AD FS servers to deploy	Recommendation and steps
Fewer than 1,000 users	2 federation servers 2 proxies	With fewer users, consider deploying the federation servers on two existing domain controllers and then implementing load balancing by using NLB. For the proxies, consider using two existing web servers or proxy servers, and then configure them both for the federation server proxy role or the Web Application Proxy role.
1,000–15,000 users	2 federation servers 2 proxies	With medium-to-large organizations, consider deploying the federation servers on two dedicated computers with NLB. Consider deploying the proxies on two dedicated computers with NLB.
15,000–60,000 users	3–5 federation servers 2 proxies	For every increment of 15,000 users over 15,000, you should deploy an additional federation server to the load-balanced farm, up to the maximum of five servers that WID supports—or more with a SQL Server database. For the proxies, consider deploying additional nodes to improve performance.
More than 60,000 users	5+ federation servers 3+ proxies	With enterprises with over 60,000 users, you should implement five or more federation servers that use SQL Server for the configuration database. You also should deploy three or more proxies that use hardware load balancing instead of NLB.

## Demonstration: Installing the AD FS server role

In this demonstration, you will see how to:

- Install AD FS.
- Add a DNS record for AD FS.
- Configure AD FS.

### Demonstration Steps

#### Install AD FS

1. On **LON-DC1**, open Windows PowerShell and use the **Add-KdsRootKey** cmdlet to create the Microsoft Group Key Distribution Service root key.
2. Use **Server Manager** to install the **Active Directory Federation Services** role.

#### Add a DNS record for AD FS

- On **LON-DC1**, use **DNS Manager** to add a new host record for AD FS in the **Adatum.com** forward lookup zone, and use the following settings:
  - Name: **adfs**
  - IP address: **172.16.0.10**

#### Configure AD FS

1. On **LON-DC1**, in the **Server Manager** notifications, click **Configure the federation services on this server**.
2. Use the following options to configure the AD FS server:
  - **Create the first federation server in a federation server farm**
  - Account for configuration: **Adatum\Administrator**
  - SSL Certificate: **adfs.adatum.com**
  - Federation Service Display Name: **A. Datum Corporation**
  - Create a Group Managed Service Account: **Adatum\ADFSService**
  - **Create a database on this server using Windows Internal Database**

**Question:** Verify the correctness of the statement by placing a mark in the column to the right.

Statement	Answer
In Windows Server 2016, the federation server proxy functionality is part of the Web Application Proxy role.	

## Lesson 3

# Deploying and configuring AD FS

The simplest deployment scenario for AD FS is within a single organization. In this scenario, a single AD FS server can operate as both the claims provider and the relying party. All users in this scenario are internal to the organization, as is the application that the users access.

This lesson provides details on the components that are required to configure AD FS in a single-organization deployment of AD FS. These components include claims, claims rules, claims provider trusts, and relying party trusts.

### Lesson Objectives

After completing this lesson, you will be able to:

- Describe AD FS claims and claims rules.
- Describe a claims provider trust.
- Describe a relying party trust.
- Explain how to configure claims provider trusts and relying party trusts.
- Explain how to install and configure AD FS.
- Explain how to configure an account partner and a resource partner.
- Explain how to configure claims rules.
- Describe how home realm discovery works.
- Explain how to manage an AD FS deployment.

### What are AD FS claims and claims rules?

AD FS claims provide the link between the claims provider and relying party roles in an AD FS deployment. An *AD FS claim* is a statement that a trusted entity, such as a claims provider, makes about a particular subject, such as a user. The claims provider creates the claims, and the relying party consumes the claims. AD FS claims provide a standards-based and flexible way for claims provider organizations to provide specific information about users in their organizations.

AD FS claims also provide a way for relying parties to define exactly what information they require to provide application access. The claim information provides the details required by applications to enable access to claims-aware applications.

- Claims provide information about users from the claims provider to the relying party
- AD FS:
  - Provides a default set of built-in claims
  - Enables the creation of custom claims
  - Requires each claim have a unique URI
- Claims can be:
  - Retrieved from an attribute store
  - Calculated based on retrieved values
  - Transformed into alternate values

### Claim types

Each AD FS claim has a claim type, such as email address, UPN, or last name. Users can be issued claims based on any defined claim type. Therefore, a user might be issued a claim with a type of **Last Name** and a value of **Weber**, for example. AD FS provides many built-in claim types. Optionally, you can create new ones based on organizational requirements.

A Uniform Resource Identifier (URI) uniquely identifies each AD FS claim type. This information is provided as part of the AD FS server metadata. For example, if the claims provider organization and the relying party organization decide to use a claim type of **AccountNumber**, both organizations must configure a claim type with this name. The claim type is published, and the claim type URI must be identical on both AD FS servers.

### How claim values are populated

Claims issued by a claims provider contain the information that is required by the relying party to enable appropriate application access. One of the first steps in planning an AD FS deployment is to define exactly what information the applications must have about each user to provide that user access to the application. After you define this information, the claims are then defined on the claims provider federation server. The AD FS server can obtain the information required to populate the claim in several ways:

- It can retrieve the claim from an attribute store. Frequently, the information required for the claim is already stored in an attribute store that is available to the federation server. For example, an organization might decide that the claim should include the user's UPN, email address, and specific group memberships. This information is already stored in AD DS, so the federation server can retrieve this information from AD DS when creating the claim. Because AD FS can use AD DS, AD LDS, SQL Server, a non-Microsoft LDAP directory, or a custom attribute store to populate claims, you can define almost any value within the claim.
- It can calculate the claim based on collected information. Claims provider federation servers also can calculate information based on data that is gathered from an attribute store. For example, you might want to provide information about a person's salary within a claim. This information is likely stored in a Human Resources database, but the actual value might be considered confidential. You can define a claim that categorizes salaries within an organization, and then have the AD FS server calculate which category a specific user belongs in. In this way, the claim includes only the salary category information, not the user's actual salary value.
- AD FS can transform the claim from one value to another. In some cases, the information that is stored in an attribute store does not exactly match the information required by the application when making authorization information. For example, the application might have different user roles defined that do not directly match the attributes that are stored in any attribute store. However, the application role might correlate to the AD DS group membership. For example, users in the Sales group might correlate to one application role, whereas users in the Sales Management group might correlate to a different application role. To establish the correlation in AD FS, you can configure a claims transformation that takes the value provided by the claims provider and translates the value into to a claim that is useful to the application in the relying party.
- If you have deployed Dynamic Access Control, AD FS can transform a Dynamic Access Control device claim into an AD FS claim. This helps to ensure that users can access an AD FS website only from trusted workstations that have been issued a valid device claim.

### Claim rules

*Claim rules* define how claims are sent and consumed by AD FS servers. Claim rules define the business logic that is applied to claims that the claims providers provide and that the relying parties accept. You can use claim rules to:

- Define which incoming claims are accepted from one or more claims providers.
- Define which outbound claims are provided to one or more relying parties.
- Apply authorization rules to enable access to a specific relying party for one or more users or groups of users.

You can define two types of claim rules:

- Claim rules for a claims provider trust. A claims provider trust is the AD FS trust relationship that is configured between an AD FS server and a claims provider. You can configure claim rules to define how the claims provider processes and issues claims.
- Claim rules for a relying party trust. A relying party trust is the AD FS trust relationship that is configured between an AD FS server and a relying party. You can configure claim rules that define how the relying party accepts claims from the claims provider.

Claim rules configured on an AD FS claims provider are all considered *acceptance transform rules*. These rules determine what claim types are accepted from the claims provider and then sent to a relying party trust. When configuring AD FS within a single organization, a default claims provider trust is configured with the local AD DS domain. This rule set defines the claims that are accepted from AD DS.

Three types of claim rules exist for a relying party trust:

- Issuance transform rules. These rules define the claims that are sent to the relying party that was defined in the relying party trust.
- Issuance authorization rules. These rules define which users are permitted or denied access to the relying party defined in the relying party trust. This rule set can include rules that explicitly permit access to a relying party and rules that explicitly deny access to a relying party.
- Delegation authorization rules. These rules define the claims that specify which users can act on behalf of other users when accessing the relying party. This rule set can include rules that explicitly permit delegates for a relying party or rules that explicitly deny delegates for a relying party.



**Note:** A single claim rule can be associated with only a single federated trust relationship. This means that you cannot create a set of rules for one trust and then reuse those rules for other trusts that you configure on your federation server.

AD FS servers are preconfigured with a set of default rules and several default templates that you can use to create common claim rules. You can create custom claim rules by using the AD FS claim rule language.

## What is a claims provider trust?

A claims provider trust is configured on the relying party federation server. The *claims provider trust* identifies the claims provider and describes how the relying party consumes the claims that the claims provider issues. You must configure a claims provider trust for each claims provider. A claims provider trust for the local AD DS is configured by default. You must configure any additional claims providers.

By default, an AD FS server is configured with a claims provider trust named Active Directory. This trust defines the claim rules, which are all acceptance transform rules that define how the AD FS server accepts AD DS credentials. For example, the default claim rules on the claims provider trust include rules that transmit user names, security identifiers (SIDs), and group SIDs to the relying party. In a single-organization AD FS deployment where AD DS authenticates all users, the default claims provider trust might be the only required claims provider trust.

- Claims provider trusts:
  - Are configured on the relying party federation server
  - Identify the claims provider
  - Configure the claim rules for the claims provider
- In a single-organization scenario, a claims provider trust called Active Directory defines how AD DS user credentials are processed
- Claims provider trusts can be configured by:
  - Importing the federation metadata
  - Importing a configuration file
  - Manually configuring the trust

When you expand an AD FS deployment to include other organizations, you must create additional claims provider trusts for each federated organization that is an identity provider. When configuring a claims provider trust, you have three options:

- Import data about the claims provider through the federation metadata. If the AD FS federation server or federation server proxy is accessible through the network from your AD FS federation server, you can enter the host name or URL for the partner federation server. Your AD FS federation server connects to the partner server and downloads the federation metadata from the server. The federation metadata includes all the information that is required to configure the claims provider trust. As part of the federation metadata download, your federation server also downloads the SSL certificate that is used by the partner federation server.
- Import data about the claims provider from a file. Use this option if the partner federation server is not directly accessible from your federation server, but the partner organization has exported its configuration and provided you the information in a file. The configuration file must include configuration information for the partner organization and the SSL certificate that the partner federation server uses.
- Manually configure the claims provider trust. Use this option if you want to configure all of the settings for the claims provider trust. When you choose this option, you must provide the features that the claims provider supports and the URL that is used to access the claims provider AD FS servers. You must also add the SSL certificate that the partner organization uses.

## What is a relying party trust?

You define a relying party trust on the claims provider federation server. The *relying party trust* identifies the relying party and defines the claim rules that define how the relying party accepts and processes claims from the claims provider.

In a single-organization scenario, the relying party trust defines how the AD FS server interacts with the applications deployed within the organization. When you configure the relying party trust in a single organization, you provide the URL for the internal application. You can also configure settings such as the URL used by the web server, the issuance authorization rules for the application, and whether the application supports SAML 2.0 or whether it requires AD FS 1.0 tokens.

Configuring a relying party trust is similar to configuring a claims provider trust. When you expand the AD FS deployment to include other organizations, you must create additional relying party trusts for each federated organization. When configuring a relying party trust, you have three options:

- Import data about the relying party through the federation metadata. If the AD FS federation server or federation server proxy is accessible through the network from your AD FS federation server, you can enter the host name or URL for the partner federation server. Your AD FS federation server connects to the partner server and then downloads the federation metadata from the server. The federation metadata includes all the information that is required to configure the relying party trust. As part of the federation metadata download, your federation server also downloads the SSL certificate that the partner federation server uses.

- Relying party trusts:
  - Are configured on the claims provider federation server
  - Identify the relying party
  - Configure the claim rules for the relying party
- In a single-organization scenario, a relying party trust defines the connection to internal applications
- You can configure relying party trusts by:
  - Importing the federation metadata
  - Importing a configuration file
  - Manually configuring the trust

- Import data about the relying party from a file. Use this option if the partner federation server is not directly accessible from your federation server. In this case, the partner organization can export its configuration information to a file and then provide it to you. The configuration file must include configuration information for the partner organization and the SSL certificate that the partner federation server uses.
- Manually configure the relying party trust. Use this option if you want to configure all of the settings for the relying party trust.

## Demonstration: Configuring claims provider and relying party trusts

In this demonstration, you will see how to:

- Configure a claims provider trust.
- Configure a WIF application for AD FS.
- Configure a relying party trust.

### Demonstration Steps

#### Configure a claims provider trust

1. On **LON-DC1**, in **Server Manager**, open **AD FS Management**.
2. Go to **Claims Provider Trusts**, and then edit the claim rules for **Active Directory**.
3. Add an acceptance transform rule with the following settings:
  - Claim rule template: **Send LDAP Attributes as Claims**
  - Claim rule name: **Outbound LDAP Attributes Rule**
  - Attribute store: **Active Directory**
  - Mapping of LDAP attributes:
    - E-Mail-Addresses: **E-Mail Address**
    - User-Principal-Name: **UPN**

#### Configure a WIF application for AD FS

1. On **LON-SVR1**, open **Server Manager**, and then open the Windows Identity Foundation Federation Utility.
2. In the **Federation Utility Wizard**, enter the following:
  - Application configuration location: **C:\inetpub\wwwroot\AdatumTestApp\web.config**
  - Application URI: **https://lon-svr1.adatum.com/AdatumTestApp/**
  - **Use an existing STS**
  - STS WS-Federation metadata document location: **https://adfs.adatum.com/federationmetadata/2007-06/federationmetadata.xml**
  - **Disable certificate chain validation,**
  - **No encryption**

## Configure a relying party trust

1. On **LON-DC1**, in the **AD FS** console, add a relying party trust with the following settings:
  - **Import data about the relying party published online or on a local network**
  - Federation Metadata address: **https://lon-svr1.adatum.com/adatumtestapp/**
  - Display name: **A. Datum Corporation Test App**
  - **Permit everyone**
2. Leave the **Edit Claims Issuance Policy for A. Datum Corporation Test App** window open for the next task. (This window might be hidden behind Server Manager.)
3. On **LON-DC1**, in the **Edit Claim Issuance Policy for A. Datum Corporation Test App** window, add a rule on the **Issuance Transform Rules** tab.
4. Complete the **Add Transform Claim Rule Wizard** with the following settings:
  - Claim rule template: **Pass Through or Filter an Incoming Claim**
  - Claim rule name: **Pass through Windows account name**
  - Incoming claim type: **Windows account name**
  - **Pass through all claim values**
5. Create three more rules to pass through the **E-Mail Address**, **UPN**, and **Name** claim types.

**Question:** What are claim rules? What can you use claim rules for?

## Installing and configuring AD FS

Before deploying your federation service, you must prepare the environment for the installation of AD FS. This might include preparing the configuration database and any required service accounts and certificates and preparing the DNS host records for access from inside and outside the corporate network.

### SQL Server

If you plan to host the configuration database for the AD FS federation server farm in SQL Server, you should deploy the SQL Server instance prior to installing the first federation server. In Windows Server 2016, AD FS supports multiple options for the high availability of your federation server farm that uses SQL Server. You should consider one of these options when preparing for the configuration database.

- You might need to prepare the following items before installing AD FS:
  - SQL Server
  - Service account
  - Certificates
  - DNS
- During the deployment of AD FS, you:
  1. Install AD FS
  2. Configure AD FS
  3. Create the first federation server in a farm
  4. Add a federation server to a farm
  5. Update AD FS



**Note:** For more information, refer to: "Federation Server Farm Using SQL Server" at: <http://aka.ms/mok3lw>



## Service account

If possible, you should consider using a group Managed Service Account (gMSA) for AD FS. During deployment, the **AD FS Installation Wizard** automatically creates and configures a gMSA if you have appropriate permissions to AD DS. Otherwise, you should create a gMSA in advance of the AD FS federation server deployment.

If you are not able to use a gMSA, you should create a standard service account in AD DS prior to deploying the AD FS federation server and configure for the password to never expire. This service account requires the following access rights on the AD FS federation server:

- Log on as a service
- Log on as a batch job

## Certificate

Although you can import the certificate during the AD FS installation, you need to request the appropriate SSL certificate required for AD FS from a publicly trusted CA prior to deployment. When you receive the certificate from the CA, install it in the Personal certificate store on the AD FS federation server. If you are deploying a federation server farm, the subject name, or certificate common name (CN) on the SSL certificate must match the Federation Service name or be a wildcard SSL certificate name. This certificate should be installed in the Personal certificate store on each of the federation servers in the farm.

## DNS

In addition to AD DS, DNS is one of the primary network services that is critical to the operation of AD FS. With DNS record sets, users and other service providers can locate your federation service over the Internet and on your corporate network.

When configuring DNS to support AD FS, you should consider the following:

- If you are deploying a federation server farm, you will need to create a DNS host record on your internal DNS servers of the cluster DNS name for your NLB federation server farm.
- If you are deploying a standalone federation server, you will need to create a DNS host record on your internal DNS servers of the DNS name for your federation server.
- If you are deploying a federation proxy array, you will need to create a DNS host record on your perimeter DNS servers of the load-balanced DNS name for your AD FS proxy server or your Web Application Proxy server array.
- If you are deploying a standalone federation proxy server, you will need to create a DNS host record on your perimeter DNS servers of the DNS name for your AD FS proxy server or your Web Application Proxy server.
- If you are not deploying a federation proxy, you will need to create a DNS host record on your perimeter DNS servers of the cluster DNS name for your NLB federation server farm or your federation server.



**Note:** You should not use CNAME records for the Federation Service name.

## Installing AD FS

In Windows Server 2016, AD FS 3.0 is installed from Server Manager as a role. The **Server Manager Configuration Wizard** performs validation checks and automatically installs all the services required by AD FS. The AD FS server role includes Windows PowerShell cmdlets that you can use to perform a deployment based on Windows PowerShell of AD FS servers and proxies.

To install the AD FS server role, use the Server Manager **Add Roles and Features Wizard**, and select the AD FS server role. The **Add Roles and Features Wizard** automatically selects the Microsoft .NET Framework and AD FS Management Tools features. No other features are required.

### Configuring AD FS

When the AD FS role is installed, the **Add Roles and Features Wizard** provides you with the option of starting the **AD FS Configuration Wizard** to configure the AD FS server. The steps for the **AD FS Configuration Wizard** vary depending on whether you are creating the first federation server in a federation server farm or adding a federation server to a federation server farm. You can also start the **AD FS Configuration Wizard** from the **Tools** menu in Server Manager or from the Start screen.

### Creating the first federation server in a federation server farm

To create the first federation server in a federation server farm:

1. In the **AD FS Configuration Wizard**, select the **Create the first federation server in a federation server farm** option.
2. On the **Connect to AD DS** page, select the account that has domain administrator permissions to AD DS. If the account that you use to install AD FS has the appropriate permissions, leave the default option, and then proceed. Otherwise, change it to the appropriate account. The account that you select should not be the credentials of your service account.
3. On the **Specify Service Properties** page, select the corresponding certificate from the **SSL Certificate** list (or import the SSL certificate if you did not install it prior to the installation), and then specify the **Federation Service Name** of the federation server farm.
4. On the **Specify Service Account** page, specify the credentials of the appropriate service account for AD FS.
5. On the **Specify Configuration Database** page, select either the option to create a database by using WID or the option to specify the location, host name, and instance of an existing SQL Server database.
6. On the **Review Options** page, note that the wizard displays your selections, including your service account actions:
  - o If you chose to use a WID database, the wizard notes that this is the primary server in the farm and that the WID database is installed.
  - o If you chose to use an existing SQL Server database, the wizard notes that this will be the first server in the server farm and provides the connection string details for connecting to SQL Server to retrieve the configuration.
7. On the **Pre-requisite Checks** page, note that the wizard displays the results of the prerequisite check before proceeding to the installation of AD FS.




**Note:** Alternatively, you can use the Windows PowerShell cmdlet **Install-AdfsFarm** to deploy the first federation server in a federation server farm.

## Adding a federation server to a federation server farm


To add an additional server to an AD FS server farm:

1. In the **AD FS Configuration Wizard**, select the **Add a federation server to federation service farm** option.
2. On the **Connect to AD DS** page, select the account that has domain administrator permissions to AD DS. If the account that you use to install AD FS has the appropriate permissions, leave the default option, and then proceed. Otherwise, change it to the appropriate account. The account that you select should not be the credentials of your service account.
3. On the **Specify Farm** page, either specify the name of the primary federation server in a farm that uses WID or specify the database host name and the instance name of an existing federation server farm that uses SQL Server.
4. On the **Specify SSL Certificate** page, either select the corresponding certificate from the **SSL Certificate** list or import the SSL certificate if you did not install it prior to the installation. As opposed to the other installation option, you are not required to specify the federation service name of the federation server farm. This is because the wizard is already aware of the federation service name based on the database information that you provided earlier.
5. On the **Specify Service Account** page, specify the credentials of the appropriate service account for AD FS. The account you specify must be the same account as the one used on the primary federation server in the farm.
6. On the **Review Options** page, note that the wizard displays your selections:
  - o If you chose to use a WID database, the wizard notes that this is the secondary server in the farm and that the WID database is installed and replicated from the primary server in the farm.
  - o If you chose to use an existing SQL Server database, the wizard notes the connection string details for connecting to SQL Server to retrieve the configuration.
7. On the **Pre-requisite Checks** page, note that the wizard displays the results of the prerequisite check before proceeding to the installation of AD FS.

 **Note:** Alternatively, you can use the Windows PowerShell cmdlet **Add-AdfsFarmNode** to add a federation server to a federation server farm.

## Updating AD FS

To help ensure that your AD FS environment is reliable and stable, you should install the recommended updates for AD FS. After installing and configuring your AD FS federation servers, you can use Microsoft Update to check for available updates.

 **Note:** For more information on all the available updates for AD FS, refer to: "Updates for Active Directory Federation Services (AD FS)" at: <http://aka.ms/r8x4zf>

## Configuring an account partner and a resource partner

In a business-to-business AD FS scenario, the terminology that you use to describe the two partners involved in an AD FS deployment changes slightly. In this scenario, another name for the claims provider organization is the *account partner*. An account partner organization is an organization in which user accounts are stored in an attribute store. An account partner handles the following tasks:

- Gathering credentials from users who are using a web-based service and then authenticating those credentials.
- Building up claims for users and then packaging the claims into security tokens. The tokens can then be presented across a federation trust to gain access to federation resources that are located at the resource partner's organization.

- An account partner is a claims provider in a business-to-business federation scenario. To configure an account partner:
  - Implement the physical topology
  - Add an attribute store
  - Configure a relying party trust
  - Add a claim description
  - Prepare the client computers for federation
- A resource partner is a relying party in a business-to-business federation scenario. To configure a relying partner:
  - Implement the physical topology
  - Add an attribute store
  - Configure a claims provider trust
  - Create claim rule sets for the claims provider trust

To configure the account partner organization to prepare for federation, use the following steps:


1. Implement the physical topology for the account partner deployment. This step can include deciding on the number of federation servers and federation server proxies to deploy and configuring the required DNS records and certificates.
2. Add an attribute store. Use the **AD FS Management** console to add the attribute store. In most cases, you use the default Active Directory attribute store, which must be used for authentication, but you can also add other attribute stores, if required, to build the user claims. You connect to a resource partner organization by creating a relying party trust. The simplest way to do this is to use the federation metadata URL that is provided by the resource partner organization. With this option, your AD FS server automatically collects the information required for the relying party trust.
3. Add a claim description. The claim description lists the claims that your organization provides to the resource partner. This information might include user names, email addresses, group membership information, or other identifying information about users.
4. Prepare the client computers for federation. This might involve two steps:
  - Add the account partner federation server. In the browsers of the client computers, add the account partner federation server to the local intranet sites list. By adding the account partner federation server to the local intranet list on the client computers, you enable IWA, which means that the users will not be prompted for authentication if they are already signed in to the domain. You can use Group Policy Objects (GPOs) to assign the URL to the local intranet site list.
  - Configure certificate trusts. This is an optional step that is required only if one or more of the servers that the clients access do not have trusted certificates. The client computer might have to connect to the account federation servers, resource federation servers, or federation server proxies and to the destination web servers. If any of these certificates are not from a trusted public CA, you might have to add the appropriate certificate or root certificate to the certificate store on the clients. You can do this by using GPOs.

## Resource partner

The *resource partner* is the relying party in a business-to-business federation scenario. The resource partner organization is where the resources exist and where they are made accessible to account partner organizations. The resource partner handles the following tasks:

- Accepting security tokens that the account partner federation server produces and validates
- Consuming the claims from the security tokens and then providing new claims to its web servers after making an authorization decision

Web servers must have either WIF or the AD FS 1.x claims-aware web agent installed to externalize the identity logic and accept claims. WIF provides a set of development tools that allow developers to integrate claims-based authentication and authorization into their applications. WIF also includes a software development kit and sample applications.

 **Note:** You can use SAML tokens to integrate applications on non-Microsoft web servers with AD FS. Additional open-source or third-party software is typically necessary to support the use of SAML tokens on a non-Microsoft web server.

Configuring a resource partner organization is similar to configuring an account partner organization and consists of the following steps:

1. Implement the physical topology for the resource partner deployment. The planning and implementation steps are the same as those for the account partner, with the addition of planning the web server location and configuration.
2. Add an attribute store. The claims provider uses the attribute store to gather data that is necessary to issue the claims. Data from the attribute stores is then projected as claims to the client.
3. Connect to an account partner organization by creating a claims provider trust.
4. Create claim rule sets for the claims provider trust.

## Configuring claims rules

In a single-organization AD FS deployment, it might be simple to design and implement claims rules. In many cases, you might need to provide only the user or group name that AD FS collects from the claim and presents to the web server. In a business-to-business scenario, it is more likely that you have to configure more complicated claims rules to define user access between widely different systems.

- Business-to-business scenarios might require more-complex claims rules
- You can create claims rules by using the following templates:
  - Send LDAP Attributes as Claims
  - Send Group Membership as a Claim
  - Pass Through or Filter an Incoming Claim
  - Transform an Incoming Claim
  - Permit or Deny Users Based on an Incoming Claim
- You can also create custom rules by using the AD FS claim rule language

Claim rules define how account partners (claims providers) create claims and how resource partners (relying parties) consume claims. AD FS provides several rule templates that you can use when you configure claim rules:

- **Send LDAP Attributes as Claims.** Use this template when you select specific attributes in an LDAP attribute store to populate claims. You can configure multiple LDAP attributes as individual claims in a single claim rule that you create from this template. For example, you can create a rule that extracts the **sn** (surname) and **givenName** AD DS attributes from all authenticated users and then sends these values as outgoing claims to be sent to a relying party.
- **Send Group Membership as a Claim.** Use this template to send a particular claim type and an associated claim value that is based on the user's AD DS security group membership. For example, you might use this template to create a rule that sends a group claim type with a value of **SalesAdmin** if the user is a member of the Sales Manager security group within the AD DS domain. This rule issues only a single claim based on the AD DS group that you select as a part of the template.
- **Pass Through or Filter an Incoming Claim.** Use this template to set additional restrictions on which claims are submitted to relying parties. For example, you might want to use a user email address as a claim but forward the email address only if the domain suffix on the email address is *adatum.com*. When you use this template, you can either pass through whatever claim you extract from the attribute store configure rules that filter whether the claim is passed on based on various criteria.
- **Transform an Incoming Claim.** Use this template to map the value of an attribute in the claims provider attribute store to a different value in the relying party attribute store. For example, you might want to provide all members of the Marketing department at A. Datum Corporation limited access to a purchasing application at Trey Research. At Trey Research, the attribute used to define the limited access level might have an attribute of **LimitedPurchaser**. To address this scenario, you can configure a claims rule that transforms an outgoing claim with a Department value of Marketing to an incoming claim with an **ApplicationAccess** attribute value of **LimitedPurchaser**. Rules created from this template must have a one-to-one relationship between the claim at the claims provider and the claim at the relying partner.
- **Permit or Deny Users Based on an Incoming Claim.** This template is available only when you configure issuance authorization rules or delegation authorization rules on a relying party trust. Use this template to create rules that allow or deny access by users to a relying party, based on the type and value of an incoming claim. This claim rule template allows you to perform an authorization check on the claims provider before claims are sent to a relying party. For example, you can use this rule template to create a rule that permits only users from the Sales group to access a relying party, whereas authentication requests from members of other groups will not be sent to the relying party.

If none of the built-in claim rule templates provides the functionality that you require, you can create more-complex rules by using the AD FS claim rules language. By creating a custom rule, you can extract claims information from multiple attribute stores and combine claim types into a single claim rule.

## How home realm discovery works


Some resource partner organizations that host claims-aware applications might want to enable multiple account partners to access their applications. In this scenario, when users connect to the web application, there must be some mechanism for directing the users to the AD FS federation server in their home domain, rather than to another organization's federation server. The process for directing clients to the appropriate account partner is *home realm discovery*.


- Home realm discovery identifies the AD FS server responsible for providing claims about a user
- Two methods for home realm discovery exist:
  - Prompt users during their first authentication
  - Include a *whr* string in the application URL
- SAML applications can use a preconfigured profile for home realm discovery


Home realm discovery occurs after the client connects to the relying party's website and is redirected to the relying party's federation server. At this point, the relying party's federation server must redirect the client to the federation server in the client's home realm so that the user can authenticate. If there are multiple claims providers configured on the relying party's federation server, it has to know which federation server to redirect the client to.

In general, two ways to implement home realm discovery exist:

- Ask the users to select their home realm. With this option, when users are redirected to the relying party's federation server, the federation server can display a webpage that asks them to identify their company. After the users select the appropriate company, the federation server can use that information to redirect the client computers to the appropriate home federation server for authentication.
- Modify the link for the web application to pass the *whr* parameter that contains the user's home realm. The relying party's federation server uses this parameter to automatically redirect the user to the appropriate home realm. This means that the user does not have to be prompted to select the home realm, because the *WHR* parameter in the URL that the user clicks includes the needed information for the relying party's federation server. The modified link might look something like the following: <https://www.adatum.com/OrderApp/?whr=urn:federation:TreyResearch>.

 **Note:** One of the options available for home realm discovery with SAML 2.0-compliant applications is a SAML profile called IdPInitiated SSO. This SAML profile configures users to access their local claims provider first, which can prepare a user's token with the claims required to access the partner's web application. AD FS in Windows Server 2012 does not fully implement the IdPInitiated SSO profile, but it provides some of the same functionality by implementing a parameter named *RelayState*.

 **Additional Reading:** For more on *RelayState*, refer to: "Supporting Identity Provider Initiated RelayState" at: <http://aka.ms/Df8hq5>

 **Note:** The home realm discovery process occurs the first time a user tries to access a web application. After the user successfully authenticates, a home realm discovery cookie is issued to the client. This helps to ensure that the user does not have to go through the process the next time. However, this cookie expires after a month, unless the user clears the cookie cache prior to expiration.

## Demonstration: Configuring claims rules

In this demonstration, you will learn how to configure claim rules on a relying party trust that forwards a group name as part of the claim. You will also see how to configure a claims rule that limits application access to members of a particular group.

### Demonstration Steps

1. On **LON-DC1**, in the AD FS Manager, in the **Edit Claim Rules for A. Datum Corporation Test App** window, add an **Issuance Transform Rule** with the following settings:
  - Claim rule template: **Pass Through or Filter an Incoming Claim**
  - Claim rule name: **Send Group Name Rule**
  - Incoming claim type: **Group**
  - **Pass through all claim values**
2. Add a new access control policy rule with the following settings:
  - Access control policy: **Permit specific group**
  - Group name: **Research**
3. Edit the Claim Issuance Policy with the following settings:
  - Claim rule name: **Pass through UPN**
  - Incoming claim type: **UPN**
  - Incoming claim value: **@adatum.com**
4. View the rule language for the **Pass through UPN** rule.

## Managing an AD FS deployment

Although AD FS is deployed to support SSO without much administrative overhead, you might need to periodically perform many management tasks after you deploy AD FS. This topic describes two of the most common tasks.

### Managing the certificate life cycle


To prevent issues that are caused by certificate expiration, the self-signed, self-generated certificates that AD FS generates support automatic rollover, which renews AD FS certificates once a year without manual intervention. This AD FS process, called *automatic certificate rollover*, generates two new token-signing certificates every year. If Office 365 is not updated with the new token-signing certificate, no user can sign in and use Office 365, because this certificate signs all assertions from the federation server. If an internal PKI is used to issue the token-signing certificate, AD FS does not provide automatic certificate rollover, and you must therefore manually renew the certificates and update them in your Office 365 tenant.

- After the installation, you might need to perform periodic AD FS management tasks, including:
  - Managing the certificate life cycle
  - Using automatic certificate rollover, which renews AD FS certificates once a year
  - Using the **Get-ADFSertificate** cmdlet to view certificate expiration dates
  - Using the **Update-MSOLFederatedDomain** cmdlet to manage certificate rollover when the AD FS token-signing certificate renews on an annual basis
  - Using the **Set-AdfsSyncProperties** cmdlet to change the primary and secondary AD FS federation servers



You can use the **AD FS Management** console to view certificate expiration dates for the service communications, token-decrypting, and token-signing certificates. In the console tree, expand **Service**, and then click **Certificates**. You also can use the Azure AD Module for Windows PowerShell to view certificate details when you use the Windows PowerShell cmdlet **Get-ADFSCertificate**.

If you prefer to use automatic certificate rollover for managing the life cycles of your certificates, you need to enable the feature in AD FS and install the Office 365 Federation Metadata Update Automation Installation Tool. This feature is enabled in AD FS with the **Set-ADFSProperties** Windows PowerShell cmdlet. After installing the tool, you can use the **Update-MsolFederatedDomain** Windows PowerShell cmdlet to automatically update the Office 365 service when the AD FS token-signing certificate renews on an annual basis. This tool should be run as a daily scheduled task on the AD FS server; otherwise, token-signing certificate renewal on the AD FS server must be manually monitored. The update tool script scheduled task should be run only on one AD FS server in a federation server farm.

 **Note:** To learn more about and download the Office 365 Federation Metadata Update Automation Installation Tool, refer to: "Microsoft Office 365 Federation Metadata Update Automation Installation Tool" at: <http://aka.ms/i1hw8d>

### Changing the primary and secondary AD FS federation servers

If you use WID as the AD FS data store, you can change the primary and secondary federation servers if you use the Azure AD Module for Windows PowerShell. This method allows you to change the database role setting for the AD FS server and then change the role.

For example, if you want to change the primary federation server AdfsServer1 to the secondary federation server AdfsServer2, you use the following procedure:


1. Identify the secondary federation server (AdfsServer2) that will become the primary federation server.
2. On the secondary federation server (AdfsServer2), at the **Microsoft Azure AD Module for Windows PowerShell** prompt, type the following command, and then press Enter.

```
Set-AdfsSyncProperties -Role PrimaryComputer
```

3. On the primary federation server (AdfsServer1), at the **Microsoft Azure AD Module for Windows PowerShell** prompt, type the following command, and then press Enter.

```
Set-AdfsSyncProperties -Role SecondaryComputer -PrimaryComputerName AdfsServer2
```

The primary federation server becomes a secondary federation server with a read-only WID database, and the secondary federation server becomes the primary federation server with a read/write WID database from which other secondary federation servers retrieve their database copies.

 **Note:** Switching AD FS federation server roles does not apply if SQL Server is used as the AD FS configuration database store. This is because all AD FS federation servers have read/write access to the SQL Server database.

## Lesson 4

# Web Application Proxy overview

Many organizations need to extend the AD FS infrastructure beyond private networks and onto the Internet. To enhance security for AD FS and AD FS applications, you use the Web Application Proxy. It also is important to consider high availability for AD FS, because it is a critical service after it is implemented.

### Lesson Objectives

After completing this lesson, you will be able to:

- Describe the new features in the Web Application Proxy in Windows Server 2016.
- Describe how to configure an application for the Web Application Proxy.
- Describe the Web Application Proxy and AD FS.
- Explain how to install and configure the Web Application Proxy.


### What is the Web Application Proxy?

The Web Application Proxy in Windows Server 2016 is a remote access role service that you can use to help secure remote access to web-based applications on your internal network. The Web Application Proxy functions as both a reverse proxy for web-based applications and as an AD FS proxy.

You must place the Web Application Proxy in a perimeter network, because external clients that access web-based applications or AD FS initiate connections with the Web Application Proxy. The Web Application Proxy then connects to the web-based application or AD FS on the internal network. You do not need any client-specific configuration to use the Web Application Proxy.

When you implement the Web Application Proxy, you enhance security for web-based applications or AD FS by isolating them from direct contact with the Internet. This can help to protect the internal, web-based application or AD FS from any malformed packets or requests that might result in a security breach. For example, the Web Application Proxy can help to protect against a zero-day attack that uses malformed requests, which can result in a denial-of-service attack on a server that hosts a web-based application. The Web Application Proxy drops invalid requests before they reach the web-based application on an internal network.

Because the Web Application Proxy is completely independent of the web server software being used, it is unlikely that the Web Application Proxy is as vulnerable to the same denial-of-service attack as a web-based application.


 **Note:** The Web Application Proxy uses AD FS to preauthenticate Internet users, and it acts as an AD FS proxy for publishing claims-aware applications.

Windows Server 2016 includes several improvements to the Web Application Proxy role, including:

- Preauthentication for HTTP Basic app publishing
- Wildcard domain publishing of apps
- HTTP to HTTPS redirection
- HTTP publishing

AD FS provides users with an SSO capability, which allows users to enter their credentials to access an organizational web application without being prompted to enter their credentials again. With the Web Application Proxy, you can publish both claims-aware applications that use AD FS preauthentication and web applications that use pass-through preauthentication.


Usually, you place the Web Application Proxy in your perimeter network between two firewall devices.

 **Note:** The AD FS server and applications that are published are located in the organizational network with domain controllers and other internal servers, and the second firewall helps to protect them. This scenario helps to provide secure access to organizational applications for users on the Internet. At the same time, this scenario helps to protect the organization's IT infrastructure from security threats from the Internet.

### Improvements in the Web Application Proxy in Windows Server 2016

Windows Server 2016 includes several improvements to the Web Application Proxy role, including:

- Preauthentication for HTTP Basic application publishing. HTTP Basic is the authorization protocol that is used by many protocols, including Exchange ActiveSync, to connect devices, including smartphones, with Exchange Server mailboxes.

 **Note:** The Web Application Proxy interacts with AD FS by using redirection, which is not supported on Exchange ActiveSync clients.

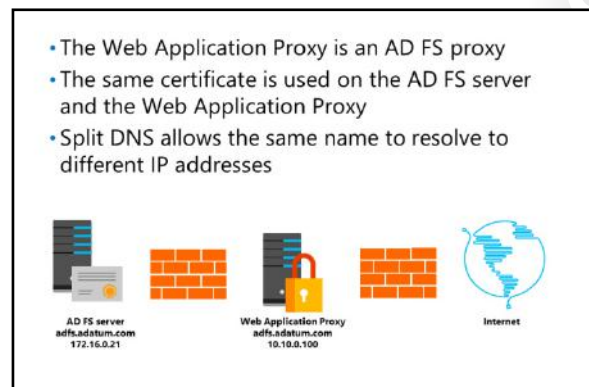
The Web Application Proxy in Windows Server 2016 allows you to publish an app that uses HTTP Basic by enabling the HTTP app to receive a non-claims relying party trust for the app to the Federation Service.

- Wildcard domain publishing for applications to simplify the publishing of Microsoft SharePoint apps. To support scenarios such as those that use SharePoint 2013, the external URL for the application can now include a wildcard that allows you to publish multiple applications from within a specific domain. An example URL is `https://*.sp-apps.adatum.com`.
- HTTP to HTTPS redirection. To help ensure that your users can access your app, even if they neglect to type **HTTPS** in the URL, the Web Application Proxy in Windows Server 2016 now supports HTTP to HTTPS redirection.
- HTTP publishing. You can now publish HTTP applications by using pass-through preauthentication.

### Web Application Proxy and AD FS proxy

Many organizations need to provide authentication for users and devices that are located on a network that is external to the organization. In most cases, allowing clients to access an AD FS server located on an internal network directly from the Internet is an unacceptable security risk. We recommend an AD FS proxy to allow clients on the Internet to access AD FS.

An AD FS proxy is a reverse proxy located in a perimeter network that is specifically for AD FS.



Clients from the Internet communicate with the AD FS proxy in the perimeter network instead of directly with the AD FS server. The AD FS proxy mitigates the risks associated with Internet connectivity for AD FS.



**Note:** The term *AD FS proxy* referenced here is a generic term for a server that provides indirect network connections to the Federation Service and is not a direct reference to the AD FS Proxy Server in Windows Server 2012.

### Authentication process

An internal AD FS server uses Windows authentication to prompt for authentication. This works well for internal computers that are joined to the domain and can automatically pass workstation credentials to AD FS to automate authentication. This prevents users from seeing a request for authentication credentials.

When computers that are not joined to the domain communicate with AD FS, the web browser presents the users with a sign-in prompt. This sign-in prompt asks for a user name and password but provides no context.

When you use an AD FS proxy, an authentication webpage is provided for computers that are not joined to the domain. This provides better compatibility than browser-based Windows authentication for AD FS clients that use non-Microsoft operating systems. You also can customize the webpage to provide more context for users, by adding a company logo, for example.

### DNS resolution

To provide seamless movement between internal and external networks, the Web Application Proxy uses the same host name when accessing AD FS internally and externally. On the internal network, the AD FS host name resolves to the IP address of the internal AD FS server. On the external network, the AD FS host name resolves to the IP address of the AD FS proxy. In both cases, the AD FS host name is different from those of the computers that host the AD FS roles.

### Certificates

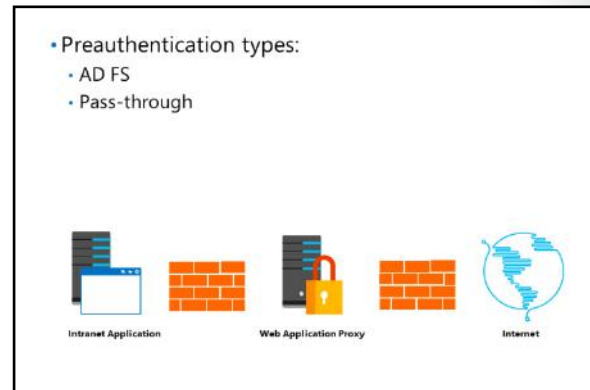
The certificate used on an internal AD FS server has a subject name that is the same as the host name for AD FS—for example, `adfs.adatum.com`. Because the same host name is used to access AD FS internally and externally through the AD FS proxy, you need to configure the AD FS proxy with the same certificate as the AD FS server. If the certificate subject does not match the host name, AD FS authentication will fail.



**Note:** To help ensure that you have a certificate with the same subject name, export the certificate from the AD FS server and import it on the Web Application Proxy server. Remember to include the private key when you export the certificate.

## Web Application Proxy authentication methods

The Web Application Proxy is used to help protect web applications and AD FS when they are accessible from the Internet. You should place the Web Application Proxy server in a perimeter network. To install the Web Application Proxy, you must have already implemented AD FS in your organization. All configuration information for the Web Application Proxy is stored in AD FS. When you use the Web Application Proxy as a reverse proxy for web applications, you need to configure each application. For each application, you need to configure the type of preauthentication for the application and URLs.



### Pass-through preauthentication

When you use pass-through preauthentication, no preauthentication is performed, and valid requests are passed to web-based applications on an internal network without performing authentication on a user. The application performs all authentication for an application only after a user is connected. You can use pass-through preauthentication for any web application.

Preauthentication helps to protect a web application from malformed packets that can cause a denial-of-service attack. However, the web application is not protected from application-level threats when the application mishandles valid data. For example, an HTTPS request with valid HTTP commands is passed through to the application, even if the actions requested by the HTTP commands might cause the web application to fail.

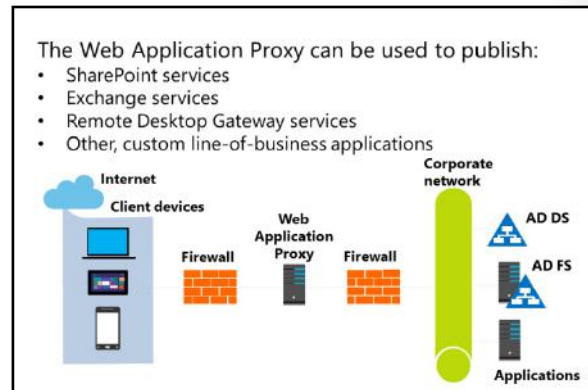
### AD FS preauthentication

You can configure the Web Application Proxy to use AD FS preauthentication or pass-through authentication. When you use AD FS for preauthentication, AD FS authenticates a user request before passing it to an internal, web-based application. This helps to ensure that only authorized users can send data to a web-based application. AD FS preauthentication provides a greater level of protection than pass-through authentication, because unauthenticated users cannot submit requests to the application.

Only a claims-aware application that uses AD FS for authentication can use AD FS preauthentication. You must configure the claims-aware application in AD FS as a relying party and select it from a list when the Web Application Proxy is configured. The Web Application Proxy is aware of the relying parties configured in AD FS because of the integration between AD FS and the Web Application Proxy.

## Scenarios for using the Web Application Proxy

With the Web Application Proxy, organizations can provide selective access to applications running on servers inside the organization to users located outside of the organization. The process to make the application externally available is known as *publishing*. Unlike traditional virtual private network (VPN) solutions, users can access only the applications that you publish through a Web Application Proxy server. Depending on support from the application, access to these applications can be from essentially any device, including mobile devices.



In addition to publishing federation services, the Web Application Proxy server is widely used to publish browser applications, such as those for SharePoint, Exchange, and Remote Desktop Gateway (RD Gateway) and other, custom line-of-business (LOB) applications. In fact, it is also possible to publish HTTP back-end services that are consumed by non-browser applications.

### Configuring URLs and certificates

For each application that you publish, you must configure an external URL and an internal server URL. External users access the application by using the external URL. The Web Application Proxy server uses the internal server URL to access the application on behalf of external users.

If you use split DNS, it is common to have the same value for both the external URL and the internal server URL. Some applications experience errors when the external URL and the internal server URL differ. When the external URL and the back-end server URL differ, only the host name in the URL changes. The path to the application remains the same. For example, if the internal URL for an application is `https://server1.adatum.com/app1`, you cannot have an external URL of `https://extranet.adatum.com/application1`.

When you define the external URL, you also need to select a certificate that contains the host name in the external URL. This certificate must be installed on the local server. However, it does not need to match the certificate used on the back-end server hosting the application. You can have one certificate for each host name used on the Web Application Proxy server or a single certificate with multiple names.

### Publishing SharePoint services


You can publish a SharePoint site through a Web Application Proxy server when the SharePoint site is configured for claims-based authentication or IWA. If you prefer to use AD FS for preauthentication, you must configure a relying party by using one of these methods:

- If the SharePoint site uses claims-based authentication, use the **Add Relying Party Trust Wizard** to configure the relying party trust for the application.
- If the SharePoint site uses IWA, use the **Add Non-Claims-Based Relying Party Trust Wizard** to configure the relying party trust for the application. If you want to use IWA with a claims-based web application, you must deploy the Kerberos Key Distribution Center to the domain controllers in the domain.



**Note:** To authenticate the users by using IWA, the Web Application Proxy server must be joined to the domain.

To provide IWA access, the Web Application Proxy server must be able to provide the impersonation of users to the published application. This impersonation is called *Kerberos constrained delegation*, and the application should be configured to support impersonation. You should configure the Web Application Proxy server for delegation to the service principal names (SPNs) of the back-end servers.

 **Additional Reading:** For more information on configuring a website to use IWA and Kerberos constrained delegation, refer to: "Configure a site to use Integrated Windows authentication" at: <http://aka.ms/Nbsbll>

If your SharePoint site is configured by using alternate access mappings or host-named site collections, you can publish your application with different external and back-end server URLs. However, if your SharePoint site is not configured by using alternate access mappings or host-named site collections, the external and back-end server URLs must be the same.

### Publishing Exchange services


Exchange Server provides multiple services for administrators and users, including Outlook Web App, Exchange Control Panel, Outlook Anywhere, and Exchange ActiveSync. These services are independent with different URLs and different authentication configurations. The following table describes the Exchange services that you can publish through the Web Application Proxy and the supported preauthentication types for these services.

Exchange service	Supported preauthentication types
Outlook Web App	<ul style="list-style-type: none"> <li>• AD FS using non-claims-based authentication</li> <li>• Pass-through</li> <li>• AD FS using claims-based authentication for Exchange Server 2013</li> </ul>
Exchange Control Panel	<ul style="list-style-type: none"> <li>• Pass-through</li> </ul>
Outlook Anywhere	<ul style="list-style-type: none"> <li>• Pass-through</li> </ul>
Exchange ActiveSync	<ul style="list-style-type: none"> <li>• Pass-through</li> </ul>

For the Outlook Anywhere service to function correctly, you need to publish three URLs:

- The Autodiscover URL
- The external host name of the Exchange Server (that is, the URL that Outlook clients access)
- The internal FQDN of the Exchange Server instance

To publish Outlook Web App by using IWA, you must use the **Add Non-Claims-Based Relying Party Trust Wizard** to configure the relying party trust for the application.

 **Note:** To allow users to authenticate by using IWA, the Web Application Proxy server must be joined to the domain.

To provide IWA access, the application on the Web Application Proxy server should be configured to support Kerberos constrained delegation. You should also register an SPN for the service account of the web service and configure the Web Application Proxy server for delegation to the SPN of the back-end servers. In a highly available Exchange environment, you should use an alternate service account.



**Additional Reading:** For more information on configuring Kerberos authentication for load-balanced Exchange servers, refer to: "Configuring Kerberos authentication for load-balanced Client Access servers" at: <http://aka.ms/Nd2avi>

## Publishing Remote Desktop Gateway services

Some organizations provide access to RD Gateway services from the Internet directly to the RD Gateway server. However, you might consider publishing RD Gateway services through the Web Application Proxy if you want to restrict access to your RD Gateway and add preauthentication for remote users. When planning your deployment, you have two options for publishing RD Gateway services through the Web Application Proxy:

- Publishing the application by using pass-through authentication.

Publishing the application with pass-through authentication provides a single point of entry into your Remote Desktop environment. However, the deployment method will vary depending on whether your Remote Desktop Web Access (RD Web Access) (**/rdweb** virtual directory) and RD Gateway (**/rpc** virtual directory) roles are on the same server or on different servers:

- If the RD Web Access and the RD Gateway roles are hosted on the same RD Gateway server, you simply publish the RD Gateway root FQDN through the Web Application Proxy (for example., <https://rdg.contoso.com/>).
- If the RD Web Access and the RD Gateway roles are hosted on separate RD Gateway servers, you need to individually publish the two virtual directories. In this scenario, the published applications can use the same or different external FQDNs. For example:
  - Using the same FQDN, the URLs might be <https://rdg.contoso.com/rdweb/> and <https://rdg.contoso.com/rpc/>.
  - Using different FQDNs, the URLs might be <https://rdweb.contoso.com/rdweb/> and <https://gateway.contoso.com/rpc/>.
- Publishing the application by using preauthentication.

Similarly, to the way you publish a claims-based application, you use the **Add Relying Party Trust Wizard** to create a *manual relying party trust* to the RD Gateway FQDN. Using this process means that you have to create a dummy relying party trust to enforce preauthentication so that clients can use preauthentication without Kerberos constrained delegation to the published server.


When a user authenticates to the application for the published RD Gateway server by using the Remote Desktop Connection client (mstsc.exe), the back-end server responds to the client that preauthentication is required. In turn, the client receives a Web Application Proxy cookie that is obtained through the browser. This cookie is then used by the Remote Desktop Connection client as proof of authentication.



**Note:** You need to disable the **HttpOnly** attribute on the published application to allow the Remote Desktop Connection client to use the Web Application Proxy cookie obtained through the browser.


Users authenticating to the RD Web Access server still use the RD Web Access sign-in form. This provides the fewest number of user authentication prompts, because the RD Web Access sign-in form creates a client-side credential store, which can then be used by the Remote Desktop Connection client for any subsequent remote app launch.



 **Additional Reading:** For more information on publishing RD Gateway through the Web Application Proxy, refer to: "Publishing Applications with SharePoint, Exchange and RDG" at: <http://aka.ms/C7f0wn>

## Installing and configuring the Web Application Proxy

In preparation for deploying your Federation Service, you might need to prepare a few items before you install the Web Application Proxy. However, you should not begin implementing the Web Application Proxy until you have deployed the AD FS federation server farm.

 **Note:** You can deploy the Web Application Proxy only on Windows Server 2012 R2 or later. Alternatively, you deploy the AD FS proxy to use a proxy for the Federation Service on Windows Server 2012 R2 or earlier.

- You might need to prepare the following items before installing the Web Application Proxy:
  - Certificates
  - Load balancing
  - DNS
- During the deployment of the Web Application Proxy, you will:
  - Install the Web Application Proxy
  - Configure the Web Application Proxy
  - Update the Web Application Proxy

### Certificate

Because you are not able to import the certificate during the installation of the Web Application Proxy, you must request the appropriate SSL certificate required for the Web Application Proxy from a publicly trusted CA prior to the deployment. Upon receiving the certificate from the CA, you must install it in the Personal certificate store on the Web Application Proxy server.

In most scenarios, you use the SSL certificate from the AD FS federation server farm for the Web Application Proxy. However, if the AD FS federation server farm is supporting IWA through the Web Application Proxy, with Extended Protection for Authentication enabled, you are required to use the same SSL certificate. If this scenario applies to your AD FS environment, you should export the SSL certificate from one of the federation servers in the farm, and then import it into the Personal certificate store on the Web Application Proxy server.

With either scenario, if you deploy more than one Web Application Proxy server in support of your AD FS environment, you need to import the appropriate SSL certificate to each of the additional Web Application Proxy servers prior to installing the Web Application Proxy. This applies to wildcard certificates, as well.

### Load balancing

When you deploy two or more Web Application Proxy servers in an array, you need to configure them for NLB. You can accomplish this with hardware, which is recommended for large deployments, or with software, which is recommended for small-to-medium deployments. For software load balancers, you can enable NLB for the Web Application Proxy array.

### DNS

You should configure a DNS host record on the perimeter DNS servers prior to installing the Web Application Proxy server. Because the Web Application Proxy server is typically placed in the perimeter network, we recommend that you:

- Configure the Web Application Proxy server to use external DNS servers for external name resolution.
- Add an internal host name that the Web Application Proxy server needs to resolve, such as that of the internal AD FS farm, to the **Hosts** file on the Web Application Proxy server.



**Note:** You should not use CNAME records for the Web Application Proxy server name.

## Installing the Web Application Proxy

On Windows Server 2012 R2 and later, the Web Application Proxy is installed from Server Manager as a role. The **Server Manager Configuration Wizard** performs validation checks and automatically installs the service required by the Web Application Proxy. The Web Application Proxy server role service includes Windows PowerShell cmdlets that you can use to perform a Windows PowerShell–based deployment.

To install the Web Application Proxy server role service, use the **Server Manager Add Roles and Features Wizard**, and select the Remote Access server role. On the **Role services** page, select the **Web Application Proxy role service**. The **Add Roles and Features Wizard** automatically installs the required features, including the **Remote Access Management** console.



**Note:** Alternatively, you can use the Windows PowerShell cmdlet **Install-WindowsFeature Web-Application-Proxy** to install the Web Application Proxy server role service.

## Configuring the Web Application Proxy

After the Web Application Proxy role server service is installed, you must launch the **Remote Access Management** console to configure Web Application Proxy for publishing AD FS. You can initiate the **Remote Access Management** console from the **Tools** menu in Server Manager or from the Start screen. The steps for configuring each Web Application Proxy server in your environment for AD FS are the same:

1. In the **Remote Access Management** console, select the option to run the **Web Application Proxy Configuration Wizard**.
2. On the **Federation Server** page, specify the name of the Federation Service farm, and use the credentials of an account with local administrator permissions on the AD FS federation servers.
3. On the **AD FS Proxy Certificate** page, select the appropriate SSL certificate to complete the configuration.



**Note:** Alternatively, you can use the Windows PowerShell cmdlet **Install-WebApplicationProxy** to configure the Web Application Proxy for publishing AD FS.

## Updating the Web Application Proxy

To help ensure that your AD FS environment is reliable and stable, you should install the recommended updates for the Web Application Proxy. After installing and configuring your Web Application Proxy servers, you can use Microsoft Update to check for available updates.



**Note:** For more information on all the available updates for AD FS, refer to: "Updates for Active Directory Federation Services (AD FS)" at: <http://aka.ms/PI09m2>

## Demonstration: Installing and configuring the Web Application Proxy

In this demonstration, you will learn how to:

- Install the Web Application Proxy.
- Export the certificate from the AD FS server.
- Import the certificate to the Web Application Proxy server.
- Configure the Web Application Proxy.

### Demonstration Steps

#### Install the Web Application Proxy

- On **LON-SVR2**, open **Server Manager**, add the **Remote Access** server role and the **Web Application Proxy** role service.

#### Export the adfs.adatum.com certificate from LON-DC1

1. On **LON-DC1**, open **Microsoft Management Console**, and then add the **Certificates** snap-in for the **Local Computer**.
2. From the **Personal** folder, export the **adfs.adatum.com** certificate by using the following settings:
  - **Yes, export the private key**
  - File format: **Personal Information Exchange - PKCS #12 (.PFX)**
  - Password: **Pa\$\$w0rd**
  - File name: **C:\adfs.pfx**

#### Import the adfs.adatum.com certificate onto LON-SVR2

1. On **LON-SVR2**, open **Microsoft Management Console**, and then add the **Certificates** snap-in for the **Local Computer**.
2. From the **Personal** folder, import the **adfs.adatum.com** certificate by using the following settings:
  - File name: **\\LON-DC1\c\$\adfs.pfx**
  - Password: **Pa\$\$w0rd**
  - **Mark this key as exportable. This will allow you to back up or transport your keys at a later time**
  - Certificate store: **Personal**

#### Configure the Web Application Proxy

1. On **LON-SVR2**, in **Server Manager**, click the **Notifications** icon, and then click **Open the Web Application Proxy Wizard**.
2. In the **Web Application Proxy Wizard**, provide the following configuration settings:
  - Federation service name: **adfs.adatum.com**
  - User name: **Adatum\Administrator**
  - Password: **Pa\$\$w0rd**
  - Certificate to be used by the AD FS proxy: **adfs.adatum.com**

**Check Your Knowledge**

Question	
<b>Which of the following statements about configuring the Web Application Proxy is true? (Choose all that apply.)</b>	
Select the correct answer.	
<input type="checkbox"/>	To install the Web Application Proxy, you must have implemented AD FS in your organization.
<input type="checkbox"/>	To install the Web Application Proxy, you need not have implemented AD FS in your organization.
<input type="checkbox"/>	For each application that you publish, you must configure an external URL and an internal server URL.
<input type="checkbox"/>	When you define the external URL, you must also select a certificate that contains the host name in the internal URL.
<input type="checkbox"/>	When you define the external URL, you must also select a certificate that contains the host name in the external URL.

## Lab: Implementing AD FS

### Scenario

A. Datum Corporation has set up a variety of business relationships with other companies and customers. Some of these partner companies and customers need to access business applications that are running on the A. Datum Corporation network. The business groups at A. Datum Corporation want to provide maximum level of functionality and access to these companies. The Security and Operations departments want to help ensure that the partners and customers can access only the resources that they are authorized for and that implementing the solution does not significantly increase the workload for the Operations team. A. Datum Corporation is also working on the migration of some parts of its network infrastructure to online services, including Azure and Office 365.

To meet these business requirements, A. Datum Corporation is planning to implement AD FS. In the initial deployment, the company is planning to use AD FS to implement SSO for internal users accessing an application on a web server. A. Datum Corporation has also entered into a partnership with another company, Trey Research. Trey Research users should be able to access the same application.

As one of the senior network administrators at A. Datum Corporation also, it is your responsibility to implement the AD FS solution. As a proof of concept, you are deploying a sample claims-aware application and configuring AD FS to allow both internal users and Trey Research users to access the same application.

### Objectives

After completing this lab, you will be able to:

- Configure the AD FS prerequisites.
- Install and configure AD FS.
- Configure and validate SSO for a single organization.
- Configure and validate SSO for a business federation scenario.

### Lab Setup

Estimated Time: 90 minutes

Virtual machines: **20742A-LON-DC1**, **20742A-LON-DC2**, **20742A-LON-SVR1**, and **20742A-LON-CL1**

User name: **Adatum\Administrator**

Password: **Pa\$\$w0rd**

Virtual machine: **20742A-TREY-DC1**.

User name: **TreyResearch\Administrator**

Password: **Pa\$\$w0rd**

For this lab, you will use the available virtual machine environment. Before you begin the lab, complete the following steps:

1. On the host computer, start **Hyper-V Manager**.
2. In Hyper-V Manager, click **20742A-LON-DC1**, and then in the **Actions** pane, click **Start**.
3. In Hyper-V Manager, click **20742A-LON-DC2**, and then in the **Actions** pane, click **Start**.
4. For both domain controllers, in the **Actions** pane, click **Connect**. Wait until the virtual machine starts.

5. Sign in by using the following credentials:
  - o User name: **Adatum\Administrator**
  - o Password: **Pa\$\$w0rd**
6. Repeat steps 3 through 5 for **20742A-LON-SVR1** and for **20742A-LON-CL1**.
7. Repeat steps 3 through 4 for **20742A-TREY-DC1**. Sign in as **TreyResearch\Administrator** with the password of **Pa\$\$w0rd**.

## Exercise 1: Configuring the AD FS prerequisites

### Scenario

To deploy AD FS at A. Datum Corporation, you must verify that all the required components are configured. You plan to verify that AD CS is deployed in the organization and then configure the certificates required for AD FS on the AD FS server and on the web servers. You also plan to configure the DNS forwarders to enable communication between Adatum.com and TreyResearch.net.

The main tasks for this exercise are as follows:

1. Configure the DNS forwarders.
2. Configure the certificate trusts.
3. Request and install a certificate for the web server.

#### ► Task 1: Configure the DNS forwarders

1. On **LON-DC1**, use DNS Manager to create a new conditional forwarder with the following settings:
  - o DNS Domain: **TreyResearch.net**
  - o IP address of the master server: **172.16.10.10**
  - o **Store this conditional forwarder in Active Directory and replicate it as follows: All DNS servers in this forest**
2. On **TREY-DC1**, use DNS Manager to create a new conditional forwarder with the following settings:
  - o DNS Domain: **Adatum.com**
  - o IP address of the master server: **172.16.0.10**
  - o **Store this conditional forwarder in Active Directory and replicate it as follows: All DNS servers in this forest**



**Note:** In a production environment, it is likely that you will use Internet DNS instead of conditional forwarders.

#### ► Task 2: Configure the certificate trusts

1. On **LON-DC1**, use File Explorer to copy **TREY-DC1.TreyResearch.net\_TreyResearchCA.crt** from **\\TREY-DC1\CertEnroll** to **C:\**.
2. Open **Group Policy Management**, and then edit the **Default Domain Policy**.
3. In **Group Policy Management Editor**, go to **Computer Configuration\Policies\Windows Settings\Security Settings\Public Key Policies\Trusted Root Certification Authorities**.
4. Import **C:\TREY-DC1.TreyResearch.net\_TreyResearchCA.crt** as a trusted root CA.

5. On **TREY-DC1**, use File Explorer to go to **\\LON-DC1\CertEnroll**.
6. Right-click **LON-DC1.Adatum.com\_AdatumCA.crt**, and then install the certificate into the **Trusted Root Certification Authorities** store.
7. On **LON-SVR1**, run **Gpupdate**.



**Note:** If you obtain certificates from a trusted CA, you do not need to configure a certificate trust between the organizations.

► **Task 3: Request and install a certificate for the web server**

1. On **LON-SVR1**, from **Server Manager**, open **Microsoft Internet Information Services (IIS) Manager**, and then view the server certificates.
2. Create a new domain certificate with the following settings:
  - Common name: **lon-svr1.adatum.com**
  - Organization: **A. Datum Corporation**
  - Organizational unit: **IT**
  - City/locality: **London**
  - State/Province: **England**
  - Country/region: **GB**
  - Certification Authority: **AdatumCA**
  - Friendly name: **AdatumTestApp Certificate**
3. Add an HTTPS binding for the default website by using the following setting:
  - SSL certificate: **AdatumTestApp Certificate**

**Results:** After completing this exercise, you should have successfully enabled DNS resolution and certificate trusts between the domains. Also, you will have enabled an SSL certificate for the website and validated access to it.

## Exercise 2: Installing and configuring AD FS

### Scenario

The first scenario for implementing the proof-of-concept AD FS application is to ensure that internal users can use SSO to access the web application. You plan to configure the AD FS server and a web application to enable this scenario. You also want to verify that internal users can access the application. To start the AD FS implementation, you will install AD FS on the A. Datum Corporation domain controller and configure the server as a standalone federation server. You will also configure the server to use a CA-signed token-signing certificate.

The main tasks for this exercise are as follows:

1. Create a DNS record for AD FS.
2. Install AD FS.
3. Configure AD FS.
4. Verify AD FS functionality.

#### ► Task 1: Create a DNS record for AD FS

- On **LON-DC1**, use DNS Manager to add a new host record for AD FS:
  - Forward lookup zone: **Adatum.com**
  - Name: **adfs**
  - IP address: **172.16.0.10**

#### ► Task 2: Install AD FS

1. On **LON-DC1**, click **Start**, right-click **Windows PowerShell**, and then click **Run as Administrator**.
2. Run the following command to create the Microsoft Group Key Distribution Service root key to generate gMSA passwords for the account that will be used later in this lab.

```
Add-KdsRootKey -EffectiveTime ((get-date).addhours(-10))
```

3. Open **Server Manager**, and then add the **Active Directory Federation Services** role.

#### ► Task 3: Configure AD FS

1. On **LON-DC1**, in **Server Manager**, click the **Notifications** icon, and then click **Configure the federation services on this server**.
2. Use the following options to configure the AD FS server:
  - **Create the first federation server in a federation server farm**
  - Account for configuration: **Adatum\Administrator**
  - SSL Certificate: **adfs.adatum.com**
  - Federation Service Display Name: **A. Datum Corporation**
  - Create a Group Managed Service Account: **Adatum\ADFSservice**
  - **Create a database on this server using Windows Internal Database**



**Note:** The adfs.adatum.com certificate was preconfigured for this task. In your own environment, you must obtain this certificate.



#### ► Task 4: Verify AD FS functionality

1. On **LON-CL1**, open Internet Explorer, and then go to **https://adfs.adatum.com/federationmetadata/2007-06/federationmetadata.xml**.
2. Verify that the file loads, and then close Internet Explorer.

**Results:** After completing this exercise, you should have successfully installed and configured AD FS. You also should have verified that it is functioning by viewing the contents of the **FederationMetaData.xml** file.

### Exercise 3: Configuring an internal application for AD FS

#### Scenario

The first scenario for implementing the proof-of-concept AD FS application is to ensure that internal users can use SSO to access the web application. You plan to configure the AD FS server and a web application to enable this scenario. You also want to verify that internal users can access the application.

The main tasks for this exercise are as follows:

1. Configure the Active Directory claims provider trust.
2. Configure the application to trust incoming claims.
3. Configure a relying party trust for the claims-aware application.
4. Configure claim rules for the relying party trust.
5. Test access to the claims-aware application.
6. Configure Internet Explorer to automatically pass local credentials to the application.

#### ► Task 1: Configure the Active Directory claims provider trust

1. On **LON-DC1**, in **Server Manager**, open AD FS Management.
2. Go to **Claims Provider Trusts**, and then edit the claim rules for **Active Directory**.
3. Add an acceptance transform rule with the following settings:
  - Claim rule template: **Send LDAP attributes as claims**
  - Name: **Outbound LDAP Attributes Rule**
  - Attribute store: **Active Directory**
  - Mapping of LDAP attributes to outgoing claim types:
    - E-Mail-Addresses: **E-Mail Address**
    - User-Principal-Name: **UPN**
    - Display-Name: **Name**

► **Task 2: Configure the application to trust incoming claims**

1. On **LON-SVR1**, open **Server Manager**, and then open the Windows Identity Foundation Federation Utility.
2. In the **Federation Utility Wizard**, use the following information:
  - Application configuration location: **C:\inetpub\wwwroot\AdatumTestApp\web.config**
  - Application URI: **https://lon-svr1.adatum.com/AdatumTestApp/**
  - **Use an existing STS**
  - STS WS-Federation metadata document location: **https://adfs.adatum.com/federationmetadata/2007-06/federationmetadata.xml**
  - **Disable certificate chain validation**
  - **No encryption**

► **Task 3: Configure a relying party trust for the claims-aware application**

1. On **LON-DC1**, in the **AD FS** console, add a relying party trust with the following settings:
  - **Import data about the relying party published online or on a local network**
  - Federation Metadata address: **https://lon-svr1.adatum.com/adatumtestapp/**
  - Display name: **A. Datum Corporation Test App**
  - **Permit everyone**
2. Leave the **Edit Claims Issuance Policy for A. Datum Corporation Test App** window open for the next task. (This window might be hidden behind Server Manager.)

► **Task 4: Configure claim rules for the relying party trust**

1. On **LON-DC1**, in the **Edit Claim Issuance Policy for A. Datum Corporation Test App** window, on the **Issuance Transform Rules** tab, add a rule.
2. Complete the **Add Transform Claim Rule Wizard** with the following settings:
  - Claim rule template: **Pass Through or Filter an Incoming Claim**
  - Claim rule name: **Pass through Windows account name**
  - Incoming claim type: **Windows account name**
  - **Pass through all claim values**
3. Create three more rules to pass through the **E-Mail Address**, **UPN**, and **Name** claim types.

► **Task 5: Test access to the claims-aware application**

1. On **LON-CL1**, use Internet Explorer to access **https://lon-svr1.adatum.com/AdatumTestApp/**.



**Note:** It is critical to use the trailing forward slash (/) in the URL for step 1.

2. When prompted, sign in as **Adatum\Adam** with the password **Pa\$\$wOrd**.
3. Review the claim information that is displayed by the application, and then close Internet Explorer.

### ► Task 6: Configure Internet Explorer to automatically pass local credentials to the application

1. On **LON-CL1**, in Internet Explorer, open **Internet Options**.
2. On the **Security** tab, add the following sites to the **Local intranet** zone:
  - **https://adfs.adatum.com**
  - **https://lon-svr1.adatum.com**
3. Use Internet Explorer to access **https://lon-svr1.adatum.com/AdatumTestApp/**.



**Note:** It is critical to use the trailing forward slash (/) in the URL for step 3.

4. Notice that you were not prompted for credentials.
5. Review the claim information that is displayed by the application, and then close Internet Explorer.

**Results:** After completing this exercise, you should have successfully configured AD FS to support authentication for an application.

## Exercise 4: Configuring AD FS for federated business partners

### Scenario

The second deployment scenario is to enable Trey Research users to access the web application. You plan to configure the integration of AD FS at Trey Research with AD FS at A. Datum Corporation and then verify that Trey Research users can access the application. You also want to confirm that you can configure access that is based on user groups. You must ensure that all users at A. Datum Corporation, and only users who are in the Production group at Trey Research can access the application.

The main tasks for this exercise are as follows:

1. Create a DNS record for AD FS at Trey Research.
2. Create a certificate for AD FS at Trey Research.
3. Install AD FS for Trey Research.
4. Configure AD FS for Trey Research.
5. Configure a claims provider trust for the Trey Research AD FS server.
6. Configure a relying party trust for the A. Datum Corporation application.
7. Verify access to the website.
8. Configure issuance authorization claim rules to allow access for only specific groups.
9. Verify access to the website with the group restrictions.
10. Prepare for the next module.

► **Task 1: Create a DNS record for AD FS at Trey Research**

- On **TREY-DC1**, use DNS Manager to add a new host record for AD FS with the following information:
  - Forward lookup zone: **TreyResearch.net**
  - Name: **adfs**
  - IP address: **172.16.10.10**

► **Task 2: Create a certificate for AD FS at Trey Research**

1. On **TREY-DC1**, open IIS Manager, and then view the server certificates.
2. Create a new domain certificate with the following settings:
  - Common name: **adfs.TreyResearch.net**
  - Organization: **Trey Research**
  - Organizational unit: **IT**
  - City/locality: **London**
  - State/Province: **England**
  - Country/region: **GB**
  - Certification Authority: **TreyResearchCA**
  - Friendly name: **adfs.TreyResearch.net**

► **Task 3: Install AD FS for Trey Research**

1. On **TREY-DC1**, click **Start**, right-click **Windows PowerShell**, and then click **Run as Administrator**.
2. Run the following command to create the Key Distribution Service root key to generate gMSA passwords for the account that will be used later in this lab.

```
Add-KdsRootKey -EffectiveTime ((get-date).addhours(-10))
```

3. Open **Server Manager**, and then add the **Active Directory Federation Services** role.

► **Task 4: Configure AD FS for Trey Research**

1. On **TREY-DC1**, in **Server Manager**, click the **Notifications** icon, and then click **Configure the federation services on this server**.
2. Use the following options to configure the AD FS server:
  - **Create the first federation server in a federation server farm**
  - Account for configuration: **TreyResearch\Administrator**
  - SSL Certificate: **adfs.treyresearch.net**
  - Federation Service Display Name: **Trey Research**
  - Create a Group Managed Service Account: **TreyResearch\ADFSService**
  - **Create a database on this server using Windows Internal Database**

► **Task 5: Configure a claims provider trust for the Trey Research AD FS server**


1. On **LON-DC1**, use the **AD FS Management** console to add a new claims provider trust with the following settings:
  - **Import data about the claims provider published online or on a local network**
  - Federation metadata address: **https://adfs.treyresearch.net**
  - Display name: **Trey Research**
  - **Open the Edit Claim Rules dialog for this claims provider trust when the wizard closes**
2. Create a claim rule for Trey Research by using the following settings:
  - Claim rule template: **Pass Through or Filter an Incoming Claim**
  - Claim rule name: **Pass through Windows account name**
  - Incoming claim type: **Windows account name**
  - **Pass through all claim values**

► **Task 6: Configure a relying party trust for the A. Datum Corporation application**

1. On **TREY-DC1**, use the **AD FS Management** console to create a new relying-party trust with the following settings:
  - **Import data about the relying party published online or on a local network**
  - Federation metadata address: **adfs.adatum.com**
  - Display name: **A. Datum Corporation**
  - **Permit everyone to access this relying party**
  - **Configure claims issuance policy for this application selected**
2. Create a new transform claim rule with the following settings:
  - Claim rule template: **Pass Through or Filter an Incoming Claim**
  - Claim rule name: **Pass through Windows account name**
  - Incoming claim type: **Windows account name**
  - **Pass through all claim values**

► **Task 7: Verify access to the website**

1. On **TREY-DC1**, add the domain **adatum.com** to the **Per Site Privacy Actions** allow list.
2. Use Internet Explorer to access **https://lon-svr1.adatum.com/adatumtestapp/**.
3. Select the **Trey Research** home realm, and then sign in as **TreyResearch\April** with the password **Pa\$\$w0rd**.
4. Verify that you can access the application.
5. Close Internet Explorer, and then connect to the same website. Verify that you are not prompted for a home realm this time.

 **Note:** You are not prompted for a home realm on the second access. After a user selects a home realm and a realm authority authenticates that user, the relying party's federation server issues a **\_LSRealm** cookie. The default lifetime for the cookie is 30 days. Therefore, to sign in multiple times, you should delete that cookie after each sign-in attempt to return to a clean state.

► **Task 8: Configure issuance authorization claim rules to allow access for only specific groups**

1. On **TREY-DC1**, in the **AD FS Management** console, remove the Issuance Policy rule named **Pass through Windows account name** from the A. Datum Corporation relying party trust.
2. Use the following settings to add an issuance transform rule to the A. Datum Corporation relying party trust that allows all users that are members of the Production group:
  - Claim rule template: **Pass Through or Filter an Incoming Claim**
  - Claim rule name: **Allow Production Members**
  - Incoming claim type: **Group**
  - Incoming claim value: **TreyResearch-Production**
3. Use the following settings to add a transform claim rule to the Active Directory claims provider trust to send group membership as a claim:
  - Claim rule template: **Send Group Membership as a Claim**
  - Claim rule name: **Production Group Claim**
  - User's group: **Production**
  - Outgoing claim type: **Group**
  - Outgoing claim value: **TreyResearch-Production**

► **Task 9: Verify access to the website with the group restrictions**

1. On **TREY-DC1**, add the domain **adatum.com** to the **Per Site Privacy Actions** allow list.
2. Use Internet Explorer to verify access to **https://lon-svr1.adatum.com/adatumtestapp/**.
3. Sign in as **TreyResearch\Ben** with the password **Pa\$\$w0rd**.
4. Verify that you can access the application because Ben is a member of the **TreyResearch\Production** group.

**Results:** After completing this exercise, you should have successfully configured access for a claims-aware application in a partner organization.

► **Task 10: Prepare for the next module**

When you finish the lab, revert the VMs to their initial state. To do this, complete the following steps:

1. On the host computer, start **Hyper-V Manager**.
2. In the **Virtual Machines** list, right-click **20742A-LON-DC1**, and then click **Revert**.
3. In the **Revert Virtual Machine** dialog box, click **Revert**.
4. Repeat steps 2 and 3 for **20742A-LON-DC2**, **20742A-LON-SVR1**, **20742A-TREY-DC1**, and **20742A-LON-CL1**.

**Question:** Why is it important to configure adfs.adatum.com to use as a host name for the AD FS service?

**Question:** How can you test whether AD FS is functioning properly?

## Module Review and Takeaways

### Best Practice

In earlier versions of AD FS, it was common to use the Security Configuration Wizard (SCW) to apply AD FS–specific security best practices to federation servers and federation server proxy computers. In Windows Server 2016, SCW was removed because features are security enhanced by default. Consequently, if you need to control specific security settings, you can use either Group Policy or Microsoft Security Compliance Manager (see <http://aka.ms/Ncq8jm>).

### Review Questions

**Question:** Your organization is planning to implement AD FS. In the short term, only internal clients will use AD FS to access internal applications. However, you must later provide access to web-based applications that are security enhanced by AD FS to users at home. How many certificates should you obtain from a third-party CA?

**Question:** Your organization has successfully implemented a single AD FS server and a single Web Application Proxy. Initially, AD FS was used for only a single application, but now it is used for several business-critical applications. AD FS must be configured to be highly available.

During the installation of AD FS, you chose to use WID. Can you use this database in a highly available configuration?



# Module 11

## Implementing and administering AD RMS

### Contents:

Module Overview	11-1
<b>Lesson 1:</b> Overview of AD RMS	11-2
<b>Lesson 2:</b> Deploying and managing an AD RMS infrastructure	11-10
<b>Lesson 3:</b> Configuring AD RMS content protection	11-18
<b>Lab:</b> Implementing an AD RMS infrastructure	11-23
Module Review and Takeaways	11-28

## Module Overview

Active Directory Rights Management Services (AD RMS) helps to protect content by going beyond encrypting storage devices through either BitLocker Drive Encryption or encrypting individual files via Encrypting File System (EFS). AD RMS helps to protect data both in transit and at rest on essentially any device or platform. AD RMS also helps to make data accessible only to authorized users for a specific duration and a specific purpose.

This module introduces you to AD RMS. It describes how to deploy AD RMS and how to configure content protection.

### Objectives

After completing this module, you will be able to:

- Describe AD RMS.
- Deploy and manage an AD RMS infrastructure.
- Configure AD RMS content protection.

## Lesson 1

# Overview of AD RMS

Prior to deploying AD RMS, you need to know how it works, how to deploy it, and what components an AD RMS deployment includes. You also need to understand the concepts behind various AD RMS certificates and licenses.

This lesson provides an overview of AD RMS and describes scenarios in which you can use AD RMS to help protect your organization's confidential data.

### Lesson Objectives

After completing this lesson, you will be able to:

- Describe AD RMS.
- Describe usage scenarios for AD RMS.
- Describe the AD RMS components.
- Describe AD RMS certificates and licenses.
- Explain how AD RMS works.
- Describe Microsoft Azure Rights Management Services (Azure RMS).

Explain the differences between Azure RMS, AD RMS, and Azure Azure RMS for Office 365.

### What is AD RMS?

AD RMS is an information protection technology that minimizes the possibility of data leakage. *Data leakage* is the unauthorized transmission of information to people within or outside of an organization who should not have access to the information. AD RMS integrates with certain existing Microsoft products, including Windows Server, Microsoft Exchange Server, Microsoft SharePoint Server, and Microsoft Office and with online services such as Office 365.

AD RMS can help to protect data that is both in transit and at rest. For example, AD RMS can help to protect documents in email by helping to prevent messages from opening that are accidentally addressed to the wrong recipients. You also can use AD RMS to help protect data that is stored on devices such as removable USB drives. A drawback to file and folder permissions is that after a file is copied to another location; the original permissions no longer apply. A file that copies to a USB drive inherits the permissions on the destination device. After a file with a read-only attribute is copied, however, it can be edited by altering the file and folder permissions. If you decide to use EFS, you can permanently help to protect the file. However, it will not be easy to share that file with other users, and you cannot configure specific permissions.

With AD RMS, you can help to protect a file in essentially any location, regardless of the file and folder permissions that grant access. With AD RMS, only the users who are authorized to open a file can view the contents of that file. Additionally, you can control file actions, such as copy, print, forward and others.

- An Information protection technology that:
- Reduces data leakage by design
  - Integrates with certain Microsoft products and Windows Server operating systems
  - Helps protect data when in transit, at rest and in essentially any location

## Usage scenarios for AD RMS

The primary use for AD RMS is to control the distribution of sensitive information. You can use AD RMS in combination with encryption techniques to help secure data that is stored or in transit. Many reasons exist to control the distribution of sensitive information, such as helping to ensure that only authorized staff members have access to a file, that sensitive email messages cannot be forwarded, or that the details of an unreleased project are not made public. Consider the following scenarios:

The primary use for AD RMS is to control the distribution of sensitive information, and typical usage scenarios include:

- Helping to prevent access to confidential documents, regardless of their location
- Using action-based permissions based on AD DS accounts
- Helping to prevent confidential emails from leaving an organization

- Scenario 1. The Chief Executive Officer (CEO) copies a spreadsheet that contains the compensation packages of the organization's executives from a protected folder on a file server to the CEO's personal USB drive. During the commute home, the CEO leaves the USB drive on the train, where someone with no connection to the organization finds it. Without AD RMS, whoever finds the USB drive can open the file. With AD RMS, you can help to ensure that unauthorized users cannot open the file.
- Scenario 2. An internal document is viewable by a certain group of authorized people within an organization. These people should not be able to edit or print the document. You can use the native functionality of Microsoft Word 2003 or later to restrict these features. Doing so requires that each person have a Microsoft account or Active Directory Domain Services (AD DS) account. With AD RMS, you can configure these permissions based on existing accounts in AD DS, or for users that are outside the organization, you can identify them by using Microsoft accounts.
- Scenario 3. People within an organization should not have access to forward sensitive email messages that have been assigned a particular classification. With AD RMS, you can enable a sender to assign a particular classification to a new email message, and that classification helps to ensure that the recipient will not be able to forward the message.

## Overview of AD RMS components

An AD RMS infrastructure consists of several components and the main component is the AD RMS cluster. The AD RMS root certification cluster is created when you deploy the first AD RMS server in a forest. The AD RMS root certification cluster manages all licensing and certification traffic for the domain in which it is installed. AD RMS stores configuration information in a Microsoft SQL Server database or in a Windows Internal Database (WID). In large environments, the SQL Server database is hosted on a server that is separate from the server that hosts the AD RMS role.

- The AD RMS cluster:
  - Is created when you deploy the first AD RMS server
- The AD RMS server:
  - Licenses AD RMS-protected content
  - Certifies the identity of trusted users and devices
- The AD RMS client:
  - Built in to Windows Vista, Windows 7 and later
  - Interacts with AD RMS-enabled apps
- AD RMS-enabled apps:
  - Allows for the publication and consumption of AD RMS protected content
  - Includes Office, Exchange Server, and SharePoint Server
  - Have the ability to be created through the AD RMS SDK

AD RMS *licensing-only clusters* are used in distributed environments. Licensing-only clusters do not provide certification, but they do allow the distribution of licenses for content consumption and publishing. Licensing-only clusters often deploy to large branch offices in organizations that use AD RMS.

## AD RMS server

The AD RMS server must be a member of an AD DS domain. When you install AD RMS, information about the location of the cluster publishes to AD DS in a location known as the *service connection point*.

Computers that are members of the domain query the service connection point to determine the location of AD RMS services. AD RMS is a server role that you can install by using Server Manager on the Windows Server 2016, Windows Server 2012, and Windows Server 2008 operating systems.

## AD RMS client

The AD RMS client is built in to the Windows 10, Windows 8.1, Windows 8, Windows 7, and Windows Vista operating systems. The AD RMS client allows AD RMS-enabled apps to enforce the functionality dictated by an AD RMS template. Without the AD RMS client, AD RMS-enabled apps cannot interact with AD RMS-protected content.

## AD RMS-enabled apps

AD RMS-enabled apps allow users to create and consume AD RMS-protected content. For example, Microsoft Outlook 2010 or later allows users to view and create protected email messages. Word 2007 or later allows users to view and create protected word-processing documents. Microsoft provides an AD RMS software development kit (SDK) to enable app developers to support AD RMS content protection.

## AD RMS certificates and licenses

To understand how AD RMS works, you need to be familiar with its different certificates and license types. Each of these certificates and licenses functions in a different way. Some certificates, such as server licensor certificates, are critically important, and you must regularly back them up.

### Server licensor certificate

The server licensor certificate is generated when you create the AD RMS cluster. It has a validity period of 250 years. A server licensor certificate allows an AD RMS cluster to issue:

- Server licensor certificates to other servers in the cluster.
- Rights Account Certificates (RACs) to clients.
- Client licensor certificates.
- Publishing licenses (PLs).
- Use licenses.
- Rights policy templates.

The server licensor certificate public key encrypts the content key in a PL. This allows an AD RMS server to extract the content key and issue end-user licenses against the publishing key.

### AD RMS machine certificate

The AD RMS machine certificate is used to identify a trusted computer or device. This certificate identifies a client computer's lockbox. The machine certificate public key encrypts the RAC private key. The machine certificate private key decrypts RACs.

AD RMS certificates and licenses include:

- Server licensor certificates
- AD RMS machine certificates
- RACs
- Client licensor certificates
- PLs
- End-user licenses

## RAC

The RAC identifies a specific user. The default validity period for a RAC is 365 days. RACs can be issued only to AD DS users who have email addresses that are associated with their accounts. A RAC is issued the first time a user attempts either to access AD RMS–protected content or to perform an AD RMS task, such as creating a protected document. You can adjust the default validity period by using the **Rights Account Certificate Policies** node of the AD RMS console.

A temporary RAC has a validity period of 15 minutes. A temporary RAC is issued when a user accesses AD RMS–protected content from a computer that is not a member of the same forest as the AD RMS cluster or trusted forest. You can adjust the default validity period by using the **Rights Account Certificate Policies** node of the AD RMS console.

AD RMS supports the following additional RACs:

- Active Directory Federation Services (AD FS) RACs. These RACs are issued to federated users and have a validity period of seven days.
- Two types of Windows Live ID RACs. Windows Live ID RACs used on private computers have a validity period of six months. Windows Live ID RACs used on public computers are valid until the user signs out.

## Client licensor certificate

A client licensor certificate allows a user to publish AD RMS–protected content when the client computer is not connected to the same network as the AD RMS cluster. The client licensor certificate public key encrypts the symmetric content key and includes it in the PL that it issues. The client licensor certificate private key signs any PLs that are issued when the client is not connected to the AD RMS cluster.

Client licensor certificates are tied to a specific user's RAC. If another user who has not been issued a RAC attempts to publish AD RMS–protected content from the same client, he or she will be unable to do so until the client is connected to the AD RMS cluster and can issue that user a RAC.

## PL

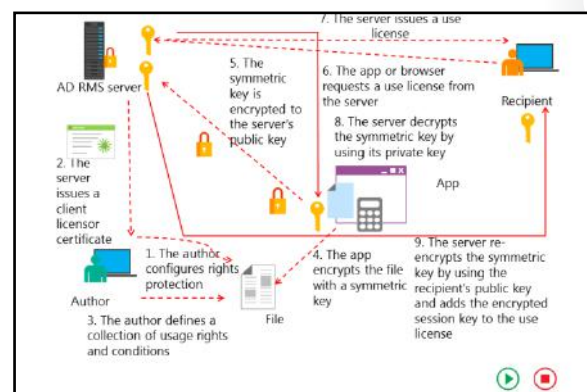
A PL determines the rights that apply to AD RMS–protected content. For example, the PL determines if a user can edit, print, or save a document. The PL contains the content key, which is encrypted by using the public key of the licensing service. It also contains the URL and the digital signature of the AD RMS server.

## End-user license

An end-user license is required to consume AD RMS–protected content. The AD RMS server issues one end-user license per user per document. End-user licenses are cached by default.

## How AD RMS works

When a user either helps to protect content with AD RMS or tries to access AD RMS–protected content, several tasks and procedures are performed in the background. For diagnosis and troubleshooting, it is important to understand how AD RMS works. Although not obviously related to Active Directory Certificate Services, AD RMS uses certificates and encryption intensively.



AD RMS works in the following manner:

1. The first time an author configures rights protection for a document—for example, within a Word app—a client licensor certificate is requested from the AD RMS server. A client locates the AD RMS server by using the service connection point in AD DS.
2. The server then issues a client licensor certificate to the client, unless the client is on the exclusion list in AD RMS.
3. When the author receives the client licensor certificate from the AD RMS server, he or she can configure usage rights on the document. The author can perform the configuration either manually or by applying pre-created templates.
4. When the author configures usage rights, the AD RMS-enabled app encrypts the file with a symmetric key. A symmetric key is generated on the client device. When AD RMS protection is applied to the document, the document is actually in an encrypted state.
5. This symmetric key is then encrypted by using the public key of the AD RMS server that the author is using. This encrypted symmetric key is distributed to the AD RMS server and stored on it. Because it is encrypted with the server's public key, it can be decrypted only by using the server's private key.
6. The author of the AD RMS-protected content distributes the file to the recipient. The recipient of the file opens it by using an AD RMS app or browser. It is not possible to open AD RMS-protected content unless the app or browser supports AD RMS. If the recipient does not have an account certificate on the current device, one is issued to the user at this point. The app or browser transmits a request to the author's AD RMS server for a use license.
7. The AD RMS server determines if the recipient is authorized. If the recipient is authorized, the AD RMS server issues a use license.
8. The AD RMS server then decrypts the symmetric key that was encrypted in step 5 by using its private key.
9. The AD RMS server re-encrypts the symmetric key by using the recipient's public key and then adds the encrypted session key to the use license. The use license and the encrypted symmetric key are then distributed to the recipient. The recipient uses his or her private key to decrypt the symmetric key. After that, the symmetric key is used to decrypt AD RMS-protected content.

## What is Azure RMS?

Implementing AD RMS in a local network infrastructure and in a single AD DS forest can help to protect information. However, it can be inefficient in scenarios where AD RMS-protected content should be shared with selected organizations or people outside of an organization. Besides establishing trusts or using a Microsoft account, you now can use the rights management capabilities of the Azure public cloud service. Additionally, in some scenarios, an organization might not have enough resources to implement a local AD RMS infrastructure.

- Azure RMS is RMS protection from the cloud
- Azure RMS is available in Office 365 Enterprise E3, Office 365 ProPlus and as a separate service
- Azure RMS provides:
  - IRM integration with Office
  - Exchange Online IRM integration
  - SharePoint Online IRM integration
  - Windows Server FCI integration
- The RMS sharing application integrates with File Explorer

Azure RMS provides you with the ability to use RMS protection from the cloud without implementing a local AD RMS infrastructure. By using Azure RMS, you can assign policies and usage restrictions to documents and then share those documents with other organizations that subscribe to the Azure service.

Because Azure RMS integrates with all the Office 365 services and apps, you can use all the RMS capabilities from both the cloud and the on-premises environment.

Azure RMS is available in the Office 365 Enterprise E3 and Office 365 ProPlus subscriptions. You can also purchase it as a separate service and use it with your cloud or on-premises resources. Azure RMS provides the following functionalities:

- Information Rights Management (IRM) integration with Office. All locally deployed Office apps can use Azure RMS to help with content protection.
- Exchange Online IRM integration. Azure RMS gives you the ability to help protect and consume email messages in either Outlook on the web or Outlook. You can also consume IRM-protected messages via Exchange ActiveSync on devices that have IRM support, such as Windows 10 Mobile or iOS-based devices. Additionally, administrators can use Outlook protection rules and Exchange transport rules for protection and decryption to help ensure that content is not inadvertently leaked outside an organization.
- SharePoint Online IRM integration. When Azure RMS is used, administrators can configure the automatic IRM protection of documents in a SharePoint library.
- Windows Server File Classification Infrastructure (FCI). If your computer runs Windows Server and has the File Server Resource Manager (FSRM) feature, you have FCI. FSRM can scan files on the server and take a configured action. For example, you can tag sensitive files as **Sensitive**. After classifying a file or folder, you can run another FSRM task to apply an Azure RMS template to the file or folder, based on the classification. Thus, if FSRM finds a folder named **Payroll** and classifies it as **Sensitive**, you can have FSRM apply an Azure RMS template to match the data type. In this case, you might use a template that limits access to the file to the Payroll department.

### Organizational benefits

These Azure RMS functionalities provide several benefits to organizations, including:

- Helping organizations to meet compliance targets. Azure RMS is certified for several industry programs, including the Health Insurance Portability and Accountability Act (HIPAA) and Payment Card Industry (PCI) Data Security Standard (DSS) Level 1. Many organizations are required to store sensitive data with encryption, and they can use Azure RMS to do so.
- Helping organizations to reduce data leakage. In many organizations, users might disseminate corporate data without authorization. For example, an organization might be preparing to announce a new product, but word of the product leaks before the organization is ready to make the announcement. This often happens because employees forward internal emails to email addresses outside of the organization, or they copy files to devices and take them offsite. Azure RMS can help to minimize data leakage by making it difficult for employees to transfer information outside of the organization without being tracked. Unlike AD RMS, which is locally deployed, Azure RMS provides you with ability to geographically track the location where a file is used.
- Helping organizations to share confidential data with partners and other, outside organizations. Because Azure RMS allows for virtually seamless collaboration with users outside of your organization, organizations can enhance security for collaboration and data sharing.

- Minimizing the chances of an organization being locked out of its own data. Imagine a scenario in which a manager is preparing to quit and decides to encrypt all the files on his or her computer by using Azure RMS protection, with only his or her user account having access. Normally, this can pose a problem, especially if the information technology (IT) department deletes the user account before anybody realizes that the manager encrypted the files. Azure RMS provides an optional feature, named the Super User feature, to help with gaining access to encrypted documents—even if the original encryption specified only a particular user who might have left the organization. A special group, named the Azure RMS Super Users group, can help to gain access to the encrypted documents.

### RMS sharing application

The RMS sharing application is a free download from Microsoft. This application enhances the way that you can protect and share documents. After being installed, the application adds an Azure RMS protection menu to the shortcut menu in File Explorer. When you right-click any file or folder, you will see a new **Protect with RMS** menu item. This item allows you to protect a file on your computer, share a protected file, track a shared file's usage, and remove the protection from a file. The functionality also ties in to the Azure RMS templates. Alternatively, you can use custom permissions.



**Reference Links:** To download the free RMS sharing application from Microsoft go to: <http://aka.ms/v1s1xd>

### Comparing AD RMS, Azure RMS, and Azure RMS for Office 365


The core features of AD RMS, Azure RMS, and Azure RMS for Office 365 are similar. They all use encryption to help protect data and integrate with the same server-based applications—Exchange Server and SharePoint Server. AD RMS and Azure RMS also integrate with Windows Server FCI, but Azure RMS for Office 365 does not. Microsoft has begun to add new features to the cloud-based versions of applications first. Therefore, Azure RMS and Azure RMS for Office 365 have features that AD RMS does not. Microsoft is likely to continue with this approach as new development moves forward. Some of the key differences among AD RMS, Azure RMS, and Azure RMS for Office 365 involve:

Feature	AD RMS	Azure RMS	Azure RMS for Office 365
IRM for on-premises Exchange Server and SharePoint Server	Yes	Yes	Yes
IRM for Exchange Online and SharePoint Online	No	Yes	Yes
The ability to share with any organization without further configuration	No	Yes	Yes
Default templates	No	Yes	Yes
The ability to protect any file type	Yes	Yes	Yes
RMS protected document tracking	No	Yes	No
Mobile device support	Yes	Yes	Yes

- Integration with server-based applications. AD RMS and Azure RMS integrate with on-premises versions of Exchange Server, SharePoint Server, and Windows Server FCI. However, Azure RMS also integrates with Office 365, Exchange Online, SharePoint Online, and Microsoft OneDrive for Business, whereas AD RMS does not. Azure RMS for Office 365 integrates with on-premises versions of Exchange Server and SharePoint Server in addition to Exchange Online, SharePoint Online, and OneDrive for Business. For organizations that are currently exploring the cloud, using the cloud, or planning a future move to the cloud, we recommend Azure RMS as the best choice.



- Sharing across different organizations. With AD RMS, you can create trusts among different organizations to share RMS-protected content among those organizations. However, that sharing requires a large amount of planning and work. One of the most limiting factors of AD RMS is the complexity of sharing RMS-protected documents across multiple organizations. Azure RMS and Azure RMS for Office 365 eliminate that barrier. With Azure RMS and Azure RMS for Office 365, trusts are in place by default. If organizations have Office 365, Azure RMS, or RMS for individuals, you can share RMS-protected content with them without setting up trusts or performing other configurations.
- Sharing via the RMS sharing application. With AD RMS, you can use the RMS sharing application to share RMS-protected documents with other people in your organization. However, you cannot share them with people outside of your organization. With Azure RMS and Azure RMS for Office 365, you can share such documents with people inside and outside of your organization. You can also use email notifications to know when someone tries to access your RMS-protected document. In addition, you receive access to a document-tracking site to track document usage and revoke documents.
- Support for Azure Multi-Factor Authentication (Azure MFA). Azure RMS and Azure RMS for Office 365 support Azure MFA, whereas AD RMS supports Azure MFA only with a local MFA server. This enables you to enhance the security of your RMS-protected content by requiring two factors of authentication.

 **Additional Reading:** For more information, refer to: "Comparing Azure Rights Management and AD RMS" at: <http://aka.ms/sndlw0>

From an administrator's perspective, additional differences exist among AD RMS, Azure RMS, and Azure RMS for Office 365:

- Infrastructure. To support on-premises AD RMS, you need to deploy a minimum of one AD RMS server. For highly available installations, you need at least two AD RMS servers. In addition, you need to have at least one server that runs SQL Server to host the databases. You also need to configure an AD DS account to use as the AD RMS service account. If you want to use federated identities to enable using your AD RMS infrastructure across multiple organizations, you need AD FS and a Web Application Proxy server in the perimeter network. Finally, you need to obtain a Secure Sockets Layer (SSL) certificate for AD RMS. For Azure RMS and Azure RMS for Office 365, Azure provides all of these infrastructure components.
- Administration and maintenance. AD RMS requires infrastructure components that need occasional administration and maintenance. For example, you might need to install a service pack for SQL Server or troubleshoot performance issues on the AD RMS server. Other tasks, such as installing the latest security updates on servers, are routine monthly tasks. For Azure RMS and Azure RMS for Office 365, Azure handles these activities.
- Support. When AD RMS stops responding or has another major issue that you cannot resolve, you need to call Microsoft Support and work with them to resolve the issue. Microsoft fixes similar issues with Azure RMS and Azure RMS for Office 365. Azure RMS and Azure RMS for Office 365, like other Azure services, have service level agreements and high availability across all of the major components.

**Question:** When does a user receives a RAC?

Verify the correctness of the statement by placing a mark in the column to the right.

Statement	Answer
Azure RMS is deployed locally on a server.	

## Lesson 2

# Deploying and managing an AD RMS infrastructure

Before you deploy AD RMS, it is important to have a plan that is appropriate for your organization's environment. AD RMS deployment in a single-domain forest is different from scenarios in which you need to support the publication and consumption of content across multiple forests, to trusted partner organizations, or across the Internet. Before deploying AD RMS, you need to understand the client requirements and have an appropriate strategy for backing up and recovering AD RMS. This lesson provides an overview of deploying AD RMS and the steps you need to take to back up, recover, and decommission an AD RMS infrastructure.

### Lesson Objectives

After completing this lesson, you will be able to:

- Describe AD RMS deployment scenarios.
- Explain how to configure the AD RMS cluster.
- Install the first server of an AD RMS cluster.
- Describe the AD RMS client requirements.
- Explain how to implement an AD RMS backup and recovery strategy.
- Explain how to decommission and remove AD RMS.
- Explain how to monitor AD RMS.
- Explain how to implement external sharing for AD RMS.

### AD RMS deployment scenarios

An AD RMS deployment consists of one or more servers, known as a *cluster*. An AD RMS cluster is not a high-availability failover cluster. When you deploy AD RMS, you should implement it on a server that is highly available. AD RMS commonly deploys as a highly available virtual machine (VM).

When you deploy AD RMS in a single forest, you have a single AD RMS cluster. This is the most common form of AD RMS deployment. You add servers to the AD RMS cluster as needed to provide additional capacity.

When you deploy AD RMS across multiple forests, each forest must have its own AD RMS root cluster, except when you deploy AD FS to use a single AD RMS cluster for multiple forests. It is necessary to configure AD RMS trusted publishing domains or trusted user domains to help ensure that AD RMS content can be protected and consumed across the multiple forests.

You can also deploy AD RMS to extranet locations. In this deployment, the AD RMS licensing server is accessible by hosts from the Internet. You use this type of deployment to support collaboration with external users.

#### Deployment scenarios for AD RMS:

- Deployed in a single forest
- Deployed in multiple forests
- Used on an extranet
- Integrated with AD FS
- Deployed in Azure as an Azure RMS service

You can deploy AD RMS with AD FS or the Azure Active Directory (Azure AD) authentication system (previously known as Microsoft Federation Gateway). In this scenario, users take advantage of federated identity to publish and consume rights-protected content.

As a best practice, you should not deploy AD RMS on a domain controller. If you deploy AD RMS on a domain controller then you must add the service account of AD RMS to the Domain Admins group. However, adding service accounts to highly privileged groups is not a best practice.

As an alternative to on-premises AD RMS deployment, you can choose to use Azure RMS as described earlier.

## Configuring the AD RMS cluster

After you install the AD RMS server role, you need to configure the AD RMS cluster before you can use AD RMS. Configuring the AD RMS cluster involves configuring the following components:

- AD RMS cluster membership. Choose whether to create a new AD RMS root cluster or join an existing cluster.
- Configuration database. Select whether to use an existing SQL Server instance in which to store the AD RMS configuration database or whether to configure and locally install WID. You can use SQL Server 2008 or newer to support an AD RMS deployment in Windows Server 2016. As a best practice, use a SQL Server database that is hosted on a separate server.
- Service account. We recommend using a standard domain user account with additional permissions. You can use a managed service account as the AD RMS service account.
- Cryptographic mode. Choose the strength of the cryptography used with AD RMS:
  - Cryptographic Mode 2 uses RSA 2048-bit keys and Secure Hash Algorithm 256 (SHA-256) hashes.
  - Cryptographic Mode 1 uses RSA 1024-bit keys and Secure Hash Algorithm 1 (SHA-1) hashes.
- Cluster key storage. Choose where the cluster key is stored. You can store it within AD RMS, or you can use a cryptographic service provider (CSP). If you use a CSP and want to add more servers, you will need to distribute the key manually.
- Cluster key password. This password encrypts the cluster key and is required if you want to either join other AD RMS servers to the cluster or restore the cluster from a backup.
- Cluster website. Choose which website on the local server will host the AD RMS cluster website.
- Cluster address. Specify the fully qualified domain name to use with the cluster. You have the option of choosing a website that is or is not encrypted with SSL. If you do not choose SSL encryption, you will be unable to add support for identity federation. After you set the cluster address and port, you cannot change them without completely removing AD RMS.
- Licensor certificate. Choose the friendly name that the server license certificate will use. It should represent the function of the certificate.

AD RMS configuration includes configuring the following components:

- New or existing cluster
- Configuration database
- Service account
- Cryptographic mode
- Cluster key storage
- Cluster key password
- Cluster website
- Cluster address
- Licensor certificate
- Service connection point registration

- Service connection point registration. Choose whether to register the service connection point in AD DS when the AD RMS cluster is created. The service connection point allows computers that are members of the domain to automatically locate the AD RMS cluster. Only users who are members of the Enterprise Admins group can register the service connection point. You can perform this step after the AD RMS cluster is created. You do not have to perform this step during the configuration process.

## Demonstration: Installing the first server of an AD RMS cluster

In this demonstration, you will see how to deploy AD RMS on a computer running Windows Server 2016.

### Demonstration Steps

#### Configure a service account

1. Sign in to **LON-DC1** as **Adatum\Administrator** with the password **Pa\$\$w0rd**.
2. Use the Active Directory Administrative Center to create an organizational unit (OU) named **Service Accounts** in the **adatum.com** domain.
3. Create a new user account in the Service Accounts OU with the following properties:
  - First name: **ADRMSSVC**
  - User UPN logon: **ADRMSSVC**
  - **User SamAccountName Logon:** **Adatum\ADRMSSVC**
  - Password: **Pa\$\$w0rd**
  - Confirm Password: **Pa\$\$w0rd**
  - Password never expires: **Enabled**
  - User cannot change password: **Enabled**

#### Prepare the Domain Name System (DNS)

- Use the **DNS Manager** console to create a host (A) resource record in the **adatum.com** zone with the following properties:
  - Name: **adrms**
  - IP Address: **172.16.0.21**

#### Install the AD RMS role

1. Sign in to **LON-SVR1** as **Adatum\Administrator** with password **Pa\$\$w0rd**.
2. Use the **Add Roles and Features Wizard** to add the **Active Directory Rights Management Services** role to **LON-SVR1** by using the following option:
  - Role services: **Active Directory Rights Management Server Services**

#### Configure AD RMS

1. In **Server Manager**, from the **AD RMS** node, click **More** to start the post-deployment configuration of AD RMS.
2. In the **AD RMS Configuration Wizard**, provide the following information:
  - **Create a new AD RMS root cluster**
  - **Use Windows Internal Database on this server**

- **Use Adatum\ADRMSSVC as the service account**
  - Cryptographic Mode: **Cryptographic Mode 2**
  - Cluster Key Storage: **Use AD RMS centrally managed key storage**
  - Cluster Key Password: **Pa\$\$w0rd**
  - Cluster Web Site: **Default Web Site**
  - Connection Type: **Use an unencrypted connection**
  - Fully Qualified Domain Name: **http://adrms.adatum.com**
  - Port: **80**
  - Licensor Certificate: **AdatumADRMS**
  - Register AD RMS Service Connection Point: **Register the SCP Now**
3. Sign out of **LON-SVR1**.



**Note:** You must sign out before you can manage AD RMS.

## AD RMS client requirements

AD RMS content is published and consumed only by computers that run the AD RMS client. Windows 10, Windows 8.1, Windows 8, Windows 7, and Windows Vista include the AD RMS client software. Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2, and Windows Server 2008 also include the AD RMS client. These operating systems do not require additional configuration to consume and publish AD RMS-protected content.

AD RMS client software is available for download for computers that run the Windows XP operating system or Mac OS X. This client software must be installed before users of these operating systems can consume and publish AD RMS-protected content.

AD RMS requires compatible apps and applications. The server applications that support AD RMS include Exchange Server 2007 and newer and Office SharePoint Server 2007 and newer.

Client apps, such as those included in Office 2003 and newer, can publish and consume AD RMS-protected content. You can use the AD RMS SDK to create apps that can publish and consume AD RMS-protected content. XML Paper Specification Viewer and Internet Explorer can also view AD RMS-protected content.

You can also use an RMS sharing app on mobile devices that run Windows 10 Mobile, iOS, and Android to help protect certain types of content.

- The client is included in Windows Vista or newer
- The client is included in Windows Server 2008 and newer
- The client is available for download for Windows XP operating systems and Mac OS X
- The AD RMS-enabled applications include Office 2007 and newer
- Exchange Server 2007 and newer support AD RMS
- The AD RMS client needs an RMS CAL



**Note:** Microsoft has released the new version of the AD RMS client software—AD RMS Client 2.1. You can download it from the Microsoft Download Center. Among other things, the new version provides a new SDK that you can also download from the Microsoft Download Center. The new AD RMS SDK provides a simple mechanism for developers to create apps and solutions that protect and consume critical content. With the new SDK, you can create rights-enabled apps and solutions much faster and more easily than before.

### AD RMS client licensing

To use AD RMS in your AD DS environment, you must have Windows Rights Management client access licenses (CALs). These CALs are different from the classic Windows Server CALs that you need to connect a client to a server. Each user that will create or use rights-protected files needs to have an RMS user CAL. Alternatively, you also can use RMS device CALs for computers that will create and view RMS-protected content.

If you need to share your RMS-protected content outside of your organization, you can acquire an RMS External Connector License. This license gives an organization the right to permit an unlimited number of external users to access or use a single license without the need to acquire a CAL for each external user.

### Implementing an AD RMS backup and recovery strategy

To help prevent data loss, you must back up an AD RMS server so that you can recover it in the event of file corruption or server failure. If the AD RMS server becomes inaccessible, all AD RMS-protected content also becomes inaccessible.

A simple AD RMS backup and recovery strategy is to run the AD RMS server as a VM and then use an enterprise backup product, such as Microsoft System Center Data Protection Manager, to perform regular VM backups. Some of the important components that require backups are the private key, certificates, AD RMS database, and templates. You also can perform a full server backup by running the AD RMS server on a VM.

- Back up the private key and the certificates
- Ensure that the AD RMS database is backed up regularly
- Export templates to back them up
- Run the AD RMS server as a VM, and perform a full server backup

As a best practice, you need to back up the AD RMS private key and all the certificates that AD RMS uses. The simplest method to do this is to export the certificates to a safer location. You must also back up the AD RMS database on a regular basis. The method you use to do this depends on whether AD RMS uses SQL Server or WID. To back up the templates, configure the templates to export to a shared folder and then back them up.

When you perform a recovery of the AD RMS role, it might be necessary to delete the **ServiceConnectionPoint** object from AD DS. You need to do this if you are recovering an AD RMS root configuration server, and that server attempts to provision itself as a licensing-only server.

## Decommissioning and removing AD RMS

Prior to removing an AD RMS server, you should decommission that server. Decommissioning AD RMS puts the cluster into a state where consumers of AD RMS–protected content can obtain special keys that decrypt that content, regardless of the existing restrictions that have been placed on the use of that content. If you do not have a decommissioning period, and if you simply remove the AD RMS server, the AD RMS–protected content will become inaccessible.

To decommission AD RMS, perform the following procedure:

1. Sign in to the server that hosts AD RMS and that you want to decommission.
2. Modify the access control list of the **Decommissioning.asmx** file. Grant the **Everyone** group **Read & execute** permission on the file. This file is stored in the **%SystemDrive%\inetpub\wwwroot\\_wmcs\decommission** folder.
3. In the **AD RMS** console, expand the **Security Policies** node, and then click the **Decommissioning** node.
4. In the **Actions** pane, click **Enable Decommissioning**, and then click **Decommission**.
5. When prompted to confirm that you want to decommission the server, click **Yes**.

After the AD RMS decommissioning process completes, prior to uninstalling the AD RMS role, you should export the AD RMS server licensor certificate.

- Decommission an AD RMS cluster prior to removing it:
  - Decommission to provide a key that decrypts previously published AD RMS content
  - Leave the server in a decommissioned state until all the AD RMS–protected content is migrated
- Export the server licensor certificate prior to uninstalling the AD RMS role

## Monitoring AD RMS

Monitoring AD RMS functionality is critical in each deployment scenario. You can monitor AD RMS by using tools that are built in to Windows Server and AD RMS or by using external monitoring services, such as System Center Operations Manager. AD RMS provides three types of reports within the AD RMS console:

- **Statistics reports.** These reports provide you with information about the number of user accounts that have received RACs from the AD RMS cluster. Because a separate CAL is required for each RAC, you can use this report to estimate the number of AD RMS CALs that you need to buy. Statistics reports provide you with the number of user accounts that are certified for AD RMS, the number of certified domain user accounts, and the number of certified federated identities.
- **Health reports.** System health reports provide you with information about requests that the AD RMS server receives within a certain time frame. By using Microsoft Report Viewer, this report generates graphs and numerical data about the total number of requests that AD RMS received. This includes the average duration for processing each request, the number of requests that were successfully

- AD RMS provides built-in monitoring and reporting capabilities
- Microsoft Report Viewer is needed for reporting
- The available reports are:
  - Statistics
  - Health
  - Troubleshooting
- Operations Manager can monitor AD RMS with an existing management pack

processed, and the number of failed requests. You also can see the percentage of successfully completed requests. If you see a large number of failed requests, it might indicate improper client configuration.

- Troubleshooting reports. These reports provide a list of numbers for the total number of successful and failed user requests for each request type. For example, you can see the total number of requests for certification, the total number of requests for finding the service location, and the total number of requests for the server licenser certificate.



**Note:** The statistics reports are available by default. However, to use the health and troubleshooting reports, you must have the Microsoft .NET Framework 3.5 installed, and Microsoft Report Viewer 2008 Service Pack 1 (SP1) or later. These are free from the Microsoft Download Center.



**Note:** You also can monitor AD RMS by using Operations Manager. You can download System Center Management Pack for AD RMS, which provides an early warning to administrators about issues that might affect services so they can investigate and take corrective action, if necessary.



**Additional Reading:** For more information, refer to: "Monitoring Scenarios" at: <http://aka.ms/Pyumg7>

## Implementing external sharing

In some scenarios, you need to enable the sharing of AD RMS–protected content with users from other organizations. AD RMS technology provides several methods to achieve this.

Trust policies allow users who are external to your organization to consume AD RMS–protected content. For example, a trust policy can allow users in Bring Your Own Device environments to consume AD RMS–protected content, even though those devices are not members of the organization's AD DS domain. AD RMS trusts are disabled by default, and you must enable them before you can use them. AD RMS supports the following trust policies:

- Trusted user domains exchange protected content between two organizations
- Trusted publishing domains consolidate the AD RMS architecture
- Federated trusts enable users from partner organizations to access and use a local AD RMS infrastructure
- Microsoft accounts enable standalone users to access AD RMS content
- The Azure authentication system enables an AD RMS cluster to work with partner organizations without requiring a direct federation trust

- Trusted user domains. This trust policy allows an AD RMS cluster to process requests for client licenser certificates or use licenses from users who have RACs issued by a different AD RMS cluster. For example, assume that A. Datum Corporation and Trey Research are separate organizations that have each deployed AD RMS. Trusted user domains allow each organization to publish and consume AD RMS–protected content to and from the partner organization without having to implement AD DS trusts or AD FS.
- Trusted publishing domains. This trust policy allows one AD RMS cluster to issue end-user licenses to content that uses PLs that are issued by a different AD RMS cluster. Trusted publishing domains consolidate the existing AD RMS infrastructure.



- Federation trust. This trust policy provides single sign-on for partner technologies. Federated partners can consume AD RMS–protected content without deploying their own AD RMS infrastructures. A federation trust requires AD FS deployment.
- Microsoft account. You can use this trust policy to allow standalone users with Microsoft accounts to consume AD RMS–protected content that is generated by users in your organization. However, Microsoft account users are unable to create content that will be protected by the AD RMS cluster.
- Azure authentication system. This trust policy allows an AD RMS cluster to process requests to publish and consume AD RMS–protected content from external organizations by accepting claims-based authentication tokens from the Azure authentication system. Rather than configuring a federation trust, each organization has a relationship with the Azure authentication system. The Azure authentication system acts as a trusted broker.

### Implementing external access to AD RMS

The type of external access that you configure depends on the types of external users who need access to your organization's content.

When you are determining which method to use, consider the following questions:

- Does the external user belong to an organization that has an existing AD RMS deployment?
- Does the external user's organization have an existing federation trust with your organization?
- Has the external user's organization established a relationship with an Azure authentication system?
- Does the external user need to publish AD RMS–protected content that is accessible to your RAC holders?

It is possible that organizations will use one solution before settling on another. For example, during the initial stages, only a small number of external users might require access to AD RMS–protected content. In this case, using Microsoft accounts for RACs might be appropriate. When more external users from a single organization require access, a different solution might be appropriate. The financial benefit of a solution for an organization must exceed the cost of implementing that solution.

### Check Your Knowledge

Question	
To implement an AD RMS cluster, which components are necessary?	
Select the correct answer.	
<input type="checkbox"/>	Office
<input type="checkbox"/>	A service account
<input type="checkbox"/>	A database
<input type="checkbox"/>	AD FS
<input type="checkbox"/>	A Secure Sockets Layer (SSL) certificate

**Question:** When you decide to remove your AD RMS cluster from AD DS, what should you do first?

## Lesson 3

# Configuring AD RMS content protection

AD RMS uses rights policy templates to enforce a consistent set of policies to help protect content. When configuring AD RMS, you need to develop strategies to help ensure that users will still be able to access AD RMS-protected content from a computer that is not connected to an AD RMS cluster. You also need to develop strategies for excluding some users from accessing AD RMS-protected content. Additionally, you need to develop strategies to help ensure that AD RMS-protected content will be recoverable if it has expired, the template has been deleted, or the author of the content is no longer available.

### Lesson Objectives

After completing this lesson, you will be able to:

- Describe rights policy templates.
- Create a rights policy template.
- Provide rights policy templates for offline use.
- Describe exclusion policies.
- Create an exclusion policy for an application.
- Describe the AD RMS Super Users group.

### What are rights policy templates?

Rights policy templates allow you to configure standard AD RMS policies across an organization. For example, you can configure standard templates that grant view-only rights; that block the ability to edit, save, and print; or that block the ability to forward or reply to messages if used with Exchange Server.

You create rights policy templates by using the AD RMS console. They are stored in the AD RMS database, and they can be stored in the XML format. When content is consumed, the client checks with AD RMS to verify that it has the most recent version of the template.

A document author can choose to help protect content by applying an existing template. The author does this by using an AD RMS-aware app. For example, in Word 2003 or later, an author applies a template by using the **Protect Document** function. Word then queries AD DS to determine the location of the AD RMS server. After the AD RMS server is located, the author can use the available templates.

AD RMS templates support the following rights:

- Full Control. Gives a user full control over an AD RMS-protected document.
- View. Gives a user the ability to view an AD RMS-protected document.
- Edit. Allows a user to modify an AD RMS-protected document.
- Save. Allows a user to use the **Save** function with an AD RMS-protected document.

#### Rights policy templates:

- Allow authors to apply standard forms of protection across an organization
- Exist in different apps, which allow different forms of rights
- Allow you to configure rights related to viewing, editing, and printing documents
- Allow you to configure content expiration rights
- Allow you to configure content revocation

- **Export (Save As).** Allows a user to use the **Save As** function with an AD RMS–protected document.
- **Print.** Allows an AD RMS–protected document to be printed.
- **Forward.** Allows the recipient of an AD RMS–protected message to forward that message. This is used with Exchange Server.
- **Reply.** Allows the recipient of an AD RMS–protected message to reply to that message. This is used with Exchange Server.
- **Reply All.** Allows the recipient of an AD RMS–protected message to use the **Reply All** function to reply to that message. This is used with Exchange Server.
- **Extract.** Allows the user to copy data from the file. If this right is not granted, the user cannot copy data from the file.
- **Allow Macros.** Allows the user to utilize macros.
- **View Rights.** Allows the user to view the assigned rights.
- **Edit Rights.** Allows the user to modify the assigned rights.


Rights can only be granted and cannot be explicitly denied. For example, to help ensure that a user cannot print a document, the template associated with the document must not include the Print right.

Administrators are also able to create custom rights that can be used with AD RMS–aware apps.

AD RMS templates can also configure documents with the following properties:

- **Content expiration.** This determines when the content expires. The options include:
  - Never. The content never expires.
  - Expires on a particular date. The content expires at a particular date and time.
  - Expires after. The content expires in a particular number of days after creation.
- **Use license expiration.** This determines the time interval in which the use license will expire and in which a new one will need to be acquired.
- **Enable users to view protected content by using a browser add-on.** This allows users to view the content by using a browser add-on and does not require them to have an AD RMS–aware app.
- **Require a new use license each time content is consumed.** When you enable this option, client-side caching is disabled. This means that the document cannot be consumed when the computer is offline.
- **Revocation policies.** This allows the use of a revocation list. This allows an author to revoke the permission to consume content. You can specify how often the revocation list is checked, with the default being once every 24 hours.

After an AD RMS policy template is applied to a document, any updates to that template will also apply to that document. For example, if you have a template without a content expiration policy that is used to help protect documents, and you modify that template to include a content expiration policy, the protected documents will then have an expiration policy. Template changes are reflected when the end-user license is acquired. If end-user licenses are configured to not expire, and a user who is accessing the document already has a license, that user might not receive the updated template.

 **Note:** You should avoid deleting templates, because documents that use those templates will become inaccessible to everyone except for members of the Super Users group. As a best practice, archive templates instead of deleting them.

You can view the rights associated with a template by selecting the template within the AD RMS console, and then on the **Actions** menu, clicking **View Rights Summary**.

## Demonstration: Creating a rights policy template

In this demonstration, you will see how to create a rights policy template that allows users to view a document but not to perform other actions.

### Demonstration Steps

- On **LON-SVR1**, in the **AD RMS** console, use the **Rights Policy Template** node to create a Distributed Rights Policy Template with the following properties:
  - Language: **English (United States)**
  - Name: **ReadOnly**
  - Description: **Read-only access. No copy or print.**
  - Users and rights: **executives@adatum.com**
  - Rights for Anyone: **View**
  - **Grant owner (author) full control right with no expiration**
  - Content Expiration: **Expires after 7 days**
  - Use license expiration: **Expires after 7 days**
  - Require a new use license every time content is consumed (disable client-side caching): **Enabled**

## Providing rights policy templates for offline use

If users publish AD RMS–connected templates when they are not connected to the network, you need to help ensure that they have access to a local copy of the available rights policy templates.

You can configure computers to automatically acquire and store published rights policy templates so that they are available offline. For you to enable this feature, the computers must run Windows Vista SP1 or later for clients and Windows Server 2008 or later for servers.

To enable this functionality, in **Task Scheduler**, enable the **AD RMS Rights Policy Template Management (Automated)** scheduled task, and then edit the following registry key:

```
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\DRM
```

Provide the following location to store templates:

```
%LocalAppData%\Microsoft\DRM\Templates
```

1. Enable the AD RMS Rights Policy Template Management (Automated) scheduled task
2. Edit the registry key to specify the template shared folder location
3. Publish templates to a shared folder

When computers that run these operating systems are connected to the domain, the AD RMS client polls the AD RMS cluster for new templates, or the client updates existing templates.

As an alternative to templates distribution, you can use shared folders as storage for templates. You can configure a shared folder for templates by performing the following procedure:

1. In the **AD RMS** console, right-click the **Rights Policy Templates** node, and then click **Properties**.
2. In the **Rights Policy Templates Properties** dialog box, specify the location of the shared folder to which templates will be published.

## What are exclusion policies?

Exclusion policies help you to prevent specific user accounts, client software, or apps from using AD RMS.

### User Exclusion

The User Exclusion policy allows you to configure AD RMS so that specific user accounts, which are identified by an email Active Directory attribute of these user accounts, cannot obtain use licenses. You do this by adding each user's RAC to an exclusion list. User Exclusion is disabled by default. After you enable User Exclusion, you can exclude specific RACs.

Exclusion policies enable you to:

- Block specific users from accessing AD RMS–protected content by blocking their RACs
- Block specific apps from creating or consuming AD RMS–protected content
- Block specific versions of AD RMS clients

You can use User Exclusion when you need to lock a specific user out of AD RMS–protected content. For example, when a user leaves the organization, you might exclude that person's RACs to help ensure that he or she is unable to access protected content. You can block RACs that are assigned to internal and external users.

### Application Exclusion

The Application Exclusion policy allows you to block specific apps, such as Microsoft PowerPoint, from creating or consuming AD RMS–protected content. You can specify apps by the names of their executable files. You also can specify a minimum and a maximum version of the app. Application Exclusion is disabled by default.



**Note:** It is possible to circumvent Application Exclusion by renaming an executable file.

### Lockbox Version Exclusion

The Lockbox Version Exclusion policy allows you to exclude AD RMS clients—such as those with specific operating systems, like Windows XP and Windows Vista. Lockbox Version Exclusion is disabled by default. After you enable Lockbox Version Exclusion, you must specify the minimum lockbox version to use with an AD RMS cluster.



**Additional Reading:** For more information, refer to: "Enabling Exclusion Policies" at: <http://aka.ms/Lnwbcr>

## Demonstration: Creating an exclusion policy for an app

In this demonstration, you will see how to exclude the PowerPoint app from AD RMS.

### Demonstration Steps

1. On **LON-SVR1**, in the **AD RMS** console, enable Application Exclusion.
2. In the **Exclude Application** dialog box, type the following information:
  - o Application File name: **Powerpnt.exe**
  - o Minimum version: **14.0.0.0**
  - o Maximum version: **16.0.0.0**

## AD RMS Super Users group

The AD RMS Super Users group is a special role, and members of this group have full control over all rights-protected content that is managed by the cluster. Super Users group members are granted full owner rights in all use licenses that are issued by the AD RMS cluster on which the Super Users group is configured. This means that members of this group can decrypt any rights-protected content file and remove rights-protection from files.

The AD RMS Super Users group provides a data recovery mechanism for AD RMS-protected content. This mechanism is useful when you need to recover AD RMS-protected data, such as when content has expired, when a template has been deleted, or when you do not have access.

- The Super Users group members are granted full owner rights in all use licenses that are issued by the AD RMS cluster on which the Super Users group is configured
- The Super Users group:
  - Is not configured by default
  - Can be used as a data recovery mechanism for AD RMS-protected content:
    - Can recover content that has expired
    - Can recover content if the template is deleted
    - Can recover content without requiring author credentials
  - Must be an Active Directory group with an assigned email address

Members of the Super Users group are assigned owner use licenses for all the content that is protected by the AD RMS cluster on which that particular Super Users group is enabled. Members of the Super Users group can reset the AD RMS server's private key password.

As a member of the Super Users group, you can access any AD RMS-protected content, although you must be especially careful when you manage the membership of this group. If you choose to use the AD RMS Super Users group, consider implementing restricted groups policy and auditing to limit group membership, and audit any changes that are made. Super Users activity is written to the Application Event log.

The Super Users group is disabled by default. You can enable the Super Users group by performing the following procedure:

1. In the **AD RMS** console, expand the server node, and then click **Security Policies**.
2. In the **Security Policies** area, under **Super Users**, click **Change Super User Settings**.
3. In the **Actions** pane, click **Enable Super Users**.

To set a particular group as the Super Users group:

1. In the **Security Policies\Super Users** area, click **Change super user group**.
2. Provide the email address associated with the Super Users group.

**Question:** What kinds of permissions does a Super Users group have?

## Lab: Implementing an AD RMS infrastructure

### Scenario

A. Datum Corporation performs highly confidential research, so their security team wants to implement additional security for some of the documents that the Research department creates. The security team is concerned that anyone with read access to the documents can modify and distribute them in any way that they choose. The security team wants to provide an extra level of protection that stays with a document even if it moves around the network or outside of the network.

As a senior network administrator at A. Datum Corporation, you need to plan and implement an AD RMS solution that will help to provide the level of protection that the security team requested. The AD RMS solution must provide many options that can be adapted for a wide variety of business and security requirements.

### Objectives

After completing this lab, you will be able to:

- Install and configure AD RMS.
- Configure AD RMS templates.
- Use AD RMS on clients.

### Lab Setup

Estimated Time: 60 minutes

Virtual machines: **20742A-LON-DC1**, **20742A-LON-DC2**, **20742A-LON-SVR1**, and **20742A-LON-CL1**

User name: **Adatum\Administrator**

Password: **Pa\$\$w0rd**

For this lab, you need to use the available virtual machine environment. Before you begin the lab, you must complete the following steps:

1. On the host computer, start **Hyper-V Manager**.
2. In Hyper-V Manager, click **20742A-LON-DC1**, and then in the **Actions** pane, click **Start**.
3. In the **Actions** pane, click **Connect**. Wait until the VM starts.
4. Sign in by using the following credentials:
  - User name: **Administrator**
  - Password: **Pa\$\$w0rd**
  - Domain: **Adatum**
5. Repeat steps 2 and 3 for **20742A-LON-DC2**, **20742A LON-SVR1**, and **20742A-LON-CL1**.

## Exercise 1: Installing and configuring AD RMS

### Scenario

The first step in deploying AD RMS at A. Datum Corporation is to deploy a single server in an AD RMS cluster. You will begin by configuring the appropriate DNS records and the AD RMS service account, and then you will continue to install and configure the first AD RMS server. You will also enable the AD RMS Super Users group.

The main tasks for this exercise are as follows:

1. Configure DNS and the AD RMS service account.
2. Install and configure the AD RMS server role.
3. Configure the AD RMS Super Users group.

► **Task 1: Configure DNS and the AD RMS service account**

1. Sign in to **LON-DC1** as **Adatum\Administrator** with the password **Pa\$\$w0rd**.
2. From **Server Manager**, open the **Active Directory Administrative Center** and create an OU named **Service Accounts** in the **Adatum.com** domain.
3. Create a new user account in the **Service Accounts** OU with the following properties:
  - First name: **ADRMSSVC**
  - User UPN logon: **ADRMSSVC**
  - **User SamAccountName Logon: Adatum\ADRMSSVC**
  - Password: **Pa\$\$w0rd**
  - Confirm Password: **Pa\$\$w0rd**
  - Password never expires: **Enabled**
  - User cannot change password: **Enabled**
4. Create a new global security group in the **Users** container named **AD RMS\_SuperUsers**. Set the email address of this group as **AD RMS\_SuperUsers@adatum.com**.
5. Create a new global security group in the **Users** container named **Executives**. Set the email address of this group as **executives@adatum.com**.
6. Add the user accounts **Aidan Norman** and **Holly Spencer** to the **Executives** group.
7. Use the **DNS Manager** console to create a host (A) resource record in the **Adatum.com** zone with the following properties:
  - Name: **adrms**
  - IP Address: **172.16.0.21**

► **Task 2: Install and configure the AD RMS server role**

1. Sign in to **LON-SVR1** as **Adatum\Administrator** with the password **Pa\$\$w0rd**.
2. From **Server Manager**, use the **Add Roles and Features Wizard** to add the **Active Directory Rights Management Services** role to **LON-SVR1** by using the following option:
  - Role services: **Active Directory Rights Management Services**
3. From the **AD RMS** node in **Server Manager**, click **More** to start the post-deployment configuration of AD RMS.
4. In the **AD RMS Configuration Wizard**, provide the following information:
  - **Create a new AD RMS root cluster**
  - **Use Windows Internal Database on this server**
  - Service Account: **Adatum\ADRMSSVC**
  - Cryptographic Mode: **Cryptographic Mode 2**
  - Cluster Key Storage: **Use AD RMS centrally managed key storage**



- Cluster Key Password: **Pa\$\$w0rd**
  - Cluster Web Site: **Default Web Site**
  - Connection Type: **Use an unencrypted connection**
  - Fully Qualified Domain Name: **http://adrms.adatum.com**
  - Port: **80**
  - Licensor Certificate: **AdatumADRMS**
  - Register AD RMS Service Connection Point: **Register the SCP Now**
5. Use the **Internet Information Services (IIS) Manager** console to enable **Anonymous Authentication** on the **Default Web Site\\_wmcs** and **Default Web Site\\_wmcs\licensing** virtual directories.
  6. Sign out of **LON-SVR1**.



**Note:** You must sign out before you can manage AD RMS. This lab uses port 80 for convenience. In production environments, you would help to protect AD RMS by using an encrypted connection.

### ► Task 3: Configure the AD RMS Super Users group

1. Sign in to **LON-SVR1** as **Adatum\Administrator** with the password **Pa\$\$w0rd**.
2. From **Server Manager**, open the **AD RMS** console, and then enable **Super Users**.
3. Set the **ADRMS\_SuperUsers@adatum.com** group as the **Super Users** group.

**Results:** After completing this exercise, you should have installed and configured AD RMS.

## Exercise 2: Configuring AD RMS templates

### Scenario

Having deployed the AD RMS server, you must now configure the rights policy templates and exclusion policies for the organization. You will then deploy both components.

The main tasks for this exercise are as follows:

1. Configure a new rights policy template.
2. Configure the rights policy template distribution.
3. Configure an exclusion policy.

### ► Task 1: Configure a new rights policy template

- On **LON-SVR1**, use the **Rights Policy Template** node of the **AD RMS** console to create a Distributed Rights Policy template with the following properties:
  - Language: **English (United States)**
  - Name: **ReadOnly**
  - Description: **Read-only access. No copy or print.**
  - Users and rights: **executives@adatum.com**

- Rights for executives@adatum.com: **View**
- **Grant owner (author) full control right with no expiration**
- Content expiration: **7 days**
- Use license expiration: **7 days**
- **Require a new use license every time content is consumed (disable client-side caching)**

► **Task 2: Configure the rights policy template distribution**

1. On **LON-SVR1**, open a Windows PowerShell command prompt, type the following commands, and then press Enter after each one:

```
New-Item c:\rmstemplatess -ItemType Directory
New-SmbShare -Name RMTEMPLATES -Path c:\rmstemplatess -FullAccess ADATUM\ADRMSSVC
New-Item c:\docshare -ItemType Directory
New-SmbShare -Name docshare -Path c:\docshare -FullAccess Everyone
```

2. In the **AD RMS** console, set the Rights Policy Templates file location to **\\LON-SVR1\RMTEMPLATES**.
3. Open **File Explorer**, and then view the **C:\rmstemplatess** folder. Verify that the **ReadOnly.xml** template is present.

► **Task 3: Configure an exclusion policy**

1. On **LON-SVR1**, in the **AD RMS** console, enable **Application Exclusion**.
2. In the **Exclude Application** dialog box, type the following information:
  - Application File name: **Powerpnt.exe**
  - Minimum version: **14.0.0.0**
  - Maximum version: **16.0.0.0**

**Results:** After completing this exercise, you should have configured AD RMS templates.

## Exercise 3: Using AD RMS on clients

### Scenario

As a final step in the deployment, you will verify that the configuration works correctly.

The main tasks for this exercise are as follows:

1. Create a rights-protected document.
2. Verify internal access to AD RMS-protected content as an authorized user.
3. Open the rights-protected document as an unauthorized user.
4. Prepare for the next module.

► **Task 1: Create a rights-protected document**

1. Sign in to **LON-CL1** as **Adatum\Aidan** with the password **Pa\$\$w0rd**.
2. From the **Start** menu, open **Internet Explorer**, and then add **http://adrms.adatum.com** to the local intranet sites.

3. Open **Word 2016**, and then create a document named **Executives Only**. In the document, type the following text: **This document is for executives only, and it should not be modified.**
4. From the **Permissions** section, choose to restrict access. Apply the **ReadOnly** permission template to the document.
5. Save the document in the share **\\lon-svr1\docshare**. Name it **Executives Only.docx**.
6. Sign out of **LON-CL1**.

► **Task 2: Verify internal access to AD RMS–protected content as an authorized user**

1. Sign in to **LON-CL1** as **Adatum\Holly** with the password **Pa\$\$w0rd**.
2. From the **Start** menu, open **Internet Explorer**, and then add **http://adrms.adatum.com** to the local intranet sites.
3. In the **\\lon-svr1\docshare** folder, open the **Executives Only** document.
4. Verify that you are unable to modify or save the document.
5. Select a line of text in the document, and then right-click it. Verify that you cannot modify this text.
6. View the document permissions.
7. Sign out of **LON-CL1**.

► **Task 3: Open the rights-protected document as an unauthorized user**

1. Sign in to **LON-CL1** as **Adatum\Harry** with the password **Pa\$\$w0rd**.
2. From the **Start** menu, open **Internet Explorer**, and then add **http://adrms.adatum.com** to the local intranet sites.
3. In the **\\lon-svr1\docshare** folder, attempt to open the **Executives Only** document.
4. Verify that **Harry** does not have permission to open the document.
5. Sign out of **LON-CL1**.

► **Task 4: Prepare for the next module**

When you finish the lab, revert the VMs to their initial state. To do this, complete the following steps:

1. On the host computer, start Hyper-V Manager.
2. In the **Virtual Machines** list, right-click **20742A-LON-DC1**, and then click **Revert**.
3. In the **Revert Virtual Machine** dialog box, click **Revert**.
4. Repeat steps 2 and 3 for **20742A-LON-SVR1**, **20742A-LON-DC2**, and **20742A-LON-CL1**.

**Results:** After completing this exercise, you should have verified that the AD RMS deployment was successful.

**Question:** What steps can you take to help ensure that you can use IRM services with the AD RMS role?

## Module Review and Takeaways

### Review Questions

**Question:** What are the benefits of having an SSL certificate installed on the AD RMS server when you perform an AD RMS configuration?

**Question:** You need to provide access to AD RMS–protected content for five users who are unaffiliated contractors and who are not members of your organization. Which method should you use to provide this access?

**Question:** You want to block users from protecting PowerPoint content by using AD RMS templates. What steps should you take to accomplish this goal?

### Best Practice

- Prior to deploying AD RMS, you must analyze your organization's business requirements and create the necessary templates. You should meet with the users to inform them of AD RMS functionality and to ask for feedback on the types of templates that they want to have available.
- Strictly control the membership of the Super Users group. Users in this group have complete access to all AD RMS–protected content.

# Module 12

## Implementing AD DS synchronization with Microsoft Azure AD

### Contents:

Module Overview	12-1
<b>Lesson 1:</b> Planning and preparing for directory synchronization	12-2
<b>Lesson 2:</b> Implementing directory synchronization by using Azure AD Connect	12-13
<b>Lesson 3:</b> Managing identities with directory synchronization	12-23
<b>Lab:</b> Configuring directory synchronization	12-37
Module Review and Takeaways	12-43

### Module Overview

Microsoft Azure Active Directory (Azure AD) is an online instance of Active Directory Domain Services (AD DS). Azure AD provides authentication and authorization for most Microsoft cloud offerings, including Microsoft Azure, Microsoft Office 365, and Microsoft Intune. Authentication through Azure AD can be on a cloud-only basis or through directory synchronization from on-premises AD DS. You also have the option to enable password synchronization or enable user authentication with on-premises user accounts through Active Directory Federation Services (AD FS) or other single sign-on (SSO) providers.

In this module, you will learn how to plan, prepare, and implement directory synchronization between local AD DS and Azure AD. This module covers how to prepare an on-premises environment for directory synchronization, install and configure directory synchronization, and manage identities after you enable directory synchronization.

### Objectives

After completing this module, you will be able to:

- Plan and prepare for directory synchronization.
- Implement directory synchronization by using Microsoft Azure Active Directory Connect (Azure AD Connect).
- Manage identities with directory synchronization.

## Lesson 1

# Planning and preparing for directory synchronization

Before you implement directory synchronization, you should first understand how directory synchronization works and the requirements to enable it. You should also know how to prepare your local AD DS for synchronization and configure an Azure AD tenant for the synchronization process.

### Lesson Objectives

After completing this lesson, you will be able to:

- Describe how to extend the scope of AD DS.
- Describe how Azure AD works as an authentication system.
- Describe directory synchronization.
- Describe how to use AD FS with Azure AD.
- Explain how to plan for directory synchronization.
- Describe the prerequisites for directory synchronization and explain how to prepare for directory synchronization.
- Explain how to configure a tenant for directory synchronization.

### Extending the scope of AD DS

AD DS offers significant business and technological benefits. However, AD DS is designed for on-premises, independently managed deployments, and most of its characteristics reflect this presumption. Its authentication and authorization mechanisms rely largely on having domain member computers permanently joined to the domain.

Communication with domain controllers involves protocols such as Lightweight Directory Access Protocol (LDAP) for directory services lookups, the Kerberos protocol for authentication, and Server Message Block (SMB) for downloading Group Policy data. None of these protocols is suitable for Internet environments.

Multitenancy is very difficult to implement within a single domain in AD DS. While it is possible to provide a higher level of autonomy by deploying additional domains within the same forest or by deploying multiple forests with trust relationships between them, such arrangements are complex to set up and manage. AD DS enables you to implement the desired mix of efficiency, control, security, and flexibility within corporate networks, but it is not well suited for today's open, Internet-facing world, dominated by cloud services and mobile devices. Also, AD DS is not designed to work with Internet applications or services.

- Limitations of AD DS is that it was designed primarily for on-premises deployments:
  - Single tenant by design
  - Employs protocols not suited for Internet communication
  - Requires domain-joined computers to deliver full functionality
- You can install AD DS domain controllers on Azure virtual machines



## Extending AD DS authentication

One way to address this shortcoming is to extend the capabilities of AD DS by using an intermediary system that handles translation of AD DS on-premises constructs and protocols (such as tokens and the Kerberos protocol) into their Internet-ready equivalents. The AD FS server role and Web Application Proxy server feature of Windows Server provide this functionality. As a result, users, devices, and applications can take advantage of the authentication and authorization features of AD DS without having to be part of the same domain or a trusted domain.

An example of a capability that is related to device authentication is Azure AD Device Registration (earlier known as Workplace Join), introduced in the Windows Server 2012 R2 operating system, which uses AD DS, AD FS, and Web Application Proxy. Device Registration facilitates the registration of devices that are not domain-joined in an AD DS database. This provides additional authentication and authorization benefits, including SSO to on-premises web applications, and support for conditional access control policies that consider whether an access request originated from a registered device.

## Federation support

The primary feature that AD FS and Web Application Proxy facilitate is federation support. A federation resembles a traditional trust relationship, but it relies on claims (contained within tokens) to represent authenticated users or devices. It relies on certificates to establish trusts and to facilitate secure communication with an identity provider. In addition, it relies on web-friendly protocols such as HTTPS, Web Services Trust Language (WS-Trust), Web Services Federation (WS-Federation), or OAuth to handle transport and processing of authentication and authorization data. Effectively, AD DS, in combination with AD FS and Web Application Proxy, can function as a claims provider that is capable of authenticating requests from web-based services and applications that are not able to, or not permitted to, access AD DS domain controllers directly.

## Microsoft Azure

You can also extend AD DS into the cloud in a different manner—by deploying AD DS domain controllers into virtual machines that are based on Azure infrastructure as a service (IaaS). However, it is critical to ensure that you protect such domain controllers from unauthorized external access. You can use such deployments to build a disaster recovery solution for an existing on-premises AD DS environment, to implement a test environment, or to provide local authentication and authorization to Azure-hosted cloud services that are part of the same virtual network.

## Azure AD as an authentication system

Although Azure AD has many similarities to AD DS, there are also many differences. It is important to realize that using Azure AD is not the same as deploying an Active Directory domain controller on an Azure virtual machine and adding it to your on-premises domain. It is important to know the following characteristics of Azure AD:

- Azure AD is primarily an identity solution, and it is designed for Internet-based applications by using HTTP (port 80) and HTTPS (port 443) communications.
- Azure AD users and groups are created in a flat structure, and there are no organizational units (OUs) or Group Policy objects (GPOs).

### Key differences between Azure AD and AD DS:

- Azure AD is designed for Internet-based applications
- In Azure AD, there are no OUs or GPOs
- Azure AD cannot be queried through LDAP
- Azure AD does not use Kerberos authentication
- Azure AD includes federation services

- Azure AD cannot be queried through LDAP; instead, Azure AD uses the REST API over HTTP and HTTPS.
- Azure AD does not use Kerberos authentication; instead, it uses HTTP and HTTPS protocols such as Security Assertion Markup Language (SAML), WS-Federation, and OpenID Connect for authentication (and OAuth for authorization).
- Azure AD includes federation services, and many third-party services (such as Facebook) are federated with and trust Azure AD.

### Azure AD authentication options

Authentication options when using Azure AD fall into one of the three main categories:

- Cloud-only. Cloud-only identities are exactly as the name suggests: the user identity only exists in the cloud, so all password management and policy control is done through Azure AD. Each user will have two entirely separate identities.
- Directory synchronization with optional password synchronization. With directory synchronization, you set up a directory synchronization server or appliance that provides either one- or two-way synchronization of users, groups, and attributes from on-premises AD DS to Azure AD. In the case of Microsoft Exchange hybrid environments, there is also synchronization of certain attributes from online to on premises. However, it is important to remember that even with password synchronization, there are still two sets of security credentials; it is just that directory synchronization and password sync are keeping them aligned. Users still authenticate to Azure AD to access Microsoft Exchange Online and other online services.
- SSO with AD FS. The SSO option gives authentication control to your directory service. Therefore, users no longer authenticate against Azure AD but against AD FS. Consequently, when a user types user@adatum.com into the sign-in page of a cloud service such as Office 365, the user receives a message telling them that they have been redirected to their organization's sign-in page. They now enter their on-premises identity and authenticate to the online services by using a delegated token that verifies that the user has been successfully authenticated by their on-premises directory service.

In the pilot phase of a deployment, you implement cloud-only identities because this option does not have any on-premises infrastructure requirements. In this phase, you plan for directory synchronization with password synchronization.

Password-synchronized users can sign in to Microsoft cloud services, such as Office 365, Microsoft Dynamics CRM, and Intune, by using the same password they use when signing in to their on-premises network. The user's password synchronizes to Azure AD via a password hash, and authentication occurs in the cloud.

When federation between AD DS and Azure AD is deployed, users will be able to sign in to Microsoft cloud services, such as Office 365, Microsoft Dynamics CRM, and Intune, by using the same password they use when signing in to their on-premises network. The users are redirected to their on-premises AD FS infrastructure for authentication.

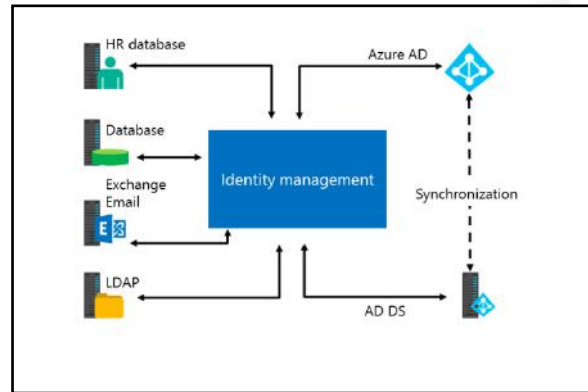


## Overview of directory synchronization

Directory synchronization is the synchronization of directory objects (users, groups, contacts, and computers) between your on-premises AD DS environment and the cloud directory infrastructure, Azure AD.

Although directory synchronization is most commonly used to synchronize data to Azure AD, new features allow two-way synchronization from Azure AD directory to your on-premises AD DS. In addition to directory objects, directory synchronization can provide two-way synchronization of user passwords as well.

Directory synchronization tools, such as Azure AD Connect, perform this synchronization and you install them on a dedicated computer in your on-premises environment.



Integrating your on-premises directories with Azure AD makes your users more productive by providing a common identity for accessing both cloud and on-premises resources. With this integration, users and organizations gain the following advantages:

- Organizations can provide users with a common hybrid identity across on-premises or cloud-based services, including consistent group membership, by leveraging AD DS and then connecting to Azure AD.
- Administrators can use policies set through AD DS to provide conditional access based on application resources, device and user identity, network location, and multifactor authentication without having to perform additional tasks in the cloud.
- Users can leverage their common identity through accounts in Azure AD to access Office 365, Intune, SaaS apps, and non-Microsoft applications.
- Support staff might experience fewer support calls, because if users have fewer passwords to remember, they are less likely to forget them.
- Security can be more certain that user identities and information are protected, because all of the servers and services used in SSO are mastered and controlled on premises.
- Security can have greater confidence in the cloud service when they have the option to use strong authentication, also called two-factor authentication.
- Developers can build applications that leverage the common identity model.

To take advantage of the integration of your on-premises directories with Azure AD, you must deploy a directory synchronization tool. Consequently, the directory synchronization tool provides the following features and functionality:

- SSO
- Two-way synchronization of user passwords
- Skype for Business hybrid environment
- Microsoft SharePoint Server hybrid environment
- Microsoft Exchange Server hybrid environment, including:
  - A shared Global Address List (GAL) between your on-premises Exchange Server environment and Exchange Online
  - A synchronized GAL information from different mail systems

- The ability to add users to and remove users from Office 365 service offerings, which requires two-way synchronization from your on-premises AD DS environment to the Azure AD directory infrastructure and an on-premises Exchange Server hybrid deployment
- The ability to move some or all mailboxes to Office 365 from an on-premises Exchange Server or vice versa
- Safe senders and blocked senders that are enabled on-premises synchronize to Exchange Online
- The ability to send email with basic delegation and send-on-behalf-of synchronize to Exchange Online
- Two-way synchronization of photos, thumbnails, conference room mailboxes, and security and distribution groups
- Filtering and scoping to individual organizational units

When you synchronize user accounts with the directory synchronization tool for the first time, they are marked as nonactivated. These users cannot access any of the services in cloud, and they are not assigned any licenses.

## Planning directory synchronization

When planning for directory synchronization, you should:

- Identify on-premises AD DS preparation tasks. For example, you might need to do AD DS attribute updates or schema extensions. You should also check if an AD DS upgrade is required to meet the minimum version requirements for the forest functional level.
- Determine the required accounts and permissions to use during deployment, configuration, and operation of the directory synchronization tool.
- Identify the network port requirements.
- Identify any requirements for auditing after you enable synchronization.
- Identify any domain controller placement issues that might affect synchronization performance and reliability.
- Plan for multiple AD DS forest or domain scenarios.
- Perform capacity planning. For example, prepare for large-scale deployments requiring Microsoft SQL Server databases, and Azure AD quota limits.
- Plan for two-way directory synchronization.
- Plan for nonroutable domain names, such as .LOCAL, by using additional user principal name (UPN) suffixes.
- Plan for Active Directory filtering to narrow the scope of which AD DS objects to synchronize to Azure AD.

### Best practices for deploying directory synchronization:

- Have a proper project plan
- If AD DS filtering is used, configure it before synchronizing objects to Azure AD
- Work with a cloud services partner
- Perform thorough capacity planning
- Remediate AD DS before deploying directory synchronization
- Add all SMTP domains as verified domains before synchronizing

Best practices for deploying directory synchronization include:

- Have a proper project plan.
- If AD DS filtering is used, configure it before synchronizing objects to Azure AD.
- Work with a cloud services partner.
- Perform thorough capacity planning.
- Remediate AD DS before deploying directory synchronization.
- Add all Simple Mail Transfer Protocol (SMTP) domains as verified domains before synchronizing. You cannot remove a domain until all synchronized objects stop using the domain as a proxy address or UPN.

### **Multiforest deployment considerations**

Although the directory synchronization tool can synchronize with multiple on-premises AD DS forests, the deployment will be more complex. If your organization has multiple forests for authentication (logon forests) and would prefer a simpler deployment option, you might need to plan for the following activities:

- Evaluate consolidating your forests. In general, more support is required to maintain multiple AD DS forests. Unless you have security constraints that dictate the need for separate forests, consider simplifying your on-premises AD DS environment prior to deploying the directory synchronization tool.
- Deploy directory synchronization to support only your primary AD DS forest.

### **Two-way directory synchronization**

By default, the directory synchronization tool writes directory information from your on-premises AD DS to your Azure AD environment. When you configure two-way synchronization in the tool, you enable writeback functionality where the directory synchronization tool copies a limited number of AD DS object attributes from Azure AD and writes them to your on-premises AD DS.

Two-way directory synchronization is required in scenarios where your organization plans to take advantage of advanced features and functionality, such as Exchange Online archiving, safe and blocked senders, and Exchange voice mail. In two-way directory synchronization, the directory synchronization tool will write back the required AD DS object attributes from Azure AD to your on-premises AD DS.



**Additional Reading:** For more information, refer to: "Azure Hybrid Identity Design Considerations Guide" at: <http://aka.ms/ibuqek>

## Prerequisites and preparation for directory synchronization

After you complete a plan for directory synchronization, you will need to review the prerequisites. These tasks will enable you to prepare the environment for directory synchronization:

- Capacity planning for your directory synchronization database server.
- Identifying the hardware requirements for your directory synchronization computer.
- Identifying whether your environment exceeds the Azure AD object quota.
- Reviewing the network ports required by directory synchronization.

When reviewing the prerequisites for directory synchronization, your tasks should include:

- Capacity planning for your directory synchronization database server
- Identifying the hardware requirements for your directory synchronization computer
- Identifying whether your environment exceeds the Azure AD object quota
- Reviewing the network ports required by directory synchronization
- Determining if any schema extensions to AD DS are required

### Capacity planning

Directory synchronization is a critical tool for integration with your cloud service offerings; therefore, you need to plan accordingly to implement directory synchronization properly. In most organizations, user objects from AD DS make up the bulk of the directory synchronization payload and influence both synchronization times and the sizing of your infrastructure.

The directory synchronization tool has a significant database dependency, so you will need to plan for database capacity requirements. If your AD DS forest has fewer than 50,000 objects, then the default Windows Internal Database (WID) should be sufficient. However, if your environment has more than 50,000 objects, then you might require a full version of SQL Server. Most directory synchronization tools scale to forests of 600,000 or more objects.

### Hardware requirements

Deployments with more than 50,000 objects in AD DS require a significant increase in memory requirements (from 4 gigabytes [GB] of random access memory [RAM] to 16 GB); therefore, it is important to implement adequate hardware resources when transitioning from the pilot to the production phase.

Number of objects in AD DS	Central processing unit (CPU)	Memory	Hard disk size
Fewer than 10,000	1.6 gigahertz (GHz)	4 GB	70 GB
10,000–50,000	1.6 GHz	4 GB	70 GB
50,000–100,000	1.6 GHz	16 GB	100 GB
100,000–300,000	1.6 GHz	32 GB	300 GB
300,000–600,000	1.6 GHz	32 GB	4,500 GB
More than 600,000	1.6 GHz	32 GB	5,000 GB

## Azure AD object quota

By default, Azure AD will allow 50,000 objects (users, mail-enabled contacts, and groups). The object quota automatically increases to 300,000 after the first domain is verified. If the object quota is exceeded during directory synchronization, the tenant administrator will receive the following email message:

The Directory Synchronization batch run was completed on <date/time> for tenant <name>.

The following errors occurred during synchronization:

- Synchronization has been stopped. The company has exceeded the number of objects that can be synchronized. Contact Technical Support and ask for an increase in your company's quota.

If you have a requirement to synchronize more than 300,000 objects, you will need to contact Microsoft Technical Support to request a limit increase to the object quota. If you have a requirement to synchronize more than 500,000 objects, you will need a license such as Office 365, Azure AD Basic, Microsoft Azure AD Premium, or Enterprise Mobility Suite. During the planning phase, it is important to plan appropriately for any quota increase requests; otherwise, this could become a deployment blocker if left to the last minute.



**Additional Reading:** For more information, refer to You receive a "This company has exceeded the number of objects that can be synchronized" error in a directory synchronization report at: <http://aka.ms/r4x1q4>

## Network ports

The network traffic for directory synchronization between the directory synchronization tool and Azure AD is over a Secure Socket Layer (SSL). Most of the traffic is outbound, initiated by the directory synchronization computer, and uses port 443. The writeback of passwords uses a Microsoft Azure Service Bus relay as an underlying communication channel, which means that you do not have to open any new ports on your firewall for this feature to work.

Network traffic between the directory synchronization computer and on-premises AD DS uses standard Active Directory-related ports. For uninterrupted directory synchronization, the directory synchronization computer must be able to contact all domain controllers in the forest.

## AD DS preparation

When you prepare for the deployment of directory synchronization, your project plan should include AD DS preparation and the requirements and functionality of Azure AD. To prepare AD DS:

- Identify the source of authority.
- Satisfy domain controller requirements.
- Clean up AD DS by removing old or unnecessary objects.
- Set up auditing.

## Source of authority

For directory synchronization, source of authority refers to the location where Active Directory service objects, such as users and groups, are mastered (an original source that defines copies of an object) in a cross-premises deployment. You can change the source of authority for an object by using one of these scenarios—activate, deactivate, or reactivate directory synchronization from within the Azure Classic Portal or with Windows PowerShell.

## Domain controller requirements

The on-premises AD DS forest must meet specific requirements for the schema master, global catalog servers, and domain controllers. It is important to carefully read the latest requirements and ensure that your on-premises AD DS servers meet those requirements.

## AD DS cleanup

If you are performing directory synchronization to use Office 365, you should prepare your AD DS forest before you begin your Office 365 directory synchronization deployment. Your directory remediation efforts should focus on the following tasks:

- Remove duplicate **proxyAddresses** and **userPrincipalName** attributes.
- Update blank and invalid **userPrincipalName** attributes with valid **userPrincipalName** attributes.
- Remove invalid and questionable characters in the **givenName**, **surname (sn)**, **sAMAccountName**, **displayName**, **mail**, **proxyAddresses**, **mailNickname**, and **userPrincipalName** attributes.

## AD DS auditing

You might want to use AD DS auditing to capture and evaluate the events that are associated with directory synchronization, such as user creation, password reset, adding users to groups, and so on. When you implement directory synchronization, auditing captures directory services logs from the AD DS domain controllers. Security logging might be disabled by default, so you will need to enable it for events to appear in the logs.

## Configuring a tenant for directory synchronization

Before you use directory synchronization to initiate synchronization, you must first enable Active Directory synchronization in your Azure AD tenant. This process can take some time to complete, so it is important to plan for this requirement ahead of the directory synchronization deployment. You can enable Active Directory synchronization in Azure Classic Portal or by using Windows PowerShell.

To enable Active Directory synchronization in the classic portal, complete these steps:

1. In the left navigation pane, click **ALL ITEMS**, and then click your Azure AD instance.
2. On the toolbar, click **DIRECTORY INTEGRATION**.
3. Under **integration with local active directory**, click **Activate**.



**Note:** At the time of writing this course, the option to activate directory synchronization is not available in the new Azure portal.

To enable Active Directory synchronization by using the Microsoft Azure Active Directory Module for Windows PowerShell, type the following command, and press Enter:

```
Set-Mso1DirSyncEnabled -EnableDirSync $true -Force
```

To enable Active Directory synchronization by using the Azure portal:

1. In the left navigation pane, click **ALL ITEMS**, and then click your Azure AD instance.
2. On the toolbar, click **DIRECTORY INTEGRATION**.
3. Under **integration with local active directory**, click **Activate**.

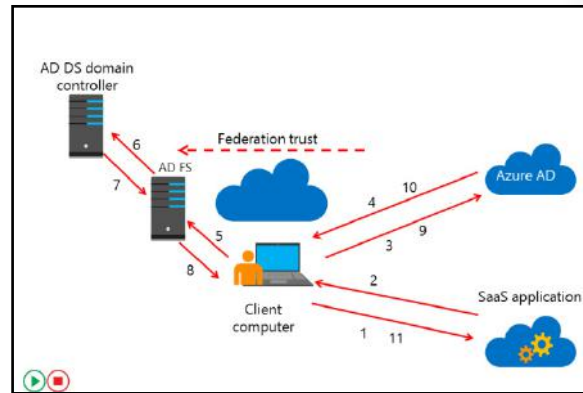
## AD FS and Azure AD

As organizations move services and applications to cloud-based services, it is increasingly important that they provide a simple authentication and authorization experience to their users. Cloud-based services add another level of complexity to the IT environment, because they are located outside the direct administrative control of IT administrators, and they can run on many different platforms.

You can use AD FS to provide an SSO experience to users across various available cloud-based platforms. For example, after users authenticate with AD DS credentials, they could then access Azure-based services such as websites or cloud services, Microsoft Online Services that rely on Azure AD authentication, such as Exchange Online or Microsoft SharePoint Online, and SaaS applications integrated with Azure AD. This functionality requires the use of the directory synchronization tools to synchronize user account information from the on-premises deployment to the corresponding Azure AD tenant.

The following steps describe the process of signing in to a browser-based SaaS application that is integrated with Azure AD when using AD FS. The steps describe what happens when a user tries to access an Azure-based SaaS application by using a web browser:

1. The user opens a web browser and sends an HTTPS request to the SaaS application.
2. The SaaS application determines that the user belongs to an integrated Azure AD instance. The SaaS application provider redirects the user to the user's Azure AD instance.
3. The user's browser sends an HTTPS authentication request to the Azure AD instance.
4. If the user's Azure AD account represents a federated identity, the user's browser is redirected again to the on-premises federation server.
5. The user's browser sends an HTTPS request to the on-premises federation server.
6. If the user is signed in to the on-premises AD DS domain, the federation server will automatically request the AD DS authentication based on the user's existing Kerberos ticket. Otherwise, the user receives a prompt to authenticate with on-premises AD DS.
7. The AD DS domain controller authenticates the user, and then sends the successful authentication message back to the federation server.
8. The federation server creates the claim for the user based on the rules defined as part of AD FS configuration. The federation server places the claims data in a digitally signed security token and forwards it to the user's browser.
9. The user's browser forwards the security token containing claims to Azure AD.
10. Azure AD verifies the validity of the AD FS security token based on the existing federation trust. It creates a new token to access the SaaS application, and then sends it back to the user's browser.
11. The user uses the Azure AD-issued token to access the SaaS application.



**Question:** Verify the correctness of the statement by placing a mark in the column to the right.

Statement	Answer
When you implement directory synchronization, user accounts and groups move from your local AD DS to Azure AD.	



## Lesson 2

# Implementing directory synchronization by using Azure AD Connect

To implement directory synchronization, you need to use the appropriate tools. Microsoft provides Azure AD Connect as a dedicated tool for establishing connection and synchronization between your on-premises AD DS and Azure AD. In this lesson, you will learn how to deploy Azure AD Connect. This lesson includes a review of the Azure AD Connect installation requirements and the options for installing and configuring the tool. You will also review the monitoring of Azure AD Connect.

### Lesson Objectives

After completing this lesson, you will be able to:

- Explain the purpose and uses of Azure AD Connect.
- Describe the Azure AD Connect requirements.
- Describe how Azure AD Connect express synchronization works.
- Describe how Azure AD Connect customized synchronization works.
- Describe how to install and configure Azure AD Connect.
- Describe the Azure AD Connect monitoring features.
- Describe Azure AD Privileged Identity Management.

### Overview of Azure AD Connect

The Azure AD Connect tool, formerly known as Windows Azure Active Directory Synchronization or DirSync, is the latest directory synchronization tool supported by Microsoft. Azure AD Connect is designed to operate as a software-based set-and-forget appliance. The purpose of the tool is to allow coexistence between your on-premises Active Directory environment and cloud-based services such as Office 365 or Microsoft Intune. When you use Azure AD Connect for directory synchronization:

- New user, group, and contact objects in on-premises AD DS are added to Azure AD.
- Attributes of existing user, group, or contact objects that are modified in on-premises AD DS are modified in Azure AD; however, not all on-premises AD DS attributes are synchronized to Azure AD.
- Existing user, group, and contact objects that are deleted from on-premises AD DS are deleted from Azure AD.
- Existing user objects that are disabled in on-premises AD DS are disabled in Azure AD.

**When you use Azure AD Connect for directory synchronization:**

- New user, group, and contact objects in on-premises AD DS are added to Azure AD
- Attributes of existing user, group, or contact objects that are modified in on-premises AD DS are modified in Azure AD
- Existing user, group, and contact objects that are deleted from on-premises AD DS are deleted from Azure AD
- Existing user objects that are disabled on premises are disabled in Azure AD

In a cloud-only deployment, all Azure AD objects are originally created (mastered) in the cloud and must be edited by using cloud-based tools (either using Azure Classic Portal or by using Windows PowerShell cmdlets). In this scenario, Azure AD is referred to as the source of authority for all Active Directory objects.

Azure AD requires a single source of authority for every object. It is important to understand, therefore, that in the scenario where you have deployed Azure AD Connect for Active Directory synchronization, you are mastering objects from within your on-premises AD DS by using tools such as Active Directory Users and Computers or Windows PowerShell—the source of authority is the on-premises AD DS. After the first synchronization cycle completes, the source of authority is transferred from the cloud to the on-premises AD DS. All subsequent changes to cloud objects (except for licensing) are mastered from the on-premises AD DS tools. The corresponding cloud objects are read-only, and Azure AD administrators cannot edit cloud objects if the source of authority is the on-premises AD DS.

## Azure AD Connect requirements

Azure AD Connect is the successor of DirSync, Azure AD Sync, and Microsoft Forefront Identity Manager with the Azure AD connector. It comes preconfigured for synchronizing user, group, contact, and computer objects from your on-premises AD DS to Azure AD.

### Azure AD requirements

To use Azure AD Connect, you need to consider the following Azure AD requirements:

- An Azure subscription or an Azure trial subscription. This is only required for accessing the Azure classic portal and not for using Azure AD Connect. If you are using Windows PowerShell or Office 365, you do not need an Azure subscription to use Azure AD Connect. If you have an Office 365 license, you can use the Office 365 portal from which you can go to the Azure classic portal.
- Add and verify the domain that you plan to use in Azure AD. For example, if you plan to use Adatum.com for your users, then you will need to ensure that the domain name has been verified in Azure AD and that you can see it is available to assign to users.
- An Azure AD directory will, by default, allow 50,000 objects. As discussed earlier in the module, when you verify your domain, the limit increases to 300,000 objects. If you need more objects in Azure AD, you need to open a support case to have the limit increased even further. If you need more than 500,000 objects, you will need a license such as Office 365, Azure AD Basic, Azure AD Premium, or Enterprise Mobility Suite.

When you identify the Azure AD Connect requirements, you should review:

- Azure AD requirements
- Domain and forest requirements
- Operating system and supporting software requirements
- Permissions and accounts
- Database requirements

### Domain and forest requirements

Azure AD Connect requires the Active Directory schema version and the forest functional level to be Windows Server 2003 or later. Azure AD Connect supports a single AD DS forest with Express Settings and supports multiple AD DS forest scenarios and multiple Exchange organizations with customized settings.



**Note:** Using Azure AD Connect for Forefront Identity Manager 2010 R2, using Azure AD Connect with a non-Microsoft directory service, and installing Azure AD Connect on a non-Windows computer are all out of scope for this course.

To integrate with Azure AD Connect, Active Directory domain controllers must run one of the following operating systems:

- Windows Server 2003 Standard Edition or Windows Server 2003 Enterprise Edition with Service Pack 1 (SP1) or later.
- If you plan to use the password writeback feature, the Active Directory domain controllers must be on Windows Server 2008 or later.

When you install Azure AD Connect with express settings, the directory synchronization computer must be a member of a domain, and for single-forest scenarios, you must join this computer to a domain within the same forest that will be synchronized. On the other hand, with customized settings you can install Azure AD Connect on a computer that is not joined to a domain. Azure AD Connect also supports installation on domain controllers. However, for production scenarios, we recommend using a member server for Azure AD Connect.

During the installation of Azure AD Connect, you will be required to select an AD DS attribute for the source anchor. This attribute, also called **sourceAnchor**, should be an attribute that is immutable during the lifetime of a user object, because it is the link between on-premises AD DS and Azure AD. In most scenarios, this might be the **objectGUID**. This attribute will not change unless you move the user account between forests/domains.

However, in a multiforest scenario where you move user accounts between forests, another attribute must be used, such as **employeeID**.



**Note:** Attributes to avoid are those that would change if a person marries or changes assignments. Other attributes that cannot be used include attributes with an at sign (@). Therefore, email addresses and **userPrincipalName** cannot be used.

## Operating system and supporting software requirements

Azure AD Connect requires the following Windows Server operating system versions (64-bit edition only):

- Windows Server 2008 or later.
- Windows Server 2012 or later.
- If you plan to use the password synchronization feature, the server must be on Windows Server 2008 R2 SP1 or later.

In addition, Azure AD Connect requires the following software prerequisites:

- Microsoft .NET Framework 4.5.1 or later
- Windows PowerShell 3.0 or later
- Microsoft Azure AD Module for Windows PowerShell (64-bit version)

## Permissions and accounts

To install and configure Azure AD Connect, you need the following accounts:

- An Azure AD Global Administrator account for the Azure AD directory with which you want to integrate.
- An Enterprise Administrator account for your on-premises AD DS if you use express settings or upgrade from the Microsoft Azure Active Directory Sync Tool (DirSync).

Azure AD Connect uses the Azure AD Global Administrator account to provision and update objects in the Azure AD tenant when you initiate directory synchronization. If you create a dedicated service account in Azure AD for directory synchronization in place of the Azure AD tenant administrator account, it is important to disable the default 90-day password expiration; otherwise, the synchronization service

will stop working when the password expires for the Azure AD tenant administrator account. In this scenario, you will need to reconfigure Azure AD Connect to update the password.

To disable password expiration for the service account in Azure AD by using Azure AD Module for Windows PowerShell, type the following command, and then press Enter:

```
Set-MsolUser -UserPrincipalName <service account>@<domain>.onmicrosoft.com -  
PasswordNeverExpires $true
```

The account used to install and configure Azure AD Connect must have the following permissions:


- Enterprise Administrator permission in your on-premises AD DS. This is required to create the directory synchronization service account in AD DS.
- Local administrator permission on the Azure AD Connect computer. This is required to install the Azure AD Connect tool.

The account used to configure Azure AD Connect and run the configuration wizard must reside in the local group **ADSyncAdmins** on the Azure AD Connect computer. By default, the account used to install Azure AD Connect (the Enterprise Administrator account) is added automatically to this group during installation.

The Enterprise Administrator account is only required when installing and configuring Azure AD Connect, and the Enterprise Administrator credential is not stored or saved by the configuration wizard.

The Enterprise Administrator account is required to:

- Create the MSOL\_<id> domain service account in the **CN=Users** container of the root domain.
- Delegate the following permissions to MSOL\_<id> on each domain partition in the forest:
  - Replicating Directory Changes
  - Replicating Directory Changes all
  - Replication Synchronization


 **Note:** Because it poses a security risk with the service account that it uses, Azure AD Connect does not support using a group Managed Service Account to connect to your on-premises AD DS environments. By default, Azure AD Connect creates service accounts with minimal privileges but with nonexpiring passwords on the computer that runs Azure AD Connect and in both the on-premises AD DS and the Azure AD tenant.

During an Azure AD Connect configuration, you can enable the Exchange hybrid deployment feature. Previously known as *rich coexistence*, this feature allows for the coexistence of Exchange mailboxes both on premises and in Azure by synchronizing a specific set of attributes from Azure AD back into your on-premises AD DS. During deployment, the Enterprise Administrator account will create an **MSOL\_Active Directory\_Sync\_RichCoexistence** group in the **CN=Users** container of the root domain automatically. In addition, the Enterprise Administrator account will delegate write permissions for particular AD DS attributes that write back from Azure AD to your on-premises AD DS.

The following accounts are created in your on-premises AD DS during Azure AD Connect configuration:

- MSOL\_<id>. This account is created during installation of Azure AD Connect. It is configured to synchronize to Azure AD. The account has directory replication permissions in your on-premises AD DS and write permission on certain attributes to enable the Exchange hybrid deployment.

- AAD\_<id>. This is the service account for the synchronization engine. It is created with a randomly generated complex password automatically configured to never expire. When the directory synchronization service runs, it uses the service account credentials to read from your on-premises AD DS and then to write the contents of the synchronization database to Azure AD by using the Azure AD tenant administrator credentials specified during configuration of Azure AD Connect.

 **Note:** Do not change this service account after installing Azure AD Connect, because directory synchronization will attempt to use the service account created during setup. If the account is changed, directory synchronization will stop running and scheduled directory synchronizations will no longer occur.

### Database requirements

Azure AD Connect requires a SQL Server database to store identity data. By default, SQL Server 2012 Express LocalDB (a light version of SQL Server Express 2012 SP1) is installed, and the service account for the service is created on the local computer. SQL Server Express has a 10 GB database limit, which allows you to manage approximately 100,000 objects. In large deployments, you might need to manage a higher volume of objects. In this scenario, configure Azure AD Connect to a full version of SQL Server. Azure AD Connect supports all versions of SQL Server, from Microsoft SQL Server 2008 (with SP4 or later) to Microsoft SQL Server 2014.

When you deploy to a different version of SQL Server, SQL Server rights are required to create the database used by Azure AD Connect and to enable the SQL Server service account with the role of **db\_owner**. You can achieve this by ensuring that the account used to install Azure AD Connect has the sysadmin permission to the SQL Server database and that the service account used to run Azure AD Connect has the public permission to the database used by Azure AD Connect.

### Azure AD Connect express synchronization

During the installation of Azure AD Connect, you can choose the express settings. This is the default option and one of the most common scenarios. When you do this, Azure AD Connect deploys synchronization with the password synchronization option. This is for a single forest only and allows your users to use their on-premises passwords to sign in to the cloud services based on Azure AD. We recommend that you use the express settings.

During the installation of Azure AD Connect with express settings, the installer:

- Installs the synchronization engine.
- Configures the on-premises AD DS connector.
- Enables password synchronization.
- Configures synchronization services.
- Configures sync services for Exchange hybrid deployment (optional).
- Enables automatic upgrade of Azure AD Connect.

- Scenarios for using the express settings include:
  - You have a single AD DS forest
  - Users sign in with the same password by using passwords synchronization
- Installing Azure AD Connect with express settings:
  - Installs the synchronization engine
  - Configures Azure AD Connector
  - Configures the on-premises AD DS connector
  - Enables password synchronization
  - Configures synchronization services
  - Configures sync services for Exchange hybrid deployment (optional)
  - Enables automatic update for Azure AD Connect

When you use the express settings, the synchronization will automatically start when the installation completes (though you can choose not to do this).

## Azure AD Connect customized synchronization

An alternative option to the express settings is installing Azure AD Connect with customized settings. This option is beneficial if you have additional configuration options or need optional features that are not covered in the express installation. You can select customized settings for the following scenarios:

- When you have multiple forests.
- When you customize your sign-in option, such as AD FS for federation, or use a non-Microsoft identity provider.
- When you customize synchronization features, such as filtering and writeback.

You can select Customized Settings for the following scenarios:

- When you have multiple forests
- When you customize your sign-in option, such as AD FS for federation, or use a non-Microsoft identity provider
- When you customize synchronization features, such as filtering and writeback


In addition to the required components that are installed as part of express settings, you might select the following optional components during installation:

- Specify a custom installation location. This optional component allows you to specify a different location to install Azure AD Connect.
- Use an existing server running SQL Server. This optional component allows you to select an existing database server.
- Use an existing service account. This optional component allows you to specify an existing service account. By default, Azure AD Connect will create a local service account for the synchronization services to use. The password is generated automatically and unknown to the person installing Azure AD Connect. If you specify a remote server running SQL Server, then you will need a service account that has a password that you know.
- Specify custom sync groups. This optional component allows you to specify existing management groups for Azure AD Connect. By default, Azure AD Connect will create four groups on the server when the synchronization services install. These groups include the Administrators group, Operators group, Browse group, and Password Reset group. Use this option if you prefer to specify your own groups. The groups must be on the server and cannot be located in the domain.

During the installation of Azure AD Connect with Customized Settings, the installer will allow you to enable the following features:


- Select the SSO Method. This feature allows you to specify the SSO method for users. The SSO methods include **password synchronization**, **federation with AD FS**, and **do not configure**.
- Connect multiple on-premises directories or forests. This feature allows you to connect to one or more AD DS domains or forests.
- Matching across forests. This feature allows you to define how Azure AD represents users from your AD DS forests. A user might either be represented only once across all forests or have a combination of enabled and disabled accounts.

- Sync filtering based on organizational units. This feature allows you to run a small pilot where only a small subset of objects is created in Azure AD. To use this feature, create an organizational unit in your AD DS and then add the users and groups that should synchronize with Azure AD to the organizational unit. You can later add or remove users from this group to maintain the list of objects that should be present in Azure AD.
- Select the Source Anchor. This feature allows you to choose the primary key that will link the on-premises user with the user in Azure AD.
- Select the login attribute. This feature allows you to choose the attribute users will use when they sign in to Azure AD and cloud services such as Office 365. Typically, this should be the **userPrincipalName** attribute. However, if this attribute is nonroutable and cannot be verified, then it is possible to select another attribute, for example email, as the attribute holding the login ID, known as **Alternate ID**.

 **Additional Reading:** For more information, refer to: "Configuring Alternate Login ID" at: <http://aka.ms/nqh5gc>

- Exchange hybrid deployment. This optional feature enables for the coexistence of Exchange mailboxes both on premises and in Office 365 by synchronizing a specific set of attributes from Azure AD back to your on-premises AD DS.
- Azure AD app and attribute filtering. This optional feature enables you to tailor the set of synchronized attributes to a specific set, based on Azure AD apps.
- Password hash synchronization. You can enable this optional feature if you selected federation as the SSO solution. You can then use password synchronization as a backup option.
- Password writeback. With this optional feature, password changes that originate in Azure AD are written back to your on-premises AD DS. You typically deploy this feature when you want to enable users for self-service password reset of their Azure AD passwords.
- Group writeback. With this optional feature, if you use the Groups in Office 365 feature, you can have these Office 365 groups synchronize to your on-premises AD DS as a distribution group. This option is only available if you have deployed Exchange Server on premises.
- Device writeback. With this optional feature, device objects in Azure AD are written back to your on-premises AD DS for conditional access scenarios.
- Directory extension attribute sync. Not available in previous directory synchronization versions, this optional feature enables you to extend the schema in Azure AD with custom attributes that are added by your organization or other attributes in your on-premises AD DS.

After you select the optional features, the Azure AD Connect installer offers the option to deploy a new Windows Server 2012 R2 or later AD FS farm or to select an existing Windows Server 2012 R2 or later AD FS farm. In addition, the Azure AD Connect installer offers the option to set up the federation relationship between AD FS and Azure AD. It configures AD FS to issue security tokens to Azure AD and configures Azure AD to trust the tokens from this specific AD FS instance.

 **Note:** The Azure AD Connect installer will only allow you to configure the trust for a single domain. You can configure additional domains at any time by opening Azure AD Connect again and performing this task.

During the final stages of the Azure AD Connect installer, you will have the option to start synchronization automatically after the installation is complete (though you can choose not to do this). You will also have the option to enable the staging mode. This process allows you to set up a new directory synchronization server in parallel with an existing server.

You can have one directory synchronization server connected to one Azure AD directory in the cloud. If you want to move from another server, for example, from a server running DirSync, you can enable Azure AD Connect in the staging mode. When enabled, the sync engine will import and synchronize data as normal, but it will not export anything to Azure AD and will turn off password sync and password writeback.

While you are working in the staging mode, it is possible to make required changes to the sync engine and review what is about to be exported. When the configuration looks good, you can run the installation wizard again and disable the staging mode. This will enable data to be exported to Azure AD.



**Note:** Ensure that you disable the other directory synchronization server at the same time you configure Azure AD Connect so that only one server exports actively to Azure AD.

## Demonstration: Installing and configuring Azure AD Connect

### Demonstration Steps

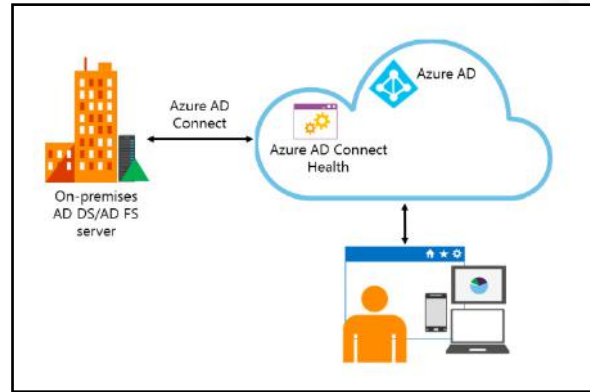
1. On **LON-SVR1**, download and run Azure AD Connect setup from <http://www.microsoft.com/en-us/download/details.aspx?id=47594>.
2. Choose to customize the setup process.
3. Choose **Password Synchronization** as a setup mode.
4. Use **SYNC@yourdomain.onmicrosoft.com** to connect to Azure AD and use **Adatum\administrator** to connect to the local AD DS.
5. Choose to synchronize only the **Research** group to Azure AD.
6. Enable **Password writeback**.
7. Wait until Azure AD Connect performs the initial synchronization.
8. Sign in to the Azure classic portal, and then verify that the objects are synchronized by going to the **USERS** tab.
9. On **LON-SVR1**, open **Synchronization Service Manager**, and then review the completed synchronization tasks.



## Azure AD Connect monitoring features

Azure AD Connect Health helps you monitor and gain insight into your on-premises identity infrastructure and the synchronization services available through Azure AD Connect. It offers you the ability to view alerts, performance, usage patterns, configuration settings, and allows you to maintain a reliable connection to Azure AD. You accomplish this by using an agent that is installed on the targeted servers.

The Azure AD Connect Health page presents the information retrieved from the agent. By using the Azure AD Connect Health portal, you can view alerts, perform performance monitoring, and review usage analytics. This information is located in one easy-to-use place for your convenience.



Azure AD Connect Health for AD FS monitors your on-premises AD FS environment and Azure AD Connect Health for Sync monitors and provides information on the synchronizations that occur between your on-premises AD DS and Azure AD. Azure AD Connect Health for Sync provides the following set of key capabilities:

- View and take action on alerts to ensure reliable synchronizations between your on-premises infrastructure and Azure AD.
- Email notifications for critical alerts.
- View performance data.

To get started with Azure AD Connect Health, perform these four steps:

1. Sign in to the Azure classic portal.
2. Access Azure AD Connect Health by going to the Marketplace and searching for it or by selecting **Marketplace**, and then selecting **Security + Identity**.
3. In the introductory window, click **Create**. This will open another window with your directory information.
4. In the directory window, click **Create**.




**Note:** You will need an Azure AD Premium license to use Azure AD Connect Health.

When you first access Azure AD Connect Health, you will see a window. In this window, you can access the following information:

- **Quick Start.** This option will open the Quick Start window. Here you can download the Azure AD Connect Health agent by selecting **Get tools, access documentation, and provide feedback**.
- **AD FS.** This option represents all of the AD FS services that Azure AD Connect Health is currently monitoring. When you select one of the instances, a window opens with information about that instance. This information includes an overview, properties, alerts, monitoring, and usage analytics.

- **Configure.** This option allows you to turn the following sub-options on or off:
  - **Auto update.** Use this option to automatically update the Azure AD Connect Health agent to the latest version. This option will automatically update the agent on your server to the latest version of the Azure AD Connect Health Agent when it becomes available. Azure AD Connect Health enables this by default.
  - **Allow Microsoft access to your Azure AD directory's health data for troubleshooting purposes only.** When you enable this option, Microsoft will be able to see the same data that you are seeing. This can help with troubleshooting and assistance with issues. Azure AD Connect Health disables this by default.

 **Additional Reading:** For more information, refer to: "Monitor your on-premises identity infrastructure and synchronization services in the cloud" at: <http://aka.ms/dqaaps>

## Azure AD Privileged Identity Management

You can use Azure AD Privileged Identity Management to control and monitor privileged identities and their access to resources that exist in the cloud. Azure AD Privileged Identity Management allows you to grant on-demand administrative access, which minimizes the security risk of granting permanent access to resources in Azure or Office 365. Temporary administrators need to complete the activation process for the assigned role to become active. The process of role activation includes providing information about the duration of the role and the information that the user needs to provide during role assignment. Additionally, you can use Azure AD Privileged Identity Management to discover the users who have administrative roles, get alerts on the usage of privileged roles, and generate reports for administrative access.

Azure AD Privileged Identity Management allows you to:

- Discover which users are the Azure AD administrators
- Enable on-demand, just-in-time administrative access to directory resources
- Get reports about administrator access history and the changes in administrator assignments
- Get alerts about access to a privileged role

You can enable Privileged Identity Management in the Azure classic portal by using an account that is a Global Administrator for the directory. After you enable Privileged Identity Management, you can use the Privileged Identity Management dashboard to monitor the number of users that are assigned privileged roles, and the number of temporary or permanent administrators.

**Question:** When you implement synchronization between AD DS and Azure AD, where do you master AD DS objects?

## Lesson 3

# Managing identities with directory synchronization

After you implement directory synchronization with Azure AD Connect, you should choose how to manage identities in your organization. Also, it is important to carefully monitor the synchronization process so that you can react if a problem arises.

In this lesson, you will learn about managing identities with Azure AD Connect and AD FS. This lesson also explains how to manage users and groups with Azure AD Connect and how to maintain directory synchronization.

## Lesson Objectives

After completing this lesson, you will be able to:

- Compare the options available for identity synchronization.
- Describe how to manage users with directory synchronization.
- Describe how to manage groups with directory synchronization.
- Describe how to modify directory synchronization.
- Describe how to monitor directory synchronization.
- Describe how to troubleshoot directory synchronization.

## Comparing options for identity synchronization

When you run Azure AD Connect, you can choose to synchronize or federate accounts from on-premises AD DS with Azure AD. Synchronization takes place by replicating the objects but optionally can include password synchronization. It is important to understand the difference between the three options for providing synchronization between on-premises AD DS and Azure AD. The three options are:

- Directory synchronization
- Directory synchronization with password synchronization
- Directory synchronization with SSO

Feature	Directory synchronization only	Directory synchronization with password synchronization	Directory synchronization with SSO
Sync users, groups, and contacts with Azure	Yes	Yes	Yes
Sync incremental updates with Azure	Yes	Yes	Yes
Enable hybrid Office 365 scenarios	Yes, limited support	Yes, limited support	Yes, full support
Users can sign in with on-premises credentials	No	Yes	Yes
Reduce password administration costs	No	Yes	Yes
Control password policies from an on-premises directory	No	Yes	Yes
Enable cloud-based MFA	Yes	Yes	Yes
Enable on-premises MFA	No	No	Yes
Authenticate against on-premises directory	No	No	Yes
Implement SSO with organizational credentials	No	No	Yes
Customize the sign-in page	No	No	Yes
Limit access to services based on location or client type	No	No	Yes

## Directory synchronization

With directory synchronization, the objects from on-premises AD DS replicate to Azure AD. For example, directory synchronization maps **user.one@contoso.com** from the on-premises AD DS to **user.one@contoso.onmicrosoft.com** in Azure AD. If you create and verify a custom domain in Azure AD, then you will be able to configure a user name match between the two directories, so that user.one@contoso.com exists in both. Although this is not a requirement for directory synchronization, you must implement it for SSO and the same sign-on to take effect. Any change in user one's attributes in on-premises Active Directory, such as the telephone number, office location, and so on, will replicate through directory synchronization to Azure AD. At this point, the two systems maintain passwords separately.

## Directory synchronization with password synchronization

Enabling password synchronization alongside the synchronization process provides same sign-in facilities. So if user one signs in to his or her domain member computer with a user name of **user.one@contoso.com** and the password of **Pa\$\$w0rd**, the user authenticates by the on-premises Active Directory. If the user then connects to an Azure-based service or application, he or she will see an authentication prompt. If the user's UPN matches between the on-premises AD DS and Azure AD, at the prompt, the user must type the same credentials—**user.one@contoso.com** as the user name and **Pa\$\$w0rd** as the password—to access the Azure-based resources. When the user accesses the Azure-based resource, Azure AD authenticates the user.

In the background, the password synchronization component takes the user's password hash from on-premises Active Directory, encrypts it, and passes it as a string to Azure. Azure decrypts the encrypted hash and stores the password hash as a user attribute in Azure AD.

When the user signs in to an Azure service, the **sign-in challenge** dialog box generates a hash of the user's password and passes that hash back to Azure. Azure then compares the hash with the one in that user's account. If the two hashes match, then the two passwords must also match and the user receives access to the resource.

The **sign-in challenge** dialog box provides the facility to save the credentials so that the next time the user accesses the Azure resource, he or she will not see an authentication prompt. However, it is important to understand that this is same sign-in, not SSO. The user still authenticates against two separate directory services albeit with the same user name and password. However, for many organizations, the simplicity of this solution, without the added complexities and costs of an AD FS implementation, makes the lack of true SSO, a small price to pay.

## Directory synchronization with SSO

Azure AD Connect provides a simple wizard to deploy and configure AD FS, which in the background uses directory synchronization to replicate objects to Azure AD. With SSO, directory synchronization synchronizes user, group, and contact information from on-premises AD DS to Azure AD. These objects appear as directory service objects in Azure AD.

The difference between password synchronization and SSO is that in SSO, instead of two separate authentication processes taking place—one in the on-premises AD DS and the other in Azure AD—a federation trust establishes between Azure AD and the on-premises AD DS. This trust relationship enables users to access applications and resources in Azure by using their domain accounts in AD DS. These users also appear as users in Azure AD because SSO integrates Azure AD with the on-premises AD DS. However, the authentication of those users does not take place in Azure AD but in the on-premises AD DS.

Authorization to access Azure resources is separate from authentication, and it takes place on the resource side, in this case Azure. The on-premises AD DS generates a token, which passes to AD FS and then to Azure by using the federation trust relationship.

## Feature comparison

The following table lists the features that each directory synchronization option supports.

Feature	Directory synchronization only	Directory synchronization with password synchronization	Directory synchronization with SSO
Sync users, groups, and contacts with Azure	Yes	Yes	Yes
Sync incremental updates with Azure	Yes	Yes	Yes
Enable hybrid Microsoft Office 365 scenarios	Yes, limited support	Yes, limited support	Yes, full support
Users can sign in with on-premises credentials	No	Yes	Yes
Reduce password administration costs	No	Yes	Yes
Control password policies from an on-premises directory	No	Yes	Yes
Enable cloud-based multifactor authentication (MFA)	Yes	Yes	Yes
Enable on-premises MFA	No	No	Yes
Authenticate against an on-premises directory	No	No	Yes
Implement SSO with organizational credentials	No	No	Yes
Customize the sign-in page	No	No	Yes
Limit access to services based on location or client type	No	No	Yes

## Requirements

The following table lists the high-level requirements for each directory synchronization option.

Requirement	Directory synchronization only	Directory synchronization with password synchronization	Directory synchronization with SSO
On-premises Azure AD Connect server	Yes	Yes	Yes
AD FS server infrastructure	No	No	Yes
AD FS proxy or Web Application Proxy infrastructure	No	No	Yes

If AD FS is unavailable, users will not be able to authenticate, and they will not be able to use Azure resources. If the Azure AD Connect with Directory Synchronization server is unavailable, recent attribute changes—including password hashes, if enabled—will not synchronize, but users will still be able to access resources. Effectively, deploying reliable and highly available SSO has much higher resource and management demands than either the directory synchronization only option or the directory synchronization with password synchronization option.

## Managing users with directory synchronization

When you successfully deploy Azure AD Connect and enable scheduled synchronization, there are several required management tasks to ensure users synchronize efficiently.


### User writeback

User accounts created in Azure AD can now synchronize back to on-premises AD DS. To enable the user writeback feature for Azure AD Connect, you need to enable the **user writeback** option during installation of Azure AD Connect, with customized settings, and then run the following Windows PowerShell cmdlets on the Azure AD Connect server:

After you deploy Azure AD Connect successfully and enable scheduled synchronization, perform these required management tasks to ensure users synchronize efficiently:

- User writeback
- Password writeback
- Device writeback
- Primary SMTP address management
- Recovery from accidental deletes
- Recovery from unsynchronized deletes
- Accidental account deletion
- Bulk activation of new accounts

```
Import-Module 'C:\Program Files\Microsoft Azure Active Directory
Connect\AdPrep\AdSyncPrep.psm1
Initialize-ADSyncUserWriteBack -AdConnectorAccount $accountName -UserWriteBackContainerDN
$userOU
```

 **Note:** **\$accountName** is the account that will be used by Azure AD Connect to manage objects in AD DS; this is usually an account in the form of an Azure AD number. **\$userOU** is the OU where these cloud users will be stored in on-premises AD DS.

 **Note:** User writeback requires that the AD DS forest be running Windows Server 2012 R2 or later.

After these cmdlets complete executing, the Azure AD Connect service account to on-premises AD DS will have permission to write objects to the **\$userOU** OU. You can view the permissions in Active Directory Users and Computers for this OU, if you enable the **Advanced** mode in the console. There should be a permission entry for this account that is not inherited from the parent OUs.

After the synchronization completes, Azure AD users will appear in the on-premises container that you selected during the configuration.



**Note:** An Azure AD Premium license is required to enable device writeback.

### Password writeback

Users can now change their passwords via the **login** page or user settings in Azure AD and have them written back to on-premises AD DS. To enable the password writeback feature for Azure AD Connect, you need to enable the password writeback option during installation of Azure AD Connect—with customized settings—and then run the following Windows PowerShell cmdlets on the Azure AD Connect server:

```
Get-ADSyncConnector | fl name,AADPasswordResetConfiguration
Get-ADSyncAADPasswordResetConfiguration -Connector "adatum.onmicrosoft.com - AAD"
Set-ADSyncAADPasswordResetConfiguration -Connector "adatum.onmicrosoft.com - AAD" -Enable
$true
$cmd = "dsac1s.exe '$passwordOU' /I:S /G '$accountName`:CA;`Reset Password`;user'"
Invoke-Expression $cmd | Out-Null
$cmd = "dsac1s.exe '$passwordOU' /I:S /G '$accountName`:CA;`Change Password`;user'"
Invoke-Expression $cmd | Out-Null
$cmd = "dsac1s.exe '$passwordOU' /I:S /G '$accountName`:WP;lockoutTime;user'"
Invoke-Expression $cmd | Out-Null
$cmd = "dsac1s.exe '$passwordOU' /I:S /G '$accountName`:WP;pwdLastSet;user'"
Invoke-Expression $cmd | Out-Null
```



**Note:** Azure AD Connect uses the **\$accountName** account to manage objects in AD DS. This is usually an account in the form of Azure AD number. **\$passwordOU** is the OU where these cloud users will be stored in on-premises AD DS.



**Note:** Password writeback requires that the AD DS forest be running Windows Server 2012 R2 or later.

After these cmdlets complete executing, the following configuration occur:

- The Azure AD Connect connectors are enabled for password reset.
- The Azure AD Connect service account to on-premises AD DS will have permission to reset passwords to objects in the **\$passwordOU** OU. You can view the permissions in Active Directory Users and Computers for this OU if you enable the **Advanced** mode in the console. There should be a permission entry for this account that is not inherited from the parent OUs.



**Note:** An Azure AD Premium license is required to enable device writeback.

### Device writeback

Devices that are enrolled with Office 365 mobile device management (MDM) or Intune can sign in to AD FS-controlled resources based on the user and the device they are on. You use device writeback to enable conditional access, based on devices, in order to access AD FS protected applications, or relying party trusts. This provides additional security and assurance that only trusted devices can access applications.

To enable the device writeback feature for Azure AD Connect, you need to enable the **device writeback** option during installation of Azure AD Connect—with customized settings—and then run the following three Windows PowerShell cmdlets on the Azure AD Connect server:

```
Install-WindowsFeature -Name AD-DOMAIN-Services -IncludeManagementTools
Import-Module 'C:\Program Files\Microsoft Azure Active Directory
Connect\AdPrep\AdSyncPrep.psm1'
Initialize-ADSyncDeviceWriteback {Optional:-DomainName [name] Optional:-
AdConnectorAccount [account]}
```



**Note:** **DomainName** is the AD DS domain where device objects are created.

**AdConnectorAccount** is the AD DS account that Azure AD Connect uses to manage objects in the directory. This is the account used by Azure AD Connect to connect to AD DS. If you installed Azure AD Connect by using the express settings, then this account name has the prefix **MSOL\_**.



**Note:**

- Device writeback requires that the AD DS forest be running Windows Server 2012 R2 or later.
- Device writeback requires that AD FS be hosted from Windows Server 2012 R2 (AD FS v3.0) or later.

After previously mentioned cmdlets complete executing, the following configuration occur:

- If not present, they create and configure new containers and objects under **CN=Device Registration Configuration,CN=Services,CN=Configuration,[forest-dn]**, where **forest-dn** is the Distinguished Name of your AD DS forest.
- If not present, they create and configure new containers and objects under **CN=RegisteredDevices,[domain-dn]**, where **forest-dn** is the Distinguished Name of your AD DS forest. Device objects are created in this container.
- They set necessary permissions on the Azure AD Connector account to manage devices on your AD DS.



**Note:** An Azure AD Premium license is required to enable device writeback.

### Primary SMTP address management

One of the key user maintenance tasks is to manage user mailbox attributes, in particular, primary SMTP addresses. For an on-premises user account to get the correct primary SMTP address, it needs to be mailbox-enabled either by using the Microsoft Exchange 2016 admin center, or by setting the **mail** attribute manually to mail-enable the user.



**Note:** If a primary SMTP address is not set for a user account, Office 365 will use a **@domain.onmicrosoft.com** as the user's default SMTP address.

If it is not possible to ensure that all synchronized users will have a valid primary SMTP address prior to synchronization, you can use user attribute filtering to ensure that all accounts without a valid UPN are excluded from the synchronization scope.



## Recovery from accidental deletes

Azure AD now supports soft deletes. After you delete a user in Azure AD, either following synchronization or if you manually remove an unsynchronized user in Azure AD, the user's data is deleted and the user's licenses can be reassigned; however, accounts remain recoverable for 30 days. After the cloud recycle bin is purged (hard delete), it is no longer possible to restore deleted accounts.

## Recovery from unsynchronized deletes

Another important maintenance task is dealing with an on-premises delete that does not synchronize to Azure AD so that the linked object is not removed from Azure AD. This situation might occur if directory synchronization has not yet completed or if directory synchronization failed to delete a specific cloud object, both of which result in an orphaned Azure AD object.

To resolve this issue, follow these steps:

1. Manually run a directory synchronization update.
2. Force directory synchronization.
3. Check that directory synchronization occurred correctly.
4. Verify directory synchronization.

If the above steps validate that directory synchronization is working correctly but the AD DS object deletion has still not propagated to Azure AD, you can manually remove the orphaned object by using one of the following Azure AD Module for Windows PowerShell cmdlets:

```
Remove-MsolContact  
Remove-MsolGroup  
Remove-MsolUser
```

For example, to manually remove an orphaned user originally created by using directory synchronization, run the following cmdlet:

```
Remove-MsolUser -UserPrincipalName <username>@<cloud domain>
```

## Accidental account deletion

If you accidentally delete a user account and a directory synchronization cycle runs, this action will delete the user in Azure AD. However, if you have the recycle bin feature enabled in AD DS, you can recover the account from the recycle bin and the link between the accounts is re-established. If you do not have the recycle bin enabled, you might need to create another account with a new GUID.

## Bulk activation of new accounts

User accounts that you create in Azure AD through directory synchronization are not automatically activated for cloud services such as Office 365. We recommend that you use scripting to manage this requirement. A simple approach makes use of the Azure AD Module for Windows PowerShell cmdlets. For example:

```
Get-MsolAccountSku (to report the Office365 SKUs that, such as EXCHANGESTANDARD)  
Get-MsolUser -UnlicensedUsersOnly | Set-MsolUser -UsageLocation <location>, such as "US"  
Get-MsolUser -UnlicensedUsersOnly | Set-MsolUserLicense -AddLicenses SKU
```

The **isLicensed** user attribute indicates whether a user has a license assigned (True) or not assigned (False). Windows PowerShell can, therefore, report on licensed Office 365 user accounts. To view all users that are licensed in Office 365, type the following command at the Azure AD Module for Windows PowerShell prompt:


```
Get-MsolUser | Where-Object {$_.isLicensed -eq "True"}
To export a list of licensed Office 365 users to CSV, use the following command:
Get-MsolUser | Where-Object { $_.isLicensed -eq "True" } | Export-Csv
C:\Labfiles\LicensedUsers.csv
```

## Managing groups with directory synchronization

Similar to the directory synchronization of users from on-premises AD DS to Azure AD, groups (as well as their membership) in AD DS also synchronize from on-premises AD DS to Azure AD. Similar to the user writeback feature, the group writeback feature also writes groups from Azure AD to on-premises AD DS. The process that Azure AD Connect uses is very similar for user and group objects and has many of the same limitations and caveats.


Although you enable the group writeback feature during installation of Azure AD Connect by selecting the group writeback feature after installing with customized settings, you also need to create the OU and appropriate permissions required for group writeback in AD DS. To help you do this, Azure AD Connect has a built-in cmdlet called **Initialize-ADSyncGroupWriteBack** that prepares AD DS automatically.

- The group writeback feature writes groups from Azure AD to on-premises AD DS
- Cmdlet **Initialize-ADSyncGroupWriteBack** prepares AD DS automatically for group writeback
- **\$groupOU** is the OU where the cloud groups are stored in on-premises AD DS
- Groups from Azure AD are represented as distribution groups in on-premises AD DS
- An Azure AD Premium license is required if you enable a group writeback without the Exchange Server hybrid writeback feature

 **Note:** Group writeback requires that the AD DS forest be running Windows Server 2012 R2 or later.


For example, use the following command to prepare AD DS for group writeback:

```
Import-Module 'C:\Program Files\Microsoft Azure Active Directory
Connect\AdPrep\AdSyncPrep.psm1'
Initialize-ADSyncGroupWriteBack -AdConnectorAccount $accountName -
GroupWriteBackContainerDN $groupOU
```

 **Note:** Azure AD Connect uses the **\$accountName** account to manage objects in AD DS—this is usually an account in the form of an Azure AD number. **\$groupOU** is the OU where these cloud groups are stored in on-premises AD DS.


After these cmdlets complete executing, the Azure AD Connect service account to on-premises AD DS will have permission to write objects to this OU. You can view the permissions in Active Directory Users and Computers for this OU if you enable the **Advanced** mode in the console. There should be a permission entry for this account that is not inherited from the parent OUs.

After the synchronization completes, groups will show up in the on-premises container that you selected during the configuration. These groups will be represented as distribution groups in on-premises AD DS.

 **Note:** At this time, group writeback in Azure AD Connect only supports the writeback of distribution groups.

Similar to user accounts synchronized from Azure AD to on-premises AD DS, the synchronized groups will not show up in the on-premises GAL. As such, you will need to run the **Update-Recipient** cmdlet first as illustrated in the following example:

```
Update-Recipient Group_af905347-5322-4183-a1aa-9522a85bfeb9ad
```

 **Note:** Alternatively, you might use the **Update-AddressList** or **Update-GlobalAddressList** cmdlets to cause the synchronized group to appear. However, these cmdlets will require more cycles on the servers running Exchange Server compared to the **Update-Recipient** cmdlet.


After this cmdlet completes executing, the group will show up in the on-premises GAL. Synchronized groups from Azure AD to on-premises AD DS also includes the membership attribute. If you have enabled user writeback in Azure AD Connect, the group memberships for user accounts created in Azure AD are also included. However, if you have not enabled user writeback in Azure AD Connect, only group memberships for user accounts created on premises are included.

## Modifying directory synchronization

In Azure AD Connect synchronization, you can enable filtering at any time. If you have already deployed the default configurations of directory synchronization and then enabled filtering, the objects that are filtered out are no longer synchronized to Azure AD. Because of this, any objects in Azure AD that were previously synchronized but were then filtered are deleted in Azure AD. If objects were inadvertently deleted because of a filtering error, you can recreate the objects in Azure AD by removing your filtering configurations, and then synchronize your directories again.

Filtering configuration types that you apply to Azure AD Connect include:

- **Domain:**
  - Enables you to select which AD DS domains are allowed to synchronize to Azure AD
  - Uses Azure AD Connect or Synchronization Service Manager
- **OU:**
  - Enables you to select which OUs in AD DS are allowed to synchronize to Azure AD
  - Uses Azure AD Connect or Synchronization Service Manager
- **Attribute:**
  - Enables you to control which objects in AD DS should synchronize to the Azure AD based on criteria of the objects' attributes
  - Uses Synchronization Rules Editor


 **Note:** Although you can enable multiple customizations of filtering in Azure AD Connect, Microsoft does not support all modifications or operations of the Azure AD Connect synchronization outside of the formally documented actions. Any of these actions might result in an inconsistent or unsupported state of Azure AD Connect sync. As a result, Microsoft cannot provide technical support for such deployments.

You might be asking yourself, "Why would I want to enable filtering if Azure AD Connect synchronizes everything I need after implementation?" In most cases, your on-premises AD DS environment contains a lot more objects (for example, user accounts, contacts, and groups) than are required within Azure AD. For instance, service accounts or administrative accounts that are only required on-premises might have no purpose to synchronize to Azure AD. Fortunately, you can filter objects so that only the objects you require online synchronize. Filtering makes synchronization more secure, with no forgotten accounts in online services, and therefore provides a smaller attack surface. Filtering can also help you limit the number of objects, which in turn can help you minimize the size of your Azure AD Connect database and

might prevent the need for a full SQL Server deployment. Remember, if your environment has more than 50,000 objects, then you might require a full version of SQL Server. In many ways, enabling filtering in Azure AD Connect promotes less complexity and increases the speed of directory synchronization.


Here are a few scenarios where filtering might be required to customize the default configuration:

- You plan to use the multiple Azure AD directory topology. For this scenario, you need to apply a filter to control which object should synchronize to a particular Azure AD directory.
- You run a pilot for Azure or Office 365 and only want a subset of users in Azure AD. In a small pilot project like this, it is not important to have a complete GAL to demonstrate the functionality.
- You have many service accounts and other nonpersonal accounts or administrative accounts that you do not want in Azure AD.
- For compliance reasons, your company does not delete any user accounts in on-premises AD DS; you only disable them. However, in Azure AD you only want active accounts to be present.


 **Note:** With the exception of outbound attribute-based filtering, the configurations in Azure AD Connect will be retained when you install or upgrade to a newer version of Azure AD Connect. It is always a best practice to verify that the configuration was not inadvertently changed after an upgrade to a newer version before running the first synchronization cycle.

There are three filtering configuration types that you can apply to Azure AD Connect (listed in order from broad filtering to more detailed filtering):

- **Domain.** This filtering configuration type enables you to select which AD DS domains are allowed to synchronize to Azure AD. You would use the Synchronization Service Manager tool to manage the properties of the Source AD Connector in Azure AD Connect. This tool is installed on the directory synchronization server automatically during deployment of Azure AD Connect.
- **OU.** This filtering configuration type enables you to select which OUs in AD DS are allowed to synchronize to Azure AD. Most organizations already have an OU structure that separates objects that are eligible for synchronization and those that are not, such as the Exchange Security Groups OU, service/administrative accounts OUs, or OUs for specific security groups. You can use Azure AD Connect or the Synchronization Service Manager tool to manage the properties of the Source AD Connector in Azure AD Connect.
- **Attribute.** This filtering configuration type enables you to control which objects in AD DS should synchronize to the Azure AD based on criteria of the objects' attributes. Even with domain filtering and OU filtering, it is possible that some objects in an OU must be excluded from synchronization. It might also be impractical to change the OU design for the purpose of filtering objects that synchronize to Azure AD. While significantly more complex than the Synchronization Service Manager tool, you should use the Synchronization Rules Editor tool to manage the synchronization rules in Azure AD Connect. This tool is installed on the directory synchronization server automatically during deployment of Azure AD Connect.


 **Note:** You use Source AD as the name for your AD DS connector. If you have multiple forests, you will have one connector per forest and the configuration must repeat for each forest.

You can use all, two, or just one filtering configuration type. Which fields you choose depends on how your on-premises AD DS domains are structured, what objects need to synchronize to Azure AD, and the filtering criteria.

 **Note:** Before making changes to filtering, you should disable the scheduled task for synchronization on the directory synchronization server to ensure that you do not accidentally export changes that have not been verified, to Azure AD.

Because filtering in Azure AD Connect can remove many objects in a very short time, you should verify changes to the filters before exporting to Azure AD. After you have completed the configuration steps, we strongly recommend that you follow the verification steps before you export and make changes to Azure AD.

To protect you from deleting multiple objects by accident, the feature that prevents accidental deletes is on by default. If you delete many objects due to filtering (500 by default) you need to follow the steps in the following article to allow the deletes to go through to Azure AD.

 **Additional Reading:** For more information, refer to: "Azure AD Connect sync: Configure Filtering" at: <http://aka.ms/au8smo>

## Monitoring directory synchronization

We recommend that you use System Center Operations Manager (Operations Manager) for monitoring the directory synchronization server and services such as AD DS to ensure that problems are detected and communicated effectively to all responsible administrators. For this purpose, you can use System Center Operations Manager Management Pack for Azure.

### Tools to monitor directory synchronization:

- Operations Manager—use the System Center Management Pack for Azure
- The Azure classic portal
- Windows PowerShell
- Synchronization Service Manager
- Event logs

### The Azure classic portal

The Azure classic portal provides multiple methods for monitoring directory synchronization. If there are any errors during directory synchronization, an email notification is sent to the email address registered as the cloud service *technical contact* when you signed up for a service.


To verify directory synchronization in real time by using the Azure classic portal:

1. Click your directory instance in Azure classic portal.
2. In the toolbar, click **DIRECTORY INTEGRATION**. In the **LAST SYNC** field, you will see the last synchronized time.

### Windows PowerShell

You can also use Windows PowerShell cmdlets and scripts to help manage Azure AD, report synchronization state, and so on. After connecting to Azure AD in Windows PowerShell, you can use the following cmdlet to verify the last time directory synchronization was successful in Azure AD:

```
Import-Module MSOnline
Connect-MsolService
Get-MsolCompanyInformation | fl LastDirSyncTime
```

 **Additional Reading:** For more information, refer to: "Azure Active Directory cmdlets" at: <http://aka.ms/pfsm1x>

## Synchronization Service Manager

Synchronization Service Manager is installed automatically as part of Azure AD Connect. This tool allows you to verify and change the directory synchronization service. From the **Operations** tab, you can select the list of various connector operations to review the **Start Time**, **End Time**, and the **Status** of the previous jobs that have completed.

### Event logs

The directory synchronization tool writes entries to the directory synchronization computer's event log. These entries indicate the start and end of a directory synchronization session. Directory synchronization errors are also reported in the event log and sent via e-mail to your organization's designated technical contact. When reviewing the event log, look for entries where the source is directory synchronization. An entry designated Event 4 and with the description **The export has completed** indicates that the directory synchronization is complete.

## Troubleshooting directory synchronization

Important troubleshooting tasks for directory synchronization include analyzing logs for errors and remediating synchronization errors with Azure AD Connect. Typical issues that can lead to problems include:

- Installation errors, such as using incorrect on-premises or Azure AD credentials.
- Inadvertently deactivating directory synchronization in the Azure classic portal or through Windows PowerShell.
- Unexpected changes in AD DS that affect OU scoping or attribute filtering.
- Corrupted AD DS requiring directory recovery.

- Troubleshooting tasks for directory synchronization include:
  - Analyzing logs for errors
  - Remediating synchronization errors with the tool
- Typical issues that can lead to problems include:
  - Installation errors, such as using incorrect on-premises or Azure AD credentials
  - Inadvertently deactivating directory synchronization in Azure classic portal or through Windows PowerShell
  - Unexpected changes in AD DS that affect OU scoping or attribute filtering
  - Corrupted AD DS requiring directory recovery

It is very important that you understand what happens when you deactivate and then reactivate synchronization in the Azure classic portal. When directory synchronization is deactivated, the source of authority is transferred from the on-premises AD DS to Azure AD. Deactivation is needed when on-premises AD DS is no longer being used to create and manage users, groups, contacts, and mailboxes, such as after a staged Exchange migration to the cloud, when the organization no longer wants to manage objects from the on-premises environment. Problems can subsequently arise if directory synchronization is then reactivated, with the source of authority transferred back from Azure AD to the on-premises AD DS.

For example, assume that an organization activated directory synchronization in January, and then created new users on premises, which synchronized to Azure AD. In this case, the source of authority is the on-premises AD DS. In July, the organization deactivated directory synchronization, resulting in transfer of the source of authority to Azure AD; from this point on, objects were edited in Azure AD. In September, the company decided to deploy AD FS and SSO. To meet this requirement, directory synchronization was reactivated, transferring the source of authority back to the on-premises AD DS. In this example, when you reactivate and run directory synchronization, any changes made to the Azure AD objects from July through to September would be overwritten and lost.



**Additional Reading:** For more information, refer to: "Integrating your on-premises identities with Azure Active Directory" at: <http://aka.ms/cdm2kk>

## Upgrading directory synchronization

It is important to use the latest version of the directory synchronization tool. When upgrading to a new version of the directory synchronization tool, some existing filters and other management agent customizations might not automatically import into the new installation. If you are upgrading to a newer version of directory synchronization, you must always manually reapply filtering configurations after you upgrade but before you run the first synchronization cycle.

## Synchronization Service Manager

To check the directory synchronization tool for issues, you will need to open **Synchronization Service Manager** in the **Azure AD Connect** group from the **Start** menu.


Within the application, you will need to view the **Operations** tab. On this tab you can confirm that the following operations have completed successfully:

- Import on the AD Connector
- Import on the Azure AD Connector
- Full Sync on the AD Connector
- Full Sync on the Azure AD Connector

Review the result from these operations to validate the directory synchronization status and to identify any errors.

By default, these operations are scheduled to run once every three hours. If you do not want to wait this long to troubleshoot an issue, use the following procedure to force manual synchronization:

1. Open the **Azure AD Connect** tool from the **Start** menu.
2. Provide the information requested on the wizard pages (you should be able to accept the default settings if the tool has already been deployed).
3. On the **Configure** page, select the **Start the synchronize process as soon as the initial configuration completes** option, and then click **Finish**.

 **Additional Reading:** For more ore information, refer to: "How to troubleshoot Azure Active Directory Sync tool installation and Configuration Wizard errors" at: <http://aka.ms/bz5cjlw>

## Check Your Knowledge

Question	
If you want to have SSO for both cloud-based and on-premises services, what do you need to deploy? Choose all that apply.	
Select the correct answer.	
<input type="checkbox"/>	Azure AD Connect Health
<input type="checkbox"/>	AD FS
<input type="checkbox"/>	Azure AD Connect
<input type="checkbox"/>	Office 365
<input type="checkbox"/>	Azure AD

**Question:** Verify the correctness of the statement by placing a mark in the column to the right.

Statement	Answer
If you implement AD FS and federation between locally deployed AD DS and Azure AD, then you do not need to use Azure AD Connect.	



# Lab: Configuring directory synchronization

## Scenario

As part of the proof-of-concept phase, your team has to configure and test synchronization between on-premises AD DS and Azure AD. You must prepare AD DS for directory synchronization, install and run Azure AD Connect, and then verify that directories synchronize.

## Objectives

After completing this lab, you will be able to:

- Prepare an on-premises AD DS domain for directory synchronization.
- Install and configure directory synchronization with Azure AD Connect.
- Manage user and group accounts by using directory synchronization.

## Lab Setup

Estimated Time: **60 minutes**

Virtual machines: **20742A-LON-DC1**, **20742A-LON-DC2**, **20742A-LON-SVR1** and **20742A-LON-CL1**

Internet Access: **MSL-TMG1**

User Name: **Adatum\Administrator**

Password: **Pa\$\$w0rd**

For this lab, you will use the available virtual machine environment. Before you begin the lab, complete the following steps:

1. On the host computer, start **Hyper-V Manager**.
2. In Microsoft Hyper-V Manager, click **20742A-LON-DC1**, and then in the **Actions** pane, click **Start**.
3. In the **Actions** pane, click **Connect**. Wait until the virtual machine starts.
4. Sign in by using the following credentials:
  - User name: **Adatum\Administrator**
  - Password: **Pa\$\$w0rd**
5. Repeat steps 2 to 4 for virtual machines **20742A-LON-DC2**, **20742A-LON-SVR1** and **20742A-LON-CL1**.
6. For Internet access you will also need to start **MSL-TMG1**.

This lab requires a Microsoft Azure Pass to activate your trial subscription. Your instructor will provide the Azure pass and sign in details required to complete the lab.

## Exercise 1: Preparing for directory synchronization

### Scenario

Before you configure directory synchronization, you must create your Azure AD tenant. In this exercise, you will create the required accounts and create a new Azure AD tenant.

The main tasks for this exercise are as follows:

1. Create a Microsoft account.
2. Create a trial Azure subscription.
3. Create an Azure AD tenant.

#### ► Task 1: Create a Microsoft account

Further tasks in this exercise require that you have an active Microsoft account without an Azure subscription assigned to it. If you do not want to use your private Microsoft account, if you do not have an account, or if you already have an Azure subscription, please follow the steps in this task to create a new Microsoft account.

1. On **LON-CL1**, start **Internet Explorer**, and then browse to **www.live.com**.
2. Click the **Create One!** link, and then use the wizard to create a new Microsoft account.
3. When you are finished, close Internet Explorer.



**Note:** Make sure that you write down the user name that you chose. For example, you can choose a user name in the *YourInitials-Date@outlook.com* format, such as **DJ-060815@outlook.com**. Use **Pa\$\$w0rd1** as the password. We recommend that you type your working email address in the **Alternate email address** text box.

#### ► Task 2: Create a trial Azure subscription

1. On **LON-CL1**, open **Internet Explorer** and browse to the **Try Microsoft Azure Pass** webpage at **http://aka.ms/cu92vo**.
2. Select your country/region, and then use the Azure voucher that the instructor provided you to activate the Azure trial subscription.
3. On the **Sign in** page, use the user ID that you configured in the previous task, or use your personal Microsoft account.
4. Wait for a few minutes until your Azure subscription has been created, and then verify that a new Azure portal opens. You can click through the portal to see the available options, but do not make any changes.
5. Close the Internet Explorer browser.

### ► Task 3: Create an Azure AD tenant

1. On **LON-CL1**, open **Internet Explorer**, and then browse to **https://manage.windowsazure.com**.
2. Use the Microsoft account that you used in the previous task for creating your Azure trial subscription to sign in.
3. When the Azure classic portal opens, navigate to **ACTIVE DIRECTORY**, and then create a new directory:
  - NAME: **Adatum**
  - DOMAIN NAME: Use your initials, with Adatum, and random numbers (for example, "DDAdatum111") to create the domain name; if you receive an **Already in use by another directory** message, change the numbers until you receive a green check mark.



**Note:** From this point, throughout the course, you should use this name when you see the *yourdomainname* variable in the labs.

- COUNTRY OR REGION: **United States**

**Results:** After completing this exercise, you should have created the Azure AD tenant.

## Exercise 2: Configuring directory synchronization

### Scenario

Now that the environment is prepared for directory synchronization, the next step is to install and configure the Azure AD Connect tool and configure an initial synchronization.

The main tasks for this exercise are as follows:

1. Configure synchronization account and add domain to Azure.
2. Install and configure Azure AD Connect.
3. Verify the initial synchronization and manage settings.

### ► Task 1: Configure synchronization account and add domain to Azure



**Note:** Due to the importance of configuring the next steps correctly, these high-level steps are a duplicate of the detailed steps in the Lab Answer Key.

1. On your host machine, on the Start screen, click **Internet Explorer**.
2. In the address bar, type **https://manage.windowsazure.com**, and then press Enter.
3. On the **Microsoft Azure** page, click **Use another account**.
4. On the **Microsoft Azure** page, type your Microsoft account that is associated with your Azure subscription, and then click **Continue**.
5. Sign in to Azure by using the Microsoft account that is associated with your trial subscription. This is the account that you used in Exercise 1 to create your Azure subscription.
6. In the Azure classic portal, click the **Adatum** directory instance.

7. Click the **USERS** tab, and then click **ADD USER**.
8. In the **TYPE OF USER** list, click **New user in your organization**.
9. In the **USER NAME** text box, type **Sync**.



**Note:** Make a note of the complete user name. This is the **USER NAME** plus the suffix shown to the right of the at sign (@), such as *Sync@yourdomain.onmicrosoft.com*.

10. Click **Next**.
11. On the **user profile** page, in the **DISPLAY NAME** text box, type **SYNC**.
12. In the **ROLE** list, click **Global Admin**.
13. In the **ALTERNATE EMAIL ADDRESS** text box, type your own email address, and then click **Next**.
14. Click **create**.
15. Make a note of the temporary password that is displayed.
16. Click **Complete**.
17. Close Internet Explorer, and then reopen it.
18. In the address bar, type **https://manage.windowsazure.com**, and then press Enter.
19. Click **Use another account**.
20. Type the user name for the **SYNC** user that you recorded earlier. It will be **SYNC@yourdomain.onmicrosoft.com**. Click **Continue**.
21. Type the temporary password that you noted when creating your synchronization account, and then click **Sign in**.
22. When prompted, type your old password, which you typed in step 21, in the **Old password** text box, in the **New password** and **Confirm password** text boxes, type **Pa\$\$w0rd**, and then click **Update password and sign in**.
23. If prompted to sign in to the portal again, use the **SYNC** account credentials and the password **Pa\$\$w0rd**. You will receive a message that there are no subscriptions found.
24. Close and reopen Internet Explorer.
25. In the address bar, type **https://manage.windowsazure.com**, and then press Enter.
26. Sign in to Azure by using the account that is associated with your trial subscription. The account should be on the list.
27. In the Azure classic portal, click **Adatum**. The **GET STARTED** page loads.
28. Click **Add domain**.
29. In the **ADD DOMAIN Wizard**, in the **DOMAIN NAME** text box, type **Adatum.com**, click **add**, and then click **Next**.
30. On the **Verify Adatum.com** page, click **Complete** (the check mark icon).
31. Minimize the **Internet Explorer** window.

## ► Task 2: Install and configure Azure AD Connect

Due to the importance of configuring the next steps correctly, these high-level steps are a duplicate of the detailed steps in the Lab Answer Key.

1. On **LON-SVR1**, sign in as **Adatum\Administrator**.
2. Open **Internet Explorer**, and then browse to **http://www.microsoft.com/en-us/download/details.aspx?id=47594**.
3. On the **Microsoft Azure Active Directory Connect** page, click **Download**, and then click **Run**.



**Note:** If you experience any problems with starting the download, add the **https://download.microsoft.com** website to your trusted sites.

4. In the **Microsoft Azure Active Directory Connect Wizard**, on the **Welcome to Azure AD Connect** page, select the **I agree to the license terms and privacy notice** check box, and then click **Continue**.
5. On the **Express Settings** page, click **Use express settings**.
6. On the **Connect to Azure AD** page, in the **USERNAME** text box, type the **SYNC** account user name. In the **PASSWORD** text box, type **Pa\$\$w0rd**, and then click **Next**.
7. On the **Connect to AD DS** page, in the **USERNAME** text box, type **Adatum\administrator**. In the **PASSWORD** box, type **Pa\$\$w0rd**, and then click **Next**.
8. On the **Azure AD sign-in configuration** page, select the check box next to **Continue without any verified domains**, and then click **Next**.
9. Click **Install**, and when installation is complete, click **Exit**.
10. At this time, synchronization of objects from your local AD DS and Azure AD begins. You must wait approximately 10 minutes for this process to complete.
11. Close the Internet Explorer window on **LON-SVR1**.

## ► Task 3: Verify the initial synchronization and manage settings

1. Switch to Internet Explorer on your host machine.
2. On the **directory** page in the Azure classic portal, click the **USERS** tab.
3. Verify that you can see the user accounts from your local AD DS.
4. Switch to **LON-SVR1**.
5. Open **Synchronization Service Manager**, and then switch to the **Operations** tab.
6. Ensure that you see the **Export, Full Synchronization**, and **Full Import** tasks.
7. Ensure that all the tasks have a current time and date in the **Start Time** and **End Time** columns. Also, ensure that all tasks have success in the **Status** column.
8. On **LON-SVR1**, open **Windows PowerShell**.
9. Use the **Get-ADSyncScheduler** cmdlet to review the synchronization settings.
10. Use the **Set-ADSyncScheduler -CustomizedSyncCycleInterval** cmdlet to set the synchronization interval to **1 hour**.

11. Use the **Start-ADSyncSyncCycle -PolicyType Delta** cmdlet to start synchronization manually.
12. Use the **Get-ADSyncScheduler** cmdlet to review the new synchronization settings.

**Results:** After completing this exercise, you should have installed Azure AD Connect with the customized settings, completed directory synchronization to Azure AD, and verified that the synchronization was successful.

## Exercise 3: Managing Active Directory users and groups

### Scenario

Now that directory synchronization is in place and working, you need to identify how managing user and group accounts has changed with directory synchronization.

The main tasks for this exercise are as follows:

1. Add new objects in AD DS.
2. Verify synchronization of the new user objects.
3. Prepare for the next module.

#### ► Task 1: Add new objects in AD DS

1. On **LON-DC1**, open **Active Directory Users and Computers**.
2. In the **Sales OU**, create a new user account with your name.
3. Add the new user account to the **Sales** group.

#### ► Task 2: Verify synchronization of the new user objects

1. On **LON-SVR1**, open **Windows PowerShell** in **Admin** mode.
2. Force the delta synchronization by executing the **Start-ADSyncSyncCycle** command.
3. Open the Azure classic portal, and then verify that the new user created in previous tasks appears in the **USERS** tab and in the **Sales** group.

**Results:** After completing this exercise, you should have identified how managing user and group accounts has changed with directory synchronization.

#### ► Task 3: Prepare for the next module

When you finish the lab, revert the virtual machines to their initial state. To do this, perform the following steps:

1. On the host computer, start **Hyper-V Manager**.
2. In the **Virtual Machines** list, right-click **20742A-LON-DC1**, and then click **Revert**.
3. In the **Revert Virtual Machine** dialog box, click **Revert**.
4. Repeat steps 2 and 3 to revert **20742A-LON-DC2**, **20742A-LON-SVR1**, and **20742A-LON-CL1**.

**Question:** What do you need to do before you begin configuring Azure AD Connect?

**Question:** Which cmdlet should you use to change the synchronization schedule for Azure AD Connect?

# Module Review and Takeaways

## Real-world Issues and Scenarios

Because directory synchronization is the link between your on-premises AD DS objects and the services in Azure AD, be careful when making changes to Azure AD Connect or Synchronization Service Manager after production deployment. For example, a minor mistake in filtering could accidentally delete all user mailboxes in Office 365.

In some environments, for example, in a test environment, you might test all changes on a separate directory synchronization server that is connected to a separate Azure AD tenant (trial). In addition, you should manually initiate run profiles for each management agent in Synchronization Service Manager and observe the pending actions before exporting to Azure AD. In some cases, it might be a good idea to create a new run profile for exporting to Azure AD that includes a maximum limit on the number of allowed deletions.

## Review Question

**Question:** What feature do you need to configure so that objects synchronize from Azure AD to your on-premises AD DS?

## Tools

The following table lists the tools that this module references:

Tool	Use for	Where to find it
Azure AD Connect	Establishing synchronization between AD DS and Azure AD	Microsoft Download Center
Azure AD Connect Health	Monitoring AD DS to Azure AD synchronization health	The Azure classic portal
The Azure classic portal	Azure AD management	<a href="http://aka.ms/n2l3cb">http://aka.ms/n2l3cb</a>

## Best Practices

- For simple environments, use the Azure AD Connect express settings.
- Enable users to use the self-service password reset functionality with at least two authentication methods.
- Consider using writeback functionalities.
- Implement Azure AD Connect Health if you have an Azure AD Premium subscription.

## Common Issues and Troubleshooting Tips

Common Issue	Troubleshooting Tip
Directory synchronization filtering is no longer working.	
After installing Azure AD Connect, you might receive a prompt with the following error message when you open Synchronization Service Manager: <b>Unable to connect to the Synchronization Service.</b>	

**MCT USE ONLY. STUDENT USE PROHIBITED**



# Module 13

## Monitoring, managing, and recovering AD DS

### Contents:

Module Overview	13-1
<b>Lesson 1:</b> Monitoring AD DS	13-2
<b>Lesson 2:</b> Managing the Active Directory database	13-11
<b>Lesson 3:</b> Active Directory backup and recovery options for AD DS and other identity and access solutions	13-18
<b>Lab:</b> Recovering objects in AD DS	13-27
Module Review and Takeaways	13-32

## Module Overview

As an Information Technology (IT) professional responsible for supporting the Windows Server operating system and Active Directory Domain Services (AD DS), maintaining the health of your domain is a critical aspect of your job. In this module, you will learn about the technologies and tools that are available to help you ensure the health and reliability of AD DS. You will explore tools that help you monitor performance in real time, and you will learn to record performance over time to spot potential problems by observing performance trends. You also will learn how to optimize and protect your directory service and related identity and access solutions so that if a service does fail, you can restart it as quickly as possible.

### Objectives

After completing this module, you will be able to:

- Monitor AD DS.
- Manage the Active Directory database.
- Describe the backup and recovery options for AD DS and other identity access solutions.

## Lesson 1

# Monitoring AD DS

Performance problems are common in real-world environments. Therefore, you must know how to analyze, evaluate, and remediate those problems. In this lesson, you will learn how to use performance and event monitoring tools in Windows Server to monitor the health of your domain controllers and AD DS.

### Lesson Objectives

After completing this lesson, you will be able to:

- Describe performance monitoring and explain performance bottlenecks.
- Describe monitoring tools in the Windows Server operating system.
- Describe how to use Performance Monitor to monitor real-time and logged performance.
- Describe how to use data collector sets to monitor performance.
- Explain how to monitor a domain controller by using Performance Monitor.

### Understanding performance and bottlenecks

Poor domain controller system performance can be attributed to insufficient system resources. The four key system resources are the central processing unit (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. After augmenting that resource, performance will improve, but it might reach a plateau when it hits a new bottleneck in another system resource.

- A *bottleneck* is a resource that is currently at peak utilization
- Key system resources:
  - CPU
  - Disk
  - Memory
  - Network

### Analyzing the key hardware components

To optimize server performance, you must understand how your operating system interacts with the following key hardware components:

- Processor. Processor speed is one important factor in determining your server's overall processor capacity. The number of operations a CPU can perform in a measured period determines processor speed. Servers with multiple processors, or processors with multiple cores generally perform processor-intensive tasks with greater efficiency and typically are faster than single processor or single-core processor computers. Domain controllers do not typically require higher processor performance, but processor performance can be important if your domain controller is performing other roles as well.
- Disk. Hard disks store programs and data. Consequently, the *throughput* (the total amount of data that the disk subsystem processes for each time unit) of disks affects the speed of a workstation or server, especially when the server is performing disk-intensive tasks such as restoring the AD DS database or replicating large amount of AD DS data to the database. Hard disk drives have moving parts, and it takes time to position the read/write heads over the appropriate disk sector to retrieve information.



**Note:** *Workload* is the amount of work processing disk requests that the disk subsystem performs in a measured time.

You can reduce potential disk subsystem bottlenecks by selecting faster disks and by using collections of disks such as RAID arrays or Storage Spaces that optimize access times. Remember that information on the disk moves into memory before the operating system uses it. If there is a surplus of memory, the Windows Server operating system creates a file cache for items recently written to, or read from the disks. If you install additional memory in a server, you often can improve disk subsystem performance because accessing the cache is faster than moving information into memory.

- **Memory.** Programs and data load from the disk into memory before the program manipulates data. You can increase the amount of memory to help improve server performance in servers that run multiple programs, or where datasets are extremely large.

Windows Server uses a memory model in which excessive memory requests are not rejected, but are managed by a process known as *paging*. During paging, data and programs in memory that is not currently being utilized by processes are moved into an area on the hard disk, known as the *paging file*. This frees up physical memory to satisfy the excessive requests, but because a hard disk is comparatively slow, it has a negative effect on workstation performance. By adding more memory, you can reduce the need for paging.

- **Network.** It is easy to underestimate the effect of a poorly performing network because it is not as easy to see or to measure as the other three components. However, the network is a critical component for performance monitoring because AD DS is a network-based service, which requires reliable network connectivity between servers and clients.

## Overview of monitoring tools

You can use several tools in Windows Server for various types of monitoring. Most of these tools are available by default as Windows Server components, and you can use them for real-time and historical monitoring of AD DS and other services. The most commonly used tools are Task Manager, Resource Monitor, Event Viewer, and Performance Monitor.

Windows Server provides the following tools to help with monitoring performance issues:

- Task Manager
- Resource Monitor
- Event Viewer
- Performance Monitor
- Windows PowerShell

### Task Manager

Task Manager provides information to help you identify and resolve performance-related problems in Windows Server. The Task Manager user interface (UI) has the following tabs:

- **Processes.** The **Processes** tab displays a list of running programs, subdivided into background and internal Windows-based processes. For each running process, this tab displays a summary of processor and memory usage.
- **Performance.** The **Performance** tab displays a summary of CPU and memory usage, and network statistics.
- **Users.** The **Users** tab displays resource consumption on a per-user basis. You also can expand the user view to see more detailed information about the specific processes that a user is running.

- **Details.** The **Details** tab lists all the running tasks on the server, providing statistics about the CPU, memory, and other resource consumption. You can use this tab to manage the running tasks. For example, you can stop a process, stop a process and all related processes, or change the processes' priority values. By changing a process's priority, you determine how much CPU resources the process can consume. By increasing the priority, you allow the process to request more CPU resources.
- **Services.** The **Services** tab provides a list of running Windows services with related information, such as whether a service is running, and the process identifier (PID) value of the corresponding service. You can start and stop services by using the list on the **Services** tab.

Generally, you might consider using Task Manager when a performance-related problem first manifests itself. For example, you might examine tasks that are running to determine if a particular program is using excessive CPU resources. Always remember that Task Manager displays a snapshot of current resource consumption, and that you also might need to examine historical data to determine a true picture of a server's performance and response under load.

### Resource Monitor

Resource Monitor provides an in-depth look at your server's real-time performance. You can use Resource Monitor to monitor the use and performance of CPU, disk, network, and memory resources in real time. With Resource Monitor, you can identify and resolve resource conflicts and bottlenecks.

By expanding the monitored elements, system administrators can identify processes that use specific resources. Furthermore, you can use Resource Monitor to track a process or processes by selecting their check boxes. When you select a process, it remains selected at the top of the screen in every pane of the Resource Monitor, which provides the information that you require regarding that process, no matter where you are in the interface.

### Event Viewer


Event Viewer provides access to Windows Server event logs. *Event logs* are logs that provide information about system events that occur within the Windows operating system. These events include information, warnings, and error messages about Windows components and applications.

Event Viewer provides categorized lists of essential Windows log events, including application, security, setup, system events, and log groupings, for individual applications and specific Windows-based component categories. Individual events provide detailed information regarding the type of event that occurred, when the event occurred, the source of the event, and detailed information to assist in troubleshooting the event.

Additionally, Event Viewer allows you to consolidate logs from multiple computers onto a centralized computer by using subscriptions. Finally, you can configure Event Viewer to perform an action based on a specific event or the occurrence of multiple events. This might include sending an email message, starting an application, running a script, or another maintenance action (or actions) that could notify you or attempt to resolve a potential issue.

Event Viewer in Windows Server contains the following important features:

- The ability to view multiple logs. You can filter for specific events across multiple logs, thereby making it simpler to investigate issues and troubleshoot problems that might appear in several logs.
- The inclusion of customized views. You can use filtering to narrow searches only to events in which you are interested, and you can save these filtered views.
- The ability to configure tasks scheduled to run in response to events. You can automate responses to events. Event Viewer integrates with Task Scheduler to perform these tasks.
- The ability to create and manage event subscriptions. You can collect events from remote computers and then store them locally.

 **Note:** To collect events from remote computers, you must create an inbound rule in Windows Firewall to permit Windows Event Log Management.

Event Viewer tracks information in several different logs. These logs provide detailed information that includes:

- A description of the event.
- An event ID number.
- The component or subsystem that generated the event.
- Information, Warning, or Error status.
- The time of the occurrence.
- The user's name on whose behalf the event occurred.
- The computer on which the event occurred.
- A link to Microsoft TechNet for more information about the event.

Event Viewer has many built-in logs, including those in the following table.

Built-in log	Description and use
Application log	This log contains errors, warnings, and informational events that pertain to the operation of applications such as Microsoft Exchange Server.
Security log	This log reports the results of auditing, if you enable it. Audit events are described as successful or failed, depending on the event. For instance, the log would report success or failure regarding whether a user was able to access a file.
Setup log	This log contains events related to operating system component setup.
System log	General events are logged by Windows components and services, and are classified as error, warning, or information. Windows predetermines the events that system components log.
Forwarded Events	By default, this log stores events that are collected from remote computers. To collect events from remote computers, you must create an event subscription.

## Performance Monitor

With Performance Monitor, you can view report-based or graphical displays of system performance. It can monitor both software and hardware components in real-time and historically. This tool is discussed in detail in the next topic.

## Windows PowerShell

You can use cmdlets in the Windows PowerShell command-line interface to monitor server performance. For example, you can use the following command to retrieve the current **% Processor Time** combined values for all processors on the local computer every two seconds until it has 100 values and displays the captured data:

```
Get-counter -Counter "\Processor(_Total)\% Processor Time" -SampleInterval 2 -MaxSamples 100
```



**Additional Reading:** For more information, refer to: "Using PowerShell To Gather Performance Data" at: <http://aka.ms/F8mxnr>

## What is Performance Monitor?

With Performance Monitor, you can view current performance statistics or historical data gathered by using data collector sets. With Windows Server, you can monitor operating system performance through performance objects and counters in the objects. Windows Server collects data from counters in various ways, including:

- A real-time snapshot.
- The total since the last computer startup.
- An average over a specific time interval.
- An average of values.
- The number per second.
- A maximum value.
- A minimum value.

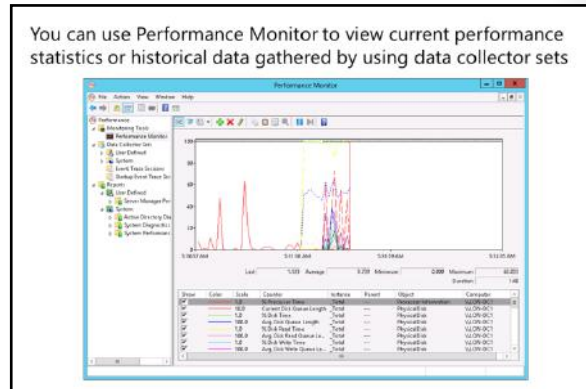
Performance Monitor works by providing you with a collection of objects and counters that record data about computer resource usage. There are many counters that you can research and consider to meet your specific requirements.

### Primary processor counters

CPU counters, a feature of the computer's CPU, stores the count of hardware-related events. The primary processor counters include:

- Processor > % Processor Time. This counter measures the percentage of elapsed time the processor spends executing a non-idle *thread*. In other words, this counter displays the percentage of elapsed time that a given thread uses the processor to run *instructions*. (An *instruction* is the basic unit of execution in a processor, and a *thread* is the object that executes instructions.) If the percentage is greater than 85 percent, the processor is overwhelmed and the server might require a faster processor. Included in this count is code that handles some hardware interrupts and trap conditions.
- Processor > Interrupts/sec. This counter displays the rate, in incidents per second, at which the processor received and serviced hardware interrupts. This value is an indirect indicator of the activity of devices that generate interrupts, such as the system clock, the mouse, disk drivers, data communication lines, network interface cards, and other peripheral devices. These devices normally interrupt the processor when they have completed a task or require attention. Normal thread execution is suspended.
- System > Processor Queue Length. This counter displays an approximate number of threads that each processor is servicing. If the value is more than two times the number of CPUs over a given time, then the server does not have enough processor power. The processor queue length (sometimes referred to as *processor queue depth*) that this counter reports is an instantaneous value that represents only a current snapshot of the processor. Therefore, you must observe this counter over a period to notice data trends. Additionally, the System > Processor Queue Length counter reports a total queue length for all processors, not just a length for each processor.

You can use Performance Monitor to view current performance statistics or historical data gathered by using data collector sets



### Primary memory counters

The Memory performance object consists of counters that describe the behavior of the computer's physical and virtual memory. *Physical memory* is the amount of random access memory (RAM) on the computer. *Virtual memory* consists of space in physical memory and on disk. Many of the memory counters monitor *paging*, which is the movement of pages of code and data between disk and physical memory.

- The Memory > Pages/sec counter measures the rate at which pages are read from or written to disk to resolve hard page faults. An increase in this counter indicates that more paging is occurring, which in turn suggests a lack of physical memory.

### Primary disk counters

The Physical Disk performance object consists of counters that monitor hard or fixed disk drives. Disks store file, program, and paging data. Disks are read to retrieve these items, and are written to when recording changes to them. The total values of physical disk counters are the total of all the values of the logical disks or partitions into which they are divided. The primary disk counters include:

- Physical Disk > % Disk Time. This counter indicates how busy a particular disk is, and it measures the percentage of time that the disk was busy during the sample interval. A counter approaching 100 percent indicates that the disk is busy nearly all of the time, and a performance bottleneck is possibly imminent. You might consider replacing the current disk system with a faster one.
- Physical Disk > Avg. Disk Queue Length. This counter indicates how many disk requests are waiting to be serviced by the input/output (I/O) manager in Windows Server at any given moment. If the value is larger than two times the number of spindles, it means that the disk itself might be the bottleneck. The longer the queue is, the less satisfactory the disk throughput is.

### Primary network counters

Most workloads require access to production networks to ensure communication with other applications and services, and to communicate with users. Network requirements include elements such as throughput and the presence of multiple network connections.

Workloads might require access to several different networks that must remain secure. Examples include connections for:

- Public network access.
- Networks for performing backups and other maintenance tasks.
- Dedicated remote-management connections.
- Network adapter teaming for performance and failover.
- Connections to the physical host computer.
- Connections to network-based storage arrays.

By monitoring network performance counters, you can evaluate your network's performance. The primary network counters include:

- Network Interface > Current Bandwidth. This counter indicates the current bandwidth being consumed on the network interface in bits per second (bps). Most network topologies have maximum potential bandwidths quoted in megabits per second (Mbps). For example, Ethernet can operate at bandwidths of 10 Mbps, 100 Mbps, 1 gigabit per second (Gbps), and higher. To interpret this counter, divide the given value by 1,048,576 for Mbps. If the value approaches the network's maximum potential bandwidth, you should consider implementing a switched network or upgrading to a network that supports higher bandwidths.

- Network Interface > Output Queue Length. This counter indicates the current length of the output packet queue on the selected network interface. A growing value, or one that is consistently higher than two, could indicate a network bottleneck, which you should investigate.
- Network Interface > Bytes Total/sec. This measures the rate at which bytes are sent and received over each network adapter, including framing characters. The network is saturated if you discover that more than 70 percent of the interface is consumed.

### Primary Active Directory counters

On a domain controller, you also should monitor at least the following performance counters exposed by the NT Directory Service (NTDS) object.

### Directory Replication Agent (DRA) counters

- NTDS\ DRA Inbound Bytes Total/sec. This counter shows the total number of bytes replicated into the AD DS database.
- NTDS\ DRA Inbound Object. This counter shows the number of Active Directory objects received from neighbors through inbound replication.
- NTDS\ DRA Outbound Bytes Total/sec. This counter shows the total number of bytes replicated out.
- NTDS\ DRA Pending Replication Synchronizations. This is the number of directory synchronizations that are queued for this server but not yet processed.

### Other counters

- Security System-Wide Statistics\ Kerberos Authentications/sec. This counter tracks the number of times that clients use a ticket to authenticate to this computer per second.
- Security System-Wide Statistics\ NTLM Authentications. This counter tracks the number of NTLM authentications processed per second.

## What are data collector sets?

A data collector set is the foundation of Windows Server performance monitoring and reporting in Performance Monitor. You can use data collector sets to gather performance-related information and other system statistics on which you can conduct analysis with tools within Performance Monitor, or with third-party tools.

Although it is useful to analyze current performance activity on a server computer, you might find it more useful to collect performance data over a set period and then analyze and compare it with data that you gathered previously. You can use this data comparison to determine resource usage to plan for growth and to identify potential performance problems.

Data collector sets can contain the following types of data collectors:

- Performance counters. This data collector provides server performance data.
- Event trace data. This data collector provides information about system activities and events, which often is useful for troubleshooting.

- You can use data collector sets to gather performance-related information
- Data collector sets can contain the following types of data collectors:
  - Performance counters
  - Event trace data
  - System configuration information



- System configuration information. This data collector allows you to record the current state of registry keys and to record changes to those keys.

You can create a data collector set from a template, from an existing set of data collectors in a Performance Monitor view, or by selecting individual data collectors and setting each individual option in the data collector set properties.

## Demonstration: Monitoring AD DS

In this demonstration, you will learn how to:

- Configure Performance Monitor to monitor AD DS.
- Create a data collector set.
- Start the data collector set.
- Analyze the resulting data in a report.

### Demonstration Steps

#### Configure Performance Monitor to monitor AD DS

1. On **LON-DC1**, open **Performance Monitor**.
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**
  - **NTDS\DRS Inbound Objects/sec**
  - **NTDS\DRS Pending Replication Synchronizations**
  - **Security System-Wide Statistics\NTLM Authentications**
  - **Security System-Wide Statistics\Kerberos Authentications**
3. Watch the performance for a few moments. Then, in the counter list below the graph, select **DS Directory Searches/sec**.
4. On the toolbar, click **Highlight** to highlight **DS Directory Searches/sec** in the graph. Then, click **Highlight** on the toolbar again to turn off the highlight.

#### Create a data collector set

1. Create a new Data Collector Set from the current view of Performance Monitor.
2. Name the Data Collector Set **Custom ADDS Performance Counters**.
3. Make a note of the default root directory in which the Data Collector Set will be saved.

### Start the data collector set

1. Click the **Data Collector Sets\User Defined** node, right-click **Custom ADDS Performance Counters**, and then click **Start**. The Custom ADDS Performance Counters node is selected automatically.



**Note:** Notice that you can identify the individual data collectors in the data collector set. In this case, only one data collector—the System Monitor Log performance counter—is contained in the data collector set. You also can identify where the output from the data collector is being saved.

2. In the console tree, right-click the **Custom ADDS Performance Counters** data collector set, and then click **Stop**.

### Analyze the resulting data in a report

- In the console tree, from the **Reports\User Defined** node, expand **Custom ADDS Performance Counters**, and then click **System Monitor Log.blg**. The graph of the log's performance counters displays.

## Lesson 2

# Managing the Active Directory database

At the core of the Active Directory environment is the Active Directory database. The Active Directory database contains all the critical information required to provide Active Directory functionality. Maintaining this database properly is a critical aspect of Active Directory management, and you should be aware of several tools and best practices so that you can manage your Active Directory database effectively. This lesson will introduce you to Active Directory database management, and it will show you the tools and methods for maintaining it.

### Lesson Objectives

After completing this lesson, you will be able to:

- Describe the Active Directory database.
- Describe the database management tools.
- Explain how to manage the Active Directory database with NtdsUtil.exe.
- Explain restartable AD DS.
- Perform AD DS database management.
- Explain how to manage Active Directory snapshots.

### Overview of the AD DS database

Active Directory information is stored within the directory database. Each directory partition (also called a *naming context*), contains objects of a particular replication scope and purpose. There are four Active Directory partitions on each domain controller, which are as follows:

- **Domain.** The domain partition contains all the objects stored in a domain, including users, groups, computers, and Group Policy containers.
- **Configuration.** The configuration partition contains objects that represent the logical structure of the forest (including information about domains), in addition to the physical topology, including sites, subnets, and services.
- **Schema.** The schema partition defines the object classes and their attributes for the entire directory.
- **Application.** Domain controllers also can host application partitions. You can use application partitions to limit replication of application-specific data to a subset of domain controllers. Active Directory–integrated Domain Name System (DNS) is a common example of an application that utilizes application partitions. Application partitions are not a mandatory component of the AD DS database.

- The directory database stores Active Directory information
- Four Active Directory partitions on each domain controller are: Domain, Configuration, Schema, and Application (optional)
- File-level components of the AD DS database are:

File	Description
Ntds.dit	<ul style="list-style-type: none"> <li>• Main AD DS database file</li> <li>• Contains Active Directory partitions and objects</li> </ul>
Edb*.log	Transaction logs
Edb.chk	Database checkpoint file
Edbres00001.jrs Edbres00002.jrs	Reserve transaction log file that allows the directory to process transactions if the server runs out of disk space

Each domain controller maintains a copy (or *replica*), of several partitions. The configuration partition replicates to every domain controller in the forest, as does the schema partition. The domain partition for a domain replicates to all domain controllers within a domain, but not to domain controllers in other domains, with the exception of global catalog servers. Therefore, each domain controller has at least three replicas: the domain partitions for its domain, configuration, and schema.

### AD DS database files

The AD DS 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 are other files that support the AD DS database. The **Edb\*.log** files are the transaction logs for AD DS. When a change must 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, AD DS rolls back the changes.

The following table describes the different file level components of the AD DS database.

File	Description
<b>Ntds.dit</b>	<ul style="list-style-type: none"> <li>• Main AD DS database file</li> <li>• Contains Active Directory partitions and objects</li> </ul>
<b>Edb*.log</b>	Transaction logs
<b>Edb.chk</b>	Database checkpoint file
<b>Edbres00001.jrs</b> <b>Edbres00002.jrs</b>	Reserve transaction log file that allows the directory to process transactions if the server runs out of disk space

### AD DS database modifications and replication

Under normal operations, the transaction log wraps around, with new transactions overwriting old transactions. However, if a large number of transactions are made within a short period, AD DS creates additional transaction log files. Therefore, if you look in the NTDS folder of a particularly busy domain controller you might see several **Edb\*.log** files. Over time, those files are removed automatically.

The **Edb.chk** file acts like a bookmark in 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 disk is hosting the AD DS database because transactions that might be pending cannot write to the logs. Therefore, AD DS maintains two additional log files, **Edbres00001.jrs** and **Edbres00002.jrs**. These are empty files of 10 megabytes (MB) each. When a disk runs out of space for normal transaction logs, AD DS recruits the space used by these two files to write the transactions that are in a queue currently. After that, it safely shuts down Active Directory services, and dismounts the database. Of course, it will be important for an administrator to remediate the issue of low disk space as quickly as possible. The files provide a temporary solution to prevent the directory service from failing to process new transactions.


## What is NtdsUtil?

**NtdsUtil.exe** is a command-line executable file that you can use to perform database maintenance, including creating snapshots, relocating database files, and offline defragmentation.

You also can use NtdsUtil.exe to clean up domain controller metadata. If a domain controller is removed from the domain while offline, the domain controller is unable to remove important information from the directory service. However, you can use NtdsUtil.exe to clean out the remnants of the domain controller, and it is very important that you do so to protect your data from being compromised.

In addition, you can use **NtdsUtil.exe** to reset the password used to sign in to the Directory Services Restore Mode (DSRM). You configure this password initially during the configuration of a domain controller. If you forget the password, you can use the **NtdsUtil.exe set dsrm** command to reset it.

- Manage and control single master operations
- Perform Active Directory database maintenance:
  - Perform offline defragmentation
  - Create and mount snapshots
  - Move database files
- Clean domain controller metadata:
  - Domain controller removal or demotion while not connected to a domain
- Reset DSRM:
  - Password
  - **set dsrm**

 **Note:** You also can use graphical tools such as Active Directory Users and Computers and Active Directory Sites and Services to manage Active Directory objects and to clean up metadata automatically.

## Understanding restartable AD DS

In most scenarios where Active Directory management is required, you should restart the domain controller in DSRM. Windows Server enables administrators to stop and start AD DS just like any other service—without restarting a domain controller—to perform some management tasks quickly. This feature is called *restartable AD DS*. You can use the **Services** console, the command prompt, or Windows PowerShell to restart AD DS. Restartable AD DS reduces the time that is required to perform certain operations. For example, you can stop AD DS so that you can apply updates to a domain controller. In addition, administrators can stop AD DS to perform tasks such as offline defragmentation of the AD DS database, without restarting the domain controller. Other services running on the server that do not depend on AD DS to function, such as Dynamic Host Configuration Protocol (DHCP), remain available to respond to client requests while AD DS is stopped. Restartable AD DS is available by default on all domain controllers that run Windows Server or later. There are no functional-level requirements or any other prerequisites for using this feature.

- Use the **Services** console to start or stop AD DS
- Three states of AD DS:
  - AD DS Started
  - AD DS Stopped
  - DSRM
- It is not possible to perform a system state restoration while AD DS is in Stopped state

 **Note:** To restore a domain controller's System state, you must start in DSRM.

Restartable AD DS requires minor changes to the existing Microsoft Management Console (MMC) snap-ins. By using the snap-in, an administrator can stop and restart AD DS more easily, in much the same way as any other service that is running locally on the server.

Although stopping AD DS is similar to signing in in DSRM, restartable AD DS provides a unique state, known as *AD DS Stopped*, for a domain controller that is running Windows Server 2012 or later.

### Domain controller states

The three possible states for a domain controller that is running Windows Server 2012 or later are as follows:

- **AD DS Started.** In this state, AD DS is started. The domain controller is able to perform AD DS–related tasks normally.
- **AD DS Stopped.** In this state, AD DS is stopped. Although this mode is unique to Windows Server 2012 or later, the server has some characteristics of both a domain controller in DSRM and a domain-joined member server.
- **DSRM.** In this state, the AD DS database (**Ntds.dit**) on the local domain controller is offline. Another domain controller can be contacted for sign-in, if one is available. If no other domain controller can be contacted, you can do one of the following by default:
  - Sign in to the domain controller locally in DSRM by using the DSRM password.
  - Restart the domain controller to sign in with a domain account.

As with a member server, the domain controller in the Stopped state is still joined to the domain. This means that Group Policy and other settings still apply to the computer. However, a domain controller should not remain in the AD DS Stopped state for an extended period because in this state, it cannot service sign-in requests or replicate with other domain controllers.

## Demonstration: Performing database management

You can use several tasks and tools to perform Active Directory database maintenance.

In this demonstration, you will learn how to:

- Stop AD DS.
- Perform an offline defragmentation of the Active Directory database.
- Check the integrity of the offline Active Directory database.
- Start AD DS.

### Demonstration Steps

#### Stop AD DS

1. On **LON-DC1**, open the **Services** console.
2. Stop the **Active Directory Domain Services** service.

## Perform an offline defragmentation of the Active Directory database

- Run the following commands at a command prompt in the Windows PowerShell command-line interface, pressing Enter after each line:

```
NtdsUtil.exe
activate instance NTDS
files
compact to C:\
```

## Check the integrity of the offline Active Directory database

1. Run the following commands from in the Windows PowerShell command-line interface, pressing Enter after each line:

```
Integrity
quit
quit
```

2. Close the **Windows PowerShell** window.

## Start AD DS

1. Open the **Services** console.
2. Start the Active Directory Domain Services service.
3. Confirm that the Status column for Active Directory Domain Services is listed as Running.

## Managing Active Directory Snapshots

You can use NtdsUtil.exe to create and mount snapshots of AD DS. A *snapshot* is the exact capture of a historical state of the directory service at the time of the snapshot. You can use tools to explore the contents of a snapshot to examine the state of the directory service at the time the snapshot was made. For example, you can use the snapshot to browse the contents of the AD DS database as it was during the time of backup. You can use the Ldifde command-line tool to connect to a mounted snapshot, and export objects from AD DS.

- Create a snapshot of AD DS with NtdsUtil
- Mount the snapshot with NtdsUtil
- View the snapshot:
  - Right-click the root node of **Active Directory Users and Computers**, and then click **Connect to Domain Controller**
  - Type **serverFQDN:port**
- View read-only snapshot:
  - Cannot directly restore data from the snapshot
- Recover data:
  - Connect to the mounted snapshot, and then export/reimport objects' attributes with Ldifde
  - Restore a backup from the same date as the snapshot

## Creating an Active Directory snapshot

To create an Active Directory snapshot, perform the following procedure:

1. Open an elevated command prompt.
2. Type the following commands, pressing Enter after each line:

```
NtdsUtil.exe
activate instance ntds
snapshot
Create
list all
```



**Note:** The **list all** command returns a message that indicates that the snapshot set generated successfully.

The GUID that displays is important for commands in later tasks, so make note of the GUID or copy it to the Clipboard.

3. Type **quit**, and then press Enter.

You should schedule snapshots of AD DS regularly. You can use Task Scheduler to execute a batch file by using the appropriate NtdsUtil.exe commands.

### Mounting an AD DS snapshot

To view the contents of a snapshot, you must mount the snapshot as a new instance of AD DS. You can accomplish this by using NtdsUtil.exe.

To mount a snapshot, perform the following procedure:

1. Open an elevated command prompt.
2. Type the following commands, pressing Enter after each line:

```
NtdsUtil.exe
activate instance ntds
snapshot
list all
```



**Note:** The **list all** command returns a list of all snapshots.

3. Type the following command, and then press Enter:

```
mount <GUID>
```



**Note:** **GUID** is the GUID returned by the create snapshot command.

4. Type the following commands, pressing Enter after each line:

```
quit
quit
dsamain -dbpath c:\$snap_datetime_volume$\windows\ntds\ntds.dit -ldapport 50000
```

A message indicates that Active Directory Domain Services startup is complete.



**Note:** The **dbpath** property is provided when you execute the **mount <GUID>** command.

1. Port number 50000 can be any unused Transmission Control Protocol (TCP) port number.
5. Do not close the Command Prompt window. Leave the command that you just ran, **Dsamain.exe**, running while you continue to the next step.



## Viewing an AD DS snapshot

After mounting the snapshot, you can use tools to connect to and explore the snapshot. Active Directory Users and Computers is one of the tools that you can use to connect to the instance.

To connect to a snapshot with Active Directory Users and Computers, perform the following procedure:

1. Open **Active Directory Users and Computers**.
2. Right-click the root node, and then click **Change Domain Controller**.
3. In the **Change Directory Server** dialog box, click **<Type a Directory Server name[:port] here>**.
4. Type **LON-DC1:50000**, and then press Enter.



**Note:** **LON-DC1** is the name of the domain controller on which you mounted the snapshot, and 50000 is the TCP port number that you configured for the instance.

5. After you verify that you now are connected to the snapshot, click **OK**.



**Note:** Note that snapshots are read-only. You cannot modify the contents of a snapshot. Moreover, there are no direct methods with which to move, copy, or restore objects or attributes from the snapshot to the production instance of AD DS.

## Unmounting an AD DS snapshot

To unmount the Active Directory snapshot, perform the following procedure:

1. Switch to the command prompt in which the snapshot is mounted.
2. Press Ctrl+C to stop Dsamain.exe.
3. Type the following commands, pressing ENTER after each line:

```
NtdsUtil.exe
activate instance ntds
snapshot
unmount <GUID>,
quit
quit
```



**Note:** *GUID* is the GUID of the snapshot.

## Lesson 3

# Active Directory backup and recovery options for AD DS and other identity and access solutions

It is important to maintain the reliability of the Active Directory data. Performing regular backups can play a part in this process, but knowing how to restore or recover data after a failure is vital. Because restoring deleted objects from AD DS often can cause AD DS downtime, Windows Server includes the Active Directory Recycle Bin feature, which provides a much easier way to restore deleted objects with no AD DS downtime. This lesson explores these Active Directory backup and recovery features.

## Lesson Objectives

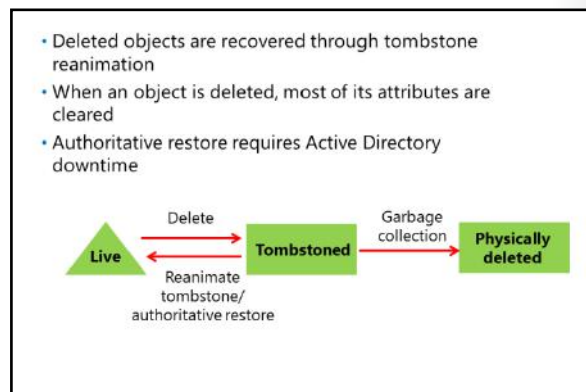
After completing this lesson, you will be able to:

- Explain how to restore deleted Active Directory objects.
- Explain how to configure the Active Directory Recycle Bin.
- Implement the Active Directory Recycle Bin.
- Describe backup and recovery tools.
- Explain Active Directory backup and recovery.

## Deleting and restoring objects from AD DS

When you delete an object in AD DS, it is moved to the Deleted Objects container and stripped of many important attributes. You can extend the list of attributes that remain when you delete an object, but you can never retain linked attribute values, such as group membership.

Depending on whether the Active Directory Recycle Bin feature is enabled determines your recovery options. If you have not enabled Active Directory Recycle Bin, providing the object has not yet reached the end of its tombstone lifetime (180 days by default), and it has not been scavenged by the garbage collection process, you can reanimate the deleted object. (*Scavenging* is a database cleanup process that removes stale records.)




- Deleted objects are recovered through tombstone reanimation
- When an object is deleted, most of its attributes are cleared
- Authoritative restore requires Active Directory downtime

**Note:** The AD DS database is fairly self-maintaining. Every 12 hours, by default, each domain controller runs garbage collection. This accomplishes two tasks. First, it removes deleted objects that have outlived their tombstone lifetime. Second, the garbage collection process performs online defragmentation.

To reanimate a deleted object, you can use the Ldp tool to perform the following procedure:

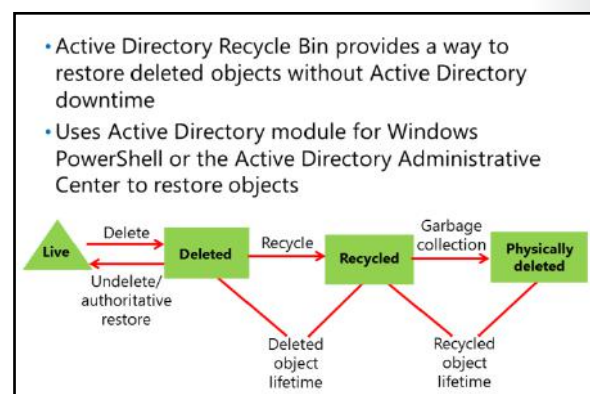
1. Click **Start**, and in the **Start Search** text box, type **Ldp.exe**. Press Ctrl+Shift+Enter, which executes the command as an administrator.
2. In the **User Account Control** dialog box, click **Use another account**.

3. In the **User name** text box, type the user name of an administrator.
4. In the **Password** text box, type the password for the administrative account, and then press Enter. Ldp opens.
5. Click the **Connection** menu, click **Connect**, and then click **OK**.
6. Click the **Connection** menu, 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, click **Tree**, and then click **OK**.
10. Expand the domain, and then double-click **CN=Deleted Objects,DC=adatum,DC=com**.
11. Right-click the deleted object, and then click **Modify**.
12. In the **Attribute** text box, type **isDeleted**. In the **Operation** section, click **Delete**, and then press Enter.
13. In the **Attribute** text box, type **distinguishedName**.
14. In the **Values** text box, type the distinguished name of the object in the parent container or the organizational unit (OU) into which you want the object's restoration to occur. For example, type the distinguished name of the object before it was deleted.
15. In the **Operation** section, click **Replace**, and then press Enter.
16. Select the **Extended** check box, click **Run**, and then click **Close**.
17. Close LDP.
18. Use **Active Directory Users and Computers** to repopulate the object's attributes, reset the password for a user object, and if disabled enable the object.

 **Note:** *Ldp.exe* is a command-line tool that you use to perform Lightweight Directory Access Protocol (LDAP) searches against the Active Directory. You also can use it to perform maintenance on AD DS or Active Directory Lightweight Directory Services (AD LDS).

## Configuring the Active Directory Recycle Bin

You can enable the Active Directory Recycle Bin to provide a simplified process for restoring deleted objects. This feature overcomes problems with authoritative restore or tombstone reanimation. With Active Directory Recycle Bin, administrators can restore deleted objects with full functionality without having to restore Active Directory data from backups, and then restart AD DS or reboot domain controllers. Active Directory Recycle Bin builds on the existing tombstone reanimation infrastructure and enhances your ability to preserve and recover accidentally deleted Active Directory objects.



## How Active Directory Recycle Bin works

When you enable Active Directory Recycle Bin, all link-valued and nonlink-valued attributes of the deleted Active Directory objects are preserved, and the objects are restored in their entirety to the same consistent logical state that they were in immediately prior to deletion. For example, restored user accounts automatically regain all group memberships and corresponding access rights that they had immediately before deletion, within and across domains. Active Directory Recycle Bin works for both AD DS and AD LDS environments.

After you enable Active Directory Recycle Bin, when an Active Directory object is deleted, the system preserves all of the object's link-valued and nonlink-valued attributes, and the object becomes logically deleted. A deleted object moves to the Deleted Objects container, and its distinguished name is obscured. A deleted object remains in the Deleted Objects container in a logically deleted state throughout the duration of the deleted object lifetime. Within the deleted object lifetime, you can recover a deleted object with Active Directory Recycle Bin and make it a live AD DS object again.

The deleted object lifetime is determined by the value of the **msDS-deletedObjectLifetime** attribute. For an item deleted after the Active Directory Recycle Bin has been enabled (recycled object), the recycled object lifetime is determined by the value of the legacy **tombstoneLifetime** attribute; by default, this value is null, which means that the deleted object lifetime is set to the value of the recycled object lifetime.

By default, the recycled object lifetime, which is stored in the **tombstoneLifetime** attribute, also is null. This means that the recycled object lifetime defaults to 180 days. You can modify these two values at any time. When **msDS-deletedObjectLife** is set to some value other than null, it no longer assumes the value of **tombstoneLifetime**.

To modify these values, you can use Windows PowerShell. For example, to set **tombstoneLifetime** to 365 days, run the following command, pressing Enter at the end of each line:

```
Set-ADObject -Identity "CN=Directory Service,CN=Windows
NT,CN=Services,CN=Configuration,DC=Adatum,DC=com" -Partition
"CN=Configuration,DC=Adatum,DC=com" -Replace:@{ "tombstoneLifetime" = 365}
```

To set the deleted object lifetime to 365 days, run the following command, pressing Enter at the end of each line:

```
Set-ADObject -Identity "CN=Directory Service,CN=Windows
NT,CN=Services,CN=Configuration,DC=Adatum,DC=com" -Partition
"CN=Configuration,DC=Adatum,DC=com" -Replace:@{ "msDS-DeletedObjectLifetime" = 365}
```

You also can use the Ldp.exe command-line tool to configure these values.

## Enabling the Active Directory Recycle Bin

You can enable the Active Directory Recycle Bin only when the forest functional level is set to Windows Server 2008 R2 or newer.

To enable the Active Directory Recycle Bin, you can perform one of the following:

- From the Active Directory module for Windows PowerShell command prompt, use the **Enable-ADOptionalFeature** cmdlet.
- From Active Directory Administrative Center, select the domain, and then click **Enable Active Directory Recycle Bin** in the Tasks pane.

Only items deleted after you turn on the Active Directory Recycle Bin can be restored from the Active Directory Recycle Bin.



**Note:** Once you have enabled the Active Directory Recycle Bin, you cannot disable it.

## Restoring items from the Active Directory Recycle Bin

The Active Directory Administrative Center provides a graphical interface for restoring deleted Active Directory objects. Once you enable the Active Directory Recycle Bin, the Deleted Objects container displays in the Active Directory Administrative Center. Deleted objects will be visible in this container until their deleted object lifetime expires. You can choose to restore the objects either to their original location, or to an alternate location within AD DS.

## Demonstration: Implementing the Active Directory Recycle Bin

In this demonstration, you will learn how to:

- Enable the Active Directory Recycle Bin.
- Create and then delete test accounts.
- Restore deleted accounts.

### Demonstration Steps

#### Enable the Active Directory Recycle Bin

1. On **LON-DC1**, from **Server Manager**, open **Active Directory Administrative Center**.
2. Enable the Recycle Bin.

#### Create and then delete test accounts

1. In Active Directory Administrative Center, create the following users in the **Research** OU. Give each a password of **Pa\$\$w0rd**:
  - **Test1**
  - **Test2**
2. Delete the **Test1** and **Test2** accounts.

#### Restore deleted accounts

1. In Active Directory Administrative Center, navigate to the **Deleted Objects** folder for the Adatum domain.
2. Restore **Test1** to its original location.
3. Restore **Test2** to the **IT** OU.
4. Confirm that **Test1** is now located in the **Research** OU and that **Test2** is in the **IT** OU.

## Additional backup and recovery tools

### Windows Server Backup

The Windows Server Backup feature in Windows Server consists of an MMC snap-in, the command **Wbadmin**, and Windows PowerShell commands. You can use wizards in the Windows Server Backup user interface to guide you through running backups and recoveries.

You can use Windows Server Backup to back up:

- Full server (all volumes).
- Selected volumes.
- Select specific items for backup, such as specific folders or the System state.

- Windows Server Backup
- Windows Azure Backup
- Data Protection Manager

Windows Server Backup in also allows you to:

- Perform a bare-metal recovery. A bare-metal backup contains all critical volumes, and it allows you to restore without first installing an operating system. You do this by using the product media on a DVD or USB key, and the Windows Recovery Environment (Windows RE). You can use this backup type together with the Windows RE to recover from a hard disk failure, or if you have to recover the whole computer image to new hardware.
- Use System state. The backup contains important information to roll back a server to a specific point in time. However, you must have an operating system installed prior to recovering the System state.
- Recover individual files and folders or volumes. The Individual files and folders option enables you to select to back up and restore specific files, folders, or volumes, or you can add specific files, folders, or volumes to the backup when you use an option such as critical volume or System state.
- Exclude selected files or file types. For example, you can exclude temporary files from the backup.
- Select from more storage locations. You can store backups on remote shares or non-dedicated volumes.
- Use Microsoft Azure Backup. Azure Backup is an off-site, cloud-based backup solution for Windows Server that enables files and folders to back up to and recover from the public or private cloud.

If there are disasters such as hard disk failures, you can perform system recovery by using a full server backup and Windows RE—this will restore your complete system onto the new hard disk.

### Azure Backup

Azure Backup is a subscription service that you can use to provide off-site protection against critical data loss caused by disasters. You back up files and folders and recover them from the public or private cloud as required.

Azure Backup is built on the Windows Azure platform and uses Windows Azure Blob storage for storing customer data. You can use the downloadable Azure Backup agent to transfer file and folder data securely to Azure Backup from Windows Server. After you install the Azure Backup Agent, the agent integrates its functionality through the Windows Server Backup interface. You can download Azure Backup Agent from the Microsoft website.

The key features that Azure Backup provides in Windows Server include:

- Simplified configuration and management. Integration with the Windows Server Backup tool provides a seamless backup and recovery experience to a local disk, or to a cloud platform. Other features include:
  - Simplified user interface to configure and monitor backups.
  - Integrated recovery experience to recover files and folders from a local disk or from a cloud platform.
  - Easy data recoverability for data that was backed up to any server of your choice.
  - Scripting capability that is provided by Windows PowerShell.
- Block-level incremental backups. The Azure Backup Agent performs incremental backups by tracking file and block-level changes, and only transfers the changed blocks. This reduces storage and bandwidth usage. Different point-in-time versions of backups use storage efficiently by storing only the changed blocks between these versions.
- Data compression, encryption, and throttling. The Azure Backup Agent ensures that data is compressed and encrypted on the server before it is sent to the Azure Backup on the network. Therefore, Azure Backup only stores encrypted data in cloud storage. The encryption passphrase is not available to Azure Backup, and therefore, data is never decrypted in the cloud. In addition, users can set up throttling and configure how Azure Backup uses network bandwidth when backing up or restoring information.
- Data integrity verified in the cloud. In addition to the secure backups, backed up data also is checked automatically for integrity after the backup completes. Therefore, you can quickly identify any corruptions that might arise because of the data transfer. These corruptions are fixed automatically in the next backup.
- Configurable retention policies for storing data in the cloud. Azure Backup accepts and implements retention policies to recycle backups that exceed the desired retention range. This helps with meeting business policies and managing backup costs.

### **Data Protection Manager**

Data Protection Manager (DPM) is a Microsoft System Center enterprise data protection and recovery product. DPM has the following features:

- Backup centralization. DPM uses a client/server architecture where the client software is installed on all the computers that are to be backed up. Those clients stream backup data to the DPM server. This allows each DPM server to support entire small to medium-sized organizations. You also can manage multiple DPM servers from one centralized Microsoft System Center Operations Manager console.
- 15-minute recovery point objective (RPO). DPM allows 15-minute snapshots of supported products. This includes most of the Microsoft enterprise suite of products, including Windows Server with its roles and services, Exchange Server, Microsoft Hyper-V, and Microsoft SQL Server.
- Supports Microsoft workloads. DPM was designed specifically by Microsoft to support Microsoft applications such as Exchange Server, SQL Server, and Hyper-V. However, DPM has not been designed to support other third-party server applications that do not have consistent states on disk, or that do not support VSS.
- Disk-based backup. DPM can perform scheduled backups to disk arrays and storage area networks (SANs). You also can configure DPM to export specific backup data to tape for retention and compliance-related tasks.

- Remote site backup. DPM uses an architecture that allows it to back up clients that are located in remote sites. This means that a DPM server that is located in a head office site can perform backups of servers and clients that are located across wide area network (WAN) links.
- Supports backup-to-cloud strategies. DPM supports backup of DPM servers to a cloud platform. This means that you can use a DPM server at a cloud-based hosting facility to back up the contents of a head office DPM server. For disaster redundancy, you also can configure DPM servers to back up each other.

## Active Directory backup and recovery

In older versions of the Windows operating system, backing up AD DS involved creating a backup of the System state, which was a small collection of files that included the AD DS database and the registry.

In Windows Server 2016, the System state concept still exists, but it is much larger. Because of interdependencies between server roles, physical configuration, and AD DS, System state is now a subset of a full server backup, and in some configurations, might be just as big. To back up a domain controller, you must back up all critical volumes fully.

- **Nonauthoritative or normal restore:**
  - Restore domain controller to previously known good state
  - Domain controller updates by using standard replication from partners
- **Authoritative restore:**
  - Restore domain controller to previously known good state
  - Mark objects that you want to be authoritative
  - Domain controller updates from its up-to-date partners
  - Domain controller sends authoritative updates to its partners
- **Full server restore:**
  - Typically perform in Windows RE
- **Alternate location restore**

### Restoring Active Directory data

When a domain controller or its directory becomes corrupted, damaged, or fails, you have several options to restore the system. To perform a restore of AD DS, you must have full access to the files on the domain controller. This requires restarting the domain controller in DSRM. If you are restarting a domain controller locally, press **F8** on startup, and choose the DSRM from the startup menu.

When you start a domain controller in DSRM, you will sign in as Administrator with the DSRM password. You then can use Windows Server Backup to restore the directory database. After completing the restoration, you must restart the server. The domain controller will ensure that its database is consistent 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.

### **Nonauthoritative restore**

In a normal restoration, you restore a backup of AD DS as of a known good date. Essentially, 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. In other words, the domain controller catches up with the rest of the domain by using standard replication mechanisms.

Normal restoration is useful when the directory on a domain controller has been damaged or corrupted, but the problem has not spread to other domain controllers. However, for certain situations a normal restoration is not sufficient. For example, normal restoration will not work where damage has replicated, such as when you delete one or more objects, and that deletion has replicated. If you restore a known good version of AD DS and restart the domain controller, the deletion—which happened subsequent to the backup—will simply replicate back to the domain controller.



## Authoritative restore

An authoritative restore is necessary when a known good copy of AD DS is restored and contains objects that must override existing objects in the AD DS database. In an authoritative restore, you restore the known good version of AD DS just as you do in a normal restore. However, before you restart the domain controller, you mark the accidentally deleted or previously corrupted objects that you wish to retain 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 virtually guaranteed to be higher than the version number on all other domain controllers.

When the restored domain controller restarts, it replicates from its replication partners all the changes that have been made to the directory. It also notifies its partners that it has changes, and the version numbers of the changes ensure that partners take the changes and replicate them throughout the directory service.

In forests with the Active Directory Recycle Bin enabled, you can use the Active Directory Recycle Bin as a simpler alternative to an authoritative restore.



**Note:** You cannot use the Active Directory Recycle Bin to recover corrupted objects.

To perform an authoritative, restore operation perform the following steps:

1. Restart the domain controller in DSRM.
2. Sign in with the Administrator account and the DSRM password.
3. Restore the directory with Windows Server Backup, as described in the previous topic.

Before restarting the domain controller, you must first 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, pressing Enter at the end of each line:

```
NtdsUtil.exe
authoritative restore
restore object <object DN>
```

*Object DN* is the distinguished name of the object being restored. For example, if you want to restore user object Candy Spoon that was in the IT OU, you would type:

```
Restore object "CN=Candy Spoon,OU=IT,DC=adatum,DC=com"
```

To mark an OU or container and all of its sub-objects as authoritative, at the command prompt, type the following commands.

```
NtdsUtil.exe
authoritative restore
restore subtree <object DN>
```

4. 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 replicate from the restored domain controller to the rest of the directory service.

**Other restore options**

The third option for restoring the directory service is to restore the entire domain controller. You can do this by starting in Windows RE, and then restoring a full server backup of the domain controller. By default, this is the normal restore method. If you also need to mark objects as authoritative, you must restart the server in the DSRM and set the desired objects as authoritative, prior to starting 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. You should not copy the files from an alternate restoration location over the production versions of those files. In addition, do not do a piecemeal restore of AD DS. However, you can use these copied files to support the **Install From Media** option for creating a new domain controller. Most of the procedures involved in performing an authoritative restore are identical to those of a nonauthoritative restore.

## Lab: Recovering Objects in AD DS

### Scenario

You were notified yesterday that one user account was deleted by accident. A few days ago, additional user accounts were deleted accidentally. You want to recover these accounts.

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 IT OU. You must recover this OU.

### Objectives

After you complete this lab, you will be able to:

- Backup and restore AD DS.
- Recover objects in AD DS.

### Lab Setup

Estimated Time: **60 minutes**

Virtual machines: **20742A-LON-DC1, 20742A-LON-DC2**

User name: **Adatum\Administrator**

Password: **Pa\$\$w0rd**

For this lab, you will use the available virtual machine environment. Before you begin the lab, you must complete the following steps:

1. On the host computer, start **Hyper-V Manager**
2. In Hyper-V Manager, click **20742A-LON-DC1**, and in the **Actions** pane, click **Start**.
3. In the **Actions** pane, click **Connect**. Wait until the virtual machine starts.
4. Sign in by using the following credentials:
  - User name: **Administrator**
  - Password: **Pa\$\$w0rd**
  - Domain: **Adatum**
5. Repeat steps 1 through 4 for **20742A-LON-DC2**.

### Exercise 1: Backing up and restoring Active Directory Domain System (AD DS)

#### Scenario

You noticed that AD DS has not been backed up recently. You decide to create a backup schedule and to perform a one-time interactive backup, to be safe. It is fortunate that you did perform the interactive backup because shortly afterward, an AD DS object was deleted inadvertently. You must restore this object authoritatively.

The main tasks for this exercise are as follows:

1. Install the Windows Server Backup feature
2. Create a scheduled backup
3. Perform an interactive backup

4. Delete an organizational unit (OU)
5. Restart in Directory Services Restore Mode (DSRM)
6. Restore System state data
7. Mark restored information as authoritative
8. Verify that the data has been restored

► **Task 1: Install the Windows Server Backup feature**

- On **LON-DC1**, from **Server Manager**, install the Windows Server Backup feature.

► **Task 2: Create a scheduled backup**

1. On **LON-DC1**, run **Windows Server Backup**.
2. Create a custom backup configuration by using the following information:
  - Items to back up: Bare metal recovery
  - Backup interval: **Once a day**
  - Time of day: **12:00 am**
  - Destination type: **Backup to a hard disk that is dedicated for backups.**
  - Destination disk: **Disk 1**
3. When the **Windows Server Backup** dialog box appears, informing you that all data on the disk will be deleted, click **Yes**.



**Note:** You will cancel the process in the next step to avoid formatting drive E.

4. Click **Cancel**. Do not format drive E.

► **Task 3: Perform an interactive backup**

1. In the **Actions** pane, click **Backup Once**.
2. Configure the backup to use the following settings:
  - Backup configuration: **Custom**
  - Backup items: **System state**
  - Advanced setting: **VSS full Backup**



**Note:** The backup will take about 10–15 minutes to complete. After the backup completes, close Windows Server Backup.

► **Task 4: Delete an organizational unit (OU)**



**Note:** Wait until the backup completes before proceeding.

1. On **LON-DC1**, from **Server Manager**, open **Active Directory Users and Computers**.
2. Delete the **Research** OU.

► **Task 5: Restart in Directory Services Restore Mode (DSRM)**

1. On **LON-DC1**, run Windows PowerShell as an administrator.
2. At the command prompt, type the following command to configure the server to start in DSRM:

```
bcdedit /set safeboot dsrepair
```

3. Restart **LON-DC1**.

► **Task 6: Restore System state data**

1. Sign in to **LON-DC1** as **.\Administrator** with the password **Pa\$\$w0rd**.
2. Run Windows PowerShell as an administrator.
3. To obtain the version identifier for the backup, at the command prompt, type the following command, and then press Enter:

```
wbadmin get versions -backuptarget:E: -machine:LON-DC1
```

4. Restore the System state information by typing the following command in the following format:

```
wbadmin start systemstaterecovery -version:<version> -backuptarget:E: -machine:LON-DC1.
```

For example:

```
wbadmin start systemstaterecovery -version:01/22/2011-10:37 -backuptarget:E: -machine:LON-DC1
```



**Note:** The restoration will take about 30–35 minutes.

5. When prompted to restart, type **Y**, and then press Enter.

► **Task 7: Mark restored information as authoritative**

1. Sign in to **LON-DC1** as **.\Administrator** with the password **Pa\$\$w0rd**.
2. Open Windows PowerShell as an administrator.
3. At the Windows PowerShell command prompt, use **NtdsUtil.exe** to perform an authoritative restore of **"OU=Research,DC=adatum,DC=com"**
4. To restart the server normally after you perform the restoration operation, type the following command, and then press Enter.

```
bcdedit /deletevalue safeboot
```

5. Restart the server.

### ► Task 8: Verify that the data has been restored

1. After the server restarts, sign in to **LON-DC1** as **Adatum\Administrator** with the password **Pa\$\$w0rd**.
2. From **Server Manager**, open **Active Directory Users and Computers**.
3. Verify the presence of the **Research** OU. Note that you may have to force a site replication in Active Directory Sites and Services to see the change immediately.

**Results:** After completing this exercise, you should have performed an interactive backup and an authoritative restore of AD DS successfully.

## Exercise 2: Recovering objects in AD DS

### Scenario

A number of user accounts have recently been deleted in error. You decide to enable the Active Directory Recycle Bin feature to help with future account recovery.

The main tasks for this exercise are as follows:

1. Verify requirements for Active Directory Recycle Bin.
2. Enable the Active Directory Recycle Bin feature.
3. Delete objects to simulate accidental deletion.
4. Perform object restoration with the Active Directory Module for Windows PowerShell.
5. Verify object restoration.
6. Prepare for the end of the course.

### ► Task 1: Verify requirements for Active Directory Recycle Bin

- On **LON-DC1**, open **Active Directory Domains and Trusts** and verify the forest functional level. It should be Windows Server 2012 R2.

### ► Task 2: Enable the Active Directory Recycle Bin feature

1. On **LON-DC1**, open **Active Directory Sites and Services** and then replicate Active Directory between **LON-DC1** and **LON-DC2**.
2. Start Active Directory Module for Windows PowerShell.
3. Enable the Active Directory Recycle Bin feature by typing the following command, and then pressing Enter:

```
Enable-ADOptionalFeature -Identity 'CN=Recycle Bin Feature,CN=Optional
Features,CN=Directory Service,CN=Windows NT,CN=Services,CN=Configuration,
DC=adatum,DC=com' -Scope ForestOrConfigurationSet -Target 'adatum.com'
```

4. Repeat step 1 to re-sync the domain.

### ► Task 3: Delete objects to simulate accidental deletion

1. Open **Active Directory Users and Computers**. Provide the account **Adatum\Administrator** with the password **Pa\$\$w0rd**.
2. Navigate to the **Sales** OU.

3. Delete **Abbie Parsons**.
4. Close Active Directory Users and Computers.

► **Task 4: Perform object restoration with the Active Directory Module for Windows PowerShell**

1. Start the Active Directory Module for Windows PowerShell.
2. At the Windows PowerShell command prompt, type the following command, and then press Enter:

```
Get-ADObject -Filter {displayName -eq "Abbie Parsons "} -IncludeDeletedObjects |  
Restore-ADObject
```

3. Close the **Windows PowerShell** window.

► **Task 5: Verify object restoration**

1. On **LON-DC1**, open the **Active Directory Users and Computers** console.
2. Make sure that **Abbie Parsons** exists within the **Sales** OU.

**Results:** After completing the exercise, you should have enabled and tested the Active Directory Recycle Bin feature successfully.

► **Task 6: Prepare for the end of the course**

When you finish the lab, revert the virtual machines to their initial state. To do this, perform the following steps:

1. On the host computer, start **Hyper-V Manager**.
2. In the **Virtual Machines** list, right-click **20742A-LON-DC1**, and then click **Revert**.
3. In the **Revert Virtual Machine** dialog box, click **Revert**.
4. Repeat steps 2 and 3 to revert **20742A-LON-DC2**.

**Question:** When you restore a deleted user or an OU with user objects by using authoritative restore, will the objects be exactly the same as before? Which attributes might not be the same?

**Question:** In the lab, would it be possible to restore these deleted objects if they were deleted before Active Directory Recycle Bin has been enabled?

## Module Review and Takeaways

### Review Question

**Question:** What kind of restoration can you perform with AD DS?

### Best Practices

- Back up your domain controllers regularly.
- Consider AD DS database recovery as one of your restore scenarios for domain controllers.
- Enable Active Directory Recycle Bin to allow for simplified recovery of deleted objects.
- Use restartable AD DS when performing database maintenance tasks.



## Course Evaluation

Your evaluation of this course will help Microsoft understand the quality of your learning experience.

Please work with your training provider to access the course evaluation form.

Microsoft will keep your answers to this survey private and confidential and will use your responses to improve your future learning experience. Your open and honest feedback is valuable and appreciated.

- Your evaluation of this course will help Microsoft understand the quality of your learning experience.
- Please work with your training provider to access the course evaluation form.
- Microsoft will keep your answers to this survey private and confidential and will use your responses to improve your future learning experience. Your open and honest feedback is valuable and appreciated.

**MCT USE ONLY. STUDENT USE PROHIBITED**

# Module 1: Installing and configuring domain controllers

## Lab: Deploying and administering AD DS

### Exercise 1: Deploying AD DS

#### ► Task 1: Install AD DS binaries

1. On **LON-DC1**, in **Server Manager**, click **Tools**, and then click **Windows PowerShell**.
2. At the command prompt in the Windows PowerShell command-line interface, type the following command, and then press Enter.

```
Install-WindowsFeature -Name AD-Domain-Services -ComputerName LON-SVR1
```

3. Type the following command to verify that the Active Directory Domain Services (AD DS) role is installed on **LON-SVR1**, and then press Enter.

```
Get-WindowsFeature -ComputerName LON-SVR1
```

4. In the output of the previous command, scroll up and search for **Active Directory Domain Services**. Verify that the check box is selected. Search for **Remote Server Administration Tools**. Look for the **Role Administration Tools** node below it, and then look for the **AD DS and AD LDS Tools** node.



**Note:** Below that node, only **Active Directory module for Windows PowerShell** has been installed and not the graphical tools, such as the Active Directory Administrative Center. If you centrally manage your servers, you will not usually need these on each server. If you want to install them, you need to specify the AD DS tools by running the **Add-WindowsFeature** cmdlet with the **RSAT-ADDS** command name.



**Note:** You might need to wait a short period of time after the installation process completes before verifying that the AD DS role has been installed. If you do not see the expected results from the **Get-WindowsFeature** command, you can try again after a few minutes.

#### ► Task 2: Prepare the AD DS installation and promote a remote server

##### Add LON-SVR1 to Server Manager on LON-DC1

1. On **LON-DC1**, in **Server Manager**, select the **All Servers** view.
2. On the **Manage** menu, click **Add Servers**.
3. In the **Add Servers** dialog box, maintain the default settings, and then click **Find Now**.
4. In the **Active Directory** list of servers, select **LON-SVR1**, click the arrow to add it to the **Selected** list, and then click **OK**.

##### Remotely configure AD DS by using Server Manager

1. On **LON-DC1**, ensure that the installation of the AD DS role on **LON-SVR1** is complete and that the server was added to **Server Manager**. Then click the **Notifications** flag symbol.
2. Note the post-deployment configuration of **LON-SVR1**, and then click the **Promote this server to a domain controller** link.

3. In the **Active Directory Domain Services Configuration Wizard**, on the **Deployment Configuration** page, under **Select the deployment operation**, verify that **Add a domain controller to an existing domain** is selected.
4. Ensure that the **Adatum.com** domain is specified, and then in the **Supply the credentials to perform this operation** section, click **Change**.
5. In the **Credentials for deployment operation** dialog box, in the **User name** box, type **Adatum\Administrator**, and then in the **Password** box, type **Pa\$\$w0rd**.
6. Click **OK**, and then click **Next**.
7. On the **Domain Controller Options** page, clear the selections for **Domain Name System (DNS) server** and **Global Catalog (GC)**. Ensure that **Read-only domain controller (RODC)** is cleared.
8. In the **Type the Directory Services Restore Mode (DSRM) password** section, type and confirm the password **Pa\$\$w0rd**, and then click **Next**.
9. On the **Additional Options** page, click **Next**.
10. On the **Paths** page, keep the default path settings for the **Database folder**, **Log files folder**, and **SYSVOL folder**, and then click **Next**.
11. On the **Review Options** page, click **View script** to open the generated Windows PowerShell script.
12. In Microsoft Notepad, edit the generated Windows PowerShell script:
  - o Delete the comment lines that begin with the number sign (#).
  - o Remove the **Import-Module** line.
  - o Remove the grave accents (`) at the end of each line.
  - o Remove the line breaks.
13. Now the **Install-ADDSDomainController** command and all the parameters are on one line. Place the cursor in front of the line, and then press Shift+End to select the whole line. on the menu, click **Edit**, and then click **Copy**.
14. Switch to the **Active Directory Domain Services Configuration Wizard**, and then click **Cancel**.
15. When prompted for confirmation, click **Yes** to cancel the wizard.
16. Switch to **Server Manager**. On the menu, click **Tools**, and then click **Windows PowerShell**.
17. At the Windows PowerShell command prompt, type the following command.

```
Invoke-Command -ComputerName LON-SVR1 { }
```

18. Place the cursor between the braces ({ }), and then paste the content of the copied script line from the clipboard. The whole line should now be as follows.

```
Invoke-Command -ComputerName LON-SVR1 {Install-ADDSDomainController -  
NoGlobalCatalog:$true -Credential (Get-Credential) -CriticalReplicationOnly:$false -  
DatabasePath "C:\Windows\NTDS" -DomainName "Adatum.com" -InstallDns:$false -LogPath  
"C:\Windows\NTDS" -NoRebootonCompletion:$false -SiteName "Default-First-Site-Name" -  
SysvolPath "C:\Windows\SYSVOL" -Force:$true }
```

19. Press Enter to start the command.
20. In the **Windows PowerShell Credential Request** dialog box, type **Adatum\Administrator** in the **User name** box, type **Pa\$\$w0rd** in the **Password** box, and then click **OK**.
21. When prompted for the password, in the **SafeModeAdministratorPassword** text box, type **Pa\$\$w0rd**, and then press Enter.

22. When prompted for confirmation, in the **Confirm password** text box, type **Pa\$\$w0rd**, and then press Enter.
23. Wait until the command runs and **Status Success** is returned. The **LON-SVR1** virtual machine restarts.
24. Close Notepad without saving the file.
25. After **LON-SVR1** restarts, on **LON-DC1**, switch to **Server Manager**, and on the left side, click the **AD DS** node. Note that **LON-SVR1** has been added as a server and that the warning notification has disappeared. You might have to click **Refresh**.

► **Task 3: Run the AD DS Best Practices Analyzer**

1. On **LON-DC1**, in **Server Manager**, go to the AD DS dashboard view.
2. Scroll down to the **Best Practices Analyzer** section, click the **Tasks** menu, and then click **Start BPA Scan**.
3. In the **Select Servers** dialog box, select **LON-DC1.Adatum.com** and **LON-SVR1.Adatum.com**.
4. Click **Start Scan**, and then wait until the Best Practices Analyzer (BPA) finishes the scan.
5. Review the results of the BPA.

**Results:** After this exercise, you should have successfully created a new domain controller and reviewed the AD DS Best Practices Analyzer (BPA) results for that domain controller.

## Exercise 2: Deploying domain controllers by performing domain controller cloning

► **Task 1: Check for domain controller clone prerequisites**

1. On **LON-DC1**, in **Server Manager**, click **Tools**, and then click **Active Directory Administrative Center**.
2. In the **Active Directory Administrative Center**, double-click **Adatum (local)**, and then in the management list, double-click the **Domain Controllers** organizational unit (OU).
3. In the management list, select **LON-DC1**, if it is not already selected, and then in the **Tasks** pane, in the **LON-DC1** section, click **Add to group**.
4. In the **Select Groups** dialog box, in the **Enter the object names to select** box, type **Cloneable**, and then click **Check Names**.
5. Ensure that the group name is expanded to **Cloneable Domain Controllers**, and then click **OK**.
6. On **LON-DC1**, on the taskbar, click the **Windows PowerShell** icon.
7. At the Windows PowerShell command prompt, type the following command, and then press Enter.

```
Get-ADDCCloningExcludedApplicationList
```

- Verify the list of critical apps, if any. (In production, verify each app or use a domain controller that has fewer apps installed by default.) Type the following command, and then press Enter.

```
Get-ADDCCloningExcludedApplicationList -GenerateXML
```

- Run the following command to create the DCCloneConfig.xml file.

```
New-ADDCCloneConfigFile
```

### ► Task 2: Copy the source domain controller

- Type the following command to shut down **LON-DC1**, and then press Enter.

```
Stop-Computer
```

- On the host computer, in Microsoft Hyper-V Manager, in the management list, select the **20742A-LON-DC1** virtual machine.
- In the **Actions** pane, in the **20742A-LON-DC1** section, click **Export**.
- In the **Export Virtual Machine** dialog box, type the location **D:\Program Files\Microsoft Learning\20742**, and then click **Export**. Wait until the export finishes.



**Note:** Depending on your classroom's setup, the **Program Files\Microsoft Learning\20742** folder might be on drive C. Please locate and use the existing folder for the remainder of the lab.

- In the **Actions** pane, in the **20742-LON-DC1** section, click **Start**, and then sign in as **Adatum\Administrator** with the password **Pa\$\$w0rd**.

### ► Task 3: Perform domain controller cloning

- On the host computer, in Hyper-V Manager, in the **Actions** pane, in the section that is named for the host computer, click **Import Virtual Machine**.
- In the **Import Virtual Machine Wizard**, on the **Before You Begin** page, click **Next**.
- On the **Locate Folder** page, click **Browse**, browse to the folder **D:\Program Files\Microsoft Learning\20742\20742A-LON-DC1**, click **Select Folder**, and then click **Next**.
- On the **Select Virtual Machine** page, select **20742A-LON-DC1** (if it is not already selected), and then click **Next**.
- On the **Choose Import Type** page, select **Copy the virtual machine (create a new unique ID)**, and then click **Next**.
- On the **Choose Folders for Virtual Machine Files** page, select the **Store the virtual machine in a different location** check box.
- For each folder location, specify **D:\Program Files\Microsoft Learning\20742\** as the path, and then click **Next**.
- On the **Choose Folders to Store Virtual Hard Disks** page, provide the path **D:\Program Files\Microsoft Learning\20742\**, and then click **Next**.
- On the **Completing Import Wizard** page, click **Finish**.
- In the management list, identify and select the newly imported virtual machine named **20742A-LON-DC1**, which has the **State** shown as **Off**. In the lower section of the **Actions** pane, click **Rename**.

11. Type **20742A-LON-DC3** as the name, and then press Enter.
12. In the **Actions** pane, in the **20742A-LON-DC3** section, click **Start**, and then click **Connect** to see the virtual machine starting.
13. While the server is starting, you may see the message **Domain Controller cloning is at x% completion**.

**Results:** After completing this exercise, you should have successfully deployed a domain controller by closing it in Hyper-V.

### Exercise 3: Administering AD DS

#### ► Task 1: Use the Active Directory Administrative Center

##### Navigate within the Active Directory Administrative Center

1. On **LON-DC1**, in **Server Manager**, click **Tools**, and then click **Active Directory Administrative Center**.
2. In the navigation pane, click the **Tree View** tab, and then expand **Adatum (local)**.

##### Perform an administrative task within the Active Directory Administrative Center

1. In the **Active Directory Administrative Center**, click **Overview**.
2. In the **Reset Password** section, in the **User name** box, type **Adatum\Adam**.
3. In the **Password** and **Confirm password** boxes, type **Pa\$\$w0rd**.
4. Clear the **User must change password at next log on** check box, and then click **Apply**.
5. In the **Global Search** section, in the **Search** box, type **Lon**, and then press Enter.

##### Create objects

1. In the **Active Directory Administrative Center**, in the navigation pane tree view, expand **Adatum (local)**, and then click the **Computers** container.
2. In the **Tasks** pane, in the **Computers** section, click **New**, and then select **Computer**.
3. In the **Create Computer** dialog box, type the following information, and then click **OK**:
  - Computer name: **LON-CL4**
  - Computer (NetBIOS) name: **LON-CL4**

##### View all object attributes

1. In the **Active Directory Administrative Center**, double-click **Adatum (local)**, and then in the management list, double-click **Computers**.
2. Select **LON-CL4**, and then in the **Tasks** pane, in the **LON-CL4** section, click **Properties**.
3. In the **LON-CL4 properties** window, scroll down to the **Extensions** section, click the **Attribute Editor** tab, and then note that all the attributes of the computer object are available here.
4. Close the **LON-CL4 properties** window by clicking **Cancel**.

### Use the Windows PowerShell History viewer

1. In the **Active Directory Administrative Center**, click the **Windows PowerShell History** toolbar at the bottom of the screen.
2. View the details for the **New-ADComputer** cmdlet that was used to perform the most recent task.
3. On **LON-DC1**, close all open windows.

**Results:** After completing this exercise, you should have successfully used the Active Directory Administrative Center to manage AD DS and reviewed the Windows PowerShell cmdlets that run behind the scenes.

### ► Task 2: Prepare for the next module

When you are finished with the lab, revert all virtual machines to their initial state:

1. On the host computer, start **Hyper-V Manager**.
2. In the **Virtual Machines** list, right-click **20742A-LON-DC1**, and then click **Revert**.
3. In the **Revert Virtual Machine** dialog box, click **Revert**.
4. Repeat steps 2 and 3 for **20742A-LON-DC2** and **20742A-LON-SVR1**.



## Module 2: Managing objects in AD DS

# Lab A: Managing AD DS objects

### Exercise 1: Creating and managing groups in AD DS

#### ► Task 1: Create groups and add members

1. On **LON-DC1**, in **Server Manager**, click **Tools**, and then click **Active Directory Administrative Center**.
2. Click **Adatum (local)**, and then click **Managers**.
3. In the **Tasks** pane, under **Managers**, click **New**, and then click **Group**.
4. In the **Group name:** field, type **Enterprise Managers**.
5. Under **Group scope**, click **Universal**.
6. Click **OK** to close the **Create Group: Enterprise Managers** window.
7. Click **Adatum (local)**, and then click the **Research** organizational unit (OU).
8. In the **Tasks** pane, under **Research**, click **New**, and then click **Group**.
9. In the **Group name:** field, type **Research Mail**.
10. In the **Group type** section, select **Distribution**.
11. In the **Email** field, type **Research@adatum.com**.
12. In the **Managed By** section, click **Edit**.
13. In the **Select Users, Contacts, Computers, Service Accounts, or Groups** dialog box, in **Enter the object names to select (examples)**, type **Cai**, click **Check Names**, and then click **OK**.
14. Select the **Manager can update membership list** check box.
15. Click **OK** to close the **Create Group: Research Mail** window.
16. In the **Tasks** pane, under **Research**, click **New**, and then click **Group**.
17. In the **Group name:** field, type **Research Managers**.
18. Scroll to the **Members** section, and then click **Add**.
19. In the **Select Users, Contacts, Computers, Service Accounts, or Groups** dialog box, in **Enter the object names to select (examples)**, type **Cai; Vera**, click **Check Names**, and then click **OK**.
20. Click **OK** to close the **Create Group: Research Managers** window.

#### ► Task 2: Configure group nesting

1. Double-click the **Managers** OU.
2. Right-click the **Enterprise Managers** group, and then click **Properties**.
3. In the navigation pane, click **Members** and then click **Add**.
4. In the **Select Users, Contacts, Computers, Service Accounts, or Groups** dialog box, in **Enter the object names to select (examples)**, type **Managers; Research Managers**, click **Check Names**, and then click **OK**.
5. Click **OK** to close the **Enterprise Managers** window.

► **Task 3: Convert a group type from distribution to security**

1. In the navigation pane, click **Adatum (local)**.
2. Double-click the **Research Mail** group.
3. Under **Group type**, click **Security**, and then click **OK**.

**Results:** After completing this exercise you will have:

- Created groups and added members
- Configured group nesting
- Converted a group type

## Exercise 2: Creating and configuring user accounts in AD DS

► **Task 1: Create and configure a user template for the Research department**

1. Ensure that the **Research** OU is selected.
  2. In the **Tasks** pane, under **Research**, click **New**, and then click **User**.
  3. In the **Create User** window, in the **First name** field, type **\_Research Template**.
  4. In the **User UPN logon** field, type **ResearchTemplate**.
  5. In the **Password** and **Confirm password** fields, type **Pa\$\$w0rd**.
  6. In the navigation pane, click **Organization**, and in the **Department** field, type **Research**.
  7. In the **Company** field, type **Adatum**.
  8. In the **Manager** field, click **Edit**.
  9. In the **Select Users, Contacts, Computers, Service Accounts, or Groups** dialog box, in **Enter the object names to select (examples)**, type **Cai**, click **Check Names**, and then click **OK**.
  10. In the navigation pane, click **Member Of**.
  11. Click **Add**.
  12. In the **Select Users, Contacts, Computers, Service Accounts, or Groups** dialog box, in **Enter the object names to select (examples)**, type **Research**, and then click **Check Names**. In the **Multiple names Found** dialog box, select **Research**, and then click **OK** twice.
  13. In the navigation pane, click **Profile**.
  14. In the **Log on script** field, type **\\LON-DC1\Netlogon\Logon.bat**, and then click **OK**.
  15. Click the **\_Research Template** account, and in the **Tasks** pane, under **\_Research Template**, click **Disable**.
  16. Close Active Directory Administrative Center.
- **Task 2: Create new users for the Research branch office based on the template**
1. In **Server Manager**, click **Tools**, and then click **Active Directory Users and Computers**.
  2. Expand **Adatum.com**, and then click the **Research** OU.
  3. Right-click the **\_Research Template** account, and then click **Copy**.

4. In the **Copy Object – User** dialog box, type **Research** in the **First name** field, and then type **User** in the **Last name** field.
5. In the **User logon name** field, type **ResearchUser**, and click **Next**.
6. In the **Password** and **Confirm password** fields, type **Pa\$\$w0rd**.
7. Clear the **Account is disabled** check box, and then click **Next**.
8. Click **Finish**.

► **Task 3: Validate the template**

1. Double-click **Research User**.
2. Click the **Profile** tab, and then ensure that the Logon script path is **\\LON-DC1\Netlogon\Logon.bat**.
3. Click the **Organization** tab, and then ensure that the **Department** is **Research**, the **Company** is **Adatum**, and the Manager is **Cai Chu**.
4. Click the **Member Of** tab, and then ensure that the user is a member of the **Research** group.
5. Click **Cancel** to dismiss the **Research User Properties** dialog box.

**Results:** After completing this exercise, you will have:

- Created and configured a user template for research users.
- Created three new users based on the template.
- Signed on to test that the accounts are functioning as expected.

### Exercise 3: Managing computer objects in AD DS

► **Task 1: Reset a computer account**

1. In **Active Directory Users and Computers**, click the **Computers** container.
2. In the details pane, right-click the **LON-CL1** computer account, and then click **Reset Account**.
3. In the **Active Directory Domain Services** dialog box, click **Yes**.
4. In the **Active Directory Domain Services** message box, click **OK**.

► **Task 2: Observe the behavior when a client attempts to sign on**

- Restart **LON-CL1** and attempt to sign in as **Adatum\Adam** with a password of **Pa\$\$w0rd**.

**Question:** What is the message displayed?

**Answer:** The trust relationship between this workstation and the primary domain failed.

► **Task 3: Resolve the computer issue**

1. Sign in to **LON-CL1** as **Adatum\Administrator** with a password of **Pa\$\$w0rd**.
2. Right-click the **Start** button, and then click **Run**.
3. Type **PowerShell**, and then press Enter.

4. In the **Administrator: Windows PowerShell** window, type the following cmdlet, and then press Enter:

```
Test-ComputerSecureChannel -Repair
```

5. Close the **Windows PowerShell** window, and then sign out.
6. Sign in as **Adatum\Adam** with a password of **Pa\$\$w0rd**. The logon will succeed now.
7. Sign out of **LON-CL1**.
8. Leave the VMs running for the next lab.

**Results:** After completing this exercise, you will have:

- Reset a computer account.
- Observed the behavior when a client signs on.
- Resolved the computer issue.

# Lab B: Administering AD DS

## Exercise 1: Delegating administration for OUs

### ► Task 1: Create a new OU for the branch office

1. On **LON-DC1**, in **Active Directory Users and Computers**, right-click **Adatum.com**, click **New**, and then click **Organizational Unit**.
2. In **New Object – Organizational Unit**, type **London** in the **Name** field, and then click **OK**.

### ► Task 2: Create groups for branch administrators and branch Help-desk personnel

1. Right-click the **London** OU, click **New**, and then click **Group**.
2. In the **New Object – Group** dialog box, type **London Admins**, and then click **OK**.
3. Repeat steps 1 and 2 to create a group named **London Helpdesk**.

### ► Task 3: Add members to the group

1. Click the **IT** OU.
2. Right-click the **Beth Burke** user account, and then click **Add to a group**.
3. In the **Select Groups** dialog box, in **Enter the object names to select (example)**: type **London Admins**. Click **Check Names**, and then click **OK**.
4. In the **Active Directory Domain Services** message box, click **OK**.
5. Right-click the **Dante Danby** user account, and then click **Add to a group**.
6. In the **Select Groups** dialog box, in **Enter the object names to select (example)**: type **London Helpdesk**. Click **Check Names**, and then click **OK**.
7. In the **Active Directory Domain Services** message box, click **OK**.

### ► Task 4: Delegate permissions to the group

1. In **Active Directory Users and Computers**, click **View** and then click **Advanced Features**.
2. Right-click the **London** OU, and then click **Properties**.
3. Click the **Security** tab, and then click **Add**.
4. In the **Select Users, Computers, Service Accounts or Groups** dialog box, in **Enter the object names to select (example)**: type **London Admins**. Click **Check Names**, and then click **OK**.
5. Ensure that the **London Admins** group is selected, check **Full Control** in the **Allow** column, and then click **OK**.
6. Right-click the **London** OU, and then click **Delegate Control**.
7. In the **Delegation of Control Wizard**, click **Next**.
8. On the **Users or Groups** page, click **Add**.
9. In the **Select Users, Computers, or Groups** dialog box, in **Enter the object names to select (example)**: type **London Helpdesk**. Click **Check Names**, click **OK**, and then click **Next**.
10. On the **Tasks to Delegate** page, click **Create a custom task to delegate**, and then click **Next**.
11. On the **Active Directory Object Type** page, click **Only the following object in this folder**.
12. Scroll to the bottom of the list. Click **User objects**, and then select the check boxes for **Create selected objects in this folder** and **Delete selected objects in this folder**, and then click **Next**.

13. On the **Permissions** page, click **Full Control**, and then click **Next**.
14. Click **Finish**.

► **Task 5: Test permissions**

1. Switch to **LON-SVR1**.
2. Click **Start**, click **Server Manager**, and then click **Add roles and features**.
3. In the **Add Roles and Features Wizard**, click **Next**.
4. On the **Select installation type** page, click **Next**.
5. On the **Select destination server** page, click **Next**.
6. On the **Select server roles** page, click **Next**.
7. On the **Select features** page, expand **Remote Server Administration Tools**, and then expand **Role Administration Tools**. Expand **AD DS and AD LDS Tools**. Select the checkbox beside **AD DS Tools** and then click **Next**.
8. Click **Install**. Wait for installation to complete.
9. When installation is complete, click **Close**.
10. Sign out of **LON-SVR1**.

**Test permissions for London Admins**

1. Sign in to **LON-SVR1** as **Beth** with a password of **Pa\$\$w0rd**.
2. Click **Start**, and then click the **Server Manager** tile.
3. Click **Tools**, and then click **Active Directory Users and Computers**.
4. Expand **Adatum.com**, and then click the **Research** OU. Notice that the icons on the toolbar to create users, groups, or OUs are grayed out.
5. Click the **London** OU. Notice that those icons are live now.
6. Right-click the **London** OU, click **New**, and then click **Organizational Unit**.
7. In the **New Object – Organizational Unit** dialog box, type **Laptops** in the **Name** field, and then click **OK**. The creation will succeed.
8. Sign out of **LON-SVR1**.

## Test permissions for London Helpdesk

1. Sign in to **LON-SVR1** as **Dante** with a password of **Pa\$\$w0rd**.
2. Click **Start**, and then click the **Server Manager** tile.
3. Click **Tools**, and then click **Active Directory Users and Computers**.
4. Expand **Adatum.com**, and then click the **London** OU. Notice that the only icon not grayed out is the create user icon.

**Results:** After completing this exercise you will have:

- Created a new OU for the branch office.
- Created groups for branch administrators and branch Help-desk personnel.
- Added members to the group.
- Delegated permission to the groups.
- Installed AD DS tools and tested permissions.

## Exercise 2: Creating and modifying AD DS objects with Windows PowerShell

### ► Task 1: Create a user account using Windows PowerShell

1. Switch to **LON-DC1**.
2. Right-click the **Start** button, and then click **Windows PowerShell (Admin)**.
3. Create a user account for Ty Carlson in the London OU by running the following command:

```
New-ADUser -Name Ty -DisplayName "Ty Carlson" -GivenName Ty -Surname Carlson -Path "ou=London,dc=adatum,dc=com"
```

4. Set the password for the account by running the following command:

```
Set-ADAccountPassword Ty
```

5. When you receive a prompt for the current password, press Enter.
6. When you receive a prompt for the desired password, type **Pa\$\$w0rd**, and then press Enter.
7. When you receive a prompt to repeat the password, type **Pa\$\$w0rd**, and then press Enter.
8. To enable the account, run the following command:

```
Enable-ADAccount Ty
```

9. Test the account by switching to **LON-CL1**, and then sign in as **Ty** with a password of **Pa\$\$w0rd**.

### ► Task 2: Create a new group by using Windows PowerShell

- On **LON-DC1**, in the **Administrator: Windows PowerShell** window, run the following command:

```
New-ADGroup LondonBranchUsers -Path "ou=London,dc=adatum,dc=com" -GroupScope Global -GroupCategory Security
```

**► Task 3: Add a member to the group by using Windows PowerShell**

1. In the **Administrator: Windows PowerShell** window, run the following command:

```
Add-ADGroupMember LondonBranchUsers -Members Ty
```

2. Confirm that the user is in the group by running the following command:

```
Get-ADGroupMember LondonBranchUsers
```

**► Task 4: Modify the .csv file**

1. On the taskbar, click the **File Explorer** icon.
2. In File Explorer, expand **Allfiles (E:)**, expand **Labfiles**, and then click **Mod02**.
3. Right-click **LabUsers.ps1**, and then click **Edit**. In **Administrator: Windows PowerShell (ISE)**, read the comments at the top of the script, and then identify the requirements for the header in the comma separated value (.csv) file.
4. In File Explorer, double-click **LabUsers.csv**.
5. In the **How do you want to open this type of file (.csv)?** message, click **Notepad**. Click **OK**.
6. In Notepad, type the following line at the top of the file:

```
FirstName,LastName,Department,DefaultPassword
```

7. Click **File**, and then click **Save**.
8. Close **Notepad**.

**► Task 5: Modify the script**

1. In the **Administrator: Windows PowerShell (ISE)** window, under **Variables**, replace **C:\path\file.csv** with **E:\Labfiles\Mod02\LabUsers.csv**.
2. Again under **Variables**, replace **"ou=orgunit,dc=domain,dc=com"** with **"ou=London,dc=adatum,dc=com"**.
3. Click **File**, and then click **Save**. Scroll down, and then review the contents of the script.
4. Close the **Administrator: Windows PowerShell (ISE)** window.

**► Task 6: Run the script**

1. Switch to the **Administrator: Windows PowerShell** window.
2. At the prompt, type **cd E:\Labfiles\Mod02**, and then press Enter.
3. Type **.\LabUsers.ps1**, and then press Enter.
4. To view the users just created, type the following command, and then press Enter:

```
Get-ADUser -Filter * -SearchBase "ou=London,dc=adatum,dc=com"
```



### ► Task 7: Prepare for the next module

When you are finished with the lab, revert all virtual machines to their initial state:

1. On the host computer, start **Hyper-V Manager**.
2. In the **Virtual Machines** list, right-click **20742A-LON-DC1**, and then click **Revert**.
3. In the **Revert Virtual Machine** dialog box, click **Revert**.
4. Repeat steps 2 and 3 for **20742A-LON-DC2**, **20742A-LON-SVR1**, and **20742A-LON-CL1**.

**Results:** After completing this lab, you will have:

- Created a user account by using Windows PowerShell.
- Created a group by using Windows PowerShell.
- Added a user to a group by using Windows PowerShell.
- Modified the .csv file.
- Modified the script.
- Run the script.

**MCT USE ONLY. STUDENT USE PROHIBITED**

## Module 3: Advanced AD DS infrastructure management

# Lab: Domain and trust management in AD DS

### Exercise 1: Implementing forest trusts

#### ► Task 1: Configure stub zones for DNS name resolution

1. On **LON-DC1**, in **Server Manager**, click the **Tools** menu, and then in the drop-down menu, click **DNS**.
2. In the **DNS tree** pane, expand **LON-DC1**, click and right-click **Forward Lookup Zones**, and then click **New Zone**.
3. In the **New Zone Wizard**, click **Next**.
4. On the **Zone Type** page, click **Stub zone**, and then click **Next**.
5. On the **Active Directory Zone Replication Scope** page, click **To all DNS servers running on domain controllers in this forest: adatum.com**, and then click **Next**.
6. In the **Zone name:** text box, type **treymresearch.net**, and then click **Next**.
7. On the **Master DNS Servers** page, click **<Click here to add an IP Address or DNS Name>**, type **172.16.10.10**, click the free space, and then click **Next**.
8. On the **Completing the New Zone Wizard** page, click **Next**, and then click **Finish**.
9. Expand **Forward Lookup Zones**, click and right-click the new stub zone **treymresearch.net**, and then click **Transfer from Master**.
10. Right-click **treymresearch.net**, and then click **Refresh**.
11. Confirm that the **treymresearch.net** stub zone contains records and then close **DNS Manager**.
12. Switch to **TREY-DC1**.
13. In **Server Manager**, click the **Tools** menu, and in the drop-down menu, click **DNS**.
14. In the tree pane, expand **TREY-DC1**, click and right-click **Forward Lookup Zones**, and then click **New Zone**.
15. In the **New Zone Wizard**, click **Next**.
16. On the **Zone Type** page, click **Stub zone**, and then click **Next**.
17. On the **Active Directory Zone Replication Scope** page, click **To all DNS servers running on domain controllers in this forest: Treymresearch.net**, and then click **Next**.
18. In the **Zone name** text box, type **adatum.com**, and then click **Next**.
19. On the **Master DNS Servers** page, click **<Click here to add an IP Address or DNS Name>**, type **172.16.0.10**, click the free space, and then click **Next**.
20. On the **Completing the New Zone Wizard** page, click **Next**, and then click **Finish**.
21. Expand **Forward Lookup Zones**, click and right-click the new stub zone **adatum.com**, and then click **Transfer from Master**.

22. Right-click **adatum.com**, and then click **Refresh**.
23. Confirm that the **adatum.com** stub zone contains records.
24. Close **DNS Manager**.

► **Task 2: Configure a forest trust with selective authentication**

1. On **LON-DC1**, on the **Tools** menu, click **Active Directory Domain and Trusts**.
2. In the **Active Directory Domains and Trusts** management console, right-click **Adatum.com**, and then click **Properties**.
3. In the **Adatum.com Properties** dialog box, click the **Trusts** tab, and then click **New Trust**.
4. On the **New Trust Wizard** page, click **Next**.
5. On the **Trust Name** page, in the **Name** text box, type **treyresearch.net**, and then click **Next**.
6. On the **Trust Type** page, click **Forest trust**, and then click **Next**.
7. On the **Direction of Trust** page, click **One-way: outgoing**, and then click **Next**.
8. On the **Sides of Trust** page, click **Both this domain and the specified domain**, and then click **Next**.
9. On the **User Name and Password** page, type **Administrator** as the user name and **Pa\$\$w0rd** as the password in the appropriate boxes, and then click **Next**.
10. On the **Outgoing Trust Authentication Level-Local Forest** page, click **Selective authentication**, and then click **Next**.
11. On the **Trust Selections Complete** page, click **Next**.
12. On the **Trust Creation Complete** page, click **Next**.
13. On the **Confirm Outgoing Trust** page, click **Next**.
14. On the **Completing the New Trust Wizard** page, click **Finish**.
15. In the **Adatum.com Properties** dialog box, click the **Trusts** tab.
16. On the **Trusts** tab, under **Domains trusted by this domain (outgoing trusts)**, click **treyresearch.net**, and then click **Properties**.
17. In the **treyresearch.net Properties** dialog box, click **Validate**.
18. Review the message that displays: **The trust has been validated. It is in place and active**.
19. Click **OK**, and then at the prompt, click **No**.
20. Click **OK** in the **TreyResearch.net Properties** dialog box and then click **OK** in the **Adatum.com Properties** dialog box.
21. Close **Active Directory Domain and Trusts**.

► **Task 3: Configure a server for selective authentication**

1. On **LON-DC1**, in the **Server Manager**, on the **Tools** menu, click **Active Directory Users and Computers**.
2. In the **Active Directory Users and Computers** console, on the **View** menu, click **Advanced Features**.
3. Expand **Adatum.com**, and then click **Computers**.
4. Right-click **LON-SVR2**, and then click **Properties**.
5. In the **LON-SVR2 Properties** dialog box, click the **Security** tab, and then click **Add**.

6. On the **Select Users, Computers, Service Accounts, or Groups** page, click **Locations**.
7. Click **treyresearch.net**, and then click **OK**.
8. In the **Enter the object name to select (examples:)** text box, type **IT**, and then click **Check Names**. When prompted for credentials, type **treyresearch\administrator** with the password as **Pa\$\$w0rd**, and then click **OK**.
9. On the **Select Users, Computers, Service Accounts, or Groups** page, click **OK**.
10. In the **LON-SVR2 Properties** window, ensure that **IT (TreyResearch\IT)** is highlighted, select the **Allow** check box that is in line with **Allowed to authenticate**, and then click **OK**.
11. Switch to **LON-SVR2**.
12. On the taskbar, click the **File Explorer** icon.
13. In the **File Explorer** window, click **Local Disk (C)**.
14. Right-click in the details pane, click **New**, and then click **Folder**.
15. In the **Name** text box, type **IT-Data**, and then press Enter.
16. Right-click **IT-Data**, point to **Share with**, and then click **Specific People**.
17. In the **File Sharing** dialog box, type **TreyResearch\IT**, and then click **Add**.
18. Click **Read**, which is under **Permission Level** of **IT**, and then click **Read/Write**. Click **Share**, and then click **Done**.
19. On **TREY-DC1**, in the **Server Manager**, on the **Tools** menu, click **Active Directory Users and Computers**.
20. In the **Active Directory Users and Computers** console, expand **TreyResearch.net**, and then click **Users**.
21. Double-click the **Domain Admins** group. On the **Members** tab, click **Add**, type **Alice**, and then click **OK** twice.
22. Sign out of **TREY-DC1**.
23. Sign in to **TREY-DC1** as **TreyResearch\Alice** with the password as **Pa\$\$w0rd**.
24. Click **Start**, and then click **Search**.
25. In the **Search** text box, type **\\LON-SVR2\IT-Data**, and then press Enter. The folder opens.

**Results:** After completing this exercise, you should have implemented forest trusts.

## Exercise 2: Implementing child domains in AD DS

### ► Task 1: Install a domain controller in a child domain

1. On **TOR-DC1**, click **Start**, and then click **Server Manager**. In the **Server Manager**, click **Manage**, and in the drop-down list box, click **Add Roles and Features**.
2. On the **Before you begin** page, click **Next**.
3. On the **Select installation type** page, confirm that **Role-based or feature-based installation** option is selected, and then click **Next**.

4. On the **Select destination server** page, ensure that the **Select a server from the server pool** option is selected and that **TOR-DC1.adatum.com** is highlighted, and then click **Next**.
5. On the **Select server roles** page, click **Active Directory Domain Services**.
6. On the **Add features that are required for Active Directory Domain Services?** page, click **Add Features**.
7. On the **Select server roles** page, click **Next**.
8. On the **Select features** page, click **Next**.
9. On the **Active Directory Domain Services** page, click **Next**.
10. On the **Confirm installation selections** page, click **Install**. This may take a few minutes to complete.
11. When the Active Directory Domain Services (AD DS) binaries have installed, click the blue **Promote this server to a domain controller** link.
12. In the **Deployment Configuration** window, click **Add a new domain to an existing forest**.
13. Verify that **Select domain type** is set to **Child Domain** and that **Parent domain name** is set to **Adatum.com**. In the **New domain name** text box, type **na**.
14. Confirm that **Supply the credentials to perform this operation** is set to **ADATUM\Administrator (Current user)**, and then click **Next**.



**Note:** If the credentials are not set to **Adatum\Administrator**, use the **Change** button to enter the credentials **Adatum\Administrator** and the password as **Pa\$\$w0rd**.

15. In the **Domain Controller Options** window, ensure that **Domain functional level** is set to **Windows Server Technical Preview**.
16. Ensure that both the **Domain Name system (DNS) server** and **Global Catalog (GC)** check boxes are selected.
17. Confirm that **Site name:** is set to **Default-First-Site-Name**.
18. Under **Type the Directory Services Restore Mode (DSRM) password**, type **Pa\$\$w0rd** in both text boxes, and then click **Next**.
19. On the **DNS Options** page, click **Next**.
20. On the **Additional Options** page, click **Next**.
21. On the **Paths** page, click **Next**.
22. On the **Review Options** page, click **Next**.
23. On the **Prerequisites Check** page, confirm that there are no issues, and then click **Install**.




**Note:** If you receive the following warning that prevents weaker cryptography algorithms when establishing security channel sessions", you may safely ignore it: "Windows Server 2016 Technical Preview 5 domain controllers have a default for the security setting named "Allow cryptography algorithms compatible with Windows NT 4.0."

After the configuration completes, the server restarts automatically.

► **Task 2: Verify the default trust configuration**

1. Sign in to **TOR-DC1** as **NA\Administrator** with the password as **Pa\$\$w0rd**.
2. Click **Start**, and then click **Server Manager**. In Server Manager, click **Local Server**.
3. Verify that **Windows Firewall** shows **Domain: Off**. If it does not, perform the following steps:
  - a. Click the underlined blue text next to **Windows Firewall**. In the **Windows Firewall** window, click **Turn Windows Firewall on or off**.
  - b. Under each section, select **Turn off Windows Firewall (not recommended)**, and then click **OK**. Ignore any warning prompts that appear regarding the Windows Firewall.
  - c. In **Server Manager**, click the **Refresh "Local Server"** icon, indicated by double arrows.
  - d. After the refresh completes, verify that **Windows Firewall** shows **Public: Off**.
4. In **Server Manager**, on the **Tools** menu, click **Active Directory Domains and Trusts**.
5. In the **Active Directory Domains and Trusts** console, expand **Adatum.com**, right-click **na.adatum.com**, and then click **Properties**.
6. In the **na.adatum.com Properties** dialog box, click the **Trusts** tab, and in the **Domain trusted by this domain (outgoing trusts)** box, click **Adatum.com**, and then click **Properties**,
7. In the **Adatum.com Properties** dialog box, click **Validate**, and then click **Yes, validate the incoming trust**.
8. In the **User name** text box, type **administrator**, and in the **Password** text box, type **Pa\$\$w0rd**, and then click **OK**.
9. When the message "The trust has been validated. It is in place and active" appears, click **OK**.

 **Note:** If you receive a message that the trust cannot be validated or that the secure channel verification has failed, ensure that you have completed step 3 and then wait for at least 10 to 15 minutes before trying again.

10. Click **OK** twice to close the **Adatum.com Properties** dialog box.

**Results:** After completing this exercise, you should have implemented child domains in AD DS.

► **Task: Prepare for the next module**

When you finish the lab, revert the virtual machines to their initial state. To do this, complete the following steps:

1. On the host computer, start **Hyper-V Manager**.
2. In the **Virtual Machines** list, right-click **20742A-LON-DC1**, and then click **Revert**.
3. In the **Revert Virtual Machine** dialog box, click **Revert**.
4. Repeat steps 2 and 3 for **20742A-LON-DC2**, **20742A-TOR-DC1**, **20742A-TREY-DC1**, and **20742A-LON-SVR2**.

**MCT USE ONLY. STUDENT USE PROHIBITED**



## Module 4: Implementing and administering AD DS sites and replication

# Lab: Implementing AD DS sites and replication

### Exercise 1: Modifying the default site

#### ► Task 1: Install the Toronto domain controller

1. On **TOR-DC1**, click **Start**, and then click **Server Manager**.
2. In **Server Manager**, click **Manage**, and then from the drop-down list, click **Add Roles and Features**.
3. On the **Before you begin** page, click **Next**.
4. On the **Select installation type** page, confirm that **Role-based or feature-based installation** is selected, and then click **Next**.
5. On the **Select destination server** page, ensure that **Select a server from the server pool** is selected and that **TOR-DC1.adatum.com** is highlighted, and then click **Next**.
6. On the **Select server roles** page, select the **Active Directory Domain Services** check box.
7. On the **Add features that are required for Active Directory Domain Services?** page, click **Add Features**, and then click **Next**.
8. On the **Select features** page, click **Next**.
9. On the **Active Directory Domain Services** page, click **Next**.
10. On the **Confirm installation selections** page, click **Install**.



**Note:** This might take a few minutes to complete.

11. When the Active Directory Domain Services (AD DS) binaries have installed, do not click **Close**, but click the blue **Promote this server to a domain controller** link.
12. In the **Deployment Configuration** window, click **Add a domain controller to an existing domain**, and then click **Next**.
13. In the **Domain Controller Options** window, ensure that both the **Domain Name system (DNS) server** and **Global Catalog (GC)** check boxes are selected.
14. Confirm that **Site name:** is set to **Default-First-Site-Name**, and then under **Type the Directory Services Restore Mode (DSRM) password**, type **Pa\$\$w0rd** in both the **Password** and **Confirm password** boxes. Click **Next**.
15. On the **DNS Options** page, click **Next**.
16. In the **Additional Options** page, click **Next**.
17. In the **Paths** window, click **Next**.
18. In the **Review Options** window, click **Next**.
19. In the **Prerequisites Check** window, click **Install**. The server will restart automatically.
20. After **TOR-DC1** restarts, sign in as **Adatum\Administrator** with the password **Pa\$\$w0rd**.

**► Task 2: Rename the default site**

1. If necessary, on **LON-DC1**, open the **Server Manager** console.
2. In **Server Manager**, click **Tools**, and then click **Active Directory Sites and Services**.
3. In **Active Directory Sites and Services**, in the navigation pane, expand **Sites**.
4. Right-click **Default-First-Site-Name**, and then click **Rename**.
5. Type **LondonHQ**, and then press Enter.
6. Expand **LondonHQ**, expand the **Servers** folder, and then verify that both **LON-DC1** and **TOR-DC1** belong to the **LondonHQ** site.

**► Task 3: Configure IP subnets that are associated with the default site**

1. If necessary, on **LON-DC1**, open the **Server Manager** console, and then open **Active Directory Site and Services**.
2. In the **Active Directory Sites and Services** console, in the navigation pane, expand **Sites**, and then click the **Subnets** folder.
3. Right-click **Subnets**, and then click **New Subnet**.
4. In the **New Object – Subnet** dialog box, under **Prefix**, type **172.16.0.0/24**.
5. Under **Select a site object for this prefix**, click **LondonHQ**, and then click **OK**.

**Results:** After completing this exercise, you should have successfully reconfigured the default site and assigned IP address subnets to the site.

## Exercise 2: Creating additional sites and subnets

**► Task 1: Create the AD DS sites for Toronto**

1. If necessary, on **LON-DC1**, open the **Server Manager** console, click **Tools**, and then click **Active Directory Sites and Services**.
2. In the **Active Directory Sites and Services** console, in the navigation pane, right-click **Sites**, and then click **New Site**.
3. In the **New Object – Site** dialog box, in the **Name** text box, type **Toronto**.
4. Under **Select a site link object for this site**, select **DEFAULTIPSITELINK**, and then click **OK**.
5. In the **Active Directory Domain Services** dialog box, click **OK**. The Toronto site displays in the navigation pane.
6. In the **Active Directory Sites and Services** console, in the navigation pane, right-click **Sites**, and then click **New Site**.
7. In the **New Object – Site** dialog box, in the **Name** text box, type **TestSite**.
8. Under **Select a site link object for this site**, select **DEFAULTIPSITELINK**, and then click **OK**. The test site displays in the navigation pane.

► **Task 2: Create IP subnets that are associated with the Toronto sites**

1. If necessary, on **LON-DC1**, open the **Server Manager** console, click **Tools**, and then click **Active Directory Sites and Services**.
2. In the **Active Directory Sites and Services** console, in the navigation pane, expand **Sites**, and then click the **Subnets** folder.
3. Right-click **Subnets**, and then click **New Subnet**.
4. In the **New Object – Subnet** dialog box, under **Prefix**, type **172.16.1.0/24**.
5. Under **Select a site object for this prefix**, click **Toronto**, and then click **OK**.
6. Right-click **Subnets**, and then click **New Subnet**.
7. In the **New Object – Subnet** dialog box, under **Prefix**, type **172.16.100.0/24**.
8. Under **Select a site object for this prefix**, click **TestSite**, and then click **OK**.
9. In the navigation pane, click the **Subnets** folder. Verify in the details pane that the two subnets are created and associated with their appropriate site.



**Note:** There are three subnets in total (**172.16.0.0** was created in Exercise 1, Task 3, "Configure IP subnets that are associated with the default site").

**Results:** After completing this exercise, you should have successfully created two additional sites representing the IP subnet addresses in Toronto.

### Exercise 3: Configuring AD DS replication

► **Task 1: Configure site links between AD DS sites**

1. If necessary, on **LON-DC1**, open the **Server Manager** console, click **Tools**, and then click **Active Directory Sites and Services**.
2. In the **Active Directory Sites and Services** console, in the navigation pane, expand **Sites**, expand **Inter-Site Transports**, and then click the **IP** folder.
3. Right-click **IP**, and then click **New Site Link**.
4. In the **New Object – Site Link** dialog box, in the **Name** text box, type **TOR-TEST**.
5. Under **Sites not in this site link**, press Ctrl on the keyboard, click **Toronto**, click **TestSite**, click **Add**, and then click **OK**.
6. Right-click **TOR-TEST**, and then click **Properties**.
7. In the **TOR-TEST Properties** dialog box, click **Change Schedule**.
8. In the **Schedule for TOR-TEST** dialog box, highlight the range from **Monday 9 AM** to **Friday 3 PM**, as follows:
  - Click the **Monday at 9:00AM** tile, press and hold the mouse button, and then drag the cursor to the **Friday at 3:00 PM** tile.
9. Click **Replication Not Available**, and then click **OK**.
10. Click **OK** to close **TOR-TEST Properties**.
11. Right-click **DEFAULTIPSITELINK**, and then click **Rename**.

12. Type **LON-TOR**, and then press Enter.
13. Right-click **LON-TOR**, and then click **Properties**.
14. Under **Sites in this site link**, click **TestSite**, and then click **Remove**.
15. In the **Replicate Every** spin box, change the value to **60** minutes, and then click **OK**.

► **Task 2: Move TOR-DC1 to the Toronto site**

1. If necessary, on **LON-DC1**, click **Tools**, and then click **Active Directory Sites and Services**.
2. In the **Active Directory Sites and Services** console, in the navigation pane, expand **Sites**, expand **LondonHQ**, and then expand the **Servers** folder.
3. Right-click **TOR-DC1**, and then click **Move**.
4. In the **Move Server** dialog box, click **Toronto**, and then click **OK**.
5. In the navigation pane, expand the **Toronto** site, expand **Servers**, and then click **TOR-DC1**.

► **Task 3: Monitor AD DS site replication**

1. On **LON-DC1**, click **Start**, and then click the **Windows PowerShell** icon.
2. At the Windows PowerShell prompt, type the following, and then press Enter:

```
Repadmin /kcc
```

This command recalculates the inbound replication topology for the server.

3. At the Windows PowerShell command prompt, type the following command, and then press Enter:

```
Repadmin /showrep1
```

4. Verify that the last replication with **TOR-DC1** was successful.
5. At the Windows PowerShell command prompt, type the following command, and then press Enter:

```
Repadmin /bridgeheads
```

This command displays the bridgehead servers for the site topology.

6. At the Windows PowerShell command prompt, type the following, and then press Enter:

```
Repadmin /replsummary
```

This command displays a summary of replication tasks. Verify that no errors appear.

7. At the Windows PowerShell command prompt, type the following, and then press Enter:

```
DCDiag /test:replications
```

8. Verify that all connectivity and replication tests pass successfully.
9. Switch to **TOR-DC1**, and then repeat steps 1 through 8 to view information from **TOR-DC1**. For step 4, verify that the last replication with **LON-DC1** was successful.


**Results:** After completing this exercise, you should have successfully configured site links and monitored replication.

## Exercise 4: Monitoring and troubleshooting AD DS replication

### ► Task 1: Produce an error

1. If necessary, on **LON-DC1**, open **Server Manager**.
2. In **Server Manager**, click **Tools**, and then click **Active Directory Sites and Services**.
3. In the **Active Directory Sites and Services** console, in the navigation pane, expand **Sites**, expand **LondonHQ**, expand the **Servers** folder, expand **LON-DC1**, and then select **NTDS Settings**.
4. In the details pane, right-click the **TOR-DC1** connection object, and then click **Replicate Now**.
5. In the **Replicate Now** dialog box, click **OK**.
6. In **Active Directory Sites and Services**, examine all the objects you created earlier, and then on the taskbar, click the **Windows PowerShell** icon.
7. At the Windows PowerShell command prompt, type the following, and then press Enter:

```
Get-ADReplicationUpToDatenessVectorTable -Target "adatum.com"
```

 **Note:** This cmdlet will show you the last several replication events. Make a note of the date and time of the last (top) event.


8. Go to **TOR-DC1**.
9. Click **Start** and then click **Windows PowerShell**.
10. At the Windows PowerShell command prompt, type the following, and then press Enter after each command:

```
CD \Labfiles\Mod04
.\Mod04Ex4.ps1
```

### ► Task 2: Monitor AD DS site replication

1. If necessary, on **TOR-DC1**, open the **Server Manager** console, click **Tools**, and then click **Active Directory Sites and Services**.
2. In the **Active Directory Sites and Services** console, in the navigation pane, expand **Sites**, expand **Toronto**, expand **Servers**, expand **TOR-DC1**, and then select **NTDS Settings**.
3. In the details pane, right click **LON-DC1**, and then select **Replicate Now**.
4. Click **OK** on the **Replicate Now** pop-up.
5. On **TOR-DC1**, on the taskbar, click the **Windows PowerShell** icon.
6. At the Windows PowerShell command prompt, type the following, and then press Enter:

```
Get-ADReplicationUpToDatenessVectorTable -Target "adatum.com"
```

 **Note:** This cmdlet will show you the last several replication events. Note that the last date and time shown (**Replication from LON-DC1**) is not updating. This indicates that one-way replication is not occurring.

- At the Windows PowerShell command prompt, type the following, and then press Enter:

```
Get-AdReplicationSubnet -filter *
```



**Note:** This cmdlet will show detailed information about any subnets assigned to any sites. Note that nothing is returned.

- At the Windows PowerShell command prompt, type the following, and then press Enter:

```
Get-AdReplicationSiteLink -filter *
```



**Note:** This cmdlet will show detailed information about any site links assigned to particular sites. Note that nothing is returned.

### ► Task 3: Troubleshoot AD DS replication

- If necessary, on **TOR-DC1**, open **Windows PowerShell**.
- At the Windows PowerShell command prompt, type the following, and then press Enter:

```
Ipconfig /all
```

- Examine the results. The DNS server address should be **10.0.0.1**.
- At the Windows PowerShell command prompt, type the following, and then press Enter:

```
Get-DnsClient | Set-DnsClientServerAddress -ServerAddresses  
("172.16.0.10", "172.16.0.25")
```

- Run the **Ipconfig /all** command again. The DNS server addresses should be **172.16.0.10** and **172.16.0.25**.
- If necessary, on **TOR-DC1**, open the **Server Manager** console, click **Tools**, and then click **Active Directory Sites and Services**.
- In the **Active Directory Sites and Services** console, in the navigation pane, expand **Sites**, expand **Toronto**, expand **Servers**, expand **TOR-DC1**, and then select **NTDS Settings**.
- In the details pane, right click **LON-DC1**, and then select **Replicate Now**.
- In **Active Directory Sites and Services**, examine all objects that you created earlier. Are any missing?
- On **TOR-DC1**, open **File Explorer**. Browse to **C:\Labfiles\Mod04**.
- Right-click the **Mod04EX4Fix.ps1** file, and then select **Run with PowerShell**. Type **Y** when prompted about execution policy, and then press Enter.
- In **Active Directory Sites and Services**, examine all the objects that you created earlier. Ensure that the site link has been created in the **Inter-Site Transports** node, and subnets have been created in the **Subnets** node.
- On **LON-DC1** and **TOR-DC1**, close all open windows, and then sign out of both virtual machines.

**Results:** After completing this exercise, you should have successfully diagnosed and resolved replication issues.

► **Task 4: Prepare for the next module**

When you finish the lab, revert the virtual machines to their initial state. To do this, complete the following steps:

1. On the host computer, start **Hyper-V Manager**.
2. On the **Virtual Machines** list, right-click **20742A-LON-DC1**, and then click **Revert**.
3. In the **Revert Virtual Machine** dialog box, click **Revert**.
4. Repeat steps 2 and 3 for **20742A-LON-DC2** and **20742A-TOR-DC1**.

**MCT USE ONLY. STUDENT USE PROHIBITED**



## Module 5: Implementing Group Policy

# Lab A: Implementing a Group Policy infrastructure

### Exercise 1: Creating and configuring GPOs

#### ► Task 1: Create and edit a GPO

1. On **LON-DC1**, from **Server Manager**, click **Tools**, and then click **Group Policy Management**.
2. In the navigation pane, expand **Forest: Adatum.com, Domains**, and **Adatum.com**, and then click the **Group Policy Objects** container.
3. In the navigation pane, right-click the **Group Policy Objects** container, and then click **New**.
4. In the **Name** text box, type **ADATUM Standards**, and then click **OK**.
5. In the details pane, right-click the **ADATUM Standards** Group Policy Object (GPO), and then click **Edit**.
6. In the **Group Policy Management Editor** window, in the navigation pane, expand **User Configuration**, expand **Policies**, expand **Administrative Templates**, and then click **System**.
7. Double-click the **Prevent access to registry editing tools** policy setting.
8. In the **Prevent access to registry editing tools** dialog box, click **Enabled**, and then click **OK**.
9. In the navigation pane, expand **User Configuration**, expand **Policies**, expand **Administrative Templates**, expand **Control Panel**, and then click **Personalization**.
10. In the details pane, double-click the **Screen saver timeout** policy setting.
11. In the **Screen saver timeout** dialog box, click **Enabled**, in the **Seconds** text box, type **600**, and then click **OK**.
12. Double-click the **Password protect the screen saver** policy setting.
13. In the **Password protect the screen saver** dialog box, click **Enabled**, and then click **OK**.
14. Close the **Group Policy Management Editor** window.

#### ► Task 2: Link the GPO

1. In the **Group Policy Management** window, in the navigation pane, right-click the **Adatum.com** domain, and then click **Link an Existing GPO**.
2. In the **Select GPO** dialog box, click **ADATUM Standards**, and then click **OK**.

#### ► Task 3: View the effects of the GPO's settings

1. Switch to **LON-CL1**, and then sign in as **Adatum\Administrator** with the password **Pa\$\$w0rd**.
2. Right-click **Start**, and then click **Control Panel**.
3. Click **System and Security**, and then click **Allow an app through Windows Firewall**.
4. In the **Allowed apps and features** list, select the following check boxes, and then click **OK**:
  - **Remote Event Log Management**
  - **Windows Management Instrumentation (WMI)**
5. Sign out, and then sign in as **Adatum\Connie** with the password **Pa\$\$w0rd**.

6. Click **Start**, type **screen saver**, and then click **Change screen saver**. (It may take a few minutes for the option to appear).
7. In the **Screen Saver Settings** dialog box, notice that the **Wait** option is dimmed—you cannot change the time-out. Notice that the **On resume, display logon screen** option is selected and dimmed and that you cannot change the settings. If the **On resume, display logon screen** option is not selected and dimmed, then perform the following steps:
  - a. Right-click **Start** and then click **Run**.
  - b. In the **Run** dialog box, in the **Open** text box, type **gpupdate /force**, and then click **OK**.
  - c. Click **Start**, type **screen saver**, and then click **Change screen saver**.
8. Click **OK**.
9. Right-click **Start**, and then click **Run**.
10. In the **Run** dialog box, in the **Open** text box, type **regedit**, and then click **OK**.
11. In the **Registry Editor** dialog box, click **OK**.

**Results:** After completing this exercise, you should have created, edited, and linked the required GPO successfully.

## Exercise 2: Managing GPO scope

### ► Task 1: Create and link the required GPOs

1. On **LON-DC1**, in **Group Policy Management Console**, in the navigation pane, if necessary, expand **Forest: Adatum.com**, expand **Domains**, expand **Adatum.com**, and then click **Research**.
2. Right-click the **Research** organizational unit (OU), and then click **Create a GPO in this domain, and Link it here**.
3. In the **New GPO** dialog box, in the **Name** text box, type **Research Application Override**, and then click **OK**.
4. In the details pane, right-click the **Research Application Override** GPO, and then click **Edit**.
5. In the console tree, expand **User Configuration**, expand **Policies**, expand **Administrative Templates**, expand **Control Panel**, and then click **Personalization**.
6. Double-click the **Screen saver timeout** policy setting.
7. Click **Disabled**, and then click **OK**.
8. Close the **Group Policy Management Editor** window.

### ► Task 2: Verify the order of precedence

- In the **Group Policy Management Console** tree, click the **Research** OU, and then click the **Group Policy Inheritance** tab. Notice that the **Research Application Override** GPO has higher precedence than the **ADATUM Standards** GPO. The screen saver time-out policy setting that you just configured in the **Research Application Override** GPO is applied after the setting in the **ADATUM Standards** GPO. Therefore, the new setting will overwrite the standards setting and will prevail. Screen saver time-out will be unavailable for users within the scope of the **Research Application Override** GPO.

► **Task 3: Configure the scope of a GPO with security filtering**

1. On **LON-DC1**, in **Group Policy Management Console**, in the navigation pane, if necessary, expand the **Research OU**, and then click the **Research Application Override** GPO under the **Research OU**.
2. In the **Group Policy Management Console** dialog box, read the message, select the **Do not show this message again** check box, and then click **OK**.
3. In the **Security Filtering** section, you will see that the GPO applies by default to all authenticated users.
4. In the **Security Filtering** section, click **Authenticated Users**, and then click **Remove**.
5. In the **Group Policy Management** dialog box, click **OK**.
6. In the details pane, click **Add**.
7. In the **Select User, Computer, or Group** dialog box, in the **Enter the object name to select (examples):** text box, type **Research**, and then click **OK**.

► **Task 4: Configure loopback processing**

1. On **LON-DC1**, in **Group Policy Management Console**, in the navigation pane, click **Adatum.com**, right-click **Adatum.com**, and then click **New Organizational Unit**.
2. In the **New Organizational Unit** dialog box, in the **Name** text box, type **Kiosks**, and then click **OK**.
3. Right-click **Kiosks**, and then click **New Organizational Unit**.
4. In the **New Organizational Unit** dialog box, in the **Name** text box, type **Conference Rooms**, and then click **OK**.
5. In the navigation pane, expand the **Kiosks OU**, and then click the **Conference Rooms OU**.
6. Right-click the **Conference Rooms OU**, and then click **Create a GPO in this domain, and Link it here**.
7. In the **New GPO** dialog box, in the **Name** text box, type **Conference Room Settings**, and then click **OK**.
8. In the navigation pane, expand **Conference Rooms**, and then click the **Conference Room Settings** GPO.
9. In the navigation pane, right-click the **Conference Room Settings** GPO, and then click **Edit**.
10. In the **Group Policy Management Editor** window, in the navigation pane, expand **User Configuration**, expand **Policies**, expand **Administrative Templates**, expand **Control Panel**, and then click **Personalization**.
11. In the details pane, double-click the **Screen saver timeout** policy setting, and then click **Enabled**.
12. In the **Seconds** text box, type **7200**, and then click **OK**.
13. In the navigation pane, expand **Computer Configuration**, expand **Policies**, expand **Administrative Templates**, expand **System**, and then click **Group Policy**.
14. In the details pane, double-click the **Configure user Group Policy loopback processing mode** policy setting, and then click **Enabled**.

15. In the **Mode** drop-down list, select **Merge**, and then click **OK**.
16. Close the **Group Policy Management Editor** window.

**Results:** After completing this exercise, you should have configured the required scope of the GPOs successfully.

► **Task 5: Prepare for the next lab**

- After you finish this lab, leave the virtual machines running for the next lab.

# Lab B: Troubleshooting Group Policy infrastructure

## Exercise 1: Verify GPO application

### ► Task 1: Perform RSoP analysis

1. Switch to **LON-CL1**, and then verify that you are signed in as **Adatum\Connie**. If necessary, use the password **Pa\$\$w0rd**.
2. Click **Start**, type **cmd**, and then press Enter.
3. At the command prompt, type the following command, and then press Enter:

```
gpupdate /force
```

4. Wait for the command to complete. Make a note of the current system time, which you will need to know for a task later in this lab. To record the system time, type the following command, and then press Enter twice:

```
Time
```

5. Restart **LON-CL1**. Wait for **LON-CL1** to restart before proceeding with the next task. Do not sign in to **LON-CL1**.
6. Switch to **LON-DC1**.
7. Switch to **Group Policy Management Console**.
8. In the navigation pane, if necessary, expand **Forest: Adatum.com**, and then click **Group Policy Results**.
9. Right-click **Group Policy Results**, and then click **Group Policy Results Wizard**.
10. On the **Welcome to the Group Policy Results Wizard** page, click **Next**.
11. On the **Computer Selection** page, select the **Another computer** option, type **LON-CL1**, and then click **Next**.
12. On the **User Selection** page, click **ADATUM\Connie**, and then click **Next**.
13. On the **Summary of Selections** page, review your settings, and then click **Next**.
14. Click **Finish**. The RSoP report appears in the details pane of **Group Policy Management Console**.
15. Review the summary results. For both the user and the 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.
16. Click the **Details** tab. Review the settings that were applied during user and computer policy application, and then identify the GPO from which the settings were obtained.
17. Click the **Policy Events** tab, and then locate the event that logs the policy refresh that you triggered with the **gpupdate** command.
18. Click the **Summary** tab, right-click an empty space on the page, and then click **Save Report**.

19. In the navigation pane, click **Desktop**, and then click **Save**.
20. On the desktop, right-click **Connie on LON-CL1.htm**, point to **Open with**, and then click **Internet Explorer**.
21. When you have examined the report, close Microsoft Internet Explorer.

► **Task 2: Analyze RSoP with GPRResult**

1. Sign in to **LON-CL1** as **Adatum\Connie** with the password **Pa\$\$w0rd**.
2. Right-click **Start**, and then click **Command Prompt**.
3. At the command prompt, type the following command, and then press Enter:

```
gprresult /r
```

4. RSoP summary results are displayed. Notice that the information is very similar to the **Summary** tab of the RSoP report that was produced by **Group Policy Results Wizard**.
5. At the command prompt, type the following command, and then press Enter:

```
gprresult /v | more
```

6. Press the spacebar to proceed through the report. Notice that many of the Group Policy settings that were applied by the client are listed in this report.
7. At the command prompt, type the following command, and then press Enter:

```
gprresult /z | more
```

8. Press the spacebar to proceed through the report. This is the most detailed RSoP report.
9. At the command prompt, type the following command, and then press Enter:

```
gprresult /h:"%userprofile%\Desktop\RSOP.html"
```

An RSoP report is saved as an HTML file to your desktop.

10. Open the saved RSoP report from your desktop. Compare the report, its information, and its formatting with the RSoP report that you saved in the previous task.
11. Sign out of **LON-CL1**.

► **Task 3: Evaluate GPO results by using Group Policy Modeling Wizard**

1. On **LON-DC1**, in **Group Policy Management Console**, in the navigation pane, click **Group Policy Modeling**.
2. Right-click **Group Policy Modeling**, and then click **Group Policy Modeling Wizard**.
3. In the **Group Policy Modeling Wizard**, click **Next**.
4. On the **Domain Controller Selection** page, click **Next**.
5. On the **User and Computer Selection** page, in the **User information** section, select the **User** option, and then click **Browse**. In the **Select User** dialog box type **Connie**, and then press Enter.
6. In the **Computer information** section, select the **Computer** option, and then click **Browse**. In the **Select Computer** dialog box, type **LON-CL1**, and then press Enter.
7. In the **Group Policy Modeling Wizard**, click **Next**.

8. On the **Advanced Simulation Options** page, select the **Loopback Processing** check box, and then select the **Merge** option. Even though the **Conference Room Settings** GPO specifies loopback processing, you must instruct **Group Policy Modeling Wizard** to consider loopback processing in its simulation. Click **Next**.
  9. On the **Alternate Active Directory Paths** page, next to **Computer location**, click **Browse**.
  10. In the **Choose Computer Container** dialog box, expand **Adatum**, expand **Kiosks**, and then click **Conference Rooms**. You are simulating the effect of **LON-CL1** as a conference room computer. Click **OK**, and then click **Next**.
  11. On the **User Security Groups** page, click **Next**.
  12. On the **Computer Security Groups** page, click **Next**.
  13. On the **WMI Filters for Users** page, click **Next**.
  14. On the **WMI Filters for Computers** page, click **Next**.
  15. Review your settings on the **Summary of Selections** page, click **Next**, and then click **Finish**.
  16. In the details pane, click the **Details** tab, if necessary expand **User Details**, expand **Group Policy Objects**, and then expand **Applied GPOs**.
  17. Verify if the **Conference Room Settings** GPO applies to Connie as a User policy when she signs in to **LON-CL1**, if **LON-CL1** is in the **Conference Rooms** OU.
  18. Scroll to, and if necessary expand, **User Details**, expand **Settings**, expand **Policies**, expand **Administrative Templates**, and then expand **Control Panel/Personalization**.
  19. Confirm that the screen saver timeout is 7,200 seconds (2 hours)—the setting configured by the **Conference Room Settings** GPO that overrides the 10-minute standard configured by the **ADATUM Standards** GPO.
- **Task 4: Review policy events and determine GPO infrastructure status**
1. Switch to **LON-CL1**. Sign in as **Adatum\Administrator** with the password **Pa\$\$w0rd**.
  2. Right-click **Start**, and then click **Event Viewer**.
  3. In the navigation pane, expand **Windows Logs**, and then click the **System** log.
  4. Click the **Source** column header to sort the **System** log by source.
  5. Locate event **1500**, **1501**, **1502**, or **1503** with **Group Policy** as the source.
  6. Review the information that is associated with Group Policy events.
  7. In the navigation pane, expand **Applications and Services Logs**, expand **Microsoft**, expand **Windows**, expand **Group Policy**, and then click **Operational**.
  8. Locate the first event related to the Group Policy refresh that you initiated in the first exercise with the **gpupdate** command. Review that event and the events that followed it.
  9. Sign out of **LON-CL1**.
  10. Switch to **LON-DC1**.
  11. In the **Group Policy Management** window, in the navigation pane, click the **Adatum.com** domain.
  12. On the **Status** tab, verify that **LON-DC1.Adatum.com** is listed as the baseline domain controller.

13. Click **Detect Now**.
14. Expand the arrow next to the green check mark. Verify that **LON-DC2.Adatum.com** is listed as the domain controller with replication in sync. Some students might see **LON-DC2.Adatum.com** listed as a domain controller with replication in progress. This is due to the lab environment.

**Results:** After completing this exercise, you should have used the RSoP tools successfully to verify the correct application of your GPOs, examined Group Policy events, and verified the health of the Group Policy infrastructure.

## Exercise 2: Troubleshooting GPOs

### ► Task 1: Read the Help desk Incident Record and simulate the problem

1. Read Help desk **Incident Record 604531** in the exercise scenario.
2. On **LON-DC1**, on the taskbar, click **File Explorer**.
3. In File Explorer, in the navigation pane, expand **Allfiles (E:)**, expand **Labfiles**, and then click **Mod05**.
4. In the details pane, right-click **Mod05-1.ps1**, and then click **Run with PowerShell**. Press **Y** and then press Enter when prompted.

### ► Task 2: Update the Plan of Action section of the Incident Record

1. Read the **Additional Information** section of the Incident Record in the exercise scenario in the student manual.
2. Update the **Plan of Action** section of the Incident Record in the student manual with your recommendations:
  - Verify the configuration for **Connie Vaughn**.
  - RSoP from **Group Policy Results Wizard** will afterward provide the configuration information for **Connie Vaughn**.
  - The **Research Application Override** GPO should provide the correct configuration. Investigate the configuration of the GPO.

### ► Task 3: Troubleshoot and resolve the problem

1. On **LON-CL1**, sign in as **Adatum\Connie** with the password **Pa\$\$w0rd**.
2. Right-click **Start**, and then click **Control Panel**.
3. In Control Panel, click **Appearance and Personalization**, and then click **Change Screen Saver**.
4. Verify that **Wait** is dimmed and has a value of **10 minutes**.
5. Sign out of **LON-CL1**.
6. Switch to **LON-DC1**.
7. In the **Group Policy Management** window, in the navigation pane, click **Group Policy Results**.
8. Right-click **Group Policy Results**, and then click **Group Policy Results Wizard**.
9. On the **Welcome to the Group Policy Results Wizard** page, click **Next**.
10. On the **Computer Selection** page, select the **Another computer** option, type **LON-CL1**, and then click **Next**.



11. On the **User Selection** page, click **ADATUM\Connie**, and then click **Next**.
12. On the **Summary of Selections** page, review your settings, and then click **Next**.
13. Click **Finish**.
14. Click the **Details** tab, and then click **Show all**.
15. In the **User Details** section, locate the **Settings** section, and then in **Control Panel/Personalization**, verify that the screen saver timeout is 600 seconds and the winning GPO is **ADATUM Standards**.
16. In the **User Details** section, locate the denied GPOs and verify that the **Research Application Override** GPO is in the list of denied GPOs with a reason of **Empty**. In this case, it appears that Connie Vaugh is no longer a member of the Research group.
17. Switch to the **Server Manager** window.
18. Click **Tools**, and then click **Active Directory Users and Computers**.
19. In the **Active Directory Users and Computers** window, if necessary expand the **Adatum.com** domain, and then click the **Research OU**.
20. In the details pane, double-click the **Research** group.
21. In the **Research Properties** dialog box, click the **Members** tab, and then verify that Connie Vaugh is not listed as a member of the group.
22. Click **Add**. In the **Select Users, Contacts, Computers, Service Accounts, or Groups** dialog box, type **Connie**, and then click **OK**.
23. In the **Research Properties** dialog box, click **OK**.
24. Close the **Active Directory Users and Computers** window.
25. Switch to **LON-CL1**.
26. On **LON-CL1**, sign in as **Adatum\Connie** with the password **Pa\$\$w0rd**.
27. Right-click **Start**, and then click **Control Panel**.
28. In Control Panel, click **Appearance and Personalization**, and then click **Change Screen Saver**.
29. Verify that **Wait** is no longer dimmed and has a value of **1 minutes**.
30. If **Wait** is still dimmed, then perform the following steps:
  - a. Right-click **Start**, hover over **Shut down or sign out** and then click **Restart**.
  - b. Sign in as **Adatum\Connie** with the password **Pa\$\$w0rd**.
  - c. Perform steps 27-29.
31. Sign out of **LON-CL1**.

**Results:** After completing this exercise, you will have resolved the GPO application problem.

► **Task 4: Prepare for the next module**

When you finish the lab, revert the virtual machines to their initial state. To do this, perform the following steps:

1. On the host computer, start **Hyper-V Manager**.
2. In the **Virtual Machines** list, right-click **20742A-LON-DC1**, and then click **Revert**.
3. In the **Revert Virtual Machine** dialog box, click **Revert**.
4. Repeat steps 2 and 3 for **20742A-LON-CL1** and **20742A-LON-DC2**.

## Module 6: Managing user settings with Group Policy

# Lab: Managing user settings with Group Policy

### Exercise 1: Using administrative templates to manage user settings

#### ► Task 1: Import administrative templates for Microsoft Office 2016

1. On **LON-DC1**, on the taskbar, click the **File Explorer** icon.
2. In File Explorer, in the navigation pane, expand **Allfiles (E:)**, expand **Labfiles** and then click **Mod06**.
3. Double-click **admintemplates\_x64\_4390-1000\_en-us.exe**.
4. In **The Microsoft Office 2016 Administrative Templates** dialog box, select the **Click here to accept the Microsoft Software License Terms** check box, and then click **Continue**.
5. In the **Browse for Folder** dialog box, click **Desktop** and then click **OK**.
6. In **The Microsoft Office 2016 Administrative Templates** dialog box, click **OK**.
7. In File Explorer, in the navigation pane, click **Desktop**, and then in the content pane, double-click **adm**.
8. Press Ctrl+A to select all files, right-click, and then click **Copy**.
9. In the navigation pane, expand **Local Disk (C:)**, expand **Windows**, right-click **PolicyDefinitions** and then click **Paste**.
10. Close **File Explorer**.

#### ► Task 2: Configure Office 2016 settings

1. On **LON-DC1**, in **Server Manager**, click **Tools** and then click **Group Policy Management**.
2. Switch to the **Group Policy Management** window.
3. In the navigation pane, expand **Forest: Adatum.com**, expand **Domains**, expand **Adatum.com**, and then click **Group Policy Objects**.
4. Right-click **Group Policy Objects**, and then click **New**.
5. In the **New GPO** dialog box, type **Office 2016 settings**, and then click **OK**.
6. In the contents pane, right-click **Office 2016 settings**, and then click **Edit**.
7. In the **Group Policy Management Editor**, in the navigation pane, expand **User Configuration**, expand **Policies**, expand **Administrative Templates**, and then click **Microsoft Excel 2016**.
8. Expand **Microsoft Excel 2016**, expand **Excel Options**, click **Customize Ribbon**, and then double-click **Display Developer tab in the Ribbon**.
9. In the **Display Developer tab in the Ribbon** dialog box, click **Enabled**, and then click **OK**.
10. In the **Group Policy Management Editor**, click **Save**, and then double-click **Default file location**.
11. In the **Default file location** dialog box, click **Enabled**, in the **Default file location** text box, type **%userprofile%\Desktop**, and then click **OK**.

12. Close the **Group Policy Management Editor**.
13. In **Group Policy Management**, right-click the **Adatum.com** domain, and then click **Link an Existing GPO**.
14. In the **Select GPO** dialog box, click **Office 2016 settings**, and then click **OK**.

► **Task 3: Apply and verify settings on the client computer**

1. Switch to **LON-CL1**.
2. Right-click **Start**, and then click **Command Prompt**.
3. In the **Command Prompt** window, type the following command, and then press Enter:  

```
Gpupdate /force
```
4. Close the **Command Prompt** window.
5. Click **Start**, click **All apps**, and then click **Excel 2016**.
6. In the **First things first** dialog box, select the **Ask me later** option, and then click **Accept**.
7. Click **Blank workbook**.
8. Verify that the **Developer** tab displays on the ribbon.
9. If the **Developer** tab is not displayed on the ribbon, perform the following steps:
  - a. Right-click **Start**, hover over **Shutdown or Sign out** and then click **Restart**.
  - b. After the computer has restarted sign in as **Adatum\Administrator** with the password **Pa\$\$w0rd**.
  - c. Perform steps 5-8 again.
10. Click **File**, click **Save**, and then click **Browse**.
11. In the **Save as** dialog box, in the address bar, verify that **Desktop** displays, and then click **Cancel**.
12. Close **Excel 2016**.

**Results:** After completing this exercise, you should have successfully extended administrative templates with templates for Office 2016 and configured some Office settings by using Group Policy.

## Exercise 2: Implementing settings by using Group Policy preferences

► **Task 1: Set up the current environment**

1. Switch to **LON-DC1**.
2. On **LON-DC1**, on the taskbar, click the **File Explorer** icon.
3. In the navigation pane, expand **Allfiles (E:)**, expand **Labfiles**, and then click **Mod06**.
4. In the details pane, right-click **Mod06-1.ps1**, and then click **Run with PowerShell**.
5. If prompted, type **Y**, and then press Enter.
6. Right-click **BranchScript.cmd**, and then click **Copy**.
7. Switch to the **Group Policy Management** window.

8. In the navigation pane, right-click **Group Policy Objects**, and then click **Refresh**.
9. Right-click the **Branch1** Group Policy Object (GPO), and then click **Edit**.
10. In the **Group Policy Management Editor** window, under **User Configuration**, expand **Policies**, expand **Windows Settings**, and then click **Scripts (Logon/Logoff)**.
11. In the details pane, double-click **Logon**.
12. In the **Logon Properties** dialog box, click **Show Files**.
13. In the details pane, right-click a blank area, and then click **Paste**.
14. Close the **Logon** window.
15. In the **Logon Properties** dialog box, click **Add**.
16. In the **Add a Script** dialog box, click **Browse**.
17. Click **BranchScript.cmd**, and then click **Open**.
18. Click **OK** twice to close all dialog boxes.
19. Close the **Group Policy Management Editor** window.

► **Task 2: Test mapped drive for Branch Office 1 users**

1. Switch to **LON-CL1**.
2. Right-click **Start**, hover over **Shut down or sign out**, and then click **Restart**.
3. When the computer has restarted, sign in as **Adatum\Abbi** with password **Pa\$\$w0rd**.
4. On the taskbar, click the **File Explorer** icon.
5. In File Explorer, click **This PC**.
6. Verify that in the details pane, in the **Network Locations** section, drive **S** displays.
7. If the S drive is not available, perform these steps:
  - a. Right-click **Start**, and click **Command Prompt**.
  - b. In the **Command Prompt** window, type the following two commands, and press Enter after each command:

```
Gpupdate /force  
Shutdown /r /t 0
```

- a. Perform steps 3-6 again.

► **Task 3: Create a Preferences GPO with the required Group Policy preferences**

1. Switch to **LON-DC1**.
2. On **LON-DC1**, switch to **Server Manager**, click **Tools** and then click **Active Directory Users and Computers**.
3. In the **Active Directory Users and Computers** window, right-click **IT**, hover over **New**, and then click **Group**.
4. In the **New Object – Group** dialog box, in the **Group name** text box, type **Computer Administrators**, and then click **OK**.
5. Switch to the **Group Policy Management Console**, right-click the **Adatum.com** domain, and then click **Refresh**.
6. Expand **Branch Office 1**, right-click the **Branch1** GPO, and then click **Delete**.

7. In the **Group Policy Management** dialog box, click **OK**.
8. Right-click the **Adatum.com** domain, and then click **Create a GPO in this domain, and Link it here**.
9. In the **New GPO** dialog box, in the **Name** text box, type **Preferences**, and then click **OK**.
10. In the navigation pane, right-click **Preferences**, and then click **Edit**.
11. Expand **User Configuration**, expand **Preferences**, expand **Windows Settings**, right-click **Shortcuts**, hover over **New**, and then click **Shortcut**.
12. In the **New Shortcut Properties** dialog box, in the **Action** list, click **Create**.
13. In the **Name** text box, type **Notepad**.
14. In the **Location** box, click the arrow, and then select **All Users Desktop**.
15. In the **Target path** box, type **C:\Windows\System32\Notepad.exe**.
16. On the **Common** tab, clear the **Run in logged-on user's security context (user policy option)** check box.
17. Select the **Item-level targeting** check box, and then click **Targeting**.
18. In the **Targeting Editor** dialog box, click **New Item**, and then click **Security Group**.
19. In the lower part of the dialog box, click the ellipsis button (...).
20. In the **Select Group** dialog box, in the **Enter the object name to select (examples)** box, type **IT**, and then click **OK**.
21. Click **OK** two more times.
22. Right-click **Drive Maps**, hover over **New**, and then click **Mapped Drive**.
23. In the **New Drive Properties** dialog box, in the **Location** text box, type **\\LON-DC1\Branch1**, and then select the **Reconnect** check box. In the **Label as** text box, type **Drive for Branch Office 1**, in the **Use** drop-down list box, select **S**.
24. On the **Common** tab, select the **Run in logged-on user's security context (user policy option)** check box.
25. Select the **Item-level targeting** check box, and then click **Targeting**.
26. In the **Targeting Editor** dialog box, click **New Item**, and then click **Organizational Unit**.
27. In the lower part of the dialog box, click the ellipsis button (...).
28. In the **Find Custom Search** dialog box, in the **Search results** list, select **Branch Office 1**, and then click **OK**.
29. Click **OK** two more times.
30. Expand **Computer Configuration**, expand **Preferences**, and then expand **Control Panel Settings**.
31. Right-click **Local Users and Groups**, hover over **New**, and then click **Local Group**.
32. In the **New Local Group Properties** dialog box, in the **Group name** text box, type **Administrators**, and then click **Add**.
33. In the **Local Group Member** dialog box, click the ellipsis button (...).
34. In the **Select User, Computer or Group** dialog box, in the **Enter the object name to select (examples)** text box, type **Computer Administrators**, and then click **OK** twice.
35. In the **New Local Group Properties** dialog box, click the **Common** tab.
36. On the **Common** tab, select the **Item-level targeting** check box, and then click **Targeting**.

37. In the **Targeting Editor** dialog box, click **New Item**, and then click **Operating System**.
38. In the **Product** drop-down list box, select **Windows Server 2016 Technical Preview 5**, and then click **OK** twice.
39. Close all open windows except **Group Policy Management** and **Server Manager**.

► **Task 4: Test the preferences**

1. Switch to **LON-CL1**.
2. Right-click **Start**, hover over **Shut down or sign out**, and then click **Restart**.
3. When the computer has restarted, sign in as **Adatum\Abbi** with the password **Pa\$\$w0rd**.
4. On the taskbar, click the **File Explorer** icon.
5. In File Explorer, click **This PC**.
6. Verify that in the details pane, in the **Network Locations** section, drive **S** displays.



**Note:** The drive label now is **Drive for Branch Office 1**, which verifies that the drive is mapped through Group Policy preferences.

7. On the desktop, verify that a shortcut exists for **Notepad**.
8. If the shortcut for **Notepad** is not available, perform these steps:
  - a. Right-click **Start**, and click **Command Prompt**.
  - b. In the **Command Prompt** window, type the following two commands, and press Enter after each command:

```
Gpupdate /force
Shutdown /r /t 0
```

- c. Perform step 3 again.
  - d. The shortcut for **Notepad** should now display on the desktop.
9. Right-click **Start**, and then click **Computer Management**.
10. In **Computer Management**, expand **Local Users and Groups**, and then click **Groups**.
11. In the details pane, double-click **Administrators**.
12. Verify that the **Computer Administrators** group is not a member of the **Administrators** group.



**Note:** The **Computer Administrators** group is not a member of the **Administrators** group because the **Preferences** setting only applies to servers.

13. Sign out of **LON-CL1**.

**Results:** After completing this exercise, you should have successfully removed the logon scripts, configured preference settings, and then assigned them by using GPOs.

## Exercise 3: Configuring Folder Redirection

### ► Task 1: Create a shared folder to store the redirected folders

1. On **LON-DC1**, on the taskbar, click the **File Explorer** icon.
2. In the navigation pane, click **This PC**.
3. In the details pane, double-click **Local Disk (C:)**, and then on the **Home** tab, click **New folder**.
4. Name the new folder **Branch1Redirect**.
5. Right-click the **Branch1Redirect** folder, click **Share with**, and then click **Specific people**.
6. In the **File Sharing** dialog box, click the drop-down list box, select **Everyone**, and then click **Add**.
7. For the **Everyone** group, click the **Permission Level** drop-down list box, and then click **Read/Write**.
8. Click **Share**, and then click **Done**.
9. Close **File Explorer**.

### ► Task 2: Create a new GPO and link it to the Branch Office 1 organizational unit (OU)

1. On **LON-DC1**, switch to **Group Policy Management**.
2. In **Group Policy Management**, expand and right-click **Branch Office 1**, and then click **Create a GPO in this domain and Link it here**.
3. In the **New GPO** dialog box, in the **Name** text box, type **Folder Redirection**, and then click **OK**.

### ► Task 3: Edit the Folder Redirection settings in the policy

1. Expand **Branch Office 1**, right-click **Folder Redirection**, and then click **Edit**.
2. In the **Group Policy Management Editor** window, under **User Configuration**, expand **Policies**, expand **Windows Settings**, and then expand **Folder Redirection**.
3. Right-click **Documents**, and then click **Properties**.
4. In the **Document Properties** dialog box, on the **Target** tab, in the **Setting** drop-down list box, select **Basic – Redirect everyone's folder to the same location**.
5. Ensure that the **Target folder location** box is set to **Create a folder for each user under the root path**.
6. In the **Root Path** text box, type **\\LON-DC1\Branch1Redirect**, and then click **OK**.
7. In the **Warning** dialog box, click **Yes**.
8. Right-click **Pictures**, and then click **Properties**.
9. In the **Pictures Properties** dialog box, on the **Target** tab, in the **Setting** drop-down list box, select **Follow the Documents folder**, and then click **OK**.
10. In the **Warning** dialog box, click **Yes**.
11. Right-click **Music**, and then click **Properties**.
12. In the **Music Properties** dialog box, on the **Target** tab, in the **Setting** drop-down list box, select **Follow the Documents folder**, and then click **OK**.
13. In the **Warning** dialog box, click **Yes**.
14. Close all open windows on **LON-DC1**.



► **Task 4: Test the Folder Redirection settings**

1. Switch to **LON-CL1**.
2. Sign in as **Adatum\Abbi** with the password **Pa\$\$w0rd**.
3. Right-click **Start**, and then click **Command Prompt**.
4. In the **Command Prompt** window, type the following command, and then press Enter:

```
gpupdate /force
```

5. When prompted, type the following and then press Enter:

```
Y
```

6. Sign out, and then sign back in to **LON-CL1** as **Adatum\Abbi** with the password **Pa\$\$w0rd**.
7. On the taskbar, click the **File Explorer** icon.
8. In File Explorer, in the navigation pane, right-click **Documents**, and then click **Properties**.
9. In the **Documents** properties dialog box, verify that the location is **\\LON-DC1\Branch1Redirect\Abbi**, and then click **OK**.



**Note:** If the location is **C:\Users\Abbi**, perform steps 3 through 9 again.

10. Click **Documents**, and verify that two subfolders, **Music** and **Pictures** exist.



**Note:** This verifies that **Music** and **Pictures** are redirected as well.

11. Sign out of **LON-CL1**.

**Results:** After completing this exercise, you should have successfully configured Folder Redirection to a shared folder on the **LON-DC1** server.

## Exercise 4: Planning Group Policy (optional)

### ► Task 1: Read the supporting documentation

- Read the documentation provided.

### ► Task 2: Update the proposal document with your planned course of action

- Answer the questions in the **proposals** section of the **A. Datum GPO Strategy Proposal** document.

#### Proposals

- Which of the requirements will necessitate creating one or more GPOs?

The central IT administrators in London must be able to manage all GPOs and settings in the organization. Administrators in each office should be able to manage only GPOs that apply to that office. Although you can complete any of the remaining tasks manually on each computer, using GPOs requires the least effort. You could implement some of the other requirements, such as the security warning or preventing access to registry editing tools, by using local policies only. However, because local policies are hard to manage, GPOs are also beneficial for these settings.

- Can you fulfill any of the requirements without creating GPOs?

You can fulfill all of the requirements without creating GPOs.

- Are there any exceptions to the default GPO application that you must consider?

Yes, there is one exception: security filtering of administrator desktops so that they will not be prevented from accessing registry editing tools.

- List the GPOs that you must create to fulfill the lab scenario's requirements. Provide the following information in the table provided:

- Name of the GPO
- The requirements that the GPO fulfills
- The configuration settings (user policies, computer policies, user preferences, or computer preferences) the GPO will contain
- The container (domain, OU, site) to which the GPO will be linked

Name	Requirements fulfilled	Configuration settings	Applies to
All_Clients	Configures the local admin accounts	Computer Configuration\Policies \Windows Settings \Security Settings \Restricted Groups	OU=Clients
All_Clients	Configures general Windows Update settings	Computer Configuration\Policies \Administrative Templates \Windows Components \Windows Update \Configure Automatic Updates	OU=Clients
All_Users_but_Admins	Prevents editing of the registry	User Configuration\Policies \Administrative Templates\System	DC=adatum

Name	Requirements fulfilled	Configuration settings	Applies to
		\Prevent access to registry editing tools	
London_Clients	Displays a compliance message	Computer Configuration \Windows Settings \Security Settings\Local Policies \Security Options\Interactive Logon: Message text for users attempting to log on  Interactive Logon: Message title for users attempting to log on	OU=London, OU=Clients
Marketing_Share	Users must have a default set of mapped drives	User Configuration\Preferences \Windows Settings\Drive Maps	OU=Marketing

- List other configuration tasks that you must perform within the Group Policy Management Console to fulfill the scenario requirements.

Other configuration tasks include:

- The All\_Users\_but\_Admins policy needs security filtering to deny access. This will apply the policy to the users but not to the administrators group, Group IT.  
You must configure the administration of GPOs as desired.

► **Task 3: Examine the suggested proposals in the Lab Answer Key**

- Compare your proposals with the ones shown previously.

► **Task 4: Discuss your proposed solution with the class, as guided by your instructor**

- Be prepared to discuss your proposals with the class.

**Results:** After completing this exercise, you should have successfully designed a GPO strategy.

► **Prepare for the next module**

When you finish the lab, revert the virtual machines to their initial state. To do this, perform the following steps:

- On the host computer, start **Microsoft Hyper-V Manager**.
- In the **Virtual Machines** list, right-click **20742A-LON-DC1**, and then click **Revert**.
- In the **Revert Virtual Machine** dialog box, click **Revert**.
- Repeat steps two and three for **20742A-LON-DC2** and **20742A-LON-CL1**.

**MCT USE ONLY. STUDENT USE PROHIBITED**

## Module 7: Securing Active Directory Domain Services

### Lab: Securing AD DS

#### Exercise 1: Implementing security policies for accounts, passwords, and administrative groups

##### ► Task 1: Identify the required settings

1. Read the documentation provided.
2. Fill in the table of settings according to the requirements of A. Datum Corporation.

Setting	Configuration for all users	Configuration for IT administrators
Enforce password history	10	10
Maximum password age	60 days	30 days
Minimum password age	1 day	1 day
Minimum password length	8 characters	10 characters
Passwords must meet complexity requirements	True	True
Store password using reversible encryption	False	False
Account lockout duration	1 hour	Administrator must unlock
Account lockout threshold	5	3
Reset account lockout counter after	20 minutes	20 minutes

3. Answer the additional questions from the proposals document.
  - a. How can you configure that IT administrators have different password and account lockout settings than regular users?  
**Answer:** Use the Default Domain Policy, which applies to all users, and create a fine-grained password policy object that applies only to the required administrative groups.
  - b. How can you identify IT administrators in terms of more restricted password and account lockout settings?  
**Answer:** The administrative password and account lockout settings should apply to the IT group and the Domain Admins group.

- c. How can you meet the requirement to limit the membership list for the local Administrators groups on all member servers to only the local Administrator account, the Domain Admins group, and the IT group?

**Answer:** Ensure that you have domain member servers in the same OU hierarchy. Assign a policy to it, and then use the restricted groups feature to restrict the local Administrators group forcefully to contain only administrators, the Domain Admins group, and the IT group.

- d. How can you meet the requirement that the Domain Admins group must include only the Administrator account and that the Enterprise Admins and Schema Admins groups must be empty during normal operations?

**Answer:** You cannot configure groups other than local groups with the restricted groups feature. For Domain Admins, Enterprise Admins, and Schema Admins, you must configure the group membership manually and audit their changes.

- e. How can you meet the requirement that other built-in groups, such as Account Operators and Server Operators, must not contain members?

**Answer:** Use the restricted groups feature.

- f. How can you meet the requirement that you must audit all changes to users or groups in Active Directory Domain Services (AD DS)?

**Answer:** Configure advanced auditing policies to audit directory services changes.

### ► Task 2: Configure password settings for all users

1. On **LON-DC1**, from **Server Manager**, click **Tools**, and then click **Group Policy Management**.
2. In the **Group Policy Management Console**, in the navigation pane, expand **Forest: Adatum.com \Domains\ Adatum.com\Group Policy Objects**, and then select the **Default Domain Policy**.
3. Right-click **Default Domain Policy**, and then click **Edit**.
4. In the **Group Policy Management Editor** window, in the navigation pane, expand **Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies**, and then double-click **Password Policy**.
5. In the details pane, double-click **Enforce password history**.
6. In the **Enforce password history Properties** dialog box, ensure that **Define this policy setting** is selected.
7. Configure **Keep password history for:** to **10 passwords remembered**, click **OK**, and then double-click **Maximum password age**.
8. In the **Maximum password age Properties** dialog box, ensure that **Define this policy setting** is selected.
9. Configure **Password will expire in** to **60 days**, click **OK**, and then double-click **Minimum password age**.
10. In the **Minimum password age Properties** dialog box, ensure that **Define this policy setting** is selected.
11. Configure **Password can be changed after** to **1 days**, click **OK**, and then double-click **Minimum password length**.
12. In the **Minimum password length Properties** dialog box, ensure that **Define this policy setting** is selected.

13. Configure **Password must be at least to 8 characters**, click **OK**, and then double-click **Password must meet complexity requirements**.
14. In the **Password must meet complexity requirements Properties** dialog box, ensure that **Define this policy setting** is selected.
15. Select **Enabled**, click **OK**, and then double-click **Store passwords using reversible encryption**.
16. In the **Store passwords using reversible encryption Properties** dialog box, ensure that **Define this policy setting** is selected.
17. Select **Disabled**, and then click **OK**.
18. In the navigation pane, click to select **Account Lockout Policy**.
19. In the details pane, double-click **Account lockout duration**.
20. In the **Account lockout duration Properties** dialog box, click **Define this policy setting**.
21. Configure **Account is locked out for to 60 minutes**, and then click **OK**.
22. In the **Suggested Value Changes** dialog box, click **OK**, and then double-click **Account lockout threshold**.
23. In the **Account lockout threshold Properties** dialog box, configure **Account will lock out after to 5 invalid logon attempts**, click **OK**, and then double-click **Reset account lockout counter after**.
24. In the **Reset account lockout counter after Properties** dialog box, configure **Reset account lockout counter after to 20 minutes**, and then click **OK**.
25. Close the **Group Policy Management Editor** window and the **Group Policy Management Console**.

► **Task 3: Configure a PSO for IT administrators**

1. On **LON-DC1**, from **Server Manager**, click **Tools**, and then click **Active Directory Administrative Center**.
2. In **Active Directory Administrative Center**, in the navigation pane, click **Adatum (local)**.
3. In the details pane, scroll to and double-click **System**, and then double-click **Password Settings Container**.
4. In the **Tasks** pane, in the **Password Settings Container** section, click **New**, and then click **Password Settings**.
5. In the **Create Password Settings** dialog box, in the **Password Settings** section, in the **Name** field, type **Adatum Administrators Password Settings**.
6. In the **Precedence** field, type **10**, and then ensure that **Enforce minimum password length** is selected.
7. In the **Minimum password length (characters)** text box, type **10**, and then ensure that **Enforce password history** is selected.
8. In the **Number of passwords remembered** text box, type **10**, ensure that **Password must meet complexity requirements** is selected, and then ensure that **Store password using reversible encryption** is not selected.
9. Under **Password age options**, ensure that **Enforce minimum password age** is selected.
10. In the **User cannot change the password within (days)** text box, type **1**, and then ensure that the **Enforce maximum password age** check box is selected.
11. In the **User must change the password after (days)** text box, type **30**, and then select the **Enforce account lockout policy** check box.

12. In the **Number of failed logon attempts allowed** text box, type **3**.
13. In the **Reset failed logon attempts count after (mins)** text box, type **20**, and then select **Account will be locked out, Until an administrator manually unlocks the account**.
14. In the **Directly Applies To** section, click **Add**.
15. In the **Select Users or Groups** dialog box, under **Enter the object names to select**, type **IT**, and then click **Check Names**.
16. The **Name Not Found** dialog box appears because IT is not a global group but a Universal Group. Click **Cancel**.
17. Switch to **Server Manager**, click **Tools**, and then click **Windows PowerShell**.
18. At the Windows PowerShell command prompt, type the following command, and then press Enter:

```
Get-ADGroup IT
```

19. Verify that the IT group has a group scope of **Universal**.
  20. At the command prompt, type the following command, and then press Enter:
- ```
Set-ADGroup IT -GroupScope Global
```
21. Switch back to the **Create Password Settings: Adatum Administrative Password Settings** dialog box.
  22. In the **Select Users or Groups** dialog box, under **Enter the object names to select**, type **IT; Domain Admins**, and then click **Check Names**. The names are both resolved. Click **OK**.
  23. Click **OK** to close the **Create Password Settings: Adatum Administrative Password Settings** dialog box and create the **Password Settings** object (PSO).
  24. In **Active Directory Administrative Center**, in the navigation pane, click **Overview**.
  25. In the details pane, in the **Global Search** box, type **Abbi Skinner**, and then press Enter. The user object of **Abbi Skinner** is found.
  26. In the **Tasks** pane, click **View resultant password settings**. Note that the **Adatum Administrative Password Settings** PSO applies (Abbi is in the IT group), and then click **Cancel**.
  27. In the **Global Search** box, type **Adam Hobbs**, and then press Enter.
  28. In the **Tasks** pane, click **View resultant password settings**. Note that no resultant fine-grained password settings apply (Adam is not in the IT group and the Default Domain Policies settings apply to him), and then click **OK**.
  29. Close **Active Directory Administrative Center** and **Windows PowerShell**.

#### ► Task 4: Implement administrative security policies

1. On **LON-DC1**, from **Server Manager**, click **Tools**, and then click **Active Directory Administrative Center**.
2. In **Active Directory Administrative Center**, in the navigation pane, click **Adatum (local)**.
3. In the **Tasks** pane, in the **Adatum (local)** section, click **New**, and then click **Organizational Unit**.
4. In the **Create Organizational Unit** dialog box, in the **Name** field, type **Adatum Servers**, and then click **OK**.



5. In **Active Directory Administrative Center**, in the details pane, double-click **Computers**, select **LON-SVR1**, and then press and hold the Shift key and click **LON-SVR2**. Both servers now are selected.
6. In the **Tasks** pane, in the **2 items selected** section, click **Move**.
7. In the **Move** dialog box, select **Adatum Servers**, and then click **OK**.
8. Close **Active Directory Administrative Center**.
9. In **Server Manager**, click **Tools**, and then click **Group Policy Management**.
10. In the **Group Policy Management Console**, under **Forests: Adatum.com\Domains\Adatum.com**, locate and click to select **Adatum Servers**. Right-click **Adatum Servers**, and then click **Create a GPO in this domain, and Link it here**.
11. In the **New GPO** dialog box, in the **Name** field, type **Restricted Administrators on Member Servers**, and then click **OK**.
12. In the details pane, right-click the **Restricted Administrators on Member Servers** GPO, and then click **Edit**.
13. In the **Group Policy Management Editor** window, expand **Computer Configuration\Policies\Windows Settings\Security Settings**, click to select **Restricted Groups**, right-click **Restricted Groups**, and then click **Add Group**.
14. In the **Add Group** dialog box, in the **Group** field, type **Administrators**, and then click **OK**.
15. In the **Administrators Properties** dialog box, under **Members of this group**, click **Add**.
16. In the **Add Member** dialog box, click **Browse**.
17. In the **Select Users, Service Accounts or Groups** dialog box, in the **Enter the object names to select** text box, type **Domain Admins; IT**, click **Check Names**, and then click **OK**.
18. In the **Add Member** dialog box, in the **Members of this group** section, add **;Administrator** to the string, and then click **OK**.
19. Verify that the **Administrator Properties** dialog box now shows the following in **Members of this group**, and then click **OK**:
  - o **ADATUM\Domain Admins**
  - o **ADATUM\IT**
  - o **Administrator**
20. Close the **Group Policy Management Editor** window.
21. On **LON-SVR1**, click **Start**, type **cmd**, and then click **Command Prompt**.
22. In the **Administrator: Command Prompt** window, type the following command, and then press Enter:

```
gpupdate /force
```
23. Wait until the command updates the Computer Policy and the User Policy.
24. On **LON-SVR1**, click **Start**, and then click **Server Manager**.
25. From **Server Manager**, click **Tools**, and then click **Computer Management**.
26. In **Computer Management**, expand **System Tools\Local Users and Groups**, and then click **Groups**.
27. Double-click **Administrators**, and then verify that **ADATUM\Domain Admins**, **ADATUM\IT**, and the local **Administrator** are members of this group.

28. Close all open windows except for **Server Manager**.
29. Switch back to **LON-DC1**, and then switch to **Group Policy Management**.
30. In the **Group Policy Management Console**, expand **Domain Controllers**, right-click the **Default Domain Controllers Policy** link, and then click **Edit**.
31. In the **Group Policy Management Editor** window, expand **Computer Configuration\Policies\Windows Settings\Security Settings**, click to select **Restricted Groups**, right-click **Restricted Groups**, and then click **Add Group**.
32. In the **Add Group** dialog box, in the **Group** field, type **Server Operators**, and then click **OK**.
33. In the **Server Operators Properties** dialog box, keep the default settings of **This group should contain no members**, and then click **OK**.
34. Repeat the steps 30 to 33 for the **Account Operators** group.
35. Close the **Group Policy Management Editor** window and the **Group Policy Management Console**.

► **Task 5: Implement administrative auditing**

1. On **LON-DC1**, from **Server Manager**, click **Tools**, and then click **Group Policy Management**.
2. In the **Group Policy Management Console**, expand **Forest: Adatum.com\Domains, Adatum.com\Group Policy Objects**, select the **Default Domain Controllers Policy**, right-click **Default Domain Controllers Policy**, and then click **Edit**.
3. In the **Group Policy Management Editor** window, expand **Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies**, and then click to select **DS Access**.
4. In the details pane, double-click **Audit Directory Services Changes**.
5. In the **Audit Directory Services Changes Properties** dialog box, select **Configure the following audit events**, select the **Success** check box, and then click **OK**.
6. In the navigation pane, navigate to **Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies**, and then click to select **Account Management**.
7. In the details pane, double-click **Audit Security Group Management**.
8. In the **Audit Security Group Management** dialog box, select **Configure the following audit events**, select the **Success** check box, and then click **OK**.
9. In the navigation pane, navigate to **Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies**, click to select **Security Options**, and then double-click the **Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings**.
10. In the **Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings** dialog box, select **Define this policy setting**, ensure that **Enabled** is selected, and then click **OK**.
11. Close the **Group Policy Management Editor** window and the **Group Policy Management Console**.
12. On **LON-DC1**, from Start screen, type **cmd**, and then click **Command Prompt**.
13. In the **Administrator: Command Prompt** window, type the following command, and then press Enter:

```
gpupdate /force
```

14. From **Server Manager**, click **Tools**, and then click **Active Directory Users and Computers**.
15. In **Active Directory Users and Computers**, from the **View** menu, enable the **Advanced Features** view.
16. In the navigation pane, click to select **Adatum.com**, right-click **Adatum.com**, and then click **Properties**.
17. In the **Adatum.com Properties** dialog box, on the **Security** tab, click **Advanced**.
18. In the **Advanced Security Settings for Adatum** dialog box, on the **Auditing** tab, double-click the **Success** auditing entry for **Everyone** with **Special** access, which applies to **This object only**.
19. In the **Auditing Entry for Adatum** dialog box, in the **Applies to** drop-down list box, select **This object and all descendent objects**.
20. Click **OK** three times to close all open dialog boxes.
21. In **Active Directory Users and Computers**, in the navigation pane, if necessary, expand **Adatum.com**, and then click to select **Users**.
22. In the details pane, double-click **Domain Admins**.
23. In the **Domain Admins Properties** dialog box, click the **Members** tab, and then click **Add**.
24. In the **Select Users, Contacts, Computers, Service Accounts, or Groups** dialog box, in the **Enter the object names to select** text box, type **Abbi**, click **Check Names**, and then click **OK** twice.
25. In **Active Directory Users and Computers**, in the navigation pane, click to select **Marketing**.
26. In the details pane, double-click **Ada Russel**.
27. In the **Ada Russel Properties** dialog box, on the **Address** tab, in the **City** text box, select **London**, type **Birmingham**, and then click **OK**.
28. Close **Active Directory Users and Computers**.
29. In **Server Manager**, click **Tools**, and then click **Event Viewer**.
30. In **Event Viewer**, expand **Windows Logs**, and then click **Security**.
31. In the details pane, search for the most recent **Event ID 4728**, and then double-click the event.
32. In the **Event Properties – Event 4728, Microsoft Windows security auditing** dialog box, you get the message "A member was added to a security-enabled global group." You can see that **ADATUM\Administrator** invoked the change and that **ADATUM\Abbi** was added to the **ADATUM\Domain Admins** group.
33. In **Event Viewer**, in the **Windows Logs\Security Log** node, search for the two most recent **Event IDs 5136**, then double-click the older of the two events.
34. In the **Event Properties – Event 5136, Microsoft Windows security auditing** dialog box, you will see the following message: "A directory service object was modified." You can see that **ADATUM\Administrator** has modified the user object **cn=Ada Russel**, and then deleted the **London** value. On the right side of the dialog box, click the **Up Arrow** to move to the next event.



**Note:** In the **Event Properties** details page, notice that **ADATUM\Administrator** modified **Ada Russel** and added the **Birmingham** value.

35. Close all open windows except for Server Manager.

**Results:** After this exercise, you should have identified and configured the security policies for A. Datum.

## Exercise 2: Deploying and configuring an RODC

### ► Task 1: Stage a delegated installation of an RODC

#### Preparation

To prestage an RODC account, the computer name must not be in use in the domain. Therefore, you first need to remove **LON-SVR1** from the domain by performing the following steps:

1. On **LON-SVR1**, in **Server Manager**, on the left side, click **Local Server**.
2. In the **Properties for LON-SVR1** section, click the domain **Adatum.com**.
3. In the **System Properties** dialog box, click **Change**.
4. In the **Computer Name/Domain Changes** dialog box, in the **Member of** section, select **Workgroup**, type **MUNICH**, and then click **OK**.
5. In the **Computer Name/Domain Changes** dialog box, click **OK**.
6. In the **Computer Name/Domain Changes** dialog box, you will see the following message: "Welcome to the MUNICH workgroup." Click **OK**.
7. In the **Computer Name/Domain Changes** dialog box, you will see the following message: "You must restart your computer to apply these changes." Click **OK**.
8. In the **System Properties** dialog box, click **Close**.
9. In the **Microsoft Windows** dialog box, click **Restart Now**.
10. Sign in as:
  - User name: **Administrator**
  - Password: **Pa\$\$w0rd**
11. Switch to **LON-DC2**. In **Server Manager**, click **Tools**, and then click **Active Directory Users and Computers**.
12. In the navigation pane, expand **Adatum.com**, click to select **Adatum Servers**, right-click **LON-SVR1**, and then click **Delete**.
13. In the **Active Directory Domain Services** dialog box, confirm the deletion by clicking **Yes**.
14. In the **Confirm Subtree Deletion** dialog box, click **Yes**.

#### Stage a delegated installation of an RODC

1. On **LON-DC2**, in **Server Manager**, click **Tools**, and then click **Active Directory Sites and Services**.
2. In **Active Directory Sites and Services**, in the navigation pane, click **Sites**. From the **Action** menu, click **New Site**.

3. In the **New Object – Site** dialog box, in the **Name** field, type **Munich**, select the **DEFAULTIPSITELINK** site link object, and then click **OK**.
4. In the **Active Directory Domain Services** dialog box, click **OK**.
5. Switch to **Server Manager**, click **Tools**, and then click **Active Directory Administrative Center**.
6. In **Active Directory Administrative Center**, in the navigation pane, click **Adatum (local)**, and then in the details pane, double-click the **Domain Controllers** OU.
7. In the **Tasks** pane, in the **Domain Controllers** section, click **Pre-create a Read-only domain controller account**.
8. In the **Active Directory Domain Services Installation Wizard**, on the **Welcome to the Active Directory Domain Services Installation Wizard** page, click **Next**.
9. On the **Network Credentials** page, click **Next**.
10. On the **Specify the Computer Name** page, type the computer name **LON-SVR1**, and then click **Next**.
11. On the **Select a Site** page, click **Munich**, and then click **Next**.
12. On the **Additional Domain Controller Options** page, accept the default selections of **DNS Server** and **Global Catalog**, and then click **Next**.
13. On the **Delegation of RODC Installation and Administration** page, click **Set**.
14. In the **Select User or Group** dialog box, in the **Enter the object name to select** field, type **Nestor**, and then click **Check Names**.
15. Verify that **Nestor Fiore** is resolved, and then click **OK**.
16. On the **Delegation of RODC Installation and Administration** page, click **Next**.
17. On the **Summary** page, review your selections, and then click **Next**.
18. On the **Completing the Active Directory Domain Services Installation Wizard** page, click **Finish**.

► **Task 2: Run the Active Directory Domain Services Installation Wizard on an RODC to complete the deployment process**

1. Switch to **LON-SVR1**. From **Server Manager**, click **Manage**, and then click **Add Roles and Features**.
2. In the **Add Roles and Features Wizard**, on the **Before You Begin** page, click **Next**.
3. On the **Select installation type** page, accept the default of **Role-based or feature-based installation**, and then click **Next**.
4. On the **Select destination server** page, accept the default with **LON-SVR1** being selected, and then click **Next**.
5. On the **Select server roles** page, in the **Roles** list, select **Active Directory Domain Services**.
6. In the **Add Roles and Features Wizard**, accept to install the features and management tools, click **Add Features**, and then click **Next**.
7. On the **Select features** page, click **Next**.
8. On the **Active Directory Domain Services** page, click **Next**.
9. On the **Confirm installation selections** page, click **Install**.
10. Wait until the role installs. You can click **Close** at any time, but monitor the **Notification** icon in Server Manager.

11. When the installation of the new role is finished, click the **Notification** icon for notifications.
12. In the **Post-deployment Configuration** message box, click **Promote this server to a domain controller**.
13. In the **Active Directory Domain Services Configuration Wizard**, on the **Deployment Configuration** page, leave the default to **Add a domain controller to an existing domain**.
14. In the **Supply the credentials to perform this operation** section, click **Change**.
15. In the **Windows Security** dialog box, enter the following credentials:
  - o User name: **Adatum\Nestor**
  - o Password: **Pa\$\$w0rd**
16. Under **Specify the domain information for this operation**, click **Select**, then select the domain **Adatum.com**, click **OK**, and then click **Next**.

You will receive a notification that an RODC account that matches the name of the server exists in the directory.
17. On the **Domain Controller Options** page, accept the default to **Use existing RODC account**, in the **Password** and **Confirm password** fields, type **Pa\$\$w0rd**, and then click **Next**.
18. On the **Additional Options** page, accept the defaults, and then click **Next**.
19. On the **Paths** page, accept the defaults, and then click **Next**.
20. On the **Review Options** page, review your options, and then click **Next**.
21. After the prerequisites check has been performed, click **Install**.



**Note:** The computer will configure AD DS and restart, but you can proceed to the next task.

### ► Task 3: Configure the domain-wide password replication policy

1. Switch to **LON-DC2**. In **Server Manager**, click **Tools**, and then click **Active Directory Administrative Center**.
2. In **Active Directory Administrative Center**, in the navigation pane, click **Adatum (local)**.
3. In the details pane, double-click **IT**.
4. Locate the **IT** group, right-click the group, and then click **Add to another group**.
5. In the **Select Groups** dialog box, in the **Enter the object names to select** text box, type **denied**, and then click **Check Names**.
6. Verify that the name of the group is expanded to **Denied RODC Password Replication Policy Group**, and then click **OK**.



**Note:** The members of the IT group have elevated permissions, so storing their password on an RODC would be a security risk. Therefore, you add the IT group to the global Deny List, which applies to every RODC in the domain.

7. Close the **Active Directory Administrative Center**.

► **Task 4: Create a group to manage password replication to the branch office RODC**

1. Switch to **Server Manager**, click **Tools**, and then click **Active Directory Users and Computers**.
2. In the navigation pane, expand **Adatum.com**, and then click **Users**.
3. On the **Action** menu, click **New**, and then click **Group**.
4. In the **New Object – Group** dialog box, type the group name **Munich Allowed RODC Password Replication Group**, click **OK**, and then double-click the **Munich Allowed RODC Password Replication Group**.
5. On the **Members** tab, click **Add**.
6. In the **Select Users, Contacts, Computers, Services Accounts, or Groups** dialog box, in the **Enter the object names to select** text box, type **Ana**, and then click **Check Names**.
7. In the **Multiple Names Found** dialog box, select **Ana Cantrell**, and then click **OK**.
8. In the **Select Users, Contacts, Computers, Service Accounts or Groups** dialog box, click **OK**, and then in the **Munich Allowed RODC Password Replication Group Properties** dialog box, click **OK**.
9. Close **Active Directory Users and Computers**.
10. In **Active Directory Administrative Center**, from the **Domain Controllers** OU, view the properties for **LON-SVR1**.
11. In the **Extensions** section, on the **Password Replication Policy** tab, click **Add**.
12. In the **Add Groups, Users and Computers** dialog box, select **Allow passwords for the account to replicate to this RODC**, and then click **OK**.
13. In the **Select Users, Computers, Service Accounts, or Groups** dialog box, in the **Enter the object names to select** text box, type **Munich**, click **Check Names**, and then click **OK**.
14. In the **LON-SVR1** dialog box, click **OK** to close the dialog box.

► **Task 5: Evaluate the resultant password replication policy**

1. In **Active Directory Administrative Center**, in the **Tasks** pane, in the **LON-SVR1** section, click **Properties**.
2. In the properties of **LON-SVR1**, in the **Extensions** section, on the **Password Replication Policy** tab, click **Advanced**.



**Note:** Note that this dialog box shows all accounts with passwords that are stored in the RODC.

3. Select **Accounts that have been authenticated to this Read-only Domain Controller**, and then note that this only shows accounts that have the permissions and already have been authenticated by this RODC.
4. Click the **Resultant Policy** tab, and then add **Ana Cantrell**. Notice that Ana Cantrell has a resultant policy of **Allow**.
5. Close all open dialog boxes.

**Results:** After this exercise, you should have deployed and configured an RODC.

## Exercise 3: Creating and associating a group MSA

### ► Task 1: Create and associate an MSA

1. On **LON-DC1**, in **Server Manager**, click **Tools**, and then click **Active Directory Module for Windows PowerShell**.
2. At the Windows PowerShell command prompt, type the following command, and then press Enter:

```
Add-KdsRootKey -EffectiveTime ((get-date).addhours(-10))
```

3. At the Windows PowerShell command prompt, type the following command, and then press Enter:

```
New-ADServiceAccount -Name Webservice -DNSHostName LON-DC1 -  
PrincipalsAllowedToRetrieveManagedPassword LON-DC1$
```

4. At the Windows PowerShell command prompt, type the following command, and then press Enter:

```
Add-ADComputerServiceAccount -identity LON-DC1 -ServiceAccount Webservice
```

5. At the Windows PowerShell command prompt, type the following command, and then press Enter:

```
Get-ADServiceAccount -Filter *
```

6. Note the output of the command, and then ensure the newly-created account is listed.
7. Minimize the Windows PowerShell command window.

### ► Task 2: Install a group MSA

1. On **LON-DC1**, at the Windows PowerShell command prompt, type the following command, and then press Enter:

```
Install-ADServiceAccount -Identity Webservice
```

2. In Server Manager, click the **Tools** menu, and then click **Internet Information Services (IIS) Manager**.
3. Expand **LON-DC1 (Adatum\Administrator)**, and then click **Application Pools**.
4. In the details pane, right-click the **DefaultAppPool**, and then click **Advanced Settings**.
5. In the **Advanced Settings** dialog box, in the **Process Model** section, click **Identity**, and then click the ellipses (...).
6. In the **Application Pool Identity** dialog box, click **Custom Account**, and then click **Set**.
7. In the **Set Credentials** dialog box, type **Adatum\Webservice\$** in the **User name** field, and then click **OK** three times.
8. In the **Actions** pane, click **Stop** to stop the application pool.
9. Click **Start** to start the application pool.
10. Close **Internet Information Services (IIS) Manager**.

**Results:** After completing this exercise, you should have configured an MSA.



► **Task: Prepare for the next module**

When you finish the lab, revert the virtual machines to their initial state. To do this, perform the following steps:

1. On the host computer, start **Hyper-V Manager**.
2. In the **Virtual Machines** list, right-click **20742A-LON-DC1**, and then click **Revert**.
3. In the **Revert Virtual Machine** dialog box, click **Revert**.
4. Repeat steps two and three for **20742A-LON-DC2** and **20742A-LON-SVR1**.

**MCT USE ONLY. STUDENT USE PROHIBITED**

## Module 8: Deploying and managing AD CS

# Lab: Deploying and configuring a two-tier CA hierarchy

### Exercise 1: Deploying an offline root CA

#### ► Task 1: Create file and printer sharing exceptions

1. Sign in to **CA-SVR1** as **Administrator** with password **Pa\$\$w0rd**.
2. Click **Start** and then click **Control Panel**.
3. In the **Control Panel** window, click **View network status and tasks**.
4. In the **Network and Sharing Center** window, click **Change advanced sharing settings**.
5. Under **Guest or Public (current profile)**, select the **Turn on file and printer sharing** option, and then click **Save changes**.
6. Switch to **LON-SVR1**.
7. Click **Start** and then click **Control Panel**.
8. In the **Control Panel** window, click **View network status and tasks**.
9. In the **Network and Sharing Center** window, click **Change advanced sharing settings**.
10. Under **Guest or Public (current profile)**, select the **Turn on file and printer sharing** option, and then click **Save changes**.

#### ► Task 2: Install and configure AD CS on CA-SVR1

1. Switch to **CA-SVR1**.
2. Click **Start**, and then click **Server Manager**. In **Server Manager**, click **Add roles and features**.
3. On the **Before you begin** page, click **Next**.
4. On the **Select installation type** page, click **Next**.
5. On the **Select destination server** page, click **Next**.
6. On the **Select server roles** page, select **Active Directory Certificate Services**. When the **Add Roles and Features Wizard** window displays, click **Add Features**, and then click **Next**.
7. On the **Select features** page, click **Next**.
8. On the **Active Directory Certificate Services** page, click **Next**.
9. On the **Select role services** page, ensure that **Certification Authority** is selected, and then click **Next**.
10. On the **Confirm installation selections** page, click **Install**.
11. On the **Installation progress** page, after installation completes successfully, click the text **Configure Active Directory Certificate Services on the destination server**.
12. In the **AD CS Configuration Wizard**, on the **Credentials** page, click **Next**.
13. On the **Role Services** page, select **Certification Authority**, and then click **Next**.
14. On the **Setup Type** page, ensure that **Standalone CA** is selected, and then click **Next**.
15. On the **CA Type** page, ensure that **Root CA** is selected, and then click **Next**.

16. On the **Private Key** page, ensure that **Create a new private key** is selected, and then click **Next**.
17. On the **Cryptography for CA** page, keep the default selections for Cryptographic Service Provider (CSP) and Hash Algorithm, but set the **Key length** to **4096**, and then click **Next**.
18. On the **CA Name** page, in the **Common name for this CA** box, type **AdatumRootCA**, and then click **Next**.
19. On the **Validity Period** page, click **Next**.
20. On the **CA Database** page, click **Next**.
21. On the **Confirmation** page, click **Configure**.
22. On the **Results** page, click **Close**.
23. On the **Installation progress** page, click **Close**.
24. On **CA-SVR1**, in **Server Manager**, click **Tools**, and then click **Certification Authority**.
25. In the **certsrv – [Certification Authority (Local)]** console, right-click **AdatumRootCA**, and then click **Properties**.
26. In the **AdatumRootCA Properties** dialog box, click the **Extensions** tab.
27. On the **Extensions** tab, in the **Select extension** drop-down list, click **CRL Distribution Point (CDP)**, and then click **Add**.
28. In the **Location** box, type **http://lon-svr1.adatum.com/CertData/**, in the **Variable** drop-down list, click **<CaName>**, and then click **Insert**.
29. In the **Variable** drop-down list, click **<CRLNameSuffix>**, and then click **Insert**.
30. In the **Variable** drop-down list, click **<DeltaCRLAllowed>**, and then click **Insert**.
31. In the **Location** box, position the cursor at the end of URL, type **.crl**, and then click **OK**.
32. Select the following options, and then click **Apply**:
  - o **Include in the CDP extension of issued certificates**
  - o **Include in CRLs. Clients use this to find Delta CRL locations**
33. In the **Certification Authority** pop-up window, click **No**.
34. In the **Select extension** drop-down list, click **Authority Information Access (AIA)**, and then click **Add**.
35. In the **Location** box, type **http://lon-svr1.adatum.com/CertData/**, in the **Variable** drop-down list, click **<ServerDNSName>**, and then click **Insert**.
36. In the **Location** box, type an underscore (**\_**), in the **Variable** drop-down list, click **<CaName>**, and then click **Insert**. Position the cursor at the end of URL.
37. In the **Variable** drop-down list, click **<CertificateName>**, and then click **Insert**.
38. In the **Location** box, position the cursor at the end of the URL, type **.crt**, and then click **OK**.
39. Select the **Include in the AIA extension of issued certificates** check box, and then click **OK**.
40. Click **Yes** to restart the Certification Authority service.
41. In the **Certification Authority** console, expand **AdatumRootCA**, right-click **Revoked Certificates**, point to **All Tasks**, and then click **Publish**.
42. In the **Publish CRL** window, click **OK**.
43. Right-click **AdatumRootCA**, and then click **Properties**.

44. In the **AdatumRootCA Properties** dialog box, click **View Certificate**.
45. In the **Certificate** dialog box, click the **Details** tab.
46. On the **Details** tab, click **Copy to File**.
47. In the **Certificate Export Wizard**, on the **Welcome** page, click **Next**.
48. On the **Export File Format** page, select **DER encoded binary X.509 (.CER)**, and then click **Next**.
49. On the **File to Export** page, click **Browse**. In the **File name** box, type **\\lon-svr1\C\$**, and then press Enter.
50. In the **File name** box, type **RootCA**, click **Save**, and then click **Next**.
51. Click **Finish**, and then click **OK** three times.
52. Open a **File Explorer** window, and then browse to **C:\Windows\System32\CertSrv\CertEnroll**.
53. In the **Cert Enroll** folder, Ctrl+click both files, right-click the highlighted files, and then click **Copy**.
54. In the File Explorer address bar, type **\\lon-svr1\C\$**, and then press Enter.
55. Right-click the empty space, and then click **Paste**.
56. Close File Explorer.

► **Task 3: Create a Domain Name System (DNS) record for an offline root CA**

1. On **LON-DC1**, in **Server Manager**, click **Tools**, and then click **DNS**.
2. In the DNS Manager console, expand **LON-DC1**, expand **Forward Lookup Zones**, click **Adatum.com**, right-click **Adatum.com**, and then click **New Host (A or AAAA)**.
3. In the **New Host** window, in the **Name** box, type **CA-SVR1**.
4. In the **IP address** window, type **172.16.0.40**, click **Add Host**, click **OK**, and then click **Done**.
5. Close DNS Manager.

**Results:** After completing this exercise, you should have successfully installed and configured the standalone root certification authority (CA) role on **CA-SVR1** server. In addition, you should have created an appropriate DNS record in Active Directory Domain Services (AD DS) so that other servers can connect to **CA-SVR1**.

## Exercise 2: Deploying an enterprise subordinate CA

► **Task 1: Install and configure AD CS on LON-SVR1**

1. On **LON-SVR1**, click **Start**, click **Server Manager**, and then click **Add roles and features**.
2. On the **Before you begin** page, click **Next**.
3. On the **Select installation type** page, click **Next**.
4. On the **Select destination server page**, click **Next**.
5. On the **Select server roles** page, select **Active Directory Certificate Services**.
6. When the **Add Roles and Features Wizard** displays, click **Add Features**, and then click **Next**.
7. On the **Select features** page, click **Next**.

8. On the **Active Directory Certificate Services** page, click **Next**.
9. On the **Select role services** page, ensure that **Certification Authority** is selected already, and then select **Certification Authority Web Enrollment**.
10. When the **Add Roles and Features Wizard** displays, click **Add Features**, and then click **Next**.
11. On the **Web Server Role (IIS)** page, click **Next**.
12. On the **Select role services** page, click **Next**.
13. On the **Confirm installation selections** page, click **Install**.
14. On the **Installation progress** page, after installation is successful, click the text **Configure Active Directory Certificate Services on the destination server**.
15. In the **AD CS Configuration Wizard**, on the **Credentials** page, click **Next**.
16. On the **Role Services** page, select both **Certification Authority** and **Certification Authority Web Enrollment**, and then click **Next**.
17. On the **Setup Type** page, select **Enterprise CA**, and then click **Next**.
18. On the **CA Type** page, click **Subordinate CA**, and then click **Next**.
19. On the **Private Key** page, ensure that **Create a new private key** is selected, and then click **Next**.
20. On the **Cryptography for CA** page, keep the default selections, and then click **Next**.
21. On the **CA Name** page, in the **Common name for this CA** box, type **Adatum-IssuingCA**, and then click **Next**.
22. On the **Certificate Request** page, ensure that **Save a certificate request to file on the target machine** is selected, and then click **Next**.
23. On the **CA Database** page, click **Next**.
24. On the **Confirmation** page, click **Configure**.
25. On the **Results** page, ignore the warning messages and click **Close**.
26. On the **Installation progress** page, click **Close**.

► **Task 2: Install a subordinate CA certificate**

1. On **LON-SVR1**, open a **File Explorer** window, and then navigate to **Local Disk (C:)**.
2. Right-click **RootCA.cer**, and then click **Install Certificate**.
3. In the **Certificate Import Wizard**, click **Local Machine**, and then click **Next**.
4. On the **Certificate Store** page, click **Place all certificates in the following store**, and then click **Browse**.
5. Select **Trusted Root Certification Authorities**, click **OK**, click **Next**, and then click **Finish**.
6. When the **Certificate Import Wizard** window appears, click **OK**.
7. In the **File Explorer** window, Ctrl+click the **AdatumRootCA.crl** and **CA-SVR1\_AdatumRootCA.crt** files, right-click the files, and then click **Copy**.
8. Double-click **inetpub**.
9. Double-click **wwwroot**.
10. Create a new folder, and then name it **CertData**.
11. Paste the two copied files into that folder.

12. Switch to **Local Disk (C:)**.
13. Right-click the file **LON-SVR1.Adatum.com\_Adatum-LON-SVR1-CA.req**, and then click **Copy**.
14. In the File Explorer address bar, type **\\CA-SVR1\C\$**, and then press Enter.
15. In the **File Explorer** window, right-click an empty space, and then click **Paste**. Make sure that the request file is copied to **CA-SVR1**.
16. Switch to the **CA-SVR1** server.
17. In the **Certificate Authority** console, right-click **AdatumRootCA**, point to **All Tasks**, and then click **Submit new request**.
18. In the **Open Request File** window, navigate to **Local Disk (C:)**, click file **LON-SVR1.Adatum.com\_Adatum- LON-SVR1-CA.req**, and then click **Open**.
19. In the **Certification Authority** console, click the **Pending Requests** container. Right-click **Pending Requests**, and then click **Refresh**.
20. In the details pane, right-click the request (with ID 2), point to **All Tasks**, and then click **Issue**.
21. In the **Certification Authority** console, click the **Issued Certificates** container.
22. In the details pane, double-click the certificate, click the **Details** tab, and then click **Copy to File**.
23. In the **Certificate Export Wizard**, on the **Welcome** page, click **Next**.
24. On the **Export File Format** page, click **Cryptographic Message Syntax Standard – PKCS #7 Certificates (.P7B)**, click **Include all certificates in the certification path if possible**, and then click **Next**.
25. On the **File to Export** page, click **Browse**.
26. In the **File name** box, type **\\lon-svr1\C\$**, and then press Enter.
27. In the **File name** box, type **SubCA**, click **Save**, click **Next**, click **Finish**, and then click **OK** twice.
28. Switch to **LON-SVR1**.
29. In **Server Manager**, click **Tools**, and then click **Certification Authority**.
30. In the **Certification Authority** console, right-click **Adatum-IssuingCA**, point to **All Tasks**, and then click **Install CA Certificate**.
31. Go to **Local Disk (C:)**, click the **SubCA.p7b** file, and then click **Open**.
32. Wait for 15–20 seconds, and then on the toolbar, click the **green** icon to start the CA service.
33. Ensure that the CA starts successfully.
34. Switch to **CA-SVR1**.
35. Shut down the server.



**Note:** From this point, you can safely put Root CA offline and use just Enterprise Subordinate CA.

► **Task 3: Publish a root CA certificate through Group Policy**

1. On **LON-DC1**, in **Server Manager**, click **Tools**, and then click **Group Policy Management**.
2. In the **Group Policy Management Console**, expand **Forest: Adatum.com**, expand **Domains**, expand **Adatum.com**, right-click **Default Domain Policy**, and then click **Edit**.
3. In the **Computer Configuration** node, expand **Policies**, expand **Windows Settings**, expand **Security Settings**, expand **Public Key Policies**, right-click **Trusted Root Certification Authorities**, click **Import**, and then click **Next**.
4. On the **File to Import** page, click **Browse**.
5. In the **file name** box, type `\\lon-svr1\C$`, and then press Enter.
6. Click file **RootCA.cer**, and then click **Open**.
7. Click **Next** two times, and then click **Finish**.
8. When the **Certificate Import Wizard** window appears, click **OK**.



**Note:** It might take 15–20 seconds for this window to appear.

9. Close the **Group Policy Management Editor** and the **Group Policy Management Console**.

**Results:** After completing this exercise, you should have successfully deployed and configured an enterprise subordinate CA. You also should have a subordinate CA certificate issued by a root CA installed on **LON-SVR1**. To establish trust between the root CA and domain-joined clients, you will use Group Policy to deploy a root CA certificate.

► **Task 4: Prepare for the next module**

1. On the host computer, start **Hyper-V Manager**.
2. In the **Virtual Machines** list, right-click **20742A-LON-DC1**, and then click **Revert**.
3. In the **Revert Virtual Machine** dialog box, click **Revert**.
4. Repeat steps 2 and 3 for **20742A-LON-SVR1**, **20742A-LON-DC2**, and **20742A-CA-SVR1**.



## Module 9: Deploying and managing certificates

# Lab: Deploying and using certificates

### Exercise 1: Configuring certificate templates

#### ► Task 1: Create a new template based on the Web Server template

1. On **LON-DC1**, in **Server Manager**, click **Tools**, and then click **Certification Authority**.
2. In the **Certification Authority** console, expand **AdatumCA**, right-click **Certificate Templates**, and then select **Manage**.
3. In the **Certificate Templates** console, locate the **Web Server** template in the list, right-click it, and then click **Duplicate Template**.
4. Click the **General** tab, and in the **Template display name** text box, type **Production Web Server**, and then type **3** in the **Validity period** text box.
5. Click the **Request Handling** tab, select **Allow private key to be exported**, and then click **OK**. Minimize the **Certificate Templates** console.
6. In the **Certification Authority** console on **LON-DC1**, right-click **Revoked Certificates**, select **All tasks**, click **Publish**, and then click **OK**.

#### ► Task 2: Create a new template for users that includes smart card sign in

1. On **LON-DC1**, in **Server Manager**, click **Tools**, then click **Certification Authority**.
2. Expand **AdatumCA**, then right-click **Certificate Templates** and click **Manage**. In the **Certificate Templates** console, right-click the **User** certificate template, and then click **Duplicate Template**.
3. In the **Properties of New Template** dialog box, click the **General** tab, and in the **Template display name** text box, type **Adatum User**.
4. On the **Subject Name** tab, clear both the **Include e-mail name in subject name** and the **E-mail name** check boxes.
5. On the **Extensions** tab, click **Application Policies**, and then click **Edit**.
6. In the **Edit Application Policies Extension** dialog box, click **Add**.
7. In the **Add Application Policy** dialog box, select **Smart Card Logon**, and then click **OK** twice.
8. Click the **Superseded Templates** tab, click **Add**, click the **User** template, and then click **OK**.
9. On the **Security** tab, click **Authenticated Users**. Under **Permissions for Authenticated Users**, select the **Allow** check boxes for **Read**, **Enroll**, and **Autoenroll**, and then click **OK**.
10. Close the **Certificate Templates** console.

#### ► Task 3: Configure the templates so that they can be issued

1. On **LON-DC1**, in the **Certification Authority** console, right-click **Certificate Templates**, point to **New**, and then click **Certificate Template to Issue**.
2. In the **Enable Certificate Templates** window, select **Adatum User** and **Production Web Server**, and then click **OK**.

**► Task 4: Enroll the Web Server certificate on LON-SVR2**

1. Switch to **LON-SVR2**.
2. Click **Start**, and then click the **Windows PowerShell** icon.
3. At the command prompt in the Windows PowerShell command-line interface, type **gpupdate /force**, and then press Enter.
4. Click **Start**, then click **Server Manager**. From **Server Manager**, click **Tools**, and then click **Internet Information Services (IIS) Manager**.
5. In the IIS console, click **LON-SVR2**, and then in the central pane, double-click **Server Certificates**.
6. In the **Actions** pane, click **Create Domain Certificate**.
7. On the **Distinguished Name Properties** page, complete the following fields, and then click **Next**:
  - Common name: **lon-svr2.adatum.com**
  - Organization: **Adatum**
  - Organizational unit: **IT**
  - City/locality: **Seattle**
  - State/province: **WA**
  - Country/region: **US**
8. On the **Online Certification Authority** page, click **Select**, click **AdatumCA**, and then click **OK**.
9. In the **Friendly name** text box, type **lon-svr2**, and then click **Finish**.
10. Ensure that the certificate displays in the **Server Certificates** console.
11. In the **IIS** console, expand **LON-SVR2**, expand **Sites**, and then click **Default Web Site**.
12. In the **Actions** pane, click **Bindings**.
13. In the **Site Bindings** window, select **Add**.
14. In the **Add Site Binding** window, select **https** from the **Type** drop-down list. In the **SSL certificate** drop-down list, click **lon-svr2**, click **OK**, and then click **Close**.
15. Close **Internet Information Services (IIS) Manager**.
16. Switch to **LON-CL1**. In the **Cortana** search field, type **Internet Explorer**. Then, click **Internet Explorer** in the search results returned.
17. In Internet Explorer, type **https://lon-svr2.adatum.com** in the Address bar, and then press Enter.
18. Ensure that the **Internet Information Services** page opens and that no certificate error displays.

**Results:** After completing this exercise, students will have configured certificate templates.

## Exercise 2: Enrolling and using certificates

### ► Task 1: Configure autoenrollment for users

1. On **LON-DC1**, in **Server Manager**, click **Tools**, and then click **Group Policy Management**.
2. Expand **Forest: Adatum.com**, expand **Domains**, expand **Adatum.com**, right-click **Default Domain Policy**, and then click **Edit**.
3. Expand **User Configuration**, expand **Policies**, expand **Windows Settings**, expand **Security Settings**, and then click to highlight **Public Key Policies**.
4. In the **Details** pane, double-click **Certificate Services Client – Auto-Enrollment**.
5. In the **Configuration Model** drop-down list, click **Enabled**, select **Renew expired certificates, update pending certificates, and remove revoked certificates** and **Update certificates that use certificate templates**, and then click **OK** to close the properties window.
6. In the right pane, double-click the **Certificate Services Client – Certificate Enrollment Policy** object.
7. On the **Enrollment Policy** tab, set the **Configuration Model** to **Enabled**, and then ensure that the **Certificate Enrollment Policy** list displays the **Active Directory Enrollment** policy. It should have a check mark next to it and display a status of **Enabled**. Click **OK** to close the window.
8. Close both the **Group Policy Management Editor** window and the **Group Policy Management** console.

### ► Task 2: Verify autoenrollment

1. On **LON-CL1**, click **Start**, type **PowerShell**, and then click the **Windows PowerShell** icon.
2. At the Windows PowerShell command prompt, type **gpupdate /force**, and then press Enter.
3. After the policy refreshes, type **mmc.exe**, and then press Enter.
4. In **Console1**, click **File**, click **Add/Remove Snap-in**, click **Certificates**, click **Add**, click **Finish**, and then click **OK**.
5. Expand **Certificates – Current User**, expand **Personal**, and then click **Certificates**.
6. Verify that a certificate based on the **Adatum User** template is issued for **Administrator**. To verify the name of template, scroll to the right in the console window.
7. Close **Console1** without saving changes.
8. Sign out of **LON-CL1**.

### ► Task 3: Configure the enrollment agent for smart card certificates

1. On **LON-DC1**, in **Server Manager**, click **Tools**, and then open **Certification Authority**.
2. In the **certsrv** console, expand **AdatumCA**, right-click **Certificate Templates**, and then click **Manage**.
3. In the **Certificate Templates** console, double-click **Enrollment Agent**.
4. Click the **Security** tab, and then click **Add**.
5. In the **Select Users, Computers, Service Accounts, or Groups** window, type **Annie**, click **Check Names**, and then click **OK**.
6. On the **Security** tab, click **Annie Conner**, select the **Allow** check box for **Read** and **Enroll** permissions, and then click **OK**.
7. Close the **Certificate Templates** console.

8. In the **certsrv** console, right-click **Certificate Templates**, point to **New**, and then click **Certificate Template to Issue**.
9. In the list of templates, click **Enrollment Agent**, and then click **OK**.
10. Switch to **LON-CL1**, and then sign in as **Adatum\Annie** with the password **Pa\$\$w0rd**.
11. Click **Start**, type **Command Prompt** and press Enter. In the **Command Prompt** window, type **mmc.exe**, and then press Enter.
12. In **Console1**, click **File**, and then click **Add/Remove Snap-in**.
13. Click **Certificates**, click **Add**, and then click **OK**.
14. Expand **Certificates – Current User**, expand **Personal**, click **Certificates**, right-click **Certificates**, point to **All Tasks**, and then click **Request New Certificate**.
15. In the **Certificate Enrollment Wizard**, on the **Before You Begin** page, click **Next**.
16. On the **Select Certificate Enrollment Policy** page, click **Next**.
17. On the **Request Certificates** page, select **Enrollment Agent**, click **Enroll**, and then click **Finish**.
18. Sign out of **LON-CL1**.
19. Switch to **LON-DC1**.
20. In the **Certification Authority** console, right-click **AdatumCA**, and then click **Properties**.
21. On the **Enrollment Agents** tab, click **Restrict Enrollment agents**.
22. On the pop-up window that displays, click **OK**.
23. In the **Enrollment agents** section, click **Add**.
24. In the **Select User, Computer or Group** field, type **Annie**, click **Check Names**, and then click **OK**.
25. Click **Everyone**, and then click **Remove**.
26. In the **Certificate Templates** section, click **Add**.
27. In the list of templates, select **Adatum User**, and then click **OK**.
28. In the **Certificate Templates** section, click **<All>**, and then click **Remove**.
29. In the **Permission** section, click **Add**.
30. In the **Select User, Computer or Group** field, type **Marketing**, click **Check Names**, and then click **OK**.
31. In the **Permission** section, click **Everyone**, click **Remove**, and then click **OK**.

► **Task 4: Use certificates for digital signing of a Microsoft Office document**

1. On **LON-CL1**, sign in as **Adatum\Administrator** with the password **Pa\$\$w0rd**.
2. Click the **Start** button, type **Word 2016**, then click **Word 2016**.



**Note:** If you receive a prompt from **Microsoft Office Activation Wizard**, click **Close**. If prompted to update, select **Ask me later**, and then click **Accept**.

3. Click **blank document**, type some text, and then save the document to the desktop.
4. On the toolbar, click **INSERT**, and then in the **Text** pane, in the **Signature Line** drop-down list, click **Microsoft Office Signature Line**.

5. In the **Signature Setup** window, type your name in the **Suggested signer** text box, type **Administrator** in the **Suggested signer's title** text box, type **Administrator@adatum.com** in the **Suggested signer's email address** text box, and then click **OK**.
6. Right-click the signature line in the document, and then click **Sign...**
7. In the **Sign** window, click **Change**.
8. In the **Certificate** list, ensure that you have a certificate issued for **Administrator**, and then click **OK**.
9. In the text box to the right of the **X**, type your name, click **Sign**, and then click **OK**. Besides typing your name, you also can select an image. This image can be your scanned handwriting signature.
10. Ensure that the document cannot be edited anymore.



**Note:** Try to type some text in the document.

11. Close Word 2016, and then save changes if you receive a prompt.
12. Sign out of **LON-CL1**.

**Results:** After completing this exercise, students will have implemented certificate enrollment.

### Exercise 3: Configuring and implementing key recovery

#### ► Task 1: Configure the certification authority (CA) to issue KRA certificates

1. On **LON-DC1**, in the **Certification Authority** console, expand the **AdatumCA** node, right-click the **Certificates Templates** folder, and then click **Manage**.
2. In the **Details** pane, right-click the **Key Recovery Agent** certificate, and then click **Properties**.
3. In the **Key Recovery Agent Properties** dialog box, click the **Issuance Requirements** tab, and then clear the **CA certificate manager approval** check box.
4. Click the **Security** tab. Notice that Domain Admins and Enterprise Admins are the only groups that have the Enroll permission, and then click **OK**.
5. Close the **Certificate Templates** console.
6. In the **Certification Authority** console, right-click **Certificate Templates**, point to **New**, and then click **Certificate Template to Issue**.
7. In the **Enable Certificate Templates** dialog box, click the **Key Recovery Agent** template, and then click **OK**.
8. Close the **Certification Authority** console.

#### ► Task 2: Acquire the KRA certificate

1. On **LON-DC1**, click **Start**, then click the **Windows PowerShell** icon.
2. At the Windows PowerShell command prompt, type **mmc.exe**, and then press Enter.
3. In the **Console1-[Console Root]** console, click **File**, and then click **Add/Remove Snap-in**.
4. In the **Add or Remove Snap-ins** dialog box, click **Certificates**, and then click **Add**.
5. In the **Certificates snap-in** dialog box, select **My user account**, click **Finish**, and then click **OK**.

6. Expand the **Certificates - Current User** node, right-click **Personal**, point to **All Tasks**, and then click **Request New Certificate**.
7. In the **Certificate Enrollment Wizard**, on the **Before You Begin** page, click **Next**.
8. On the **Select Certificate Enrollment Policy** page, click **Next**.
9. On the **Request Certificates** page, select the **Key Recovery Agent** check box, click **Enroll**, and then click **Finish**.
10. Refresh the console, and then view the Key Recovery Agent (KRA) in the personal store; scroll across the certificate properties and verify that **Certificate Template Key Recovery Agent** is present.
11. Close **Console1** without your saving changes.

► **Task 3: Configure the CA to allow key recovery**

1. On **LON-DC1**, in **Server Manager**, click **Tools**, then click **Certification Authority**. In the **Certification Authority** console, right-click **AdatumCA**, and then click **Properties**.
2. In the **AdatumCA Properties** dialog box, click the **Recovery Agents** tab, and then select **Archive the key**.
3. Under **Key recovery agent certificates**, click **Add**.
4. In the **Key Recovery Agent Selection** dialog box, click the certificate that is for KRA purpose (it will most likely be last on the list), and then click **OK** twice.
5. When prompted to restart the CA, click **Yes**.

► **Task 4: Configure a custom template for key archival**

1. On **LON-DC1**, in the **Certification Authority** console, right-click the **Certificates Templates** folder, and then click **Manage**.
2. In the **Certificate Templates** console, right-click the **User** certificate, and then click **Duplicate Template**.
3. In the **Properties of New Template** dialog box, on the **General** tab, in the **Template display name** text box, type **Archive User**.
4. On the **Request Handling** tab, select the **Archive subject's encryption private key** check box.
5. If a pop-up window displays, click **OK**.
6. Click the **Subject Name** tab, clear the **E-mail name** and **Include E-mail name in subject name** check boxes, and then click **OK**.
7. Close the **Certificate Templates** console.
8. In the **Certification Authority** console, right-click the **Certificates Templates** folder, point to **New**, and then click **Certificate Template to Issue**.
9. In the **Enable Certificate Templates** dialog box, click the **Archive User** template, and then click **OK**.
10. Close the **Certification Authority** console.

► **Task 5: Verify key archival functionality**

1. Sign in to **LON-CL1** as **Adatum\Aidan** with the password **Pa\$\$w0rd**.
2. On the Start screen, type **mmc.exe**, and then press Enter. If prompted, click **Yes** in **User Account Control** window.
3. In the **Console1-[Console Root]** console, click **File**, and then click **Add/Remove Snap-in**.

4. In the **Add or Remove Snap-ins** dialog box, click **Certificates**, click **Add**, and then click **OK**.
5. Expand the **Certificates - Current User** node, right-click **Personal**, click **All Tasks**, and then click **Request New Certificate**.
6. In the **Certificate Enrollment Wizard**, on the **Before You Begin** page, click **Next**.
7. On the **Select Certificate Enrollment Policy** page, click **Next**.
8. On the **Request Certificates** page, select the **Archive User** check box, click **Enroll**, and then click **Finish**.
9. Refresh the console, and then view that a certificate is issued to **Aidan** based on the **Archive User** certificate template.
10. Simulate the loss of a private key by deleting the certificate. In the central pane, right-click the certificate that you just enrolled, select **Delete**, and then click **Yes** to confirm.
11. Switch to **LON-DC1**.
12. Open the **Certification Authority** console, expand **AdatumCA**, and then click the **Issued Certificates** store.
13. In the **Details** pane, double-click a certificate with **Requestor Name** of **Adatum\Aidan** and a **Certificate Template** name of **Archive User**.
14. Click the **Details** tab, copy the **Serial number**, and then click **OK**. You might either copy the number by selecting it and pressing Ctrl+C or by noting it in a document.
15. Click the **Start** button, and then click the **Windows PowerShell** icon.
16. At the Windows PowerShell command prompt, type the following command, where *<serial number>* is the serial number that you copied, and then press Enter:

```
Certutil -getkey <serial number> outputblob
```



**Note:** If you copy and paste the serial number, remove the spaces between the numbers or enclose the serial number between double quotes.

17. Verify that the **Outputblob** file now displays in the **C:\Users\Administrator** folder.
18. To convert the **Outputblob** file into a .pfx file, at the Windows PowerShell command prompt, type the following command, and then press Enter:

```
Certutil -recoverkey outputblob aidan.pfx
```

19. When prompted for the new password, type **Pa\$\$w0rd**, and then confirm the password.
20. After the command executes, close Windows PowerShell.
21. Go to **C:\Users\Administrator**, and then verify that **aidan.pfx**—the recovered key—is created.
22. Switch to **LON-CL1**.
23. Open **File Explorer** and then browse to **\\LON-DC1.adatum.com\c\$**. When prompted for credentials, use **Adatum\Administrator** with the password **Pa\$\$w0rd**.
24. Go to **\\LON-DC1.adatum.com\c\$\users\administrator**.
25. Right-click the **aidan.pfx** file, and then select **Copy**. Go to **C:\Users\aidan**. In the empty space, right-click, and then select **Paste**.

26. Double-click the **aidan.pfx** file.
27. On the **Welcome to the Certificate Import Wizard** page, click **Next**.
28. On the **File to Import** page, click **Next**.
29. On the **Password** page, type the password **Pa\$\$w0rd**, and then click **Next**.
30. On the **Certificate Store** page, click **Next**, click **Finish**, and then click **OK**.
31. In **Console1**, expand the **Certificates - Current User** node, expand **Personal**, and then click **Certificates**.
32. Refresh the console, and then verify that the certificate for Aidan is restored.

**Results:** After completing this exercise, students will have configured key recovery.

#### ► Task 6: Prepare for the next module

When you finish the lab, revert the virtual machines to their initial state. To do this, complete the following steps:

1. On the host computer, start **Hyper-V Manager**.
2. In the **Virtual Machines** list, right-click **20742A-LON-DC1**, and then click **Revert**.
3. In the **Revert Virtual Machine** dialog box, click **Revert**.
4. Repeat steps 2 and 3 for **20742A-LON-CL1**, **20742A-LON-SVR1**, and **20742A-LON-SVR2**.



# Module 10: Implementing and administering AD FS

## Lab: Implementing AD FS

### Exercise 1: Configuring the AD FS prerequisites

#### ► Task 1: Configure the DNS forwarders

1. On **LON-DC1**, in the **Server Manager** window, click **Tools**, and then click **DNS**.
2. In **DNS Manager**, expand **LON-DC1**, and then click **Conditional Forwarders**.
3. Right-click **Conditional Forwarders**, and then click **New Conditional Forwarder**.
4. In the **New Conditional Forwarder** window, in the **DNS Domain** box, type **TreyResearch.net**.
5. In the **IP addresses of the master servers** box, type **172.16.10.10**, and then press Enter.
6. Select the **Store this conditional forwarder in Active Directory, and replicate it as follows** check box, select **All DNS servers in this forest**, and then click **OK**.
7. Close **DNS Manager**.
8. On **TREY-DC1**, in the **Server Manager** window, click **Tools**, and then click **DNS**.
9. In **DNS Manager**, expand **TREY-DC1**, and then click **Conditional Forwarders**.
10. Right-click **Conditional Forwarders**, and then click **New Conditional Forwarder**.
11. In the **New Conditional Forwarder** window, in the **DNS Domain** box, type **Adatum.com**.
12. In the **IP addresses of the master servers** box, type **172.16.0.10**, and then press Enter.
13. Select the **Store this conditional forwarder in Active Directory, and replicate it as follows** check box, select **All DNS servers in this forest**, and then click **OK**.
14. Close DNS Manager.



**Note:** In a production environment, it is likely that you will use the Internet Domain Name System (DNS) instead of conditional forwarders.

#### ► Task 2: Configure the certificate trusts

1. On **LON-DC1**, open **File Explorer**, go to **\\TREY-DC1\CertEnroll**, and then copy **TREY-DC1.TreyResearch.net\_TreyResearchCA.crt** to **C:\**.
2. Close File Explorer.
3. In **Server Manager**, click **Tools**, and then click **Group Policy Management**.
4. In **Group Policy Management**, expand **Forest: Adatum.com**, expand **Domains**, expand **Adatum.com**, right-click **Default Domain Policy**, and then click **Edit**.
5. In the **Group Policy Management Editor**, under **Computer Configuration**, expand **Policies**, expand **Windows Settings**, expand **Security Settings**, expand **Public Key Policies**, and then click **Trusted Root Certification Authorities**.
6. Right-click **Trusted Root Certification Authorities**, and then click **Import**.
7. In the **Certificate Import Wizard**, on the **Welcome to the Certificate Import Wizard** page, click **Next**.

8. On the **File to Import** page, type **C:\TREY-DC1.TreyResearch.net\_TreyResearchCA.crt**, and then click **Next**.
9. On the **Certificate Store** page, click **Place all certificates in the following store**, select **Trusted Root Certification Authorities**, and then click **Next**.
10. On the **Completing the Certificate Import Wizard** page, click **Finish**, and then click **OK** to close the success message.
11. Close the **Group Policy Management Editor**.
12. Close **Group Policy Management**.
13. On **TREY-DC1**, open **File Explorer**, and then go to **\\LON-DC1\CertEnroll**.
14. Right-click **LON-DC1.Adatum.com\_AdatumCA.crt**, and then click **Install Certificate**.
15. In the **Certificate Import Wizard**, on the **Welcome to the Certificate Import Wizard** page, click **Local Machine**, and then click **Next**.
16. On the **Certificate Store** page, click **Place all certificates in the following store**, and then click **Browse**.
17. In the **Select Certificate Store** window, click **Trusted Root Certification Authorities**, and then click **OK**.
18. On the **Certificate Store** page, click **Next**.
19. On the **Completing the Certificate Import Wizard** page, click **Finish**, and then click **OK** to close the success message.
20. Close File Explorer.
21. On **LON-SVR1**, click **Start** and then click **Windows PowerShell**.
22. At the Windows PowerShell command prompt, type **gpupdate**, and then press Enter.
23. Close Windows PowerShell.



**Note:** If you obtain certificates from a trusted certification authority (CA), you do not need to configure a certificate trust between the organizations.

### ► Task 3: Request and install a certificate for the web server

1. On **LON-SVR1**, open **Server Manager**, click **Tools**, and then click **Internet Information Services (IIS) Manager**.
2. In **Microsoft Internet Information Services (IIS) Manager**, click **LON-SVR1 (ADATUM\Administrator)**, and then double-click **Server Certificates**.
3. In the **Actions** pane, click **Create Domain Certificate**.
4. In the **Create Certificate Wizard**, on the **Distinguished Name Properties** page, type the following information, and then click **Next**:
  - Common name: **lon-svr1.atum.com**
  - Organization: **A. Datum Corporation**
  - Organizational unit: **IT**

- City/locality: **London**
  - State/Province: **England**
  - Country/region: **GB**
5. On the **Online Certification Authority** page, click **Select**.
  6. In the **Select Certification Authority** page, click **AdatumCA**, and then click **OK**.
  7. On the **Online Certification Authority** page, in the **Friendly name** box, type **AdatumTestApp Certificate**, and then click **Finish**.
  8. In **IIS Manager**, expand **LON-SVR1 (ADATUM\Administrator)**, expand **Sites**, click **Default Web Site**, and then in the **Actions** pane, click **Bindings**.
  9. In the **Site Bindings** window, click **Add**.
  10. In the **Add Site Binding** window, in the **Type** list, select **https**.
  11. In the **SSL certificate** list, select **AdatumTestApp Certificate**, and then click **OK**.
  12. In the **Site Bindings** window, click **Close**.
  13. Close IIS Manager.

**Results:** After completing this exercise, you should have successfully enabled DNS resolution and certificate trusts between the domains. Also, you will have enabled an SSL certificate for the website and validated access to it.

## Exercise 2: Installing and configuring AD FS

### ► Task 1: Create a DNS record for AD FS

1. On **LON-DC1**, in **Server Manager**, click **Tools**, and then click **DNS**.
2. In **DNS Manager**, expand **LON-DC1**, expand **Forward Lookup Zones**, and then click **Adatum.com**.
3. Right-click **Adatum.com**, and then click **New Host (A or AAAA)**.
4. In the **New Host** window, in the **Name** box, type **adfs**.
5. In the **IP address** box, type **172.16.0.10**, and then click **Add Host**.
6. In the **DNS** window, click **OK**.
7. Click **Done**, and then close **DNS Manager**.

### ► Task 2: Install AD FS

1. On **LON-DC1**, click **Start**, right-click **Windows PowerShell**, and then click **Run as Administrator**.
2. At the command prompt, type the following command, and then press Enter.

```
Add-KdsRootKey -EffectiveTime ((get-date).addhours(-10))
```

This command creates the Microsoft Group Key Distribution Service root key to generate group Managed Service Account (gMSA) passwords for the account that will be used later in this lab. You should receive a globally unique identifier (GUID) as a response to this command.

3. Click **Start**, click **Server Manager**, click **Manage**, and then click **Add Roles and Features**.

4. In the **Add Roles and Features Wizard**, on the **Before you begin** page, click **Next**.
5. On the **Select installation type** page, click **Role-based or feature-based installation**, and then click **Next**.
6. On the **Select destination server** page, click **Select a server from the server pool**, click **LON-DC1.Adatum.com**, and then click **Next**.
7. On the **Select server roles** page, select the **Active Directory Federation Services** check box, and then click **Next**.
8. On the **Select features** page, click **Next**.
9. On the **Active Directory Federation Services (AD FS)** page, click **Next**.
10. On the **Confirm installation selections** page, click **Install**.
11. When the installation is complete, click **Close**.

► **Task 3: Configure AD FS**

1. On **LON-DC1**, in **Server Manager**, click the **Notifications** icon, and then click **Configure the federation service on this server**.
2. In the **Active Directory Federation Services Configuration Wizard**, on the **Welcome** page, click **Create the first federation server in a federation server farm**, and then click **Next**.
3. On the **Connect to Active Directory Domain Services** page, click **Next** to use **Adatum\Administrator** to perform the configuration.
4. On the **Specify Service Properties** page, in the **SSL Certificate** list, select **adfs.adatum.com**.
5. In the **Federation Service Display Name** box, type **A. Datum Corporation**, and then click **Next**.
6. On the **Specify Service Account** page, click **Create a Group Managed Service Account**.
7. In the **Account Name** box, type **ADFSService**, and then click **Next**.
8. On the **Specify Configuration Database** page, click **Create a database on this server using Windows Internal Database**, and then click **Next**.
9. On the **Review Options** page, click **Next**.
10. On the **Pre-requisite Checks** page, click **Configure**.
11. On the **Results** page, click **Close**.



**Note:** The adfs.adatum.com certificate was preconfigured for this task. In your own environment, you must obtain this certificate.

► **Task 4: Verify AD FS functionality**

1. On **LON-CL1**, click **Start**, click **All apps**, click **Windows Accessories**, and then click **Internet Explorer**.
2. In Internet Explorer, on the address bar, type **https://adfs.adatum.com/federationmetadata/2007-06/federationmetadata.xml**, and then press Enter.
3. Verify that the file loads, and then close Internet Explorer.

**Results:** After completing this exercise, you should have successfully installed and configured AD FS. You also should have verified that it is functioning by viewing the contents of the **FederationMetaData.xml** file.

### Exercise 3: Configuring an internal application for AD FS

► **Task 1: Configure the Active Directory claims provider trust**

1. On **LON-DC1**, in **Server Manager**, click **Tools**, and then click **AD FS Management**.
2. In the **AD FS Management** console, click **Claims Provider Trusts**.
3. In the list of **Claims Provider Trusts**, right-click **Active Directory**, and then click **Edit Claim Rules**.
4. In the **Edit Claim Rules for Active Directory** window, on the **Acceptance Transform Rules** tab, click **Add Rule**.
5. In the **Add Transform Claim Rule Wizard**, on the **Select Rule Template** page, in the **Claim rule template** list, select **Send LDAP Attributes as Claims**, and then click **Next**.
6. On the **Configure Rule** page, in the **Claim rule name** box, type **Outbound LDAP Attributes Rule**.
7. In the **Attribute store** list, select **Active Directory**.
8. In the **Mapping of LDAP attributes to outgoing claim types** section, select the following values for the **LDAP Attribute** and the **Outgoing Claim Type**, and then click **Finish**:
  - E-Mail-Addresses: **E-Mail Address**
  - User-Principal-Name: **UPN**
  - Display-Name: **Name**
9. In the **Edit Claim Rules for Active Directory** window, click **OK**.

► **Task 2: Configure the application to trust incoming claims**

1. On **LON-SVR1**, open **Server Manager**, click **Tools**, and then click **Windows Identity Foundation Federation Utility**.
2. On the **Welcome to the Federation Utility Wizard** page, in the **Application configuration location** box, type **C:\inetpub\wwwroot\AdatumTestApp\web.config** for the location of the sample **web.config** file.
3. In the **Application URI** box, type **https://lon-svr1.adatum.com/AdatumTestApp/** to indicate the path to the sample application that will trust the incoming claims from the federation server, and then click **Next**.

4. On the **Security Token Service** page, click **Use an existing STS**, and then in the **STS WS-Federation metadata document location** box, type **https://adfs.adatum.com/federationmetadata/2007-06/federationmetadata.xml**. Click **Next**.
5. On the **STS signing certificate chain validation error** page, click **Disable certificate chain validation**, and then click **Next**.
6. On the **Security token encryption** page, click **No encryption**, and then click **Next**.
7. On the **Offered claims** page, review the claims that will be offered by the federation server, and then click **Next**.
8. On the **Summary** page, review the changes that will be made to the sample application by the **Federation Utility Wizard**, scroll through the items to understand what each item is doing, and then click **Finish**.
9. In the **Success** window, click **OK**.

► **Task 3: Configure a relying party trust for the claims-aware application**

1. On **LON-DC1**, in the **AD FS** console, click **Relying Party Trusts**.
2. In the **Actions** pane, click **Add Relying Party Trust**.
3. In the **Add Relying Party Trust Wizard**, on the **Welcome** page, click **Start**.
4. On the **Select Data Source** page, click **Import data about the relying party published online or on a local network**.
5. In the **Federation Metadata address (host name or URL)** box, type **https://lon-svr1.adatum.com/adatumtestapp/**, and then click **Next**. This downloads the metadata configured in the previous task.
6. On the **Specify Display Name** page, in the **Display name** box, type **A. Datum Corporation Test App**, and then click **Next**.
7. On the **Choose Access Control Policy** page, click **Permit everyone**, and then click **Next**.
8. On the **Ready to Add Trust** page, review the relying party trust settings, and then click **Next**.
9. On the **Finish** page, click **Close**.

► **Task 4: Configure claim rules for the relying party trust**

1. On **LON-DC1**, in the **AD FS Management** console, in the list of **Relying Party Trusts**, click **A. Datum Corporation Test App**, and then select **Edit Claim Issuance policy**.
2. In the **Edit Claim Issuance Policy for A. Datum Corporation Test App** window, on the **Issuance Transform Rules** tab, click **Add Rule**.
3. In the **Claim rule template** box, select **Pass Through or Filter an Incoming Claim**, and then click **Next**.
4. In the **Claim rule name** box, type **Pass through Windows account name**.
5. In the **Incoming claim type** list, click **Windows account name**, and then click **Finish**.
6. On the **Issuance Transform Rules** tab, click **Add Rule**.
7. In the **Claim rule template** box, select **Pass Through or Filter an Incoming Claim**, and then click **Next**.
8. In the **Claim rule name** box, type **Pass through E-Mail Address**.
9. In the **Incoming claim type** list, click **E-Mail Address**, and then click **Finish**.

10. On the **Issuance Transform Rules** tab, click **Add Rule**.
11. In the **Claim rule template** box, select **Pass Through or Filter an Incoming Claim**, and then click **Next**.
12. In the **Claim rule name** box, type **Pass through UPN**.
13. In the **Incoming claim type** list, click **UPN**, and then click **Finish**.
14. On the **Issuance Transform Rules** tab, click **Add Rule**.
15. In the **Claim rule template** dialog box, select **Pass Through or Filter an Incoming Claim**, and then click **Next**.
16. In the **Claim rule name** box, type **Pass through Name**.
17. In the **Incoming claim type** list, click **Name**, and then click **Finish**.
18. On the **Issuance Transform Rules** tab, click **OK**.

► **Task 5: Test access to the claims-aware application**

1. On **LON-CL1**, open **Internet Explorer**.
2. In Internet Explorer, on the address bar, type **https://lon-svr1.adatum.com/AdatumTestApp/**, and then press Enter.



**Note:** It is critical to use the trailing forward slash (/) in the URL for step 2.

3. In the **Windows Security** window, sign in as **Adatum\Adam** with the password **Pa\$\$w0rd**.
4. Review the claim information that is displayed by the application.
5. Close Internet Explorer.

► **Task 6: Configure Internet Explorer to automatically pass local credentials to the application**

1. On **LON-CL1**, click **Start**, type **Internet Options**, and then click **Internet Options**.
2. In the **Internet Properties** window, on the **Security** tab, click **Local intranet**, and then click **Sites**.
3. In the **Local intranet** window, click **Advanced**.
4. In the **Local intranet** window, in the **Add this website to the zone** box, type **https://adfs.adatum.com**, and then click **Add**.
5. In the **Add this website to the zone** box, type **https://lon-svr1.adatum.com**, click **Add**, and then click **Close**.
6. In the **Local intranet** window, click **OK**.
7. In the **Internet Properties** window, click **OK**.
8. On **LON-CL1**, open **Internet Explorer**.
9. In Internet Explorer, on the address bar, type **https://lon-svr1.adatum.com/AdatumTestApp/**, and then press Enter.



**Note:** It is critical to use the trailing forward slash (/) in the URL for step 9.

10. Notice that you were not prompted for credentials.

11. Review the claim information that is displayed by the application.
12. Close Internet Explorer.

**Results:** After completing this exercise, you should have successfully configured AD FS to support authentication for an application.

## Exercise 4: Configuring AD FS for federated business partners

### ► Task 1: Create a DNS record for AD FS at Trey Research

1. On **TREY-DC1**, in **Server Manager**, click **Tools**, and then click **DNS**.
2. In **DNS Manager**, expand **TREY-DC1**, expand **Forward Lookup Zones**, and then click **TreyResearch.net**.
3. Right-click **TreyResearch.net**, and then click **New Host (A or AAAA)**.
4. In the **New Host** window, in the **Name** box, type **adfs**.
5. In the **IP address** box, type **172.16.10.10**, and then click **Add Host**.
6. In the **DNS** window, click **OK**.
7. Click **Done**, and then close DNS Manager.

### ► Task 2: Create a certificate for AD FS at Trey Research

1. On **TREY-DC1**, in **Server Manager**, click **Tools**, and then click **Internet Information Services (IIS) Manager**.
2. In IIS Manager, click **TREY-DC1 (TREYRESEARCH\Administrator)**, and then double-click **Server Certificates**.
3. In the **Actions** pane, click **Create Domain Certificate**.
4. In the **Create Certificate** window, on the **Distinguished Name Properties** page, type the following information, and then click **Next**:
  - Common name: **adfs.TreyResearch.net**
  - Organization: **Trey Research**
  - Organizational unit: **IT**
  - City/locality: **London**
  - State/Province: **England**
  - Country/region: **GB**
5. On the **Online Certification Authority** page, click **Select**.
6. In the **Select Certification Authority** window, click **TreyResearchCA**, and then click **OK**.
7. On the **Online Certification Authority** page, in the **Friendly name** box, type **adfs.TreyResearch.net**, and then click **Finish**.
8. Close IIS Manager.



### ► Task 3: Install AD FS for Trey Research

1. On **TREY-DC1**, click **Start**, right-click **Windows PowerShell** and then click **Run as Administrator**.
2. At the command prompt, type the following command, and then press Enter.

```
Add-KdsRootKey -EffectiveTime ((get-date).addhours(-10))
```

This command creates the Key Distribution Service root key to generate gMSA passwords for the account that will be used later in this lab. You should receive a GUID as a response to this command.

3. Click **Start**, click **Server Manager**, click **Manage**, and then click **Add Roles and Features**.
4. In the **Add Roles and Features Wizard**, on the **Before you begin** page, click **Next**.
5. On the **Select installation type** page, click **Role-based or feature-based installation**, and then click **Next**.
6. On the **Select destination server** page, click **Select a server from the server pool**, click **TREY-DC1.TreyResearch.net**, and then click **Next**.
7. On the **Select server roles** page, select the **Active Directory Federation Services** check box, and then click **Next**.
8. On the **Select features** page, click **Next**.
9. On the **Active Directory Federation Services (AD FS)** page, click **Next**.
10. On the **Confirm installation selections** page, click **Install**.
11. When the installation completes, click **Close**.

### ► Task 4: Configure AD FS for Trey Research

1. On **TREY-DC1**, in **Server Manager**, click the **Notifications** icon, and then click **Configure the federation service on this server**.
2. In the **Active Directory Federation Services Configuration Wizard**, on the **Welcome** page, click **Create the first federation server in a federation server farm**, and then click **Next**.
3. On the **Connect to Active Directory Domain Services** page, click **Next** to use **TreyResearch\Administrator** to perform the configuration.
4. On the **Specify Service Properties** page, in the **SSL Certificate** list, select **adfs.treyresearch.net**.
5. In the **Federation Service Display Name** box, type **Trey Research**, and then click **Next**.
6. On the **Specify Service Account** page, click **Create a Group Managed Service Account**.
7. In the **Account Name** box, type **ADFSService**, and then click **Next**.
8. On the **Specify Configuration Database** page, click **Create a database on this server using Windows Internal Database**, and then click **Next**.
9. On the **Review Options** page, click **Next**.
10. On the **Pre-requisite Checks** page, click **Configure**.
11. On the **Results** page, click **Close**.

### ► Task 5: Configure a claims provider trust for the Trey Research AD FS server

1. On **LON-DC1**, in **Server Manager**, click **Tools**, and then click **AD FS Management**.
2. In the **AD FS Management** console, click **Claims Provider Trusts**.
3. In the **Actions** pane, click **Add Claims Provider Trusts**.

4. In the **Add Claims Provider Trust Wizard**, on the **Welcome** page, click **Start**.
  5. On the **Select Data Source** page, click **Import data about the claims provider published online or on a local network**.
  6. In the **Federation metadata address (host name or URL)** box, type **https://adfs.treyresearch.net**, and then click **Next**.
  7. On the **Specify Display Name** page, in the **Display name** box, type **Trey Research**, and then click **Next**.
  8. On the **Ready to Add Trust** page, review the claims provider trust settings, and then click **Next** to save the configuration.
  9. On the **Finish** page, click **Close**.
  10. In the list of **Claims Provider Trusts**, right-click **Trey Research**, and then select **Edit Claim Rules...**
  11. In the **Edit Claim Rules for Trey Research** window, on the **Acceptance Transform Rules** tab, click **Add Rule**.
  12. In the **Add Transform Claim Rule Wizard**, on the **Select Rule Template** page, in the **Claim rule template** list, select **Pass Through or Filter an Incoming Claim**, and then click **Next**.
  13. On the **Configure Rule** page, in the **Claim rule name** box, type **Pass through Windows account name**.
  14. In the **Incoming claim type** list, select **Windows account name**.
  15. Select **Pass through all claim values**, and then click **Finish**.
  16. In the **AD FS Management** dialog box, click **Yes** to acknowledge the warning.
  17. In the **Edit Claim Rules for Trey Research** window, click **OK**, and then close the **AD FS Management** console.
- **Task 6: Configure a relying party trust for the A. Datum Corporation application**
1. On **TREY-DC1**, in the **Server Manager**, click **Tools**, and then click **AD FS Management**.
  2. In the **AD FS Management** console, click **Relying Party Trusts**.
  3. In the **Actions** pane, click **Add Relying Party Trust**.
  4. In the **Add Relying Party Trust Wizard**, on the **Welcome** page, click **Start**.
  5. On the **Select Data Source** page, click **Import data about the relying party published online or on a local network**.
  6. In the **Federation metadata address (host or URL)** box, type **adfs.adatum.com**, and then click **Next**.
  7. On the **Specify Display Name** page, in the **Display name** box, type **A. Datum Corporation**, and then click **Next**.
  8. On the **Choose Access Control Policy** page, select **Permit everyone**, and then click **Next**.
  9. On the **Ready to Add Trust** page, review the relying party trust settings, and then click **Next** to save the configuration.
  10. On the **Finish** page, select the **Configure claims issuance policy for this application** check box, and then click **Close**.
  11. In the **Edit Claim Issuance Policy for A. Datum Corporation** window, on the **Issuance Transform Rules** tab, click **Add Rule**.

12. In the **Add Transform Claim Rule Wizard**, on the **Select Rule Template** page, in the **Claim rule template** box, select **Pass Through or Filter an Incoming Claim**, and then click **Next**.
13. On the **Configure Rule** page, in the **Claim rule name** box, type **Pass through Windows account name**.
14. In the **Incoming claim type** list, select **Windows account name**.
15. Click **Pass through all claim values**, click **Finish**, and then click **OK**.
16. In the **Edit Claim Issuance Policy for A. Datum Corporation** window, click **OK**.
17. Close the **AD FS Management** console.

► **Task 7: Verify access to the website**

1. On **TREY-DC1**, in Internet Explorer, open **Internet Options**, select **Privacy**, and then select **Sites**.
2. On the **Per Site Privacy Actions** page, in the **Address of website** box, type **adatum.com**, click **Allow**, click **OK** to close the **Per Site Privacy Actions** page, and then click **OK** to close the **Internet Options** window.
3. In Internet Explorer, on the address bar, type **https://lon-svr1.adatum.com/adatumtestapp/**, and then press Enter.
4. On the **A. Datum Corporation** page, click **Trey Research**.
5. In the **Windows Security** dialog box, sign in as **TreyResearch\April** with the password **Pa\$\$w0rd**.
6. After the application loads, close Internet Explorer.
7. Open **Internet Explorer**.
8. In Internet Explorer, on the address bar, type **https://lon-svr1.adatum.com/adatumtestapp/**, and then press Enter.
9. In the **Windows Security** dialog box, sign in as **TreyResearch\April** with the password **Pa\$\$w0rd**.
10. Close Internet Explorer.



**Note:** You are not prompted for a home realm on the second access. After a user selects a home realm and a realm authority authenticates that user, the relying party's federation server issues a **\_LSRealm** cookie. The default lifetime for the cookie is 30 days. Therefore, to sign in multiple times, you should delete that cookie after each sign-in attempt to return to a clean state.

► **Task 8: Configure issuance authorization claim rules to allow access for only specific groups**

1. On **TREY-DC1**, in **Server Manager**, click **Tools**, and then click **AD FS Management**.
2. In the **AD FS Management** console, click **Relying Party Trusts**.
3. Right-click **A. Datum Corporation**, and then click **Edit Claim Issuance Policy**.
4. In the **Edit Claim Issuance Policy for A. Datum Corporation** window, on the **Issuance Transform Rules** tab, click **Remove Rule**, and then click **Yes**.
5. Click **Add Rule**.
6. In the **Claim rule template** box, select **Pass Through or Filter an Incoming Claim** and then click **Next**.

7. On the **Claim rule name** box, type **Allow Production Members**.
8. On the **Incoming claim type**, select **Group**.
9. Click **Pass through only a specific claim value**, and then in the Incoming claim value, type **TreyResearch-Production**.
10. Click **Finish** and then click **OK**.
11. In the **AD FS Management** console, click **Claims Provider Trusts**, right-click **Active Directory**, and then click **Edit Claim Rules**.
12. In the **Edit Claim Rules for Active Directory** window, click **Add Rule**.
13. In the **Add Transform Claim Rule Wizard**, on the **Select Rule Template** page, in the **Claim rule template** box, select **Send Group Membership as a Claim**, and then click **Next**.
14. On the **Configure Rule** page, in the **Claim rule name** box, type **Production Group Claim**.
15. To set the **User's group**, click **Browse**, type **Production**, and then click **OK**.
16. In the **Outgoing claim type** box, select **Group**.
17. In the **Outgoing claim value** box, type **TreyResearch-Production**, and then click **Finish**.
18. In the **Edit Claim Rules for Active Directory** window, click **OK**.
19. Close the **AD FS Management** console.

► **Task 9: Verify access to the website with the group restrictions**

1. On **TREY-DC1**, in Internet Explorer, open **Internet Options**, select **Privacy**, and then select **Sites**.
2. On the **Per Site Privacy Actions** page, in the **Address of website** box, type **adatum.com**, click **Allow**, click **OK** to close the **Per Site Privacy Actions** page, and then click **OK** to close the **Internet Options** window.
3. In Internet Explorer, on the address bar, type **https://lon-svr1.adatum.com/adatumtestapp/**.
4. In the **Windows Security** dialog box, sign in as **TreyResearch\Ben** with the password **Pa\$\$w0rd**.
5. Verify that you can access the application because Ben is a member of the **TreyResearch\Production** group.
6. Close Internet Explorer.

**Results:** After completing this exercise, you should have successfully configured access for a claims-aware application in a partner organization.

► **Task 10: Prepare for the next module**

When you finish the lab, revert the VMs to their initial state. To do this, complete the following steps:

1. On the host computer, start **Hyper-V Manager**.
2. In the **Virtual Machines** list, right-click **20742A-LON-DC1**, and then click **Revert**.
3. In the **Revert Virtual Machine** dialog box, click **Revert**.
4. Repeat steps 2 and 3 for **20742A-LON-DC2**, **20742A-LON-SVR1**, **20742A-TREY-DC1**, and **20742A-LON-CL1**.

# Module 11: Implementing and administering AD RMS

## Lab: Implementing an AD RMS infrastructure

### Exercise 1: Installing and configuring AD RMS

#### ► Task 1: Configure DNS and the AD RMS service account

1. Sign in to **LON-DC1** as **Adatum\Administrator** with the password **Pa\$\$w0rd**.
2. In **Server Manager**, click **Tools**, and then click **Active Directory Administrative Center**.
3. Select and then right-click **Adatum (local)**, click **New**, and then click **Organizational Unit**.
4. In the **Create Organizational Unit** dialog box, in the **Name** box, type **Service Accounts**, and then click **OK**.
5. Right-click the **Service Accounts** organizational unit (OU), click **New**, and then click **User**.
6. In the **Create User** dialog box, provide the following details, and then click **OK**:
  - First name: **ADRMSSVC**
  - User UPN logon: **ADRMSSVC**
  - User SamAccountName Logon: **Adatum\ADRMSSVC**
  - Password: **Pa\$\$w0rd**
  - Confirm Password: **Pa\$\$w0rd**
  - Password never expires: **Enabled** (you should click on Other password options to be able to select this)
  - User cannot change password: **Enabled**
7. Right-click the **Users** container, click **New**, and then click **Group**.
8. In the **Create Group** dialog box, type the following details, and then click **OK**:
  - Group name: **ADRMS\_SuperUsers**
  - E-mail: **ADRMS\_SuperUsers@adatum.com**
9. Right-click the **Users** container, click **New**, and then click **Group**.
10. In the **Create Group** dialog box, type the following details, and then click **OK**:
  - Group name: **Executives**
  - E-mail: **executives@adatum.com**
11. Double-click the **Managers** OU, and then Ctrl+click the following users:
  - **Aidan Norman**
  - **Holly Spencer**
12. In the **Tasks** pane, click **Add to group**.
13. In the **Select Groups** dialog box, type **Executives**, and then click **OK**.
14. Close the **Active Directory Administrative Center**.
15. In **Server Manager**, click **Tools**, and then click **DNS**.

16. In the **DNS Manager** console, expand **LON-DC1**, and then expand **Forward Lookup Zones**.
17. Select and then right-click **Adatum.com**, and then click **New Host (A or AAAA)**.
18. In the **New Host** dialog box, type the following information, and then click **Add Host**:
  - o Name: **adrms**
  - o IP address: **172.16.0.21**
19. Click **OK**, and then click **Done**.



**Note:** This is the address of **LON-SVR1**, where you will install AD RMS.

20. Close the **DNS Manager** console.

► **Task 2: Install and configure the AD RMS server role**


1. Sign in to **LON-SVR1** as **Adatum\Administrator** with the password **Pa\$\$w0rd**.
2. Click **Start**, click **Server Manager**, click **Manage**, and then click **Add Roles and Features**.
3. In the **Add Roles and Features Wizard**, click **Next** three times.
4. On the **Select server roles** page, click **Active Directory Rights Management Services**.
5. In the **Add Roles and Features Wizard** dialog box, click **Add Features**, click **Next** six times, click **Install**, and then when the installation completes, click **Close**.
6. In **Server Manager**, click the **AD RMS** node.
7. Next to **Configuration required for Active Directory Rights Management Services at LON-SVR1**, click **More**.
8. On the **All Servers Task Details and Notifications** page, click **Perform additional configuration**.
9. On the **AD RMS** page, in the **AD RMS Configuration: LON-SVR1.adatum.com** window, click **Next**.
10. On the **AD RMS Cluster** page, click **Create a new AD RMS root cluster**, and then click **Next**.
11. On the **Configuration Database** page, click **Use Windows Internal Database on this server**, and then click **Next**.
12. On the **Service Account** page, click **Specify**.
13. In the **Windows Security** dialog box, type the following details, click **OK**, and then click **Next**:
  - o User name: **ADRMSSVC**
  - o Password: **Pa\$\$w0rd**




**Note:** If you get an error when you try to use the ADRMSSVC service account, force replication between **LON-DC1** and **LON-DC2**, and then try the step again.

14. On the **Cryptographic Mode** page, click **Cryptographic Mode 2**, and then click **Next**.
15. On the **Cluster Key Storage** page, click **Use AD RMS centrally managed key storage**, and then click **Next**.
16. On the **Cluster Key Password** page, type **Pa\$\$w0rd** twice, and then click **Next**.
17. On the **Cluster Web Site** page, verify that **Default Web Site** is selected, and then click **Next**.


18. On the **Cluster Address** page, provide the following information, and then click **Next**:
  - o Connection Type: **Use an unencrypted connection (http://)**
  - o Fully Qualified Domain Name: **adrms.adatum.com**
  - o Port: **80**

 **Note:** This lab uses port 80 for convenience. In production environments, you would help to protect Active Directory Rights Management Services (AD RMS) by using an encrypted connection.

19. On the **Licensor Certificate** page, type **AdatumADRMS**, and then click **Next**.
20. On the **SCP Registration** page, click **Register the SCP now**, and then click **Next**.
21. On the **Confirmation** page, click **Install**, and then click **Close**.
22. In **Server Manager**, click **Tools**, and then click **Internet Information Services (IIS) Manager**.
23. In the **Internet Information Services (IIS) Manager** console, expand **LON-SVR1\Sites\Default Web Site**, and then click **\_wmcs**.
24. Under the **/\_wmcs** node, double-click **Authentication**, click **Anonymous Authentication**, and then in the **Actions** pane, click **Enable**.
25. In the **Connections** pane, expand **\_wmcs**, and then click **licensing**.
26. Under the **/\_wmcs/licensing** node, double-click **Authentication**, click **Anonymous Authentication**, and then in the **Actions** pane, click **Enable**.

 **Note:** You will not enable Anonymous Authentication in a production environment. This is just to make the configuration easier in the lab.

27. On the Start screen, click **Administrator**, and then click **Sign Out**.

 **Note:** You must sign out before you can manage AD RMS.

### ► Task 3: Configure the AD RMS Super Users group

1. Sign in to **LON-SVR1** as **Adatum\Administrator** with the password **Pa\$\$w0rd**.
2. Open **Server Manager**, click **Tools**, and then click **Active Directory Rights Management Services**.
3. In the **AD RMS** console, expand the **lon-svr1 (Local)** node, and then click **Security Policies**.
4. In the **Security Policies** area, under **Super Users**, click **Change super user settings**.
5. In the **Actions** pane, click **Enable Super Users**.
6. In the **Super Users** area, click **Change super user group**.
7. In the **Super Users** dialog box, in the **Super user group** box, type **ADRMS\_SuperUsers@adatum.com**, and then click **OK**.

**Results:** After completing this exercise, you should have installed and configured AD RMS.

## Exercise 2: Configuring AD RMS templates

### ► Task 1: Configure a new rights policy template

1. Ensure that you are signed in to **LON-SVR1**.
2. In the **AD RMS** console, click the **Rights Policy Templates** node.
3. In the **Actions** pane, click **Create Distributed Rights Policy Template**.
4. In the **Create Distributed Rights Policy Template Wizard**, on the **Add Template Identification information** page, click **Add**.
5. On the **Add New Template Identification Information** page, provide the following information, click **Add**, and then click **Next**:
  - Language: **English (United States)**
  - Name: **ReadOnly**
  - Description: **Read-only access. No copy or print.**
6. On the **Add User Rights** page, click **Add**.
7. On the **Add User or Group** page, type **executives@adatum.com**, and then click **OK**.
8. When **executives@adatum.com** is selected, under **Rights**, click **View**. Verify that **Grant owner (author) full control right with no expiration** is selected, and then click **Next**.
9. On the **Specify Expiration Policy** page, select the following settings, and then click **Next**:
  - Content Expiration: **Expires after the following duration (days): 7**
  - Use license expiration: **Expires after the following duration (days): 7**
10. On the **Specify Extended Policy** page, click **Require a new use license every time content is consumed (disable client-side caching)**, and then click **Next**.
11. On the **Specify Revocation Policy** page, click **Finish**.

### ► Task 2: Configure the rights policy template distribution

1. On **LON-SVR1**, click **Start** and then click **Windows PowerShell**.
2. At the Windows PowerShell command prompt, type the following command, and then press Enter:

```
New-Item c:\rmstemplates -ItemType Directory
```
3. At the Windows PowerShell command prompt, type the following command, and then press Enter:

```
New-SmbShare -Name RMSTEMPLATES -Path c:\rmstemplates -FullAccess ADATUM\ADRMSSVC
```
4. At the Windows PowerShell command prompt, type the following command, and then press Enter:

```
New-Item c:\docshare -ItemType Directory
```
5. At the Windows PowerShell command prompt, type the following command, and then press Enter:

```
New-SmbShare -Name docshare -Path c:\docshare -FullAccess Everyone
```
6. Type **exit**, and then press Enter to exit Windows PowerShell.
7. Switch to the **AD RMS** console, click the **Rights Policy Templates** node, and then in the **Distributed Rights Policy Templates** area, click **Change distributed rights policy templates file location**.



8. In the **Rights Policy Templates** dialog box, click **Enable export**.
9. In the **Specify templates file location (UNC)** box, type `\\LON-SVR1\RMSTEMPLATES`, and then click **OK**.
10. On the taskbar, click **File Explorer**.
11. Navigate to the **C:\rmstemplates** folder, and then verify that **ReadOnly.xml** is present.
12. Close the **File Explorer** window.

► **Task 3: Configure an exclusion policy**

1. On **LON-SVR1**, switch to the **AD RMS** console, click the **Exclusion Policies** node, and then click **Manage application exclusion list**.
2. In the **Actions** pane, click **Enable Application Exclusion**.
3. In the **Actions** pane, click **Exclude Application**.
4. In the **Exclude Application** dialog box, type the following information, and then click **Finish**:
  - Application File name: **Powerpnt.exe**
  - Minimum version: **14.0.0.0**
  - Maximum version: **16.0.0.0**
5. Close the **AD RMS** console.

**Results:** After completing this exercise, you should have configured AD RMS templates.

### Exercise 3: Using AD RMS on clients

► **Task 1: Create a rights-protected document**

1. Sign in to **LON-CL1** as **Adatum\Aidan** with the password **Pa\$\$w0rd**.
2. Click **Start**, type **Internet**, and then click **Internet Explorer**. In the **Internet Explorer** window, right-click the toolbar, click **Menu bar**, click **Tools**, and then select **Internet options**.
3. In the **Internet options** dialog box, click **Security**, click **Local intranet**, click **Sites**, click **Advanced**, and then under **Add this website to the zone**, type `http://adrms.adatum.com`. Click **Add**, click **Close**, and then click **OK** two times.

 **Note:** Note that you added adrms.adatum.com to the local intranet sites to achieve a single sign on experience when signing in to the AD RMS servers.

4. Close Internet Explorer.
5. On the **Start** menu, type **Word**, and then in the results area, click **Word 2016**. If the **First things first** window appears, click **Ask me later**, and then click **Accept**. If the **Welcome to your new Office** window appears, close it.
6. In the Microsoft Word 2016 app, click **Blank document**.
7. In the Word document, type the following text: **This document is for executives only, and it should not be modified**. Click **File**, click **Protect Document**, click **Restrict Access**, and then click **Read Only**.



**Note:** If the **ReadOnly** template does not appear, you might need to first click **Connect to Rights Management Servers and get templates**.

8. Click **Save**, and then click **Browse**.
9. In the **Save As** dialog box, save the document to the **\\lon-svr1\docshare** location with the name **Executives Only.docx**.
10. Close Word 2016.
11. Click the **Start** menu, click the **Aidan Norman** icon, and then click **Sign out**.

► **Task 2: Verify internal access to AD RMS–protected content as an authorized user**

1. Sign in to **LON-CL1** as **Adatum\Holly** with the password **Pa\$\$w0rd**.
2. Click **Start**, type **Internet**, and then click **Internet Explorer**. In the **Internet Explorer** window, right-click the toolbar, click **Menu bar**, click **Tools**, and then select **Internet options**.
3. In **Internet options**, click **Security**, click **Local intranet**, click **Sites**, click **Advanced**, and then under **Add this website to the zone**, type **http://adrms.adatum.com**. Click **Add**, click **Close**, and then click **OK** twice.
4. Close Internet Explorer.
5. On the taskbar, click the **File Explorer** icon.
6. In the **File Explorer** window, navigate to **\\lon-svr1\docshare**.
7. In the **docshare** folder, double-click the **Executives Only** document.
8. When the document opens, verify that you are unable to modify or save the document. If the **First things first** window appears in Word, click **Ask me later**, and then click **Accept**. If the **Welcome to your new Office** window appears, close it.
9. Select a line of text in the document, right-click it, and then verify that you cannot make changes.
10. Click **View Permission**, review the permissions, and then click **OK**. You can see that Holly has only the View permission. She is a member of the Executives group and can access the content.
11. Close Word 2016.
12. Click the Start screen, click the **Holly Spencer** icon, and then click **Sign Out**.

► **Task 3: Open the rights-protected document as an unauthorized user**

1. Sign in to **LON-CL1** as **Adatum\Harry** with the password **Pa\$\$w0rd**.
2. Click **Start**, type **Internet** and then click **Internet Explorer**. In the **Internet Explorer** window, right-click the toolbar, click **Menu bar**, click **Tools**, and then select **Internet options**.
3. In **Internet options**, click **Security**, click **Local intranet**, click **Sites**, click **Advanced**, and then under **Add this website to the zone**, type **http://adrms.adatum.com**. Click **Add**, click **Close**, and then click **OK** twice.
4. Close Internet Explorer.
5. On the taskbar, click the **File Explorer** icon.
6. In the **File Explorer** window, navigate to **\\lon-svr1\docshare**.
7. In the **docshare** folder, double-click the **Executives Only** document, and then click **OK** in the **Microsoft Office** window.

8. Verify that Harry is unable to open the document. Note that Harry cannot open the document because the document is protected with an RMS template that allows only the Executives group to view the document. Click **OK** in the **Microsoft Word** window.
9. Close Word 2016.
10. Click the Start screen, click the **Harry Lawrence** icon, and then click **Sign Out**.

► **Task 4: Prepare for the next module**

When you finish the lab, revert the VMs to their initial state. To do this, complete the following steps:

1. On the host computer, start **Hyper-V Manager**.
2. In the **Virtual Machines** list, right-click **20742A-LON-DC1**, and then click **Revert**.
3. In the **Revert Virtual Machine** dialog box, click **Revert**.
4. Repeat steps 2 and 3 for **20742A-LON-SVR1**, **20742A-LON-DC2**, and **20742A-LON-CL1**.

**Results:** After completing this exercise, you should have verified that the AD RMS deployment was successful.

**MCT USE ONLY. STUDENT USE PROHIBITED**

## Module 12: Implementing AD DS synchronization with Microsoft Azure AD

# Lab: Configuring directory synchronization

### Exercise 1: Preparing for directory synchronization

#### ► Task 1: Create a Microsoft account

Further tasks in this exercise require that you have an active Microsoft account without a Microsoft Azure subscription assigned to it. If you do not want to use your private Microsoft account, if you do not have one, or if you already have an Azure subscription, please follow the steps in this task to create a new Microsoft account.

1. On **LON-CL1**, click **Start**, click **All Apps**, expand **Windows Accessories**, and then click the **Internet Explorer** icon.
2. In the address bar, type **www.live.com** and then press Enter.
3. At the bottom of the page, look for the **"No account?"** text, and then click the **Create one!** link.
4. On the **Create an account** page, fill in the required fields with appropriate data. In the **User name** text box, type a new email address in the Outlook.com domain.



**Note:** Make sure that you write down the user name that you chose. For example, you can choose a user name in the *YourInitials-Date@outlook.com* format, such as *DJ-060815@outlook.com*. Use **Pa\$\$wOrd1** as the password. We recommend that you type your working email address in the **Alternate email address** text box.

5. After you fill out all the fields, at the bottom of the page, click **Create account**.
6. Ensure that your Outlook.com inbox opens in a web browser window.
7. If the **Welcome to your new inbox** page appears, click **Continue to inbox**.
8. If the **Same Address, Smarter Inbox** window appears, click the **Close** icon to show the inbox.
9. When you are finished, close Internet Explorer.

#### ► Task 2: Create a trial Azure subscription

1. On **LON-CL1**, open **Internet Explorer**.
2. In the address bar, type **http://aka.ms/cu92vo**, and then press Enter.
3. When the page opens, select your country/region from the drop-down list, type the voucher code that you received from your instructor, and then click **Submit**. If your country/region is not listed, select **United States**.
4. On the next page, click **Sign in**.
5. On the **Azure Pass** page, sign in with your Microsoft account that you created in the previous task.



**Note:** You can choose to use your personal Microsoft account or the one created earlier in the lab. The **Sign-in** page might not ask for a password if you still have a tab with your Microsoft account inbox open.

6. On the **Microsoft Azure** page, verify your details, and then click **Submit**.
7. On the **Azure Pass** page, click **Activate**. A new tab will open in Internet Explorer browser.
8. On the **Sign up** page, fill out your contact phone number, click **I agree to the subscription agreement, offer details, and privacy statement**, and then click **Sign up**.
9. Wait for a few minutes until your Azure subscription has been created.
10. Click **Start managing my service**, and then verify that a new Azure classic portal opens. You can click through the portal to see available options, but do not make any changes.
11. Close the browser window.

► **Task 3: Create an Azure AD tenant**

1. On **LON-CL1**, open **Internet Explorer**, and then browse to **https://manage.windowsazure.com**.
2. If prompted, on the **Microsoft Azure** page, type the Microsoft account that is associated with your Azure subscription (the same account that you used to create your Azure trial subscription in the previous task), and then click **Continue**.
3. On the **Sign-in** page, sign in with the Microsoft account that is associated with your Azure subscription.
4. If the **WINDOWS AZURE TOUR** page appears, close it. If **The new Azure Portal is here!** window appears, close it.
5. In the left navigation pane, click **ACTIVE DIRECTORY**, click **NEW**, click **DIRECTORY**, and then click **CUSTOM CREATE**.
6. In the **Add directory** dialog box, configure the following settings, and then click **Complete** (the check mark icon):
  - **DIRECTORY:** **Create new directory**
  - **NAME:** **Adatum**
  - **DOMAIN NAME:** Use your initials, with Adatum and random numbers (for example, "DDAdatum111") to create domain name; if you receive an **Already in use by another directory** message, change the numbers until you receive a green check mark.



**Note:** From this point, through the course, you should use this name when you see *yourdomainname* variable in the labs.

- **COUNTRY OR REGION:** **United States**
7. Leave the Azure classic portal open and wait until a new directory instance is created.

**Results:** After completing this exercise, you should have created the Azure AD tenant.

## Exercise 2: Configuring directory synchronization

### ► Task 1: Configure synchronization account and add domain to Azure

1. On your host machine, on the Start screen, click **Internet Explorer**.
2. In the address bar, type **https://manage.windowsazure.com**, and then press Enter.
3. On the **Microsoft Azure** page, click **Use another account**.
4. On the **Microsoft Azure** page, type your Microsoft account that is associated with your Azure subscription, and then click **Continue**.
5. Sign in to Azure by using the Microsoft account that is associated with your trial subscription. This is the account that you used in Exercise 1 to create your Azure subscription.
6. In the Azure classic portal, click the **Adatum** directory instance.
7. Click the **USERS** tab, and then click **ADD USER**.
8. In the **TYPE OF USER** list, click **New user in your organization**.
9. In the **USER NAME** text box, type **Sync**.



**Note:** Make a note of the complete user name. This is the **USER NAME** plus the suffix shown to the right of the at sign (@), such as *Sync@yourdomain.onmicrosoft.com*.

10. Click **Next**.
11. On the **user profile** page, in the **DISPLAY NAME** text box, type **SYNC**.
12. In the **ROLE** list, click **Global Admin**.
13. In the **ALTERNATE EMAIL ADDRESS** text box, type your own email address, and then click **Next**.
14. Click **create**.
15. Make a note of the temporary password that is displayed.
16. Click **Complete**.
17. Close Internet Explorer, and then reopen it.
18. In the address bar, type **https://manage.windowsazure.com**, and then press Enter.
19. Click **Use another account**.
20. Type the user name for the **SYNC** user that you recorded earlier. It will be **SYNC@yourdomain.onmicrosoft.com**. Click **Continue**.
21. Type the temporary password that you noted when creating your synchronization account, and then click **Sign in**.
22. When prompted, type your old password, which you typed in step 21, in the **Old password** text box, in the **New password** and **Confirm password** text boxes, type **Pa\$\$w0rd**, and then click **Update password and sign in**.
23. If prompted to sign in to the portal again, use the **SYNC** account credentials and the password **Pa\$\$w0rd**. You will receive a message the there are no subscriptions found.
24. Close and reopen Internet Explorer.
25. In the address bar, type **https://manage.windowsazure.com**, and then press Enter.

26. Sign in to Azure by using the account that is associated with your trial subscription. The account should be on the list.
27. In the Azure classic portal, click **Adatum**. The **GET STARTED** page loads.
28. Click **Add domain**.
29. In the **ADD DOMAIN** wizard, in the **DOMAIN NAME** text box, type **Adatum.com**, click **add**, and then click **Next**.
30. On the **Verify Adatum.com** page, click **Complete** (the **check mark** icon).
31. Minimize the **Internet Explorer** window.

### ► Task 2: Install and configure Azure AD Connect

1. On **LON-SVR1**, sign in as **Adatum\Administrator**.
2. Open **Internet Explorer**, and then browse to **http://www.microsoft.com/en-us/download/details.aspx?id=47594**.
3. On the **Microsoft Azure Active Directory Connect** page, click **Download**, and then click **Run**.



**Note:** If you experience any problems with starting the download, add the **https://download.microsoft.com** website to your **Trusted** sites.

4. In **Microsoft Azure Active Directory Connect Wizard**, on the **Welcome to Azure AD Connect** page, select the **I agree to the license terms and privacy notice** check box, and then click **Continue**.
5. On the **Express Settings** page, click **Use express settings**.
6. On the **Connect to Azure AD** page, in the **USERNAME** text box, type the **SYNC** account user name. In the **PASSWORD** text box, type **Pa\$\$w0rd**, and then click **Next**.
7. On the **Connect to AD DS** page, in the **USERNAME** text box, type **Adatum\administrator**. In the **PASSWORD** box, type **Pa\$\$w0rd**, and then click **Next**.
8. On the **Azure AD sign-in configuration** page, select the check box next to **Continue without any verified domains**, and then click **Next**.
9. Click **Install**, and when installation is complete, click **Exit**.
10. At this time, synchronization of objects from your local Active Directory Domain Services (AD DS) and Microsoft Azure Active Directory (Azure AD) begins. You must wait approximately 10 minutes for this process to complete.
11. Close the Internet Explorer window on **LON-SVR1**.

### ► Task 3: Verify the initial synchronization and manage settings

1. Switch to **Internet Explorer** on your host machine. You should have the Azure classic portal open.
2. On the **directory** page, click the **USERS** tab.
3. Verify that you can see the user accounts from your local AD DS. You should be able to see all users from your local adatum.com domain.
4. On **LON-SVR1**, click **Start**, and then click **All Apps**. Expand **Azure AD Connect**, and then click **Synchronization Service**.
5. In the **Synchronization Service Manager on LON-SVR1** window, click the **Operations** tab.



6. Ensure that you see the **Export, Full Synchronization**, and **Full Import** tasks.
7. Ensure that all the tasks have a current time and date in the **Start Time** and **End Time** columns. Also, ensure that all tasks have success in the **Status** column.
8. Close Synchronization Service Manager.
9. On **LON-SVR1**, open **Windows PowerShell**.
10. In the **Administrator: Windows PowerShell** window, type the following command, and then press Enter:

```
Get-ADSyncScheduler
```



**Note:** If this command returns an error, restart the **LON-SVR1** computer and repeat step 10.

11. Review the results. Ensure that the **AllowedSyncCycleInterval** value and the **CurrentlyEffectiveSyncCycleInterval** value are set to **30 minutes**.
12. In the **Administrator: Windows PowerShell** window, type the following command, and then press Enter:

```
Set-ADSyncScheduler -CustomizedSyncCycleInterval 01:00:00
```

13. In the **Administrator: Windows PowerShell** window, type the following command, and then press Enter:

```
Start-ADSyncSyncCycle -PolicyType Delta
```

14. Wait for approximately two minutes.
15. In the **Administrator: Windows PowerShell** window, type the following command, and then press Enter:

```
Get-ADSyncScheduler
```

16. Ensure that new value is applied for the **CurrentlyEffectiveSyncCycleInterval** variable.
17. Close the **Windows PowerShell** window.

**Results:** After completing this exercise, you should have installed Azure AD Connect with the customized settings, completed directory synchronization to Azure AD, and verified that the synchronization was successful.

### Exercise 3: Managing Active Directory users and groups

#### ► Task 1: Add new objects in AD DS

1. Switch to **LON-DC1**.
2. Open **Server Manager**, click **Tools**, and then click **Active Directory Users and Computers**.
3. In the navigation pane, expand **Adatum.com**, right-click **Sales**, click **New**, and then click **User**.
4. In the **New Object – User** dialog box, in the **Full name** text box, type your name.

5. In the **User logon** text box, type **your first name**, and then click **Next**.
6. In the **Password** and **Confirm password** boxes, type **Pa\$\$w0rd**, and then clear the **User must change password at next logon** check box.
7. Click **Next**, click **Finish**, and then click **Sales**.
8. Right-click your user account, and then click **Add to a group**.
9. In the **Select Groups** dialog box, in the **Enter the object names to select (examples)** text box, type **Sales**, and then click **OK**.
10. In the **Active Directory Domain Services** dialog box, click **OK**.

► **Task 2: Verify synchronization of the new user objects**

1. On **LON-SVR1**, right-click **Start**, and then click **Windows PowerShell (Admin)**.
2. In the **Administrator: Windows PowerShell** window, type the following command, and then press Enter:

```
Start-ADSyncSyncCycle -PolicyType Delta
```

3. Wait for approximately 4 minutes. Do not close the **Administrator: Windows PowerShell** window. However, you can minimize it.
4. Switch to **Internet Explorer** on your host machine, where you have the Azure classic portal open.
5. Refresh the web page, click **USERS**, and then verify the presence of the user account that you just added.
6. Click **GROUPS**, and then click **Sales**.
7. Verify that your account was also added to the **Sales** group.
8. Minimize the **Internet Explorer** window.

**Results:** After completing this exercise, you should have identified how managing user and group accounts has changed with directory synchronization.

► **Task 3: Prepare for the next module**

When you finish the lab, revert the virtual machines to their initial state. To do this, perform the following steps:

1. On the host computer, start **Hyper-V Manager**.
2. In the **Virtual Machines** list, right-click **20742A-LON-DC1**, and then click **Revert**.
3. In the **Revert Virtual Machine** dialog box, click **Revert**.
4. Repeat steps 2 and 3 to revert **20742A-LON-DC2**, **20742A-LON-SVR1**, and **20742A-LON-CL1**.

# Module 13: Monitoring, managing, and recovering AD DS

## Lab: Recovering objects in AD DS

### Exercise 1: Backing up and restoring Active Directory Domain System (AD DS)

#### ► Task 1: Install the Windows Server Backup feature

1. Switch to **LON-DC1**.
2. In Server Manager, click **Manage**, and then click **Add roles and features**.
3. In the **Add Roles and Features Wizard**, on the **Before you begin page**, click **Next**.
4. On the **Select installation type** page, click **Next**.
5. On the **Select destination server** page, click **Next**.
6. On the **Select server roles** page, click **Next**.
7. On the **Select features** page, in the **Features** list, select the **Windows Server Backup** check box, and then click **Next**.
8. On the **Confirm installation selections** page, click **Install**.
9. When the installation finishes, click **Close**.

#### ► Task 2: Create a scheduled backup

1. On **LON-DC1**, in Server Manager, click **Tools**, and then click **Windows Server Backup**.
2. In Windows Server Backup, click **Local Backup** and then click **Backup Schedule**.
3. In the **Backup Schedule Wizard**, on the **Getting Started** page, click **Next**.
4. On the **Select Backup Configuration** page, click **Custom**, and then click **Next**.
5. On the **Select Items for Backup** page, click **Add Items**.
6. In the **Select Items** dialog box, select **Bare metal recovery**, click **OK**, and then click **Next**.
7. On the **Specify Backup Time** page, click **Once a day**.
8. In the **Select time of day** list, select **12:00 am**, and then click **Next**.
9. On the **Specify Destination Type** page, click **Back up to a hard disk that is dedicated for backups (recommended)**, and then click **Next**.
10. On the **Select Destination Disk** page, click **Show All Available Disks**.
11. In the **Show All Available Disks** dialog box, select the **Disk 1** check box, and then click **OK**.
12. On the **Select Destination Disk** page, select the **Disk 1** check box, and then click **Next**.
13. When the **Windows Server Backup** dialog box appears, informing you that all data on the disk will be deleted, click **Yes** to continue.



**Note:** You will cancel the process in the next step to avoid formatting drive E.

14. On the **Confirmation** page, click **Cancel** to avoid formatting drive E.

► **Task 3: Perform an interactive backup**

1. In the **Actions** pane, click **Backup Once**.
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 Items for Backup** page, click **Add Items**.
5. In the **Select Items** dialog box, click **System state**, and then click **OK**.
6. Click **Advanced Settings**, and then click the **VSS Settings** tab.
7. Click **VSS full Backup**, click **OK**, and then click **Next**.
8. On the **Specify Destination Type** page, click **Next**.
9. On the **Select Backup Destination** page, click **Next**.
10. On the **Confirmation** page, click **Backup**, and then click **Close**.



**Note:** The backup will take about 10–15 minutes to complete. After the backup completes, close Windows Server Backup.

► **Task 4: Delete an organizational unit (OU)**



**Note:** Wait until the backup completes before proceeding.

1. On **LON-DC1**, in Server Manager, click **Tools**, and then click **Active Directory Users and Computers**.
2. On the **Menu** bar, click **View**, and then click **Advanced Features**.
3. In the console tree, expand **Adatum.com**, and then click the **Research** OU.
4. Right-click **Research**, and then click **Properties**.
5. In the **Research Properties** dialog box, on the **Object** tab, clear the **Protect object from accidental deletion** check box, and then click **OK**.
6. In the navigation pane, right-click **Research**, and then click **Delete**.
7. When a confirmation message appears, click **Yes**.
8. When a warning message appears, click **Yes**.
9. Wait for the deletion to complete.
10. Verify that the Research OU was deleted.

**► Task 5: Restart in Directory Services Restore Mode (DSRM)**

1. On **LON-DC1**, click **Start**, right-click **Windows PowerShell**, and then click **Run as Administrator**.
2. In the Windows PowerShell command-line interface, at the command prompt, type the following command, and then press Enter:

```
bcdedit /set safeboot dsrepair
```

3. At the command prompt, type the following command, and then press Enter:

```
shutdown /t 0 /r
```

**► Task 6: Restore System state data**

1. Sign in to **LON-DC1** as **.\Administrator** with the password **Pa\$\$w0rd**.
2. Click **Start**, right-click **Windows PowerShell**, click **More**, and then click **Run as Administrator**.
3. At the Windows PowerShell command prompt, type the following command, and then press Enter:

```
wbadmin get versions -backuptarget:E: -machine:LON-DC1
```

4. Note the version identifier that is returned.
5. At the command prompt, type the following command, where *version* is the number that you recorded in the previous step, and then press Enter:

```
wbadmin start systemstaterecovery -version:<version> -backuptarget:E: -machine:LON-DC1
```

For example:

```
wbadmin start systemstaterecovery -version:01/22/2011-10:37 -backuptarget:E: -  
machine:LON-DC1
```

6. Type **Y**, and then press Enter.
7. Type **Y**, and then press Enter.



**Note:** The restoration will take about 30–35 minutes. Depending on the host machine, it could take up to an hour.

8. When prompted to restart, type **Y**, and then press Enter.

**► Task 7: Mark restored information as authoritative**

1. Sign in to **LON-DC1** as **.\Administrator** with the password **Pa\$\$w0rd**.
2. When prompted press Enter.
3. Click **Start**, right-click **Windows PowerShell**, point to **More**, and then click **Run as administrator**.
4. At the Windows PowerShell command prompt, type the following command, and then press Enter:

```
NtdsUtil.exe
```

5. At the command prompt, type the following command, and then press Enter:

```
activate instance ntds
```

- At the command prompt, type the following command, and then press Enter:

```
authoritative restore
```

- At the command prompt, type the following command, and then press Enter:

```
restore subtree "ou=Research,dc=adatum,dc=com"
```

- In the confirmation dialog message box that displays, click **Yes**.
- Type **quit**, and then press Enter.
- Type **quit**, and then press Enter.

- At the command prompt, type the following command, and then press Enter:

```
bcdedit /deletevalue safeboot
```

- At the command prompt, type the following command, and then press Enter:

```
shutdown /t 0 /r
```

#### ► Task 8: Verify that the data has been restored

- Wait for **LON-DC1** to restart.
- Sign in to **LON-DC1** as **Adatum\Administrator** with the password **Pa\$\$w0rd**.
- In Server Manager, from the **Tools** menu, click **Active Directory Users and Computers**.
- In the console tree, expand **Adatum.com**, and then verify that the **Research** OU is restored. Note that you may have to force a site replication in Active Directory Sites and Services to see the change immediately.

**Results:** After completing this exercise, you should have performed an interactive backup and an authoritative restore of AD DS successfully.

## Exercise 2: Recovering objects in AD DS

### ► Task 1: Verify requirements for Active Directory Recycle Bin

- On **LON-DC1**, in Server Manager, click **Tools**, and then click **Active Directory Domains and Trusts**.
- In the Active Directory Domains and Trusts console, right-click **Active Directory Domains and Trusts**, and then click **Raise Forest Functional Level**.
- Confirm that the value of **Current forest functional level** is Windows Server 2012 R2, and then click **Cancel**.
- Close the Active Directory Domains and Trust console.

### ► Task 2: Enable the Active Directory Recycle Bin feature

- On **LON-DC1**, in Server Manager, click **Tools**, and then click **Active Directory Sites and Services**.
- Expand **Sites**, expand **Default-First-Site-Name**, expand **Servers**, expand **LON-DC1**, and then click **NTDS Settings**.
- Right-click **<automatically generated>**, click **Replicate Now**, and then click **OK**.

4. Expand **LON-DC2**, and then click **NTDS Settings**.
5. Right-click **<automatically generated>**, click **Replicate Now**, and then click **OK**.
6. In Server Manager, click **Tools**, and then click **Active Directory Module for Windows PowerShell**.
7. At the command prompt, type the following command, and then press Enter:

```
Enable-ADOptionalFeature -Identity 'CN=Recycle Bin Feature,CN=Optional
Features,CN=Directory Service,CN=Windows NT,CN=Services,CN=Configuration,
DC=adatum,DC=com' -Scope ForestOrConfigurationSet -Target 'adatum.com'
```

8. Type **y**, and then press Enter.
9. After the command prompt is returned to you, close the **Windows PowerShell** window.
10. Repeat steps 1-5 to re-sync the domain.

### ► Task 3: Delete objects to simulate accidental deletion

1. In Server Manager, click **Tools**, and then click **Active Directory Users and Computers**.
2. Navigate to the **Sales** OU.
3. Right-click **Abbie Parsons**, and then click **Delete**.
4. In the confirmation window, click **Yes**.
5. Close Active Directory Users and Computers.

### ► Task 4: Perform object restoration with the Active Directory Module for Windows PowerShell

1. In Server Manager, click **Tools**, and then click **Active Directory Module for Windows PowerShell**.
2. Type the following command, and then press Enter:

```
Get-ADObject -Filter {displayName -eq "Abbie Parsons"} -IncludeDeletedObjects |
Restore-ADObject
```

3. Close the **Windows PowerShell** window.

### ► Task 5: Verify object restoration

1. On **LON-DC1**, in Server Manager, click **Tools**, and then click **Active Directory Users and Computers**.
2. Make sure that **Abbie Parsons** exists within the **Sales** OU.

**Results:** After completing the exercise, you should have enabled and tested the Active Directory Recycle Bin feature successfully.

### ► Task 6: Prepare for the end of the course

When you finish the lab, revert the virtual machines to their initial state. To do this, perform the following steps:

1. On the host computer, start **Hyper-V Manager**.
2. In the **Virtual Machines** list, right-click **20742A-LON-DC1**, and then click **Revert**.
3. In the **Revert Virtual Machine** dialog box, click **Revert**.
4. Repeat steps 2 and 3 to revert **20742A-LON-DC2**.

**MCT USE ONLY. STUDENT USE PROHIBITED**