Microsoft

OFFICIAL MICROSOFT LEARNING PRODUCT

20740A

Installation, Storage, and Compute with Windows Server 2016

Product Number: 20740A

Part Number: X21-18463

Released: 09/2016

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 tent that Microsoft, not the third party, licenses to you under this agreement. Notices, if any, for the third party code ntent 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.

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 dues consommateurs, que ce contrat ne peut modifier. La ou elles sont permises par le droit locale, 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[1]. Ask your instructor about Microsoft Certification exam promotions and discounts that may be available to you.

- **Customer Satisfaction Guarantee**—Our Certified Partners for Learning Solutions offer a satisfaction guarantee and we hold them accountable for it. At the end of class, please complete an evaluation of today's experience. We value your feedback!

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

Sincerely,

Microsoft Learning
www.microsoft.com/learning

Microsoft | Learning

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

Acknowledgments

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

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, and holds an MBA in finance. Prior to starting his own company, Jason worked for almost 20 years at Microsoft in almost every product team, including Microsoft Official Curriculum (MOC), Windows client and Windows Server, Microsoft SQL Server, and the Microsoft 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.

Andrew J. Warren – Content Developer

Andrew Warren has more than 25 years of experience in the information technology (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 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.

Byron Wright – Content Developer

Byron Wright is a partner in a consulting firm where he performs network consulting, computer-systems implementation, and technical training. Byron also is a sessional instructor for the Asper School of Business at the University of Manitoba, where he teaches management information systems and networking. Byron has authored and coauthored a number of books on Windows Server and Windows client operating systems, and Exchange Server, including the *Windows Server 2008 Active Directory Resource Kit*. To recognize Byron's commitment to sharing knowledge with the technical community, he has been awarded the Microsoft Most Valuable Professional (MVP) Award for Exchange Server.

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 Domain Services (AD DS), Exchange Server, Microsoft Lync Server, identity management, and Microsoft 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.

Vladimir Meloski – Content Developer

Vladimir Meloski, a Microsoft Certified Trainer (MCT) and MVP on Microsoft Office Servers and Services, is a consultant who provides solutions for unified communications and infrastructures based on Exchange Server, Skype for Business, Office 365, and Windows Server. Vladimir has 20 years of professional IT experience, and has been involved in Microsoft conferences in Europe and the United States as a speaker, moderator, proctor for hands-on labs, and as a technical expert. He also has been involved as a Subject Matter Expert and technical reviewer for MOC courses on Exchange Server, Office 365, and Windows Server.

Joshua Shackelford – Content Developer

Joshua Shackelford has more than 12 years of experience in the IT industry as an engineer, architect, consultant, and administrator. Joshua has extensive experience consulting on the Microsoft System Center suite of products, Hyper-V, and AD DS. His clients include large energy corporations, financial institutions, and retail organizations. Joshua has been involved as a Subject Matter Expert on Windows Server, Hyper-V, and failover clustering.

Dave Franklyn – Content Developer

David M. Franklyn, Microsoft Certified Solutions Expert (MCSE), Microsoft Certified IT Professional (MCITP), Microsoft MVP Windows and Devices for IT, is also an Eastern USA Regional Lead MCT. Dave has been a Microsoft MVP since 2011, and a Senior Information Technology Trainer and Consultant at Auburn University in Montgomery Alabama, since 1998. He is the owner of DaveMCT, Inc. LLC, and is a training partner with Dunn Training. Working with computers since 1976, Dave started out in the mainframe world and moved early into the networking arena. Before joining Auburn University, Dave spent 22 years in the United States Air Force as an electronic communications and computer systems specialist, retiring in 1998. Dave is president of the Montgomery Windows IT Professional Group, and a guest speaker at many events involving Microsoft products.

David Susemiehl – Content Developer

David Susemiehl has worked as consultant, trainer, and courseware developer since 1996. David has extensive experience consulting on Microsoft Systems Management Server, System Center Configuration Manager 2007, AD DS, Exchange Server, and Terminal Server/Citrix deployments. David has developed courseware development for Microsoft and Hewlett-Packard, and has delivered those courses successfully in Europe, Central America, and across North America. For the last several years, David has been writing courseware for Microsoft Learning, and consulting on infrastructure transitions in Michigan.

Contents

Lab Answer Keys

About This Course

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

Course Description

This five-day course is designed primarily for information technology (IT) professionals who have some experience with Windows Server. It is designed for professionals who will be responsible for managing storage and compute by using Windows Server 2016, and who need to understand the scenarios, requirements, and storage and compute options that are available and applicable to Windows Server 2016.

Audience

This course is intended for IT professionals who have some experiencing working with Windows Server, and who are looking for a single five-day course that covers storage and compute technologies in Windows Server 2016. This course will help them update their knowledge and skills related to storage and compute for Windows Server 2016.

Candidates suitable for this course would be:

- Windows Server administrators who are relatively new to Windows Server administration and related technologies, and who want to learn more about the storage and compute features in Windows Server 2016.
- IT professionals with general IT knowledge who are looking to gain knowledge about Windows Server, especially around storage and compute technologies in Windows Server 2016.

The secondary audience for this course is IT professionals looking to take the Microsoft 70-740 certification exam, Installation, Storage and Compute with Windows Server 2016.

Student Prerequisites

Before attending this course, students must have:

- A basic understanding of networking fundamentals.
- An awareness and understanding of security best practices.
- An understanding of basic Active Directory Domain Services (AD DS) concepts.
- Basic knowledge of server hardware.
- Experience supporting and configuring Windows client operating systems such as Windows 8 or Windows 10.

Additionally, students would benefit from having some previous Windows Server operating system experience, such as experience as a Windows Server systems administrator.

Course Objectives

After completing this course, students will be able to:

- Prepare and install Nano Server and, Server Core, and plan a server upgrade and migration strategy.
- Describe the various storage options, including partition table formats, basic and dynamic disks, file systems, virtual hard disks, and drive hardware, and explain how to manage disks and volumes.
- Describe enterprise storage solutions, and select the appropriate solution for a given situation.
- Implement and manage Storage Spaces and Data Deduplication.
- Install and configure Microsoft Hyper-V, and configure virtual machines.

- Deploy, configure, and manage Windows and Hyper-V containers.
- Describe the high availability and disaster recovery technologies in Windows Server 2016.
- Plan, create, and manage a failover cluster.
- Implement failover clustering for Hyper-V virtual machines.
- Configure a Network Load Balancing (NLB) cluster, and plan for an NLB implementation.
- Create and manage deployment images.
- Manage, monitor, and maintain virtual machine installations.

Course Outline

The course outline is as follows:

Module 1, "Installing, upgrading, and migrating servers and workloads," describes the new features of Windows Server 2016, and explains how to prepare for and install Nano Server and Server Core. This module also describes how to plan a server upgrade and migration strategy, and explains how to perform a migration of server roles and workloads within and across domains. Finally, this module explains how to choose an activation model based on your environment characteristics.

Module 2, "Configuring local storage," explains how to manage disks and volumes in Windows Server 2016.

Module 3, "Implementing enterprise storage solutions," discusses direct-attached storage (DAS), network-attached storage (NAS), and storage area networks (SANs). It also explains the purpose of Microsoft Internet Storage Name Service (iSNS) Server, data center bridging, and Multipath I/O (MPIO). Additionally, this module compares Fibre Channel, Internet Small Computer System Interface (iSCSI), and Fibre Channel Over Ethernet (FCoE), and describes how to configure sharing in Windows Server 2016.

Module 4, "Implementing Storage Spaces and Data Deduplication," explains how to implement and manage Storage Spaces. This module also explains how to implement Data Deduplication.

Module 5, "Installing and configuring Hyper-V and virtual machines," provides an overview of Hyper-V and virtualization. It explains how to install Hyper-V, and how to configure storage and networking on Hyper-V host servers. Additionally, it explains how to configure and manage Hyper-V virtual machines.

Module 6, "Deploying and managing Windows and Hyper-V containers," provides an overview of containers in Windows Server 2016. Additionally, this module explains how to deploy Windows Server and Hyper-V containers. It also explains how to install, configure, and manage containers by using Docker.

Module 7, "Overview of high availability and disaster recovery," provides an overview of high availability and high availability with failover clustering in Windows Server 2016. It further explains how to plan high availability and disaster recovery solutions with Hyper-V virtual machines. Additionally, this module explains how to back up and restore the Windows Server 2016 operating system and data by using Windows Server Backup.

Module 8, "Implementing failover clustering," explains how to plan for failover clustering. It also explains how to create, manage, and troubleshoot a failover cluster.

Module 9, "Implementing failover clustering with Windows Server 2016 Hyper-V," describes how Hyper-V integrates with failover clustering. It also explains how to implement Hyper-V virtual machines in failover clusters.

Module 10, "Implementing Network Load Balancing," provides an overview of NLB clusters. It also explains how to plan and configure an NLB cluster implementation.

Module 11, "Creating and managing deployment images," provides an overview of the Windows Server 2016 image deployment process. It also explains how to create and manage deployment images by using the Microsoft Deployment Toolkit (MDT). Additionally, it describes different workloads in the virtual machine environment.

Module 12, "Managing, monitoring, and maintaining virtual machine installations," provides an overview on Windows Server Update Services (WSUS) and the requirements to implement WSUS. It explains how to manage the update process with WSUS. Additionally, this module provides an overview of Windows PowerShell Desired State Configuration (DSC) and Windows Server 2016 monitoring tools. Finally, this module describes how to use Performance Monitor, and how to manage event logs.

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 website*:*** 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, modules 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, go to www.microsoft.com/learning/help. To inquire about the Microsoft Certification Program, send an email to mcphelp@microsoft.com.

Virtual Machine Environment

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

Virtual Machine Configuration

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

Important: Pay close attention to the steps at the end of each lab that explain what you need to do with the virtual machines. In most labs, you will revert the virtual machine to the checkpoint that you create during classroom setup. In some labs, you will not revert the virtual machines, but will keep them running for the next lab.

The following table shows the role of each virtual machine that you will use in this course:

Virtual machine	Role
20740A-LON-DC1 (-B)	Domain controller for the Adatum.com domain
20740A-LON-SVR1 (-B) 20740A-LON-SVR2 20740A-LON-SVR3 20740A-LON-SVR4 20740A-LON-SVR5	Windows Server 2016 member servers in the Adatum.com domain
20740A-LON-SVR6	Virtual machine with no OS installed
20740A-NANO-SVR1	Windows Server 2016 Nano server
20740A-LON-CL1	Windows 10 client workstation
20740A-LON-HOST1	Windows Server 2016 host machine
20740A-LON-NVHOST1	Windows Server 2016 nested virtualization host

Software Configuration

The following software is installed on the virtual machines:

- Windows Server 2016
- Windows 10 client (Windows 10 Enterprise)
- Microsoft Office 2016

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 Learning Partner classrooms in which Official Microsoft Learning Product courseware is taught. These configuration requirements include:

- Processor: 64-bit Intel Virtualization Technology (Intel VT) or AMD Virtualization (AMD-V) processor (2.8 gigahertz (GHz) dual core or better recommended)
- Hard Disk: Dual 500 gigabyte (GB) hard disks 7200 RPM SATA labeled drive C and drive D. Solid state drives (SSDs) are strongly recommended
- Random access memory (RAM): 32 GB or higher
- DVD/CD: DVD; dual layer recommended
- Network adapter
- Sound card with amplified speakers
- Monitor: Dual SVGA monitors 17" or larger supporting 1440 x 900 minimum resolution

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, upgrading, and migrating servers and workloads

Contents:

Module Overview

For your organization to effectively manage storage and compute functions, you need to understand the new features available in Windows Server 2016. This module introduces you to Windows Server 2016 and describes the various editions and installation options. You will learn how to install the new Nano Server edition along with Server Core. You will also learn how to plan a server and migration strategy, along with how to perform a migration of server roles and workloads. Finally, you will learn how to choose the most appropriate activation model for your organization.

Objectives

After completing this module, you will be able to:

- Describe the new features of Windows Server 2016.
- Prepare for and install Nano Server and Server Core.
- Plan a server upgrade and migration strategy.
- Perform a migration of server roles and workloads within a domain and across domains.
- Choose an appropriate activation model.

Lesson 1
Introducing Windows Server 2016

Knowing the capabilities of the Windows Server 2016 operating system enables you to use it effectively and take full advantage of what it can offer your organization. Some of the many improvements to Windows Server 2016 include increased scalability and performance; improved virtualization; improved management tools; and additional deployment options, including Nano Server. This lesson explores these new features and capabilities in Windows Server 2016, in particular those in the computer and storage space, along with the various installation options available.

Lesson Objectives

After completing this lesson, you will be able to:

- Select a suitable Windows Server 2016 edition.
- Describe the hardware requirements for Windows Server 2016.
- Describe installation options for Windows Server 2016.
- Describe the tools available for remoting managing Windows Server 2016.
- Explain how to use Windows PowerShell 5.0 to manage servers.
- Describe the new and improved features of Windows Server 2016.

Selecting a suitable Windows Server 2016 edition

You can choose one of several editions of Windows Server 2016. These editions allow organizations to select a version of Windows Server 2016 that best meets their needs, rather than pay for features they do not require. When deploying a server for a specific role, system administrators can save substantially by selecting the appropriate edition. The following table describes the Windows Server 2016 editions.

- Windows Server 2016 Essentials
- Windows Server 2016 Standard
- Windows Server 2016 Datacenter
- Microsoft Hyper-V Server 2016
- Windows Storage Server 2016 Workgroup
- Windows Storage Server 2016 Standard

Edition	Description
Windows Server 2016 Essentials edition	Windows Server 2016 Essentials edition is designed for small businesses. It corresponds to Windows Small Business Server from earlier versions of Windows Server. This edition allows up to 25 users and 50 devices. It supports two processor cores and up to 64 gigabytes (GB) of random access memory (RAM). It does not support many of the features of Windows Server 2016, including virtualization.
Windows Server 2016 Standard edition	Windows Server 2016 Standard edition is designed for physical server environments with little or no virtualization. It provides many of the roles and features available for the Windows Server 2016 operating system. This edition supports up to 64 sockets and up to 4 terabytes (TB) of RAM. It includes licenses for up to two virtual machines and supports Nano Server installation.

Edition	Description
	Note: You can run two virtual machines on one physical host, using one standard license, as long as the physical host is only used for hosting and managing the virtual machines. If the physical host is used to run other services, such as DNS, you can only run one virtual machine. For more information about Windows licensing, speak with a Microsoft licensing specialist.
Windows Server 2016 Datacenter edition	Windows Server 2016 Datacenter edition is designed for highly virtualized infrastructures, including private cloud and hybrid cloud environments. It provides all of the roles and features available for the Windows Server 2016 operating system. This edition supports up to 64 sockets, up to 640 processor cores, and up to 4 TB of RAM. It includes unlimited Windows Server–based virtual machine licenses for virtual machines that run on the same hardware. It also includes new features such as Storage Spaces Direct and Storage Replica, along with new Shielded Virtual Machines and features for software—defined datacenter scenarios.
Microsoft Hyper-V Server 2016	Acts as a stand-alone virtualization server for virtual machines, including all the new features around virtualization in Windows Server 2016. The host operating system has no licensing cost, but virtual machines must be licensed separately. This edition supports up to 64 sockets and up to 4 TB of RAM. It supports domain joining. It does not support Windows Server 2016 roles other than limited file service features. This edition has no GUI but does have a UI that displays a menu of configuration tasks.
Windows Storage Server 2016 Workgroup edition	Acts as an entry-level unified storage appliance. This edition allows 50 users, one processor core, and 32 GB of RAM. It supports domain joining.
Windows Storage Server 2016 Standard edition	Supports up to 64 sockets but is licensed on a two-socket, incrementing basis. This edition supports up to 4 TB of RAM. It includes two virtual machine licenses. It supports domain joining. It supports some roles, including Domain Name System (DNS) and Dynamic Host Configuration Protocol (DHCP) server roles, but does not support others, including Active Directory Domain Services (AD DS), Active Directory Certificate Services (AD CS), or Active Directory Federation Services (AD FS).

Hardware requirements

The hardware requirements needed to support Windows Server 2016 depend on the services that the server is hosting, the load on the server, and how responsive you want the server to be. The services and features of each role put a unique load on network, disk I/O, processor, and memory resources.

- Windows Server 2016 has the following minimum hardware requirements for Server Core installation:

Hardware	Requirement
Processor architecture	x64
Processor speed	1.4 GHz
RAM	512 MB
Hard drive space	32 GB

The following table shows the absolute minimum required for a Server Core installation on a physical machine.

Component	Requirement
Processor architecture	64-bit
Processor speed	1.4 gigahertz (GHz)
RAM	512 MB
Hard drive space	32 GB

Virtualized deployments of Windows Server 2016 must match the same hardware specifications as those required for physical deployments. However, during installation you will need to allocate extra memory to the VM, which you can then deallocate after installation, or you will need to create an installation partition during the boot process.

Desktop Experience

If you want to install Windows Server 2016 with the Desktop Experience installed, the hard drive space requirement is approximately 4 GB greater.

Nano Server

The requirements for Nano Server depend on the features and roles installed. Nano Server runs from a VHD, either from within Hyper-V, or you can boot directly from the VHD at startup. The smallest Nano Server VHD will be approximately 440 MB, before installing features such as IIS or commonly used drivers. A VHD with IIS and commonly used drivers will be just over 500 MB.

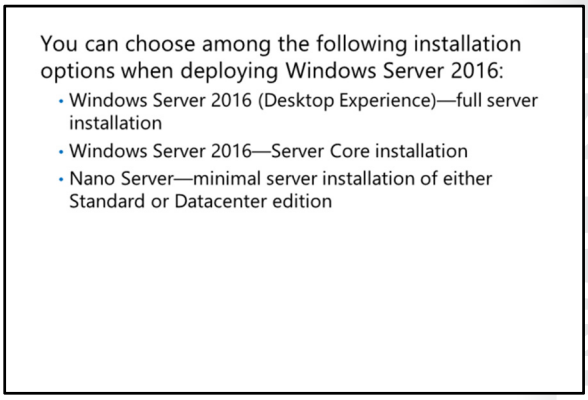
Other hardware requirements

In addition to the previously referenced requirements, there are a variety of other hardware requirements to keep in mind, depending on your specific organizational needs and installation scenarios:

- Greater disk space is required for network installations or for computers with more than 16 GB of RAM.
- Storage and network adapters must be PCI Express compliant.
- A Trusted Platform Module (TPM) 2.0 chip is required for certain features such as BitLocker Drive Encryption.

Overview of installation options

When you install Windows Server 2016, you can select one of three installation options:



- Windows Server 2016 (Desktop Experience). This is a full server installation and includes a complete graphical management interface. This installation option supports all Windows Server roles.
- Windows Server 2016. This is the equivalent of Server Core in earlier versions of Windows Server and provides for a command-line management interface. This installation option has a reduced hardware footprint but does not support all Windows Server roles.
- Nano Server. This is a new installation option for which Windows Server 2012 and earlier versions have no equivalent. Nano Server is administered remotely and optimized for hosting in private clouds and datacenters, and for running applications that are developed by using cloud application patterns.

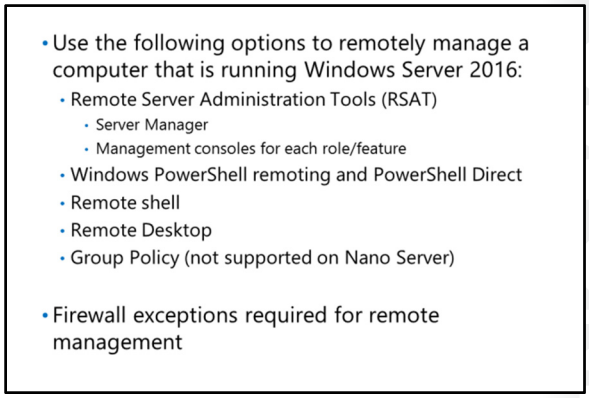
  Nano Server cannot be directly installed from the installation media during setup. Nano Server is installed as a VHD or as a Windows Imaging (WIM) file that is built using Windows PowerShell cmdlets. The VHD file can be booted from within Hyper-V or booted directly from a physical machine. The WIM file can be applied after booting into the Windows Preinstallation Environment (WinPE).

When creating the VHD for a Nano Server, you can select either the Standard or Datacenter edition of Nano Server and select various *Packages* that are used to add server roles and features to a VHD image. Some of these roles and features include:

- Hyper-V role
- Failover Clustering
- File Server role
- DNS Server role
- IIS
- Host support for Windows Containers

Note: Installing Server Core and Nano Server is covered in detail in the next lesson.

Managing servers remotely



Performing the interactive management of Windows Server is not the best practice. With Server Core and, to a greater extent, Nano Server, your local management options are very limited. After you have configured the network and firewall settings of Server Core or Nano Server, you must perform other management tasks remotely. When you install a role or feature, you will be prompted to install the appropriate administrative tools. The best practice is to manage servers remotely by using the Remote Server Administration Tools (RSAT) available for Windows 10. RSAT includes the full set of administrative tools, including Server Manager, the Active Directory Administrative Center, and management consoles. You can later choose to disable the tools by using **Turn Windows features on or off** in **Control Panel**.

Note: For a full list of all the tools included in RSAT for Windows 10, refer to: "Remote Server Administration Tolls (RSAT) for Windows Client and Windows Server (dsform2wiki)" at: http://aka.ms/hz53ry

To download Remote Server Administration Tools, see http://aka.ms/wzpq0j

Server Manager

Server Manager is part of the Windows Server 2016 Desktop Experience, or you can run it from a Windows 10 workstation when installed as part of RSAT. Server Manager is the primary GUI tool to manage computers running Windows Server 2016. The Server Manager console can manage both local and remote servers. You can also manage servers as groups, allowing you to perform the same administrative tasks quickly across multiple servers. You can also use Server Manager to run the Best Practices Analyzer to determine if the roles are functioning properly on the servers in your network.

Windows PowerShell remoting and PowerShell Direct

You can use Windows PowerShell to run Windows PowerShell commands or scripts against correctly configured remote servers if the script is hosted on the local server. With Windows PowerShell remoting, where necessary, you can also load Windows PowerShell modules locally, such as those part of Server Manager, and run the cmdlets available in that module against appropriately configured remote servers. In Windows Server 2016, you also have the option of using PowerShell Direct to run PowerShell scripts or cmdlets on virtual machines from a Hyper-V host.

Note: More information about PowerShell Direct is provided in Module 5, "Installing and configuring Hyper-V and virtual machines."

Remote Shell

Windows Remote Shell (WinRS) is a command-line tool that allows you to execute remote commands on a target server that supports Windows Remote Management (WinRM). WinRM is a collection of standards-based technologies that enables administrators to manage server hardware when signed in directly or over the network. Server Manager and Windows PowerShell remoting also rely on WinRM in Windows Server 2016.

Remote desktop

You can connect to a remote server computer that is running the Server Core installation or the full installation by using Remote Desktop. On Server Core, you must enable Remote Desktop by using **Sconfig.cmd**. You cannot use Remote Desktop to remotely manage Nano Server.

Group Policy

You can use Group Policy to manage Server Core and full installations of Windows Server 2016, just like you can manage any other computer running Windows. However, you cannot use Group Policy to manage Nano Server. Later topics in this module discuss options for using Windows PowerShell for applying Group Policy settings to Nano Server installations.

Firewall settings

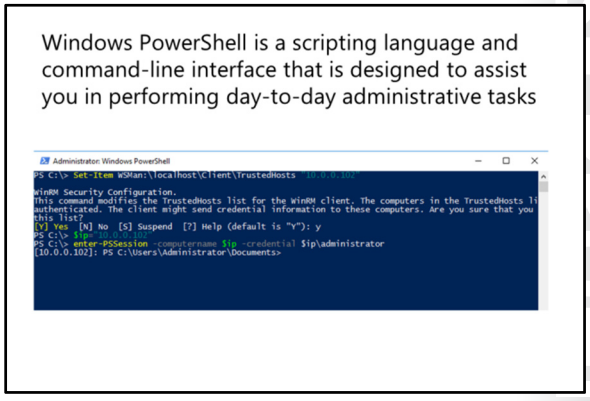
Microsoft Management Console (MMC) and some other tools used for remote server management rely on the Distributed Component Object Model (DCOM). Even Server Manager, when managing servers running Windows Server 2008 without the Windows Management Framework updates installed, depends on DCOM. DCOM, unlike WinRM, requires Windows Firewall on the computer running the remote management tools to be configured to allow exceptions to multiple rules. These exceptions include:

- COM+ Network Access (DCOM-In)
- Remote Event Log Management (NP-In)
- Remote Event Log Management (RPC)
- Remote Event Log Management (RPC-EPMAP)

Additional Reading: For more information about configuring firewall settings to support remote management, refer to the procedure: "To configure MMC or other tool remote management over DCOM" in the topic "Configure Remote Management in Server Manager" at: http://aka.ms/eyxjjf

Using Windows PowerShell 5.0 to manage servers

Windows PowerShell 5.0 is a scripting language and command-line interface that is designed to assist you in performing day-to-day administrative tasks. Windows PowerShell cmdlets execute at a Windows PowerShell command prompt or combine into Windows PowerShell scripts. With the introduction of Nano Server, a *headless server* environment, it is necessary to use Windows PowerShell to manage servers remotely. A headless server has no graphical user interface and there is no capability for local sign-in.



Importing modules

Some Windows PowerShell cmdlets are not available in the default Windows PowerShell library. When you enable some Windows features or want to administer particular environments, you must obtain additional Windows PowerShell functions. These additional functions are packaged in modules. For example, to manage Nano Server, Windows Server containers, and Azure AD with Windows PowerShell, you must import the required modules.

To do this, use an **import-module** cmdlet:

```
Import-Module NanoServerImageGenerator.psm1
```

The preceding cmdlet imports the required Windows PowerShell module for Nano Server in preparation for performing additional Nano Server management by using Windows PowerShell remoting.

Windows PowerShell remote management

You can use Windows PowerShell to remotely run cmdlets on other Windows systems. This is called *remoting*. Windows PowerShell remoting depends on the WinRM service running on the target systems. This service can be enabled manually or by running the **Enable-PSRemoting** cmdlet on the target.

The simplest way to use remoting is one-to-one remoting, which allows you to bring up an interactive Windows PowerShell session on the remote system. After the connection is established, the Windows PowerShell prompt displays the name of the remote computer.

PowerShell Direct

Many administrators choose to run some or all of their servers running Windows Server in virtualized environments. To enable a simpler administration of Windows Server Hyper-V virtual machines, Windows 10 and Windows Server 2016 both support a new feature called PowerShell Direct.

PowerShell Direct enables you to run a Windows PowerShell cmdlet or script inside a virtual machine from the host operating system without regard to network and firewall configurations, and regardless of remote management configuration.

 **Note:** You must still authenticate to the virtual machine by using guest operating system credentials.

To use PowerShell Direct, from your host, run the following Windows PowerShell cmdlet:

```
Enter-PSSession -VMName VMName
```

You can then run the same cmdlets that you normally run in the same way as with any other remote Windows PowerShell situation.

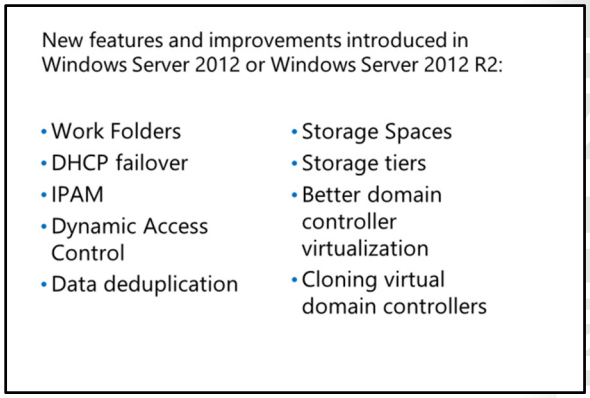
Windows PowerShell Desired State Configuration (DSC)

Windows PowerShell DSC is a set of Windows PowerShell extensions, cmdlets, and resources that support configuring and managing remote computers in a scalable and standardized manner by pushing or pulling declarative configurations.

 **Note:** Windows PowerShell DSC is covered in detail in Module 12, "Managing, monitoring, and maintaining virtual machine installations."

What's new since Windows Server 2008 was released?

Windows Server 2016 provides many new features and a number of significant improvements over earlier versions of Windows Server. Some of these features and improvements were first introduced in Windows Server 2012 or Windows Server 2012 R2, whereas others are new to Windows Server 2016.



New features and improvements introduced in Windows Server 2012 or Windows Server 2012 R2

The following features and feature improvements in Windows Server 2016 were first introduced in Windows Server 2012 or Windows Server 2012 R2:

- Work Folders. Provides a mechanism for both domain-joined computers and those that are not domain joined to access and synchronize corporate data files.
- DHCP failover. Enables you to deploy two DHCP servers containing overlapping DHCP scopes. If a DHCP server goes offline, DHCP client computers can renew their IP configurations from the failover DHCP server.
- IP Address Management (IPAM). Provides administrative and monitoring capabilities for the IP address infrastructure within your organization's networks. With IPAM, you can monitor, audit, and manage servers running DHCP and DNS.
- Dynamic Access Control. This claims-based authorization platform enables you to control access to file resources within your organization. This is in addition to any folder or shared folder permissions already protecting the resource. Dynamic Access Control enables you to apply access control permissions based on rules that can include the sensitivity of the resources, the job or role of the user, and the configuration of the device that is used to access these resources.
- Data deduplication. Involves finding and removing duplication within data. By segmenting files into small, variable-sized pieces; identifying duplicate pieces; and maintaining a single copy of each piece, data deduplication enables you to store more data in less space.
- Storage Spaces. Enables cost-effective, highly available, scalable, and flexible storage for critical deployments. Storage Spaces are based on virtual disks that are created from free space in a storage pool. Storage pools are collections of physical disks that enable you to aggregate disks, expand capacity in a flexible manner, and delegate administration.
- Storage tiers. Automatically moves frequently accessed data to faster storage and less-frequently accessed data to slower storage.
- Better support for domain controller virtualization. Although many organizations have virtualized domain controllers for several years, potential issues can affect the reliability of this configuration. A feature known as *GenerationID* changes whenever the virtual machine experiences an event that affects its position in time. During startup and normal operations, a virtual domain controller compares the current value of GenerationID against the expected value. A mismatch is interpreted as a rollback event, and the domain controller employs safeguards to prevent the virtual domain controller from creating duplicate security principals.
- The ability to clone virtual domain controllers. Enables you to deploy new virtual domain controllers by cloning existing ones.

 **Note:** This is not a complete list of all the new or improved features in Windows Server 2012 or Windows Server 2012 R2.

New features and improvements introduced in Windows Server 2016

The following features and feature improvements were introduced in Windows Server 2016:

- Nano Server. Nano Server is a new installation option for Windows Server 2016. With no graphical or command prompt interface, it has a significantly lower hardware requirement than Server Core. Nano Server is the ideal platform for Hyper-V, Hyper-V cluster, and scale-out file servers and cloud service apps.
- Windows Server containers and Hyper-V containers. Containers enable you to isolate your apps from the operating system environment. This improves security and reliability. Windows containers are isolated from one another but run on the host operating system. Hyper-V containers are further isolated, because they run within a virtual machine.
- Docker. Docker is a technology for managing containers. Although Docker is usually associated with Linux, Windows Server 2016 provides support for Docker for managing Windows containers and Hyper-V containers.
- Rolling upgrades for Hyper-V and storage clusters. These upgrades enable you to add Windows Server 2016 nodes to an existing Windows Server 2012 R2 failover cluster. The cluster continues to operate at a Windows Server 2012 R2 functional level until all the nodes are upgraded.
- The ability to *hot add* and *hot remove* virtual memory and network adapters from virtual machines. In Hyper-V in Windows Server 2016, you can now add or remove virtual memory and network adapters while the virtual machines are running.
- Nested virtualization. In Hyper-V in Windows Server 2016, you can enable nested virtualization, enabling you to run Hyper-V virtual machines within a virtual machine.
- Shielded virtual machines. Shielding your virtual machines enables you to help protect the data on them from unauthorized access.
- PowerShell Direct. This feature enables you to run Windows PowerShell commands against a guest operating system in a virtual machine without handling security policies, host network settings, or firewall settings.
- Windows Defender. Windows Defender is provided to help protect your server against malware. Although the Windows Defender interface is not installed by default, the antimalware patterns are automatically kept up-to-date.
- Storage Spaces Direct. This feature enables you to build highly available storage with directly attached disks on each node in a cluster. The Server Message Block 3 (SMB3) protocol provides resiliency.
- Storage Replica. This feature enables you to synchronously or asynchronously replicate volumes at the block level.
- Microsoft Passport. This service replaces passwords with two-factor authentication that consists of an enrolled device and a *Windows Hello* (biometric) or PIN. This helps provide a more secure and convenient sign-in experience.
- Remote Desktop Services. You can now use an Azure SQL database to create a high availability environment for Remote Desktop Connection Broker.
- Active Directory Domain Services (AD DS). AD DS improvements include support for privileged access management (PAM), support for Azure AD Join, along with support for Microsoft Passport.

 **Note:** Windows Server 2016 includes many other improvements to existing features. For a full list of all the changes in Windows Server 2016, refer to: "What's New in Windows Server 2016 Technical Preview 5" at: http://aka.ms/S4u2tt

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

Statement	Answer
Docker is a container that enables you to run an app in an isolated and portable operating environment.	

Question: What new features in Windows Server 2016 do you think will be useful in your organization?

Lesson 2

Preparing and installing Nano Server and Server Core

When you prepare to install Windows Server 2016, you must understand whether a particular hardware configuration is suitable. You must also select among the installation options: Windows Server 2016 (Desktop Experience), Server Core, or Nano Server. This lesson describes each of these installation options and provides guidance on how to perform an installation of Windows Server 2016.

The installation process for Windows Server 2016 requires minimal input from the installer. However, following the installation, you must configure a number of important settings before you can use your server. In addition, because both Server Core and Nano Server provide no graphical management tools and, in the case of Nano Server, not even a command prompt for management, you must know how to enable and perform the remote management of your server infrastructure. This lesson identifies the important post-installation configuration options, and explains how to enable and use the remote management tools.

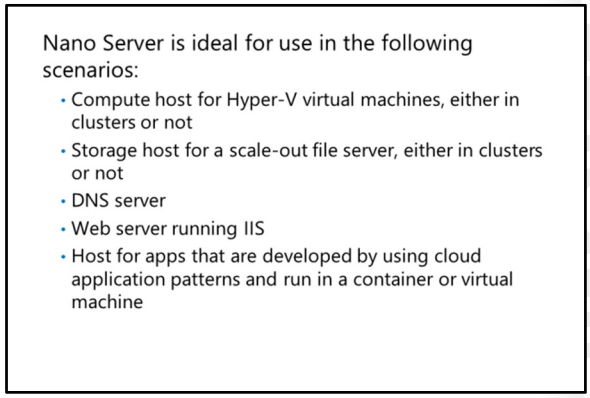
Lesson Objectives

After completing this lesson, you will be able to:

- Describe Nano Server.
- Explain how to install Nano Server.
- Explain how to manage and configure Nano Server.
- Explain how to plan for Server Core.
- Compare Server Core and Nano Server to a full installation.
- Explain how to install Server Core.
- Explain the post-installation configuration for Server Core.
- Explain how to select a suitable installation type.

What is Nano Server?

Nano Server is a new installation option for Windows Server 2016 that is similar to Windows Server in Server Core mode. However, although it has a significantly smaller hardware footprint, it has no local sign-in capability and supports only 64-bit apps, tools, and agents. Setup is significantly faster, and after installation, the operating system requires far fewer updates.



Note: Nano Server is not available for selection through the Windows Server 2016 setup wizard. Instead, you must create a virtual hard drive by using Windows PowerShell. You can then use this virtual hard drive on a virtual machine to support a virtualized Nano Server in Hyper-V, or you can configure your server computer to start from a .vhd file for a physical Nano Server deployment option.

Use scenarios

Nano Server is ideal for use in the following scenarios:

- Hyper-V host for virtual machines, either in clusters or not (*compute* host)
- As a storage host for a scale-out file server, either in clusters or not
- As a DNS server
- As a web server running Microsoft Internet Information Services (IIS)
- As a host for applications that are developed by using cloud application patterns and run in a container or virtual machine guest operating system

Server roles available in Nano Server

The following table shows the server roles and features that you can either install when you deploy Nano Server or subsequently install by using Windows PowerShell on a previously deployed Nano Server.

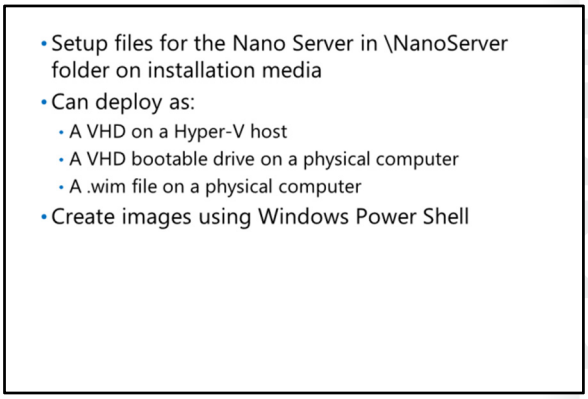
Role or feature	Option to install
Hyper-V role	**-Compute**
Failover clustering	**-Clustering**
Drivers for a variety of network adapters and storage controllers (this is the same set of drivers included in a Server Core installation of Windows Server 2016)	**-OEMDrivers**
File Server role and other storage components	**-Storage**
Windows Defender Antimalware, including a default signature file	**-Defender**
DNS Server role	**-Packages Microsoft-NanoServer-DNS-Package**
Desired State Configuration	**-Packages Microsoft-NanoServer-DSC-Package**
IIS	**-Packages Microsoft-NanoServer-IIS-Package**
Host support for Windows Containers	**-Containers**
System Center Virtual Machine Manager agent	**-Packages Microsoft-Windows-Server-SCVMM-Package** **-Packages Microsoft-Windows-Server-SCVMM-Compute-Package**
Network Performance Diagnostics Service (NPDS)	**-Packages Microsoft-NanoServer-NPDS-Package**
Data Center Bridging	**-Packages Microsoft-NanoServer-DCB-Package**
Boot and run from a RAM disk	**-Packages Microsoft-NanoServer-Guest-Package**
Deploy on a virtual machine	**-Packages Microsoft-NanoServer-Host-Package**

Role or feature	Option to install
Secure Startup	**-Packages Microsoft-NanoServer-SecureStartup-Package**
Shielded Virtual Machine	**-Packages Microsoft-NanoServer-ShieldedVM-Package**

While many roles are supported by Nano Server, several important roles and features are not supported, including AD DS, AD CS, and DHCP.

Overview of installing Nano Server

As mentioned previously, Nano Server cannot be directly installed from the installation media during setup. The files required for setting up Nano Server are located in the **\NanoServer** folder located on the Windows Server 2016 Installation media. Nano Server is installed using one of three methods:



- Deploying a VHD image that will be hosted as a virtual machine on a Hyper-V host.
- Deploying a VHD as a bootable drive on a physical computer.
- Deploying a Nano Server WIM file on a physical computer.

The steps are similar for each option:

1. Copy the **NanoServerImageGenerator** folder from the **NanoServer** folder on the Windows Server 2016 installation media to a folder on your local machine.
2. Start Windows PowerShell as an administrator and change the directory to the **NanoServerImageGenerator** folder on your local drive.
3. Import the **NanoServerImageGenerator** module by using the following Windows PowerShell **Import-Module** cmdlet:

```
Import-Module .\NanoServerImageGenerator -Verbose
```

4. Create the VHD or WIM by using the **New-NanoServerImage** cmdlet with the following syntax:

```
New-NanoServerImage -Edition <edition> -DeploymentType <deployment type> -MediaPath
<media path> -BasePath <base path> -TargetPath <target path> -ComputerName <computer
name> -Packages <packages> -<other package switches>
```

   where:

   - Edition – is the Windows Server 2016 edition the Nano Server will be based on; either Standard or Datacenter.
   - Deployment type – The type of deployment; *Host* for WIM or bootable VHD, *Guest* for VHDs hosted in Hyper-V.
   - Media path – The path to the root of the Windows Server 2016 installation media.

- Base path – This optional switch is used when creating a WIM file. When creating a WIM file, the Nano Server binaries will be copied to this folder so that the **New-NanoServerWim** cmdlet can be used to create a new image without specifying the **-MediaPath** switch.
- Target path – The path and file name, including extension, of the Nano Server Image. The file type created depends on the file extension specified: .vhd for a Generation 1 virtual machine, .vhdx for a Generation virtual machine, and .wim for a WIM file.
- Computer name – The name of the target Nano Server computer.
- Packages – The **-Packages** switch is used to install certain roles and features, listed in the previous topic on Nano Server. Multiple packages can be combined in a comma-separated list.
- Other package switches – Some Packages are installed using their own switches. See the previous topic for a complete list. If you want to deploy a Nano Server to a physical machine, be sure to use the **-OEMDrivers** switch to install the basic set of device drivers that are included in the Standard edition installation.

The Windows PowerShell script prompts you for an administrator account and password when it is run.

Deploying the Nano Server VHD in Hyper-V

Once you create the VHD for the Nano Server, the steps for deploying the Nano Server in Hyper-V is similar to deploying any virtual machine:

1. Create a new virtual machine, by using the VHD, in Hyper-V Manager.
2. Boot and then connect to the virtual machine from Hyper-V Manager.
3. Log on to the Nano Server Recovery Console using the administrator account and password.
4. Obtain the IP address for the virtual machine and connect to the Nano Server by using the remote management tools to manage the server.

Deploying the Nano Server VHD on a physical computer

You can also run the Nano Server on a physical computer by using the VHD that you created. As noted previously, you must ensure that the OEM drivers for the most common hardware are installed by using the **-OEMDrivers** switch during VHD creation. The steps for deploying the VHD to the physical computer are as follows:

1. Sign in to the physical computer as an administrator.
2. Copy the VHD to the local computer.
3. Configure the VHD to boot by using the following steps:
   a. Mount the VHD.
   b. Run the **bcdboot** command targeting the VHD. For example, if the VHD is mounted to the E:\ drive:

      ```
      bcdboot e:\windows
      ```

   c. Unmount the VHD.
4. Boot the computer into the Nano Server VHD.

Deploying a Nano Server WIM

Creating a Nano Server WIM is as simple as specifying .wim as the file extension when providing the **-TargetPath** value. Once the WIM file is created you can deploy it by using WinPE:

1. Ensure the .wim file is accessible from WinPE.
2. Boot into WinPE on the local server.
3. Use Diskpart.exe to prepare the local hard drive.
4. Apply the Nano Server image by using Dism.exe.
5. Remove the WinPE media if applicable, and reboot the system by using the following command:

```
Wpeutil.exe reboot
```

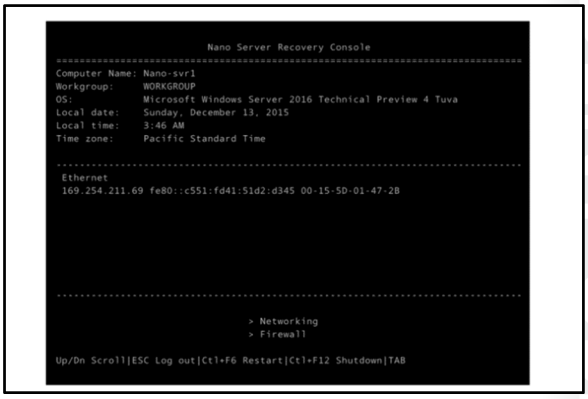
After you reboot the Nano Server from whichever deployment method you used:

1. Sign in to the Nano Server Recovery Console by using the administrator account and password.
2. Obtain the IP address of the Nano Server computer and use the remote management tools or Windows PowerShell to connect and manage the server.

Managing and configuring Nano Server

You can perform only the most fundamental management tasks interactively on Nano Server. After you have signed in, the Nano Server Recovery Console appears. This identifies:

- The computer name
- The workgroup or domain name
- The installed operating system
- Local data, the local time, and the time zone
- The current network configuration



Configuring networking

You can change the basic network configuration by using the Tab key to navigate to **Networking** and then pressing Enter. You can then select the appropriate network adapter from the list by using the cursor keys to navigate to the correct adapter and then pressing Enter.

The current network settings are displayed. You can press either F11 to configure IPv4 settings or F12 for IPv6 settings. If you choose to configure IPv4, use the F4 key to switch the settings. For example, to enable or disable DHCP, press F4. To enter a manual IPv4 configuration, disable DHCP and then use the number keys to type a suitable IP address, subnet mask, and default gateway. Press Enter twice to update the configuration. Press Esc repeatedly to return to the main menu.

Configuring the firewall

You might need to configure firewall settings to enable remote management. From the main Nano Server Recovery Console, press the Tab key to navigate to **Firewall**, and then press Enter. A list of firewall rules is displayed. Use the cursor keys to navigate up and down the list and press Enter for a rule you want to configure.

For example, to enable remote event log management, locate the remote event log management (RPC) rule and press Enter. Press F4 to Enable/Disable. Press ESC and select the next rule, and then repeat the procedure. When you have configured all rules, press ESC to return to the main menu.

Ongoing management

Once you have configured the networking settings and enabled the appropriate remote management firewall ports for inbound communications, you can manage the Nano Server remotely by using either Server Manager, Windows PowerShell, or any other management tool by using the **Connect to** option to select the Nano Server. Typical management tasks include:

- Adding the computer to a domain
- Adding roles and features to the server

Adding the Nano Server to a domain online

You perform an online domain join by harvesting a domain data blob from a computer already joined to the domain and using that data blob when joining the domain. The basic steps for this follow.

1. Harvest the domain data blob from a computer running Windows Server 2016 that is already joined to the domain by using the following command:

```
Djoin.exe /provision /domain <domain name> /machine <Nano Server machine name>
/savefile <path and name of blob file>
```

2. Enable File and Printer Sharing on the Nano Server.

   a. Using Windows PowerShell Remoting, connect to the Nano Server with the following commands from a Windows PowerShell session running as administrator:

```
Set-Item WSMan:\localhost\client\TrustedHosts "<Nano Server IP address>"
$ipaddress = "<Nano Server IP address>"
Enter-PSSession -ComputerName $ipaddress -Credential $ipaddress\Administrator
```

   b. Provide the Administrator password and set the firewall rule to enable file and printer sharing:

```
Netsh advfirewall firewall set rule group="File and Printer Sharing" new
enable=yes
```

3. Copy the data blob file to the Nano Server by using the following commands:

```
Net use z: \\<Nano Server IP address>\c$
Md z:\temp
copy <name of blob file> z:\temp
```

4. Using the Windows PowerShell Remoting session, join the domain by using the following command:

```
Djoin.exe /requestodj /loadfile c:\temp\<name of blob file> /windowspath c:\windows
/localos
```

5. Use the following commands to restart the Nano Server computer and exit the Windows PowerShell Remoting session:

```
shutdown /r /t 5
Exit-PSSession
```

Note: You can also join the Nano Server to the domain during creation of the server image. Either use the **-DomainName** parameter of the **New-NanoServerImage** cmdlet, if the local machine where you are creating the image is joined to the domain; or use the **-DomainBlobPath** parameter to provide a domain data blob file from a different server running Windows Server 2016 that is already joined to the domain.

You can also join the domain by adding the contents of the domain data blob to an Unattend.xml file and applying the settings during boot of the VHD.

For more information about these options, refer to: "Joining Nano Server to a domain" in the "Getting Started with Nano Server" topic at: http://aka.ms/lzumn4

Adding roles and features to Nano Server online

To install new roles and features to Nano Server online without editing or rebuilding the VHD, you will need to find and install those roles and features from the online repository by using the PackageManagement PowerShell module and the NanoServerPackage provider.

You install the provider by using the following PackageManagement cmdlets:

```
Install-PackageProvider NanoServerPackage
Import-PackageProvider NanoServerPackage
```

Once the NanoServerPackage provider is installed you can find and install Nano Server packages by using either Nano Server specific cmdlets or the generic PackageManagement variations of those cmdlets. The Nano Server package cmdlets are:

- **Find-NanoServerPackage**
- **Save-NanoServerPackage**
- **Install-NanoServerPackage**

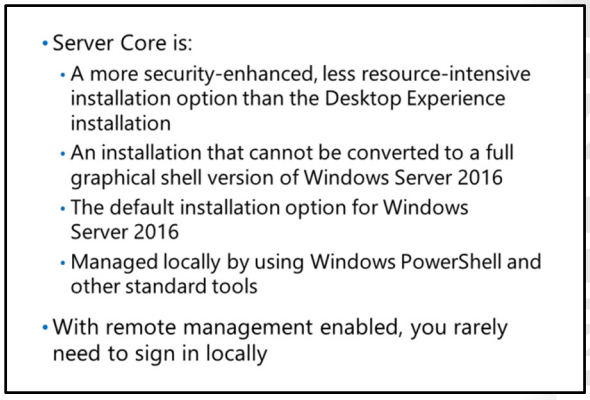
You can use the **Install-NanoServerPackage** cmdlet to install packages to both online images and offline images.

You can also install roles and features by using Deployment Image Servicing and Management (DISM.exe) and providing the package information in an Unattend.xml file.

Note: For more information about installing Nano Server packages, refer to: "Installing roles and features online" in the "Getting Started with Nano Server" topic at: http://aka.ms/lzumn4

Planning for Server Core

Server Core is the default installation option when you run the **Windows Server 2016 Setup** wizard. It uses fewer hardware resources than the full installation option. One of the ways it does this is by not installing a GUI for management purposes. Instead, you can manage Server Core locally by using Windows PowerShell or a command-line interface, or you can manage it remotely by using one of the remote management options described in the last lesson.



Server Core has the following advantages over the full Windows Server 2016 installation option:

- Reduced update requirements. Because Server Core installs fewer components, its deployment requires you to install fewer software updates. This reduces the number of monthly restarts required and the amount of time required for an administrator to service Server Core.
- A reduced hardware footprint. Computers running Server Core require less RAM and less hard drive space. When Server Core is virtualized, this means that you can deploy more servers on the same host.
- Smaller attack surface. Installing fewer components, especially the client interface, reduces the potential surface for security vulnerabilities for hackers to exploit.

There are some drawbacks to installing Server Core instead of the Desktop Experience. If an application depends on the GUI, it will fail when the GUI call is made. For example, and error might occur when a dialog box appears. Also, as mentioned previously, there are more limited local management options. However, when you are connected locally, you can also use the tools that are listed in the following table to manage Server Core deployments of Windows Server 2016.

Tool	Function
Cmd.exe	Allows you to run traditional command-line tools, such as ping.exe, ipconfig.exe, and netsh.exe.
PowerShell.exe	Launches a Windows PowerShell session on the Server Core deployment. You then can perform Windows PowerShell tasks normally. Windows Server 2016 comes with Windows PowerShell version 5.0 installed.
Regedt32.exe	Provides registry access within the Server Core environment.
Msinfo32.exe	Allows you to view system information about the Server Core deployment.
Taskmgr.exe	Launches Task Manager.

Note: Sconfig.cmd, which served as a command-line, menu-driven tool to perform common server administrative tasks has been deprecated. You should use Windows PowerShell or other administrative tools instead.

Server roles available in Server Core

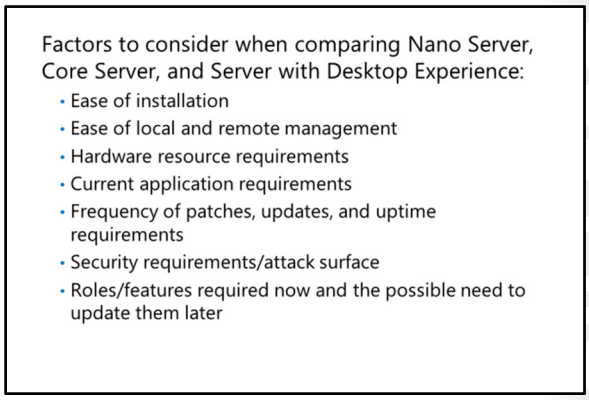
The following server roles are available on Server Core deployments:

- AD CS
- AD DS
- DHCP Server
- DNS Server
- File Services (including File Server Resource Manager)
- Active Directory Lightweight Directory Services (AD LDS)
- Hyper-V
- Print and Document Services
- Streaming Media Services
- Web Server (including a subset of ASP.NET)
- Windows Server Update Server
- Active Directory Rights Management Server
- Routing and Remote Access Server and the following subroles:
  - Remote Desktop Connection Broker
  - Licensing
  - Virtualization

Comparing Server Core with Nano Server and a full installation

With the introduction of Nano Server, you must decide when it is most appropriate to perform an installation of Nano Server instead of Server Core, or a full installation that includes Desktop Experience.

When comparing the three installation types, take into account of the following factors:



- Ease of installation. Core Server is the default installation option from the installation media. Desktop Experience is also supported from the installation media. The Nano Server installation is not available directly from the setup program and requires using PowerShell to create an installation image.
- Ease of local management. A Desktop Experience installation provides the most options for local management of roles and features. A Core Server installation provides far fewer options, but still provides for local sign-in and use of some local management tools in addition to remote administration tools. A Nano Server installation depends almost entirely on remote management.
- Physical hardware and virtual machine requirements. Nano Server has the lowest demand on hardware resources, especially when running on a virtual machine. When running on a physical machine, additional device drivers need to be provided. Core Server requires more resources, but also

more directly supports installation on a physical computer and a core set of device drivers is provided as part of the installation. The full server installation has the greatest resource demand but also supports the greatest variety of hardware.

- Support for existing applications and refactoring of existing code. Because Nano Server and Core Server do not include all of the APIs in the full installation of Windows Server 2016, you might need to modify existing applications to work in those environments. Nano Server has the fewest number of supported APIs, so the need to update your applications is greatest when running there. Server Core requires fewer changes to your code, but still needs some coding, especially any code that calls the GUI.
- Ease of maintenance and uptime. With the smaller set of features in Nano Server and Core Server, there are far fewer updates and patches that are applicable. Nano Server will have the fewest updates and therefore the fewest reboots, and the highest uptime as a result. Core Server will have fewer updates and reboots, and more uptime, than the full installation with Desktop Experience, but more downtime than with Nano Server.
- Security requirements. The reduced attack surface from vulnerabilities that results from the reduced set of features, services, open ports, and so on that come with Nano Server and Core Server is a major advantage over the full Desktop Experience installation. Nano Server provides the smallest possible attack surface thanks to its smaller footprint that only installs the binaries for a specific role or feature. Core Server's attack surface is larger than that of Nano Server, but still far smaller than that of the full installation.
- Current and future roles and features. Nano Server is optimized for installing as few roles and features as possible upon installation. Also, some roles, such as AD DS and data collection package (DCP) are not available on Nano Server. You can add supported roles and features later, but this requires some effort because the binaries that were not specified in the initial installation are not already on the server. Core Server supports a more limited set of roles than the full installation, but more roles than are available for Nano Server, and the binaries for all of the roles it supports are included on the server in the initial installation. This makes adding them later relatively easy. However, you cannot later convert the Core Server to a full Desktop Experience installation. To use the Desktop Experience, you must perform a full server installation.

Installing Server Core and Server with Desktop Experience

Installing Windows Server 2016 is largely the same whether you are installing Server Core or Server with Desktop Experience. Before installing Windows Server 2016 you should perform several tasks to prepare for installation:

1. Perform preinstallation tasks:
   - Disconnect UPS
   - Back up server if applicable
   - Disable antivirus software
2. Run the **Windows Setup Wizard** from the installation media:
   1. Provide locale information (language, date, currency, keyboard)
   2. Select **Server Core Installation**
   3. Review and accept license
   4. Select installation location
   5. Provide administrator password

- Disconnect any uninterruptible power supply (UPS) that is connected to the destination computer with a serial cable. Setup attempts to detect any devices connected to serial ports and UPS equipment can cause problems with this process.
- Back up your server if this is not a clean install.
- Disable virus protection software that might be installed on the target computer.
- Copy any mass storage driver files provided by the manufacturer to a disk, flash drive, or other portable media so that the driver can be provided during setup.

The actual installation process includes the following steps:

1. Connect to the installation source. Options for this include:
   - Insert a DVD-ROM containing the installation files, and boot from the DVD-ROM.
   - Connect a specially prepared USB drive that hosts the installation files.
   - Perform a PXE boot, and connect to a Windows Deployment Services server.
2. On the first page of the **Windows Setup Wizard**, select the following locale-based information:
   - Language to install
   - Time and currency format
   - Keyboard or input method
3. On the second page of the **Windows Setup Wizard**, click **Install now**.

   You also can use this page to select **Repair Your Computer**. You use this option if an installation has become corrupted and you are no longer able to boot into Windows Server 2016.
4. In the **Windows Setup Wizard**, on the **Select The Operating System You Want To Install** page, choose from the available operating system installation options. The default option is **Server Core Installation**.
5. On the **License Terms** page, review the terms of the operating system license. You must choose to accept the license terms before you can proceed with the installation process.
6. On the **Which Type Of Installation Do You Want** page, you have the following options:
   - **Upgrade**. Select this option if you have an existing installation of Windows Server that you want to upgrade to Windows Server 2016.

     You should launch upgrades from within the previous version of Windows Server rather than booting from the installation source.
   - **Custom**. Select this option if you want to perform a new installation.
7. On the **Where do you want to install Windows** page, choose an available disk on which to install Windows Server 2016.

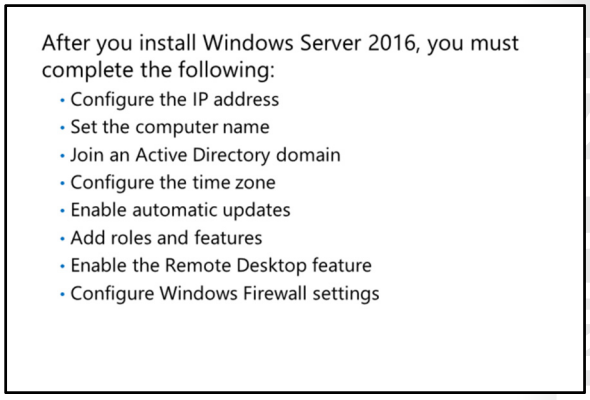
   You can also choose to repartition and reformat disks from this page. When you click **Next**, the installation process will copy files and reboot the computer several times.
8. On the **Settings** page, provide a password for the local Administrator account.

Note: Unlike Windows Server 2012, you cannot convert from Server Core to Server with Desktop Experience, or from Server with Desktop Experience to Server Core.

Note: You can also install Windows Server 2016 as a preconfigured VHD from the TechNet Evaluation Center. Refer to: "Evaluate Windows Server Technical Preview" at: http://aka.ms/Uphshk

Post-installation configuration settings

In earlier versions of Windows Server, the installation process required you to configure network connections, the computer name, user accounts, and domain membership information. The Windows Server 2016 installation process reduces the number of questions that you must answer. The only information that you provide during installation is the password that the default local Administrator account uses.



After you have installed Windows Server 2016, you typically should complete the following:

- Configure the IP address
- Set the computer name
- Join an Active Directory domain
- Configure the time zone
- Enable automatic updates
- Add roles and features
- Enable the Remote Desktop feature
- Configure Windows Firewall settings

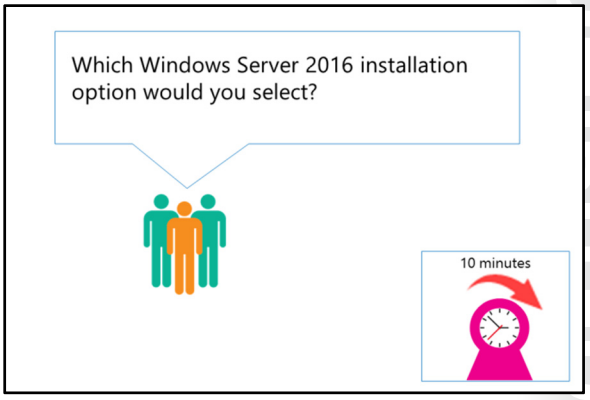
The installation type selected (with Desktop Experience or without) during setup determines which tools you can use to complete these configuration tasks. For example, on Windows Server 2016 (Desktop Experience), you can use Server Manager on the local server to complete these post-installation tasks. On Server Core, you can use Windows PowerShell or other command-line tools, such as Netsh.exe, locally. Or, you can enable remote management and then complete these tasks by using Windows PowerShell Remoting. You can also use Server Manager to configure the Server Core installation remotely.

Note: You can also use an XML answer file to provide this information during an automated installation.

Discussion: Selecting a suitable Windows Server edition and installation type

Which Windows Server 2016 installation option would you select?

Question: Your customer, a small legal firm, has a requirement for a single server that they want you to deploy at their only office. Which Windows Server 2016 installation option would be best?



Question: One of your enterprise customers has a new branch office. You must deploy Windows Server 2016 to support the local users at this new branch. The server will be managed remotely from IT staff located in the head office. The server will support the DNS, DHCP, and AD DS server roles. Your customer wants to minimize resource consumption on the server. Which Windows Server 2016 installation option would be best?

Question: Your customer wants to run a web server based on IIS. The server must use as few hardware resources as possible. Which Windows Server 2016 installation option would be best?

Demonstration: Installing Nano Server

In this demonstration, you will see how to install Nano Server.

Demonstration Steps

1. On **LON-DC1**, open an elevated command prompt.
2. Change to the root directory of drive C, and then create a folder named **Nano**.
3. Copy all the files with a .ps* extension from the **D:\NanoServer\NanoServerImageGenerator** folder to **C:\Nano**.
4. Open an elevated Windows PowerShell window.
5. Run **Import-Module c:\nano\NanoServerImageGenerator.psm1**. This command imports the required Windows PowerShell module for Nano Server.
6. Run **new-NanoServerImage -Edition Standard -mediapath D:\ -Basepath c:\nano -targetpath c:\nano\nano-svr1.vhdx -DeploymentType Guest -computername NANO-SVR1 -storage -packages Microsoft-NanoServer-IIS-Package**. Type the password **Pa$$w0rd** when prompted. This command creates a VHDX file for your Nano Server with the following options:
   - **Mediapath** identifies the source of the installation files.
   - **Basepath** indicates where to create the VHDX file and supplemental files.
   - **Targetpath** identifies the name and location of the VHDX file.
   - **Computername** identifies the name of this instance of Nano Server.
   - **Storage** installs the File Server role.
   - **Packages** enables the additional installation of other roles—in this case, the IIS role.
   - **DeploymentType** configure the VHDX for use as a guest.
7. In **C:\Nano**, you can see the files that were created, including the **Nano-svr1.vhdx** file. Ordinarily, you now copy this file to a Hyper-V host, and then create a virtual machine to use the virtual hard drive. You can also reconfigure startup settings on your host so that it can start from this VHDX file. A virtual machine is preconfigured with the VHDX file. Switch to **NANO-SVR1**.
8. Sign in as **Administrator**/**Pa$$w0rd**.
9. By using this console, you can perform basic administration of Nano Server, including making basic changes to IP configuration and firewall settings, enabling the computer to be managed remotely.
10. Observe that the computer name is **Nano-Svr1**, and that the computer belongs to a workgroup.
11. In **Network Adapter Settings**, notice that DHCP is providing the IP configuration.

Check Your Knowledge

Question	
Which of the following tools can you use to locally manage an installation of Windows Server 2016 Nano Server?	
Select the correct answer.	
	PowerShell.exe
	Sconfig.cmd
	Taskmgr.exe
	All of the above
	None of the above

Check Your Knowledge

Question	
Which of the following commands do you use to initiate remote Windows PowerShell management?	
Select the correct answer.	
	Enter-PSSession -Name
	Enter-PSRemote -Name
	Enter-PSSession -ComputerName
	Enter-PSRemote -ComputerName

Lesson 3
Preparing for upgrades and migrations

One of the key tasks when deploying Windows Server 2016 is identifying when you should upgrade an existing Windows Server deployment by using the existing hardware, or when you should migrate the roles and features to a clean installation of Windows Server 2016 on new hardware.

You will also want to use available guidance documentation and tools to determine which options are most suitable and use tools to automate the process. This lesson describes the considerations for performing an in-place upgrade or migrating to a new server. It also provides scenarios you can compare to your current business requirements and explains the benefits of migrating to a clean installation of Windows Server 2016. The lesson also provides you information about tools and guidance you can use to assess your own environment and help you deploy Windows Server 2016.

Lesson Objectives

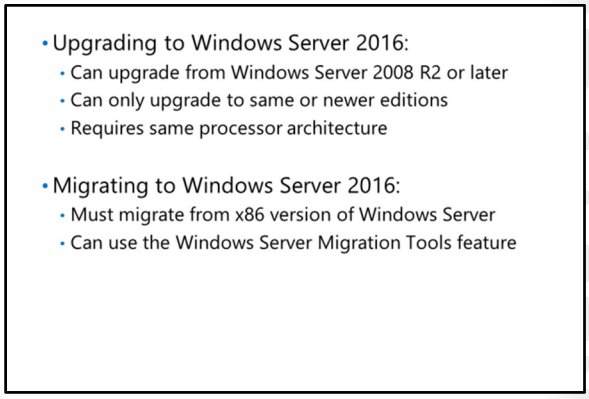
After completing this lesson, you will be able to:

- Describe the differences between an in-place upgrade and migration.
- Identify scenarios when an in-place upgrade is appropriate.
- Identify the benefits of migrating to Windows Server 2016.
- List solution accelerators available to help with your upgrade or migration.
- Describe best practices for server consolidation.

In-place upgrades vs. server migration

When deploying Windows Server 2016, organizations must make the following choice:

- Use existing hardware and upgrade from supported editions of Windows Server 2008 or later.
- Install Windows Server 2016 on new hardware, and, if required, migrate the roles, features, and settings from servers that are running supported earlier Windows Server editions.



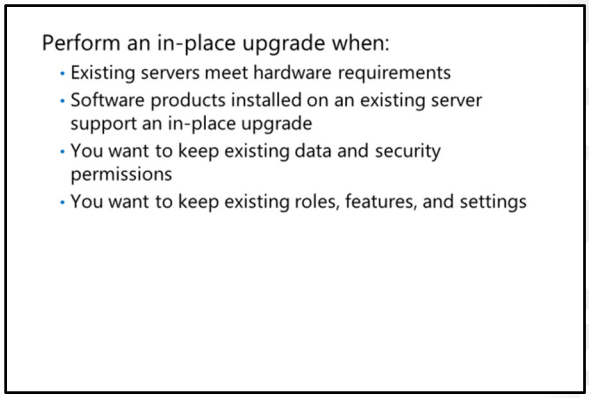
When planning whether to upgrade or migrate a server to Windows Server 2016, consider the options in the following table.

Installation option	Description
Upgrade	An upgrade preserves the files, settings, and applications that are installed on the original server. You perform an upgrade when you want to keep all these items and want to continue using the same server hardware. An upgrade requires x64 processor architecture and an x64 edition of the Windows Server operating system. If you are upgrading from Windows Server 2008 R2, you must install Service Pack 1 (SP1). You start an upgrade by running the **Windows Server 2016 Setup** wizard from the original Windows Server operating system.

<table>
<tr><th>Installation option</th><th>Description</th></tr>
<tr><td></td><td>You can perform the following upgrades to Windows Server 2016:
<table>
<tr><td>Original operating system and edition</td><td>Upgrade edition</td></tr>
<tr><td>Windows Server 2008 R2 Standard or Windows Server 2008 R2 Enterprise</td><td>Windows Server 2016 Standard, Windows Server 2016 Datacenter</td></tr>
<tr><td>Windows Server 2008 R2 Datacenter</td><td>Windows Server 2016 Datacenter</td></tr>
<tr><td>Windows Web Server 2008 R2</td><td>Windows Server 2016 Standard</td></tr>
<tr><td>Windows Server 2008 R2 Datacenter with SP1</td><td>Windows Server 2016 Datacenter</td></tr>
<tr><td>Windows Server 2008 R2 Enterprise with SP1</td><td>Windows Server 2016 Standard or Windows Server 2016 Datacenter</td></tr>
<tr><td>Windows Server 2008 R2 Standard with SP1</td><td>Windows Server 2016 Standard or Windows Server 2016 Datacenter</td></tr>
<tr><td>Windows Web Server 2008 R2 with SP1</td><td>Windows Server 2016 Standard</td></tr>
<tr><td>Windows Server 2012 Datacenter or Windows Server 2012 R2 Datacenter</td><td>Windows Server 2016 Datacenter</td></tr>
<tr><td>Windows Server 2012 Standard or Windows Server 2012 R2 Standard</td><td>Windows Server 2016 Standard or Windows Server 2016 Datacenter</td></tr>
</table></td></tr>
<tr><td>Migration</td><td>Use migration when you migrate from an x86 edition of Windows Server 2003, Windows Server 2003 R2, or Windows Server 2008. You can use the Windows Server Migration Tools feature in Windows Server 2016 to transfer files and settings from computers that are running the following editions:
Windows Server 2003
Windows Server 2003 R2
Windows Server 2008
Windows Server 2008 R2
Windows Server 2012
Windows Server 2012 R2</td></tr>
</table>

Additional Reading: For more information on migration, refer to: "Install, Use, and Remove Windows Server Migration Tools" at: http://aka.ms/p3xxrr

In-place upgrade scenarios



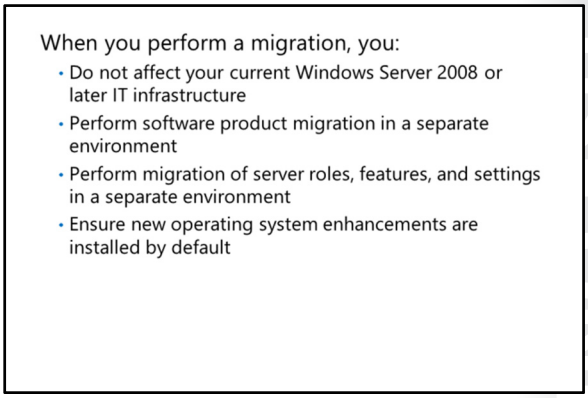
An in-place upgrade involves upgrading a Windows Server operating system on the server that is running an earlier Windows Server edition. A benefit of an in-place upgrade is that you avoid hardware expenses because you install Windows Server 2016 on the existing hardware. Another benefit is that files, settings, and programs are kept intact on the server. You would choose an in-place upgrade of the Windows Server operating system in the following scenarios:

- When the hardware configuration of the existing servers meets the requirements for Windows Server 2016. Because the hardware requirements for Windows Server 2016 do not differ significantly from those for Windows Server 2012 R2, you can most likely perform an in-place upgrade on those servers.
- When the software products that run on the existing servers support in-place upgrade of Windows Server 2016. Before performing an in-place upgrade, you must list all of the software products that are running on the server, such as SQL Server, Exchange Server, non-Microsoft software, and antivirus software. Next, verify that these products support an in-place upgrade of Windows Server 2016. If so, refer to the specific product's documentation to determine how to perform an in-place upgrade, including any issues or risks that might occur.
- When you want to keep all user data that is on the existing servers, such as data stored on file servers, and security permissions for accessing those data. When performing an in-place upgrade, user data and security permissions for accessing the data remain unchanged. This scenario is convenient, because after the in-place upgrade, users can continue to access their data that on the same file servers.
- When you want to install Windows Server 2016, but you want to keep all roles, features, and settings of the existing server. Before performing an in-place upgrade on a server that has specific roles, features, or settings—such as Dynamic Host Configuration Protocol (DHCP), Domain Name System (DNS), or AD DS—list those configurations. Then, check if those configurations support an in-place upgrade of Windows Server 2016. If so, refer to the detailed instructions for the specific roles, features, or settings on how to perform the in-place upgrade, including any issues or risks that might occur.

If any of these scenarios do not meet your organization's requirements, then you should perform a migration to Windows Server 2016.

Benefits of migrating to Windows Server 2016

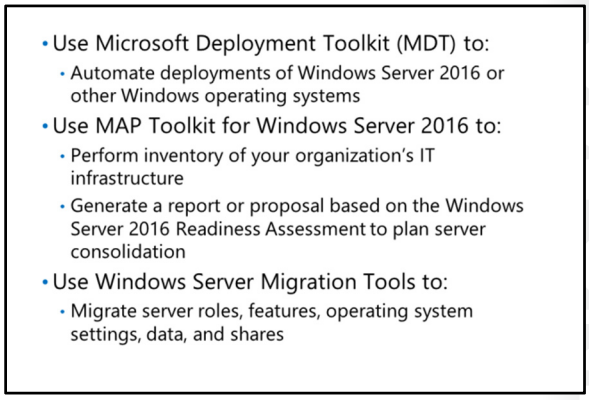
When deploying Windows Server 2016, some organizations should consider migration instead of an in-place upgrade. There can be risks that arise from an in-place upgrade, such as server unavailability or data being inaccessible. Therefore, your organization might choose to perform a migration because of the following benefits:



- You will deploy servers with the Windows Server 2016 operating system installed, and they will not affect the current IT infrastructure. Once you install Windows Server 2016, you can perform tests, such as drivers or system performance tests, before you introduce that server to the domain. In this way, the process of installation and testing is less likely to affect your current IT infrastructure.
- You will perform software product migration in a separate environment. For any software solution with an earlier Windows Server edition, you must refer to the product documentation for information about how to migrate that solution to Windows Server 2016. In some scenarios, software products that you are using are not supported for installation on Windows Server 2016, and you will require newer editions of those software products. In this case, by using migration, you can perform systematic installation of the operating system and the software products, in a separate environment. This ensures that the migration does not affect the availability of current services that the software provides.
- You will perform migration of server roles, features, and settings in a separate environment. As with the migration of software products, refer to the documentation on how to migrate the specific roles, features, or settings, such as DHCP, DNS, or AD DS, to Windows Server 2016. Again, migration enables you to perform systematic configuration in a separate environment, which means that the migration should not affect availability of server roles, features, and settings.
- New operating system enhancements are installed by default. When performing an in-place upgrade, for compatibility reasons, Windows Server 2016 is configured with settings for Windows Server 2008 or Windows Server 2008 R2. This means that many enhancements that Windows Server 2016 introduces, such as security, functionality, or performance enhancements, are not enabled by default. When performing migration, Windows Server 2016 deploys as a clean installation with all new enhancements installed. This ensures that the operating system is more secure and has new functionalities installed by default.

Using solution accelerators

Organizations should consider using software tools to help them plan their upgrade and migration to Windows Server 2016. Along with guidance content to help you design and plan your Windows Server 2016 deployment, Microsoft also provides solution accelerators to assist in the process.



Microsoft Deployment Toolkit

Microsoft Deployment Toolkit (MDT) is both a process and a lightweight tool for automated server (and desktop) deployments. It is used for deploying standardized images. MDT is based on a variety of Microsoft technologies including PXE, Windows Deployment Services (WDS), and System Center Configuration Manager (SCCM). MDT automates the deployment process by configuring unattended Setup files and packaging the files into an image file that you can deploy to a target computer.

Additional Reading: For more information about using MDT as part of a complete deployment solution, refer to: "Automate and manage Windows operating system deployments" at: http://aka.ms/Mi7wfx

For more information about MDT, including the latest updates, refer to: "Microsoft Deployment Toolkit" at: http://aka.ms/de2ej0

Microsoft Assessment and Planning Toolkit (MAP)

The **Microsoft Assessment and Planning Toolkit** (MAP) is a solution accelerator that analyzes the inventory of an organization's server infrastructure, performs an assessment, and then creates reports that you can use for upgrade and migration plans. MAP is available for Windows Server 2016, Windows Server 2012 R2, Windows 10, Windows 8.1, and for other products, such as SQL Server 2014 and Hyper-V.

Use MAP to perform the following tasks:

- Inventory your organization's IT infrastructure. Based on the inventory, MAP displays a detailed report about which machines are capable of running Windows Server 2016, which machines are capable of running Windows Server 2016 with minimum system requirements, and which machines are not capable of running Windows Server 2016. MAP also recommends specific upgrades that ensure computers are capable of running Windows Server 2016.
- Generate a report or proposal based on the Windows Server 2016 Readiness Assessment. The report or proposal is a document that contains an Executive Overview, Assessment Results, Next Steps, and a worksheet summarizing Windows Server 2016 readiness for computers that are running Windows Server.
- Capture the performance metrics of the current IT infrastructure, to help plan consolidation and server virtualization. The performance assessment generates reports on performance and presents the server consolidation recommendations.
- Estimate server utilization based on that metric before and after the virtualization. You also can choose which current physical servers are the best candidates for virtualization, and the hosts on which you should place those virtual machines.

Reference Links: For more information about the Microsoft Assessment and Planning (MAP) Toolkit, refer to: http://aka.ms/u7x2mf

Win Server migration tools

Windows Server 2016 includes tools to assist you in migrating server roles and features from one computer to another. These Windows PowerShell cmdlets are part of a snap-in that are installed as part of a full installation or Core Server installation. Microsoft also provides detailed migration guides for specific roles.

Additional Reading: For more information about the Windows Server Migration Tools and migration guides for specific roles and features, refer to: "Migrate Roles and Features to Windows Server" at: http://aka.ms/mr3jqp

Recommendations for server consolidation

- Analyze if cohosting of multiple roles is supported
- Deploy roles that are not supported for cohosting on additional servers
- Determine if cohosting multiple roles affects server performance (it should not)
- Analyze if cohosted roles are supported for high availability

When Deploying Windows Server 2016, you should plan your placements of server roles, such as AD DS, DNS, and DHCP, to make the best use of hardware and network resources. Organizations should consider cohosting multiple roles, where possible, to achieve the most economical solution. Virtualization is also considered as a consolidation of the server roles. Nano Server is particularly helpful in consolidating multiple server roles to a single machine. However, you should not implement cohosting if it affects server performance or available disk space. Therefore, organizations should evaluate and test whether installing multiple server roles on a server would result in lower overall performance and disk usage. Furthermore, organizations should evaluate the security risks of collocating server roles. For example, the server that hosts the root Active Directory Certificate Services role should not be collocated with other server roles and should be offline most of the time.

Smaller organizations should consider the following best practices:

- Plan which server roles you need. If the operating system supports cohosting of those roles on one server, then multiple roles can be installed and cohosted on a single server. If cohosting multiple server roles on one physical server affects the performance of the physical server, then administrators should not cohost the server roles, and should install server roles on different physical servers.
- If the operating system on a physical host does not support that multiple server roles are cohosted, then administrators should deploy server roles on multiple physical servers.

Medium and large organizations should consider the following performance and high-availability issues when cohosting:

- If you are cohosting multiple roles on a single server, there might be performance issues because of the large number of client computers that are connecting to that server. In this situation, organizations should consider adding multiple servers that cohost the same multiple roles. They also should consider relocating some of the roles from the first server to the other physical servers.
- High availability configurations of roles have specific requirements and setting, which might not support cohosting of multiple roles. In this situation, organizations could have a high availability solution for one server role, and then must locate remaining roles on other servers.

Demonstration: Using MAP

In this demonstration you will see how to:

- Review the MAP options.
- Perform an inventory assessment by using MAP.
- Review the inventory from a sample database.

Demonstration Steps

Review the MAP options

1. On **LON-CL1**, run the **Microsoft Assessment and Planning Toolkit**.
2. In the **Microsoft Assessment and Planning Toolkit** console, review the default window that displays the **Overview** page.
3. In the **Microsoft Assessment and Planning Toolkit** console, in the left pane, select **Cloud**, and then review the readiness information for the different cloud scenarios.
4. In the **Microsoft Assessment and Planning Toolkit** console, in the left pane, click **Desktop**, and review the readiness information for the different desktop scenarios.
5. Repeat step 4 for all remaining items in the left pane: **Server**, **Desktop Virtualization**, **Server Virtualization**, **Database**, **Usage Tracking**, and **Environment**.

Perform inventory

1. On **LON-CL1**, in the **Microsoft Assessment and Planning Toolkit** console, in the left pane, select **Overview**, and then in the **Overview** page, create an inventory database named **INVENTORY**.
2. On the **Overview** page, select **Perform an inventory**.
3. In the **Inventory and Assessment Wizard** window, perform the following steps:
   a. On the **Inventory Scenarios** page, select the following check boxes:
      - **Windows computers**
      - **Exchange Server**
      - **Lync Server**
      - **SQL Server**
      - **Windows Azure Platform Migration**
   b. On the **Discovery Methods** page, select **Use Active Directory Domain Services**, **Use Windows networking protocols**, and **Scan an IP address range**.
   c. On the **Active Directory Credentials** page, in the **Domain** field, enter **Adatum.com**. In the **Domain Account** field, enter **Adatum\Administrator**, and then in the **Password** field, type **Pa$$w0rd**, and on the next two pages accept the default settings.
   d. On the **Scan an IP Address Range** page, enter the range from **172.16.0.1** to **172.16.0.100**.
   e. On the **All Computers Credentials** page, accept the default settings.
   f. On the **Summary** page, review the inventory options, and then cancel the wizard.

Note: You cancel the inventory procedure because the lab does not contain an environment with older operating systems for MAP to discover. In the next step, you review the test inventory that you import from the sample database in MAP.

Review the MAP inventory from a sample database

1. In the **Microsoft Assessment and Planning Toolkit** console, on the **File** menu, select **Manage Databases**.
2. In the **Microsoft Assessment and Planning Toolkit** dialog box, import the sample database using the following steps:
   a. Select **Manage**.
   b. Import the sample database located in following path: In the **File name** field, type **C:\Program Files\Microsoft Assessment and Planning Toolkit\Sample \MAP_SampleDB.bak**.
   c. In the **Database Name** field, type **MAPDEMO**.
   d. In the **Microsoft Assessment and Planning Toolkit** window, choose the **Use an existing database** option, and then select **MAPDEMO** database.
3. In the **Microsoft Assessment and Planning Toolkit** console, review the default window that displays the **Overview** page that includes inventory information from the sample database. Refresh the window in **Overview** page, if necessary.
4. In the **Microsoft Assessment and Planning Toolkit** console, in the left pane, click **Cloud**, and then review the readiness information on the different cloud scenarios that displays with inventory information from the sample database.
5. In the **Microsoft Assessment and Planning Toolkit** console, in the left pane, click **Desktop**, and then review the readiness information on the different desktop scenarios that appear with inventory information from the sample database.
6. Repeat step 4 for all remaining items in the left pane: **Server**, **Desktop Virtualization**, **Server Virtualization**, **Database**, **Usage Tracking**, and **Environment**.

Question: How does virtualization help in server role consolidation?

Lesson 4
Migrating server roles and workloads

Organizations should plan to spend time creating a server upgrade and migration plan. Planning is critical for organizations that are considering new operating system deployments. There are different elements that affect the planning for a new operating system deployment, such as analyzing current IT infrastructure, choosing an operating system edition, creating an upgrade or migration strategy, and creating a strategy for backup, restoring, monitoring, and maintaining the operating system.

You must also determine which roles you can migrate, which you can cohost, and which you can consolidate into a virtual environment. Finally, you must plan for migrating roles within the same domain or across domains.

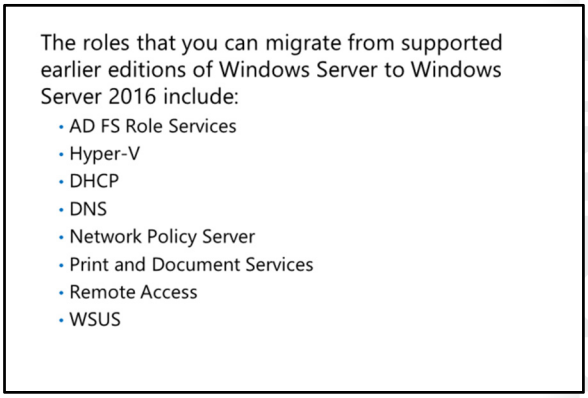
Lesson Objectives

At the end of this lesson, you will be able to:

- Explain how to implement server migrations.
- Explain how to migrate servers across domains.

Migrating server roles within a domain

When planning to migrate servers, you must create a list of the server roles that you want to migrate and the steps that each involves. For each server role that you plan to migrate, you should refer to the technical documentation and migration guides about how to perform the migration. When performing migration, you should use the Windows Server Migration Tools, which are available with Windows Server 2016.



The roles that you can migrate include:

- Active Directory Certificate Services
- Active Directory Federation Services (AD FS) Role Services
- File and Storage Services
- DHCP
- DNS
- Hyper-V
- Network Policy Server
- Print and Document Services
- Remote Access
- Remote Desktop Services
- Cluster Role Services
- Windows Server Update Services (WSUS)

Installing and preparing the Windows Server Migration Tools consists of the following steps:

1. Install the tools on destination servers as part of Windows Server 2016 setup.
2. Create a deployment folder containing a copy of the tools on the destination server.
3. Copy the deployment folder from destination server to source server.
4. Register Windows Server Migration Tools on the source server by using the **SmigDeploy.exe** tool included in the deployment folder.

Once the migration tools are installed, you can run them by using one of the following methods:

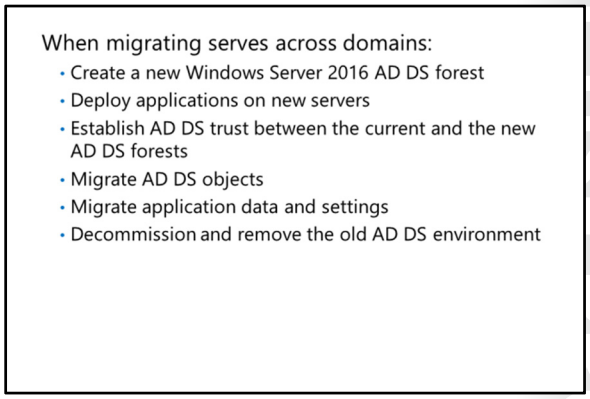
- Run **Windows Server Migration Tools** as an administrator from the Windows Start screen.
- Load the Windows Server Migration Tools snap-in into an elevated Windows PowerShell session.
- On source computers running earlier versions of Windows Server, run **Windows Server Migration Tools** under the **Windows PowerShell** folder, which is under the **All Programs** folder of the **Start** menu.

Note: You can migrate roles only from supported earlier Windows Server editions to Windows Server 2016.

Additional Reading: For more information about determining which roles and features to migrate, refer to the migration guides for Windows Server 2016 in "Migrate Roles and Features to Windows Server" at: http://aka.ms/mr3jqp

Migrating server roles across domains or forests

Organizations could choose to deploy Windows Server 2016 in a new AD DS forest. In this scenario, administrators should plan the migration steps carefully to provide users with seamless access to data and services during the migration process. Once the migration is complete, administrators should begin the process of decommissioning and removing the infrastructure of the previous operating system environment.



To migrate a server across domains:

- Create a new Windows Server 2016 AD DS forest that is independent from the forest that is running a previous operating system version.
- Deploy new servers that are running the Windows Server 2016 operating system.
- Deploy Microsoft applications, such as Exchange Server, SQL Server, and Microsoft SharePoint server in the new AD DS forest.
- Deploy corporate custom applications or third-party applications in the new AD DS forest that the previous infrastructure environment used.
- Configure DNS infrastructure in both forests.
- Establish AD DS trust between the current and the new AD DS forests.

- Migrate AD DS objects, such as users, computers, groups, and mailboxes.
- Migrate application data and settings for Microsoft applications, corporate custom applications, and third-party applications.
- Ensure that users can connect to corporate IT resources in the new AD DS forest.
- Decommission and remove the environment, based on previous operating system's AD DS forest.

Note: For each product and application that you plan to migrate to Windows Server 2016 AD DS forest, read the product documentation and best practices, including the supported migration procedures.

You will find this information on the website of each of the products.

Note: You must use a tool, such as the Active Directory Migration Tool (ADMT), to migrate resources such as users, computers, and groups across forests or within the same forest. For more information about using ADMT, refer to: "ADMT Guide: Migrating and Restructuring Active Directory Domains" at: http://aka.ms/Lb96ie

Question: What are some reasons you would do a cross-forest migration instead of a migration within the same domain?

Lesson 5
Windows Server activation models

As part of planning your server upgrade and migration process, you should also consider how you will manage operating system licensing and activation. Your choice of activation model will be based on the characteristics of your environment.

Lesson Objectives

After this lesson you will be able to:

- Describe the volume licensing and activation options for Windows Server 2016.
- Plan a suitable volume activation process.

Windows Server 2016 licensing and activation

To ensure that your organization has the proper licenses, and to receive notices for product updates, you must activate every copy of Windows Server 2016 that you install. Windows Server 2016 requires that you activate the operating system after installation. This verifies that the products are licensed and that you receive important update information. There is no activation grace period. If you do not activate Windows Server 2016, you cannot customize your operating system. There are two general activation strategies:

Organizations can choose between two activation strategies:

Activation strategy	When used
Manual	Suitable when deploying small number of servers
Automatic	Suitable when deploying larger number of servers

- Manual activation. This strategy is suitable when you deploy a small number of servers.
- Automatic activation. This strategy is suitable when you deploy a larger numbers of servers.

Manual activation

When you use manual activation, you must enter the product key. Microsoft or an administrator performs the activation over the phone or through a special clearinghouse website.

You can perform manual activation by using the retail product key or the multiple activation key. You can use a retail product key to activate only a single computer. However, a multiple activation key has a set number of activations that you can use. This allows you to activate multiple computers, up to a set activation limit.

OEM keys are a special type of activation key that a manufacturer receives, and which enable automatic activation when a computer starts. You typically use this type of activation key with computers that are running Windows client operating systems, such as Windows 7 and Windows 8. You rarely use OEM keys with computers that are running Windows Server operating systems.

Automatic activation

Performing activation manually in large-scale server deployments can be cumbersome. Microsoft provides a method of activating large numbers of computers automatically, without having to enter product keys manually on each system.

There are a several technologies available that help automate the process of activating Windows Server licenses:

- Key Management Services (KMS). KMS is a service that helps you activate licenses on systems within your network from a server where a KMS host has been installed. The KMS host completes the activation process instead of individual computers connecting to Microsoft to complete activation.
- Volume Activation Services server role. This server role helps you to automate issuing and managing Microsoft software volume licenses. Volume Activation Services allows you to install and configure KMS and Active Directory-based Activation. KMS requires activating at least five servers and 25 clients. KMS is the default key for volume activation.
- Active Directory-Based Activation. This is a service that lets you use AD DS to store activation objects. A computer running Windows Server (or client) automatically contacts AD DS to receive an activation object, without the need to contact Microsoft. You can use Active Directory-based activation when activating servers and clients running Windows Server 2012 or later, and Windows 8 or later. Your AD DS schema must also be Windows Server 2012 or later.
- Volume Activation Tools console. The Volume Activation Tools console is used to install, activate, and manage volume license activation keys in AD DS or KMS.
- Volume Activation Management Tool (VAMT). The VAMT is a no cost tool that you can use to manage volume activation using Multiple Activation Keys (MAKs) or to manage KMS. You can use VAMT to generate license reports and manage client and server activation on enterprise networks.
- Multiple Activation Key (MAK). A MAK is a volume license key that you can use for independent activation by connecting with Microsoft or through proxy activation, where a single computer gathers the activation information for multiple computers and contacts Microsoft for them. Use MAK when your systems have poor—or no—connection with your organization's central network.
- Automatic Virtual Machine Activation (AVMA). AVMA lets you install VMs on a virtualization server with no product key.

 **Reference Links:** For more information on VAMT, refer to: "Introduction to VAMT" at: http://aka.ms/b07bed

Licensing changes since Windows Server 2008

As part of planning your deployment, you must ensure you have the proper number of licenses for your Windows Server 2016 installation. Windows Server 2016, like Windows Server 2012, is licensed by processor core, not by server. You can purchase additional licenses for two processor cores at a time.

Discussion: Planning volume activation

To implement a volume-activation process, you must consider which activation type is most suitable for your organization. Not all companies have the same IT infrastructure, and therefore scenarios differ for each company. You should consider the two scenarios that are shown on the slide when planning your organization's volume activation process.

Discuss both scenarios. Based on the scenario, what type of volume activation should you implement?

Question: Your organization's IT infrastructure consists of personal computers and servers that are running different editions of Windows client operating systems and Windows Server operating systems. Next month, your organization plans to deploy 500 Windows 10 client computers and 20 Windows Server 2016 servers. Because of a legacy application in the finance department, you must deploy 10 client computers that are running Windows 8.1 and two servers that are running Windows Server 2012 R2. What type of volume activation should you implement?

Question: Your organization's IT infrastructure was upgraded from different editions of Windows client operating systems and Windows Server operating systems to Windows 10 and Windows Server 2016, respectively. What type of volume activation should you implement?

Lab: Installing and configuring Nano Server

Scenario

You are responsible for implementing many of the new features in Windows Server 2016. To become familiar with the new operating system, you decide to install a new server running Windows Server 2016 and complete the post-installation configuration tasks.

Objectives

After completing this lab, you will be able to:

- Install the Nano Server option for Windows Server 2016.
- Configure Nano Server.

Lab Setup

Estimated Time: 60 minutes

Virtual machines: **20740A-LON-DC1**, **20740A-NANO-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 Microsoft Hyper-V Manager, click **20740A-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 and 3 for **20740A-NANO-SVR1**.
6. On **20740A-LON-DC1**, in the virtual machine connection window, click **Media**, point to **DVD Drive**, and then click **Insert Disk**.
7. Browse to **D:\Program Files\Microsoft Learning\20740\Drives** and then select **WinServer2016_TP5.iso**.
8. Click **Open**.

Exercise 1: Installing Nano Server

Scenario

You determine that Nano Server offers you the best installation option and decide to deploy a web server that uses Nano Server.

The main tasks for this exercise are as follows:

1. Copy the required Windows PowerShell scripts.
2. Import Windows PowerShell modules.
3. Create a virtual hard drive.
4. Sign in to the NANO-SVR1 virtual machine.

▶ Task 1: Copy the required Windows PowerShell scripts

1. On **LON-DC1**, open an elevated Windows PowerShell prompt.
2. Change to the root directory of drive C, and then make a folder called **Nano**.
3. Copy all the files with a .ps* extension from the **D:\NanoServer\NanoServerImageGenerator** folder to **C:\Nano**.

▶ Task 2: Import Windows PowerShell modules

- Run **Import-Module c:\nano\NanoServerImageGenerator.psm1**. This command imports the required Windows PowerShell module for Nano Server.

▶ Task 3: Create a virtual hard drive

1. Run **new-NanoServerImage -Edition Standard -mediapath D:\ -Basepath c:\nano -targetpath c:\nano\nano-svr1.vhdx -DeploymentType Guest -computername NANO-SVR1 -storage -packages Microsoft-NanoServer-IIS-Package**, and when prompted, type the password **Pa$$w0rd**.
2. Verify that **C:\Nano** contains a file called **nano-svr1.vhdx**.

Note: Normally, you would now create a virtual machine to use the **nano-svr1.vhdx** file. However, to expedite the process, you will start a virtual machine that has already been created.

▶ Task 4: Sign in to the NANO-SVR1 virtual machine

- On **NANO-SVR1**, sign in by using the following credentials:
  - User name: **Administrator**
  - Password: **Pa$$w0rd**

Results: After completing this exercise, you will have successfully created the required virtual hard drive for Nano Server.

Exercise 2: Completing post-installation tasks on Nano Server

Scenario

You must now complete the installation of Nano Server by configuring the post-installation settings and joining it to the Adatum.com domain.

The main tasks for this exercise are as follows:

1. Use the Nano Server Recovery Console to view basic settings.
2. Add Nano Server to the domain.
3. Use Windows PowerShell to configure the settings of Nano Server.

▶ Task 1: Use the Nano Server Recovery Console to view basic settings

1. On **NANO-SVR1**, observe that the computer name is **NANO-SVR1** and that the computer is in a workgroup.
2. In **Network Adapter Settings**, notice that DHCP is providing the IP configuration. Make a note of the IP address: _____

▶ Task 2: Add Nano Server to the domain

1. On **LON-DC1**, in the **Administrator: Windows PowerShell** window, run **djoin.exe /provision /domain adatum /machine nano-svr1 /savefile .\odjblob**. This creates a file that you will use to complete the process of adding Nano Server to the domain.

Note: Replace the IP address 172.16.0.X in the following commands with the IP address you recorded earlier from your Nano Server installation.

2. The following commands are used to enable Windows PowerShell remoting:

```
Set-Item WSMan:\localhost\Client\TrustedHosts "172.16.0.X"
$ip = "172.16.0.X"
Enter-PSSession -ComputerName $ip -Credential $ip\Administrator
```

3. In the **Windows PowerShell credential request** dialog box, in the **Password** box, type **Pa$$w0rd**, and then click **OK.**
4. To enable file sharing through the firewall, run **netsh advfirewall firewall set rule group="File and Printer Sharing" new enable=yes**.
5. Close the Windows PowerShell remoting session by running **Exit-PSSession**.
6. Map a network drive to the C drive on Nano Server. (**net use z: \\172.16.0.X\c$**)
7. Switch to the Z drive and then copy **C:odjblob** to the root of the C drive on Nano Server.
8. Reestablish a Windows PowerShell remoting session to Nano Server.
9. Run **djoin /requestodj /loadfile c:\odjblob /windowspath c:\windows /localos** to complete the process of adding the computer to the domain.
10. Run **shutdown /r /t 5** to restart Nano Server.
11. On **NANO-SVR1**, in the domain **Adatum**, sign in as **Administrator**/**Pa$$w0rd**.
12. In the **Nano Server Recovery Console**, observe that the computer is in the adatum.com domain.

▶ Task 3: Use Windows PowerShell to configure the settings of Nano Server

1. On **LON-DC1**, close Windows PowerShell.
2. Open an elevated Windows PowerShell prompt.
3. Run **get-windowsfeature –comp Nano-svr1** to list the installed roles and features on Nano Server.
4. To add the File Server role to Nano Server, run **install-windowsfeature Fs-fileserver –comp Nano-svr1**.
5. To verify the role is installed, run **get-windowsfeature –comp Nano-svr1**.
6. Enable a Windows PowerShell remoting session with Nano Server. Remember to change X to the last octet of the IP address of your Nano server:
   a. Run **$ip = "172.16.0.X"**.
   b. Run **Enter-PSSession -ComputerName $ip -Credential $ip\Administrator**.
7. When prompted, type **Pa$$w0rd** as the password.
8. To view the IP configuration of Nano Server, run **get-netipaddress**.
9. To view the startup environment of Nano Server, run **bcdedit /enum**.
10. To view the shared folders, run **net share**. Only default shares exist.
11. At the command prompt, type the following cmdlet, and then press Enter.

```
Exit-PSSession
```

Results: After completing this exercise, you will have successfully configured the domain and network settings of Nano Server and installed an additional role.

Exercise 3: Performing remote management

The main tasks for this exercise are as follows:

1. Enable remote management with Server Manager.
2. Test the file server and web server on Nano Server.
3. Prepare for the next module.

▶ Task 1: Enable remote management with Server Manager

1. On **LON-DC1**, in **Server Manager**, add **Nano-SVR1** to the **Computer** list.
2. In **Server Manager**, expand **File and Storage Services**, click **Shares**, and then in the **TASKS** list, click **New Share**.
3. Create a new shared folder:
   - Type: **SMB Share - Quick**
   - Server: **nano-svr1**
   - Share name: **Data**

▶ Task 2: Test the file server and web server on Nano Server

1. If necessary, on **LON-DC1**, map drive Z to **\\Nano-svr1\c$**.
2. Start **Notepad**, and then create a file with the following line.

```
<H1> Nano Server Website </H1>
```

3. Save the file called **Default.htm** to **z:\Inetpub\wwwroot**.
4. Open **Windows Internet Explorer**, and then navigate to **http://nano-svr1**. Does your web page display?
5. Map drive Y to **\\Nano-svr1\data**.
6. Open **WordPad**, create a file, and then save the file to the root of drive **Y**.
7. Use **File Explorer** to verify that your file is saved on **Nano-Svr1**.

▶ Task 3: Prepare for the next module

After you finish the lab, revert the virtual machines to their initial state by completing the following steps:

1. On the host computer, switch to the **Hyper-V Manager** console.
2. In the **Virtual Machines** list, right-click **20740A-LON-DC1**, and then click **Revert**.
3. In the **Revert Virtual Machine** dialog box, click **Revert**.
4. Repeat steps 2 and 3 for **20740A-NANO-SVR1**.

Question: In the lab, you used a virtual machine to run Nano Server. Having created your virtual hard drive, if you want to run Nano Server on a physical host, what commands do you use to configure the startup environment?

Module Review and Takeaways

Common Issues and Troubleshooting Tips

Common Issue	Troubleshooting Tip
Windows PowerShell cmdlets are not available	
You need a non-GUI interface method to shut down or restart a computer that is running Server Core	
You are unable to join a computer to the domain	

Review Questions

Question: When creating a virtual hard drive for Nano Server by using the Windows PowerShell cmdlet **New-NanoServerImage**, when do you use the **-Guestdrivers** switch?

Question: When using the **Nano Server Recovery Console**, which two fundamental components can you configure?

Question: Which role can you use to manage KMS?

Tools

These tools were mentioned in this module.

RSAT	Used for managing servers remotely from a Windows 10 workstation	Download from the Microsoft download center
DISM.exe	Used for image servicing and management	Start from a command prompt or Windows PowerShell console
Windows Server Migration Tools	Use for assistance in migrating from one version of Windows Server to another version	Download from the Microsoft download center
Volume Activation Management Tool	Use the VAMT to manage Multiple Activation Keys (MAKs)	Download from the Microsoft download center

Module 2

Configuring local storage

Contents:

Module Overview

Storage is one of the key components that you must consider when planning and deploying the Windows Server 2016 operating system. Most organizations require a great deal of storage because users work regularly with apps that create new files, which in turn require storage in a central location. When users keep their files for longer periods of time, all the while adding more files, storage demands increase. Therefore, it is important that you know how to manage disks and volumes in Windows Server 2016 to help meet the storage needs of your users.

Objectives

After completing this module, you will be able to:

- Manage disks in Windows Server.
- Manage volumes in Windows Server.

Lesson 1
Managing disks in Windows Server

Identifying which storage technology that you want to deploy is the first critical step in addressing the data-storage requirements of your organization. However, this is only the first step. You also must determine the best way to manage that storage, and should ask yourself the following questions:

- Which disks are you going to allocate to a storage solution?
- Which file systems will you use?

This lesson explores these questions.

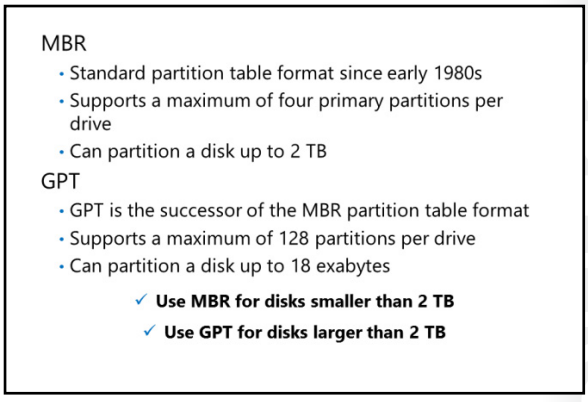
Lesson Objectives

After completing this lesson, you will be able to:

- Explain how to select a partition table format.
- Describe the difference between basic and dynamic disk types.
- Explain how to select a file system.
- Describe a resilient file system.
- Configure Resilient File System (ReFS).
- Implement virtual hard disks.
- Determine the disk type that best meets your requirements. .

Selecting a partition table format

A partition table format (or *partition style*) refers to the method that an operating system such as Windows Server 2016 uses to organize partitions or volumes on a disk. For Windows operating systems, you can decide between a master boot record (MBR) and a globally unique identifier (GUID) partition table (GPT).



MBR

The *MBR partition table format* is the standard partitioning scheme that has been used on hard disks since the inception of personal computers in the 1980s. The MBR partition table format has the following characteristics:

- An MBR partition supports a maximum of four primary partitions per drive.
- It can have a maximum size of 2 terabytes (TB) (2.19 x 10^12 bytes).
- If you initialize a disk larger than 2 TB using MBR, the disks stores volumes only up to 2 TB, and the rest of the storage is not used. You must convert the disk to GPT if you want to use all of its space.

Note: You can use the MBR partition table format for disk drives that never surpass 2 TB in size. This provides you with a bit more space, because GPT requires more disk space than MBR.

GPT

The GPT format was introduced with Windows Server 2003 and the Windows XP 64-bit edition to overcome the limitations of MBR, and to address the requirement of larger disks. GPT has the following characteristics:

- GPT supports a maximum of 128 partitions per drive.
- A partition can have up to 18 exabytes.
- A hard disk can have up to 8 zettabytes (ZB), with 512 kilobytes (KB) logical block addressing (LBA).
- To boot from a GPT partition table, your BIOS must support GPT.

Note: If your hard disk is larger than 2 TB, you must use the GPT partition table format.

Additional Reading: For more information, refer to: "Frequently asked questions about the GUID Partitioning Table disk architecture" at: http://aka.ms/sha5x0

Selecting a disk type

When selecting a type of disk for use in Windows Server 2016, you can choose between basic and dynamic disks.

Basic disks are:
- Disks initialized for basic storage
- The default storage for the Windows operating system

Dynamic disks can:
- Be modified without restarting the Windows system
- Provide several options for configuring volumes

Disk volume requirements include:
- A system volume for hardware-specific files that are required to start the server
- A boot volume for the Windows operating system files

Basic disk

Basic storage uses partition tables that are used by all versions of the Windows operating system. A basic disk is initialized for simple storage, and contains partitions, such as primary partitions and extended partitions. You can subdivide extended partitions into logical volumes.

By default, when you initialize a disk in the Windows operating system, the disk is configured as a basic disk. It is easy to convert basic disks to dynamic disks without any data loss. However, when you convert a dynamic disk to basic disk, all data on the disk is lost.

There is no performance gain when you convert basic disks to dynamic disks, and some programs cannot address data that is stored on dynamic disks. For these reasons, most administrators do not convert basic disks to dynamic disks, unless they need to use some of the additional volume-configuration options that dynamic disks provide.

Dynamic disk

Dynamic storage enables you to perform disk and volume management without having to restart computers that are running Windows operating systems. A *dynamic disk* is a disk that you initialize for dynamic storage, and that contains dynamic volumes. Dynamic disks are used for configuring fault tolerant storage.

When you configure dynamic disks, you create volumes rather than partitions. A *volume* is a storage unit that is made from free space on one or more disks. You can format the volume with a file system and then assign it a drive letter, or configure it with a mount point.

Required Disk Volumes

Regardless of which type of disk you use, you must configure both a system volume and a boot volume on one of the server's hard disks:

- System volumes. The system volume contains the hardware-specific files that the Windows operating system needs to load, such as Bootmgr and BOOTSECT.bak. The system volume can be the same as the boot volume, although this is not required.
- Boot volumes. The boot volume contains the Windows operating system files that are in the %Systemroot% and %Systemroot%\System32 folders. The boot volume can be the same as the system volume, although this is not required.

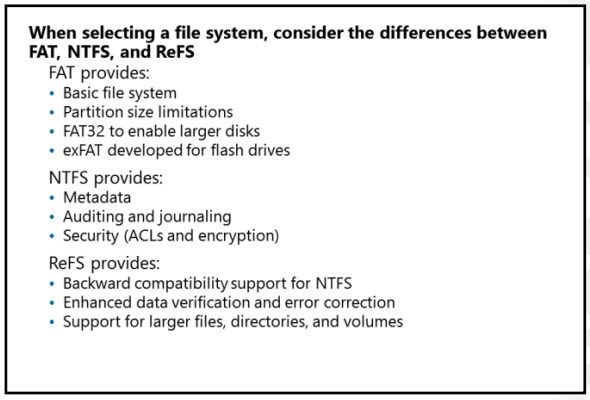
Note: When you install the Windows 10 operating system or the Windows Server 2016 operating system in a clean installation, a separate system volume is created to that you can subsequently choose to use to enable encrypting the boot volume by using BitLocker Drive Encryption.

Additional Reading: For more information, refer to: "How Basic Disks and Volumes Work" at: http://aka.ms/afknbd

For more information, refer to: "Dynamic disks and volumes" at: http://aka.ms/b8yl5i

Selecting a file system

When you configure your disks in Windows Server 2016, you can choose between file allocation table (FAT), the NTFS file system, and ReFS file systems.



FAT

The FAT file system is the most simplistic of the file systems that the Windows operating system supports. The FAT file system is characterized by a table that resides at the top of the volume. To protect the volume, two copies of the FAT file system are maintained in case one becomes damaged. Additionally, the file allocation tables and the root directory must be stored in a fixed location, so that the system's boot files can be located.

A disk formatted with the FAT file system is allocated in clusters, and the size of the volume determines the size of the clusters. When you create a file, an entry is created in the directory, and the first cluster number containing data is established. This entry in the table either indicates that this is the last cluster of the file, or points to the next cluster. There is no organization to the FAT directory structure, and files are given the first open location on the drive.

Because of the size limitation with the file allocation table, the original release of FAT could only access partitions that were less than 2 gigabyte (GB) in size. To enable larger disks, Microsoft developed FAT32, which supports partitions of up to 2 TB.

FAT does not provide any security for files on the partition. You should never use FAT or FAT32 as the file system for disks attached to Windows Server 2016 servers. However, you might consider using FAT or FAT32 to format external media such as USB flash media.

The file system designed especially for flash drives is Extended FAT (exFAT). You can use it when FAT32 is not suitable, such as when you need a disk format that works with a television, which requires a disk that is larger than 2 TB. A number of media devices support exFAT, such as modern flat panel TVs, media centers, and portable media players.

NTFS

NTFS is the standard file system for all Windows operating systems beginning with the Windows NT Server 3.1 operating system. Unlike FAT, there are no special objects on the disk, and there is no dependence on the underlying hardware, such as 512-byte sectors. In addition, in NTFS there are no special locations on the disk, such as the tables.

NTFS is an improvement over FAT in several ways, including better support for metadata, and the use of advanced data structures to improve performance, reliability, and disk space utilization. NTFS also has additional extensions such as security access control lists (ACLs), which you can use for auditing, file-system journaling, and encryption.

NTFS is required for a number of Windows Server 2016 roles and features such as Active Directory Domain Services (AD DS), Volume Shadow Copy Service (VSS), Distributed File System (DFS), and file replication service (FRS). NTFS also provides a significantly higher level of security than FAT or FAT 32.

ReFS

Windows Server 2012 first introduced ReFS to enhance the capabilities of NTFS. ReFS improves upon NTFS by offering larger maximum sizes for individual files, directories, disk volumes, and other items. Additionally, ReFS offers greater resiliency, meaning better data verification, error correction, and scalability.

You should use ReFS with Windows Server 2016 for very large volumes and file shares, to overcome the NTFS limitation of error checking and correction. However, you cannot use ReFS for the boot volume.

Additional Reading:

- For more information, refer to: "How FAT Works" at: http://aka.ms/j4j5nm
- For more information, refer to: "How NTFS Works" at: http://aka.ms/H6hp4c

Sector size

When you format a disk using a particular file system, you must specify the appropriate sector size. In the **Format Partition** dialog box, the sector size is described as the *Allocation unit size*. You can select from 512 bytes through to 64 KB. To improve performance, try and match the allocation unit size as closely as possible to the typical file or record size that will be written to the disk. For example, if you have a database that writes 8,192 byte records, the optimum allocation unit size would be 8 KB. This setting would allow for the operating system to write a complete record in a single allocation unit on the disk. By using a 4 KB allocation unit size, the operating system would have to split the record across two allocation units and then update the disk's master file table with the fact that the allocation units were linked. By using an allocation unit at least as big as the record, you can reduce the workload on the server's disk subsystem.

Be aware that the smallest writable unit is the allocation unit. If your database records are all 4,096 bytes, and your allocation unit size is 8 KB, then you will be wasting 4,096 bytes per database write.

Question: What file system do you currently use on your file server and will you continue to use it?

Implementing ReFS

ReFS is a file system that is based on the NTFS file system. It provides the following advantages over NTFS:

- Metadata integrity with checksums
- Expanded protection against data corruption
- Maximizes reliability, especially during a loss of power (while NTFS has been known to experience corruption in similar circumstances)
- Large volume, file, and directory sizes
- Storage pooling and virtualization, which makes creating and managing file systems easier
- Redundancy for fault tolerance
- Disk scrubbing for protection against latent disk errors
- Resiliency to corruptions with recovery for maximum volume availability
- Shared storage pools across machines for additional failure tolerance and load balancing

ReFS has a number of advantages over NTFS:

Metadata integrity with checksums
Integrity streams with user data integrity
Allocation on write transactional model
Large volume, file, and directory sizes (2^78 bytes with 16 KB cluster size)
Storage pooling and virtualization
Data striping for performance and redundancy
Disk scrubbing for protection against latent disk errors
Resiliency to corruptions with recovery
Shared storage pools across machines

ReFS inherits some features from NTFS, including the following:

- BitLocker Drive Encryption
- ACLs for security
- Update sequence number (USN) journal
- Change notifications
- Symbolic links, junction points, mount points and reparse points
- Volume snapshots
- File IDs

ReFS uses a subset of NTFS features, so it maintains backward compatibility with NTFS. Therefore, programs that run on Windows Server 2016 can access files on ReFS just as they would on NTFS. However, an ReFS-formatted drive is not recognized when placed in computers that are running Windows Server operating systems that were released previous to Windows Server 2012. You can use ReFS drives with Windows 10 and Windows 8.1, but not with Windows 8.

NTFS enables you to change a volume's allocation unit size. However, with ReFS, each volume has a fixed size of 64 KB, which you cannot change. ReFS does not support Encrypted File System (EFS) for files.

As its name implies, the new file system offers greater resiliency, meaning better data verification, error correction, and scalability.

Compared to NTFS,ReFS offersing larger maximum sizes for individual files, directories, disk volumes, and other items, which the following table lists.

Attribute	Limit
Maximum size of a single file	Approximately 16 exabytes (EB) (18.446.744.073.709.551.616 bytes)
Maximum size of a single volume	2^78 bytes with 16 KB cluster size (2^64 * 16 * 2^10) Windows stack addressing allows 2^64 bytes
Maximum number of files in a directory	2^64
Maximum number of directories in a volume	2^64
Maximum file name length	32,000 Unicode characters
Maximum path length	32,000
Maximum size of any storage pool	4 petabytes (PB)
Maximum number of storage pools in a system	No limit
Maximum number of spaces in a storage pool	No limit

When to use ReFS

ReFS is ideal in the following situations:

- Microsoft Hyper-V workloads. ReFS has performance advantages when using both .vhd and .vhdx files.
- Storage Spaces Direct. In Windows Server 2016, nodes in a cluster can share direct attached storage. In this situation, ReFS provides improved throughput, but also supports higher capacity disks used by the cluster nodes.
- Archive data. The resiliency that ReFS provides means it is a good choice for data that you want to retain for longer periods.

 **Additional Reading:** For more information about ReFS, refer to: "Building the next generation file system for Windows: ReFS" at: http://aka.ms/orvy9u

Demonstration: Configuring ReFS

In this demonstration, you will see how to:

- Retrieve the volume and sector information for an NTFS volume by using the **fsutil** command.
- Reformat the NTFS volume as a ReFS volume.
- Retrieve the volume and sector information for the ReFS volume by using the **fsutil** command.

Demonstration Steps

Retrieve information for an NTFS volume

1. On **LON-SVR1**, open **Disk Management** and create a new NTFS Simple Volume with all available space on Disk 2.
2. Assign drive letter **F** to the new volume.
3. Run the **fsutil fsinfo volumeinfo f:** command to view information about the NTFS volume.
4. Run the **fsutil fsinfo sectorinfo f:** command to view the sector information about the NTFS volume.

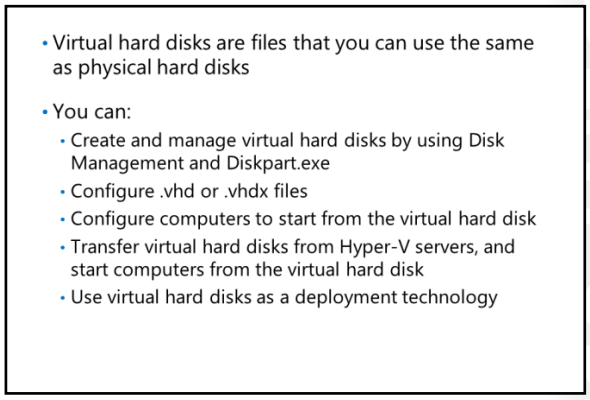
Reformat the volume

- Reformat the NTFS volume as an ReFS volume.

Retrieve information for an ReFS volume

1. Run the **fsutil fsinfo volumeinfo f:** to view information about the ReFS volume.
2. Run the **fsutil fsinfo sectorinfo f:** command to view the sector information about the ReFS volume.
3. Scroll back through the output to view the differences between the file system capabilities.

Using .vhd and .vhdx file types



You can manage virtual hard disks within Windows Server 2016 in much the same way that you can manage physical disks. For example, you can create and attach a virtual hard disk and use it for storing data. The virtual hard disk appears as another drive letter in the disk or folder management tools.

Virtual hard disks are files that represent a traditional hard disk drive. Typically, in Hyper-V, you use virtual hard disks as the operating system disk and storage disks for virtual machines. In Windows Server 2016, you can access the same virtual hard disks from within the operating system. The virtual hard disks have the following characteristics:

- In Windows 7 and Windows Server 2008 R2, you can only work with .vhd files.
- In Windows 8, Windows 8.1, Windows 10, or Windows Server 2012 or later, you also can create and manage .vhdx files, which enable much larger disk sizes and provide other benefits.
- You can create and attach virtual hard disks by using disk management tools such as Disk Management and **Diskpart.exe**. After creating and attaching the virtual hard disk, you can create volumes on the drive and format the partition. Additionally, in Windows 8 or newer versions, and Windows Server 2012 or newer versions, you can mount virtual hard disks in File Explorer.
- You can configure Windows Server 2016 to start from a virtual hard disk using the native virtual hard disk boot feature. This feature enables you to configure multiple operating systems on a single computer and choose which operating system to use when you start the computer.

- You can attach virtual hard disks that you create by using Hyper-V, or that you create on another computer. For example, if you create a virtual hard disk in Hyper-V, you can copy that virtual hard disk to another computer, and then use the native virtual hard disk boot feature to start the computer using the virtual disk that you created in Hyper-V.
- You can use virtual hard disks as a deployment technology. For example, you can use Hyper-V to create a standard image for desktop or server computers, and then distribute the image to other computers.

You can use Windows PowerShell to create and manage virtual hard disks in Windows Server 2016. You must first have the Windows PowerShell Hyper-module installed. Then, you can use the following commands and cmdlets to create and manage virtual hard disks:

- **New-vhd**. Use this cmdlet to create virtual hard disk files. When you specify the path, using the extension .vhd or .vhdx defines the virtual hard disk file type. For example, the following cmdlet creates a new dynamically resizing .vhd file of 10 GB in size.

```
New-VHD -Path c:\sales.vhd -Dynamic -SizeBytes 10Gb
```

- **Mount-VHD**. Use this command to mount the VHD to create volumes and format files systems.
- **Initialize-disk**. Use this command to initialize the disk in preparation for creating volumes.
- **Get-vhd**. Use this command to retrieve information about a named .vhd file.
- **Set-vhd**. Use this cmdlet to configure the .vhd file properties. For example, the following cmdlet changes the physical sector size of the Sales.vhdx file.

```
Set-VHD –Path c:\Sales.vhdx –PhysicalSectorSizeBytes 4096
```

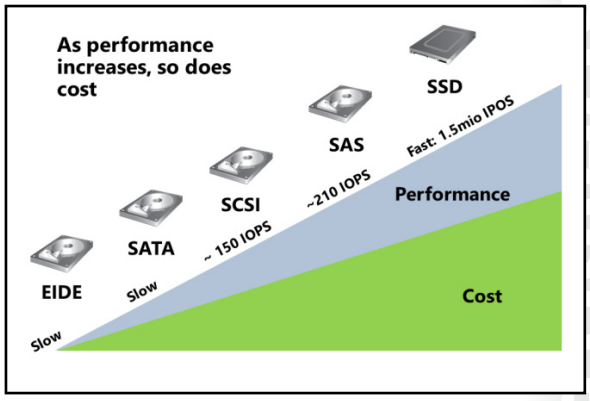
- **Convert-vhd**. You can use the Convert-vhd cmdlet to change from a VHD to a VHDX file format.

One of the benefits of using Windows PowerShell is the ability to script cmdlets, or to link them by using the pipe (**|**) operator. This can enable you to perform several tasks in one step. The following command will create a new virtual hard disk of type .vhd, and assign it a dynamic size of 10 GB. The .vhd is then mounted, and partitions and volumes created and formatted.

```
New-VHD -Path c:\sales.vhd -Dynamic -SizeBytes 10Gb | Mount-VHD -Passthru |Initialize-Disk -
Passthru |New-Partition -AssignDriveLetter -UseMaximumSize |Format-Volume -FileSystem NTFS -
Confirm:$false -Force
```

Selecting a disk type

There are various types of disks available that you can use to provide storage to server and client systems. The speed of disks is measured in input/output per second (IOPS). The most common types of disks are:



- Enhanced Integrated Drive Electronics (EIDE). EIDE is based on standards that were created in 1986. The integrated drive electronics (IDE) interface supports both the Advanced Technology Attachment 2 (ATA-2) and Advanced Technology Attachment Packet Interface (ATAPI) standards. *Enhanced* refers to the ATA-2 (Fast ATA) standard.

Due to the addressing standards of this technology, there is a 128 GB limitation on storage using EIDE. In addition, the speed of an EIDE drive is limited to a maximum of 133 megabytes (MB) per second (mbps). EIDE drives are seldom used today.

- Serial Advanced Technology Attachment (SATA). Introduced in 2003, SATA is a computer bus interface, or *channel*, for connecting the motherboard or device adapters to mass storage devices such as hard disk drives and optical drives. SATA was designed to replace EIDE. It can use the same low-level commands as EIDE, but SATA host adapters and devices communicate by using a high-speed serial cable over two pairs of conductors. SATA can operate at speeds of 1.5, 3.0, and 6.0 GB per second, depending on the SATA revision (1, 2 or 3 respectively).

  SATA disks are generally low-cost disks that provide mass storage. Because SATA drives are less expensive than other drive options (but also provide reduced performance), organizations might choose to deploy SATA drives when they require large amounts of storage but not high performance. SATA disks are also less reliable compared to serial attached SCSI (SAS) disks. A variation on the SATA interface is eSATA, which is designed to enable high-speed access to externally-attached SATA drives.

- Small computer system interface (SCSI). SCSI is a set of standards for physically connecting and transferring data between computers and peripheral devices. SCSI was originally introduced in 1978 and became a standard in 1986. Similar to EIDE, SCSI was designed to run over parallel cables; however, recently the usage has been expanded to run over other mediums. The 1986 parallel specification of SCSI had initial speed transfers of 5 mbps. The more recent 2003 implementation, Ultra 640 SCSI (also known as *Ultra 5*), can transfer data at speeds of 640 mbps. SCSI disks provide higher performance than SATA disks, but are also more expensive.

- SAS. SAS is a further implementation of the SCSI standard. SAS depends on a point-to-point serial protocol that replaces the parallel SCSI bus technology, and uses the standard SCSI command set. SAS offers backward-compatibility with second generation SATA drives. SAS drives are reliable and made for 24 hours a day, seven days a week (24/7) operation in data centers. With up to 15,000 rotations per minute, these disks are also the fastest traditional hard disks.

- Solid-state drives (SSDs). SSDs are data storage devices that use solid-state memory to store data rather than using the spinning disks and movable read/write heads that are used in other disks. SSDs use microchips to store the data and do not contain any moving parts. SSDs provide fast disk access, use less power, and are less susceptible to failure from being dropped than traditional hard disks such as SAS drives. However, they also are much more expensive per GB of storage. SSDs typically use a SATA interface, so you typically can replace hard disk drives with SSDs without any modifications.

 **Note:** Fibre Channel, FireWire, or USB-attached disks are also available storage options. They define either the transport bus or the disk type. For example, USB-attached disks are used mostly with SATA or SSD drives to store data.

Question: What disk types are you most commonly using in your organization, and do you have a management and provisioning strategy for storage usage in particular scenarios?

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

Statement	Answer
ReFS supports data deduplication in Windows Server 2016.	

Lesson 2
Managing volumes in Windows Server

A *volume* is a usable area of space on one or more physical disks, formatted with a file system. In Windows Server 2016, you can choose to use several different types of volumes to create high-performance storage, fault-tolerant storage, or a combination of both. This lesson explores how create and manage volumes in Windows Server 2016.

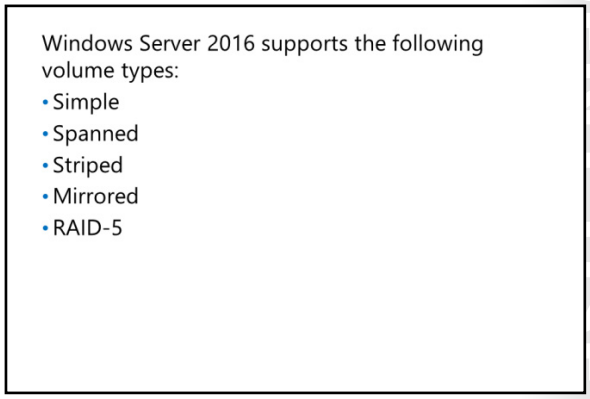
Lesson Objectives

After completing this lesson, you will be able to:

- Describe Windows Server 2016 disk volumes.
- Manage volumes.
- Configure volumes.
- Resize disk volumes.
- Describe Redundant Array of Independent Disks (RAID).
- Explain each of the RAID levels.

What are disk volumes?

In Windows Server 2016, if you are using dynamic disks, you can create a number of different types of disk volumes:



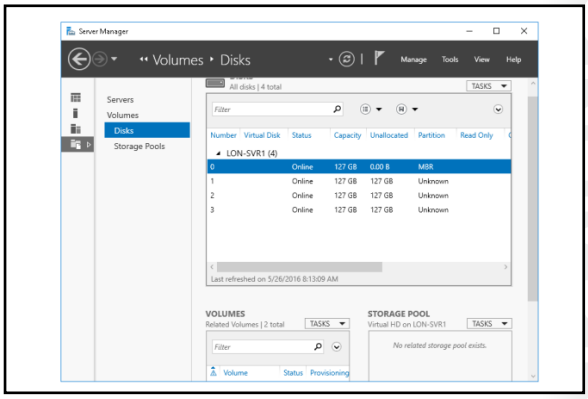
- Simple volumes. A *simple volume* is a volume that uses free space from a single disk. It can be a single region on a disk, or consist of multiple, concatenated regions. You can extend a simple volume within the same disk or extend it to additional disks. If you extend a simple volume across multiple disks, it becomes a spanned volume.
- Spanned volumes. A *spanned volume* is a volume that is created from the free disk space from multiple disks that are linked together. You can extend a spanned volume onto a maximum of 32 disks. You cannot mirror a spanned volume, and they are not fault-tolerant. Therefore, if you lose one disk, you will lose the entire spanned volume.
- Striped volumes. A *striped volume* is a volume that has data that is spread across two or more physical disks. The data on this type of volume is allocated alternately and evenly to each of the physical disks. A striped volume cannot be mirrored or extended, and is not fault tolerant. This means that the loss of one disk causes the immediate loss of all the data. Striping also is known as *RAID-0*.
- Mirrored volumes. A *mirrored volume* is a fault-tolerant volume that has all data duplicated onto two physical disks. All of the data on one volume is copied to another disk to provide data redundancy. If one of the disks fails, you can access the data from the remaining disk. However, you cannot extend a mirrored volume. Mirroring also is known as *RAID-1*.

- RAID-5 volumes. A *RAID-5 volume* is a fault-tolerant volume that has data striped across a minimum of three or more disks. Parity also is striped across the disk array. If a physical disk fails, you can recreate the portion of the RAID-5 volume that was on that failed disk by using the remaining data and the parity. You cannot mirror or extend a RAID-5 volume.

Options for managing volumes

To create and manage volumes, you can use one of the following tools:

- Server Manager
- Disk Management
- Diskpart.exe
- Windows PowerShell



Using Server Manager

To use Server Manager to create and manage disk volumes in Windows Server 2016, open **Server Manager**, and then complete the following procedure:

1. In the navigation pane, click **File and Storage Services**, and then under **Volumes**, click **Disks**.
2. In the **DISKS** pane, if necessary, right-click each offline disk, and then click **Bring Online**.
3. In the **TASKS** list, click **New Volume**.
4. In the **New Volume Wizard**, on the **Before you begin** page, click **Next**.
5. When all disks with available space display, select the appropriate disk from the **Disk** list, and then click **Next**.
6. When you are prompted to initialize the disk by using GPT, click **OK**.
7. On the **Specify the size of the volume** page, enter the desired size, and then click **Next**.
8. On the **Assign to a drive letter or folder** page, select a drive letter or choose a folder in an existing volume in which to mount the drive, and then click **Next**.
9. On the **Select file system settings** page, choose the appropriate file system, enter a volume label, and then click **Next**.
10. Finally, click **Create** to create the new volume.
11. Click **Close** after the volume has been created.

To manage volumes by using Server Manager, in the **Files and Storage Services** node, click **Volumes**, and then in the details pane, in the **Volumes** list, click the volume you want to manage. Right-click the desired volume, and then choose from the following options:

- **Manage Drive Letter And Access Paths**
- **Format**
- **Extend Volume**

- **Delete Volume**
- **Properties**

Using Disk Management

You also can use Disk Management to initialize and configure your newly installed disks. To access Disk Management, open **Computer Management**, and then click **Disk Management**. Use the following procedure to create and configure your volumes:

1. If your disks have not been initialized, you are prompted to initialize them. Click **OK** to initialize them as MBR disks. If you prefer to use GPT, click the **GPT** button, and then click **OK**.
2. Right-click an area of unallocated space on any disk and then click one of the following:
    - **New Simple Volume**
    - **New Spanned Volume**
    - **New Striped Volume**
    - **New Mirrored Volume**
    - **New RAID-5 Volume**

The procedure varies slightly depending on your previous choice. However, to create a mirrored volume, use the following procedure:

1. In the **New Mirrored Volume Wizard**, click **Next**.
2. On the **Select Disks** page, select two disks.
3. Enter the volume size to allocate across these two disks, and then click **Next**.
4. On the **Assign Drive Letter or Path** page, either select a drive letter for the mirrored volume or choose to mount the volume in the file system, and then click **Next**.
5. On the **Format Volume** page, choose a file system and a volume label, and then click **Next**.
6. Click **Finish** to create your mirrored volume.

Using Diskpart.exe

Although using Server Manager or Disk Management is a relatively simplified process, sometimes it is more efficient to use a command-line tool. You can use the **Diskpart.exe** command-line tool to create and manage your disk volumes by using the following procedure:

1. Open an elevated command prompt.
2. Type **Diskpart**, and then press Enter.
3. Type **Select Disk <*x*>**, (where *x* is the disk that you want to manage), and then press Enter.
4. Type **Convert dynamic**, and then press Enter. This command converts the disk into a dynamic disk.
5. Type **Create volume simple size=<*y*> disk=<*x*>**, (where *X* is the disk you want to manage, and *Y* is the size of the volume you want to create), and then press Enter. You also can create spanned, mirrored, and RAID drives by changing the word *simple*.
6. To assign a drive letter, type **assign letter=Z**, and then press Enter.

Using Windows PowerShell

You also can use Windows PowerShell cmdlets to manage disk partitions and volumes. The following list explains some of the more common disk management cmdlets:

- **Get-disk**. Lists all available disks installed in the server computer.
- **Clear-disk**. Removes all partitions and volumes from the specified disk.
- **Initialize-disk**. Enables you to initialize a disk in readiness for creation of volumes.
- **Get-volume**. Lists all accessible volumes.
- **Format-volume**. Enables you to format a volume with NTFS.

Demonstration: Managing volumes

In this demonstration, you will see how to:

- Create a new volume with Diskpart.
- Create a mirrored volume.

Demonstration Steps

Create a new volume with Diskpart

1. Use the following command-line tools to view the available disks, and then create and format an NTFS simple volume:

```
list disk
select disk 3
Convert dynamic
Create volume simple size=500 disk=3
Assign letter = g
Format
```

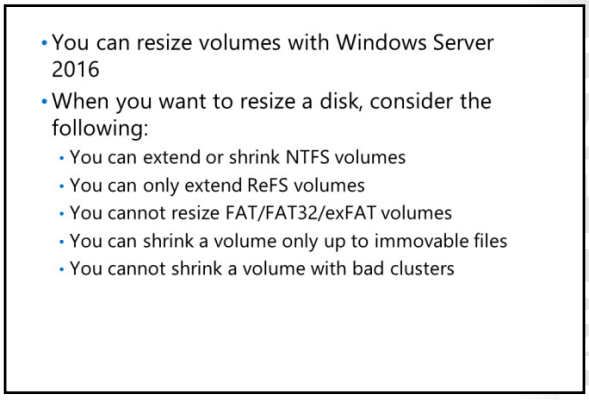
2. Switch to **Disk Management** to verify the newly created volume.

Create a mirrored volume

- In **Disk Management**, create a new mirrored volume with the following properties:
    - Disks: **Disk 3** and **Disk 4**
    - File system: **ReFS**
    - Quick format: **Yes**
    - Volume label: **Mirror**

Extending and shrinking a volume

In Windows Server 2016, it is simple to extend or shrink a volume. However, when you want to resize a volume, you must be aware of the following:



- You only have the ability to shrink or extend NTFS volumes. You cannot resize FAT, FAT32, or exFAT volumes.
- You can only extend ReFS volumes; you cannot shrink them.
- You can extend a volume by using free space both on the same disk and on other disks. When you extend a volume with other disks, you create a dynamic disk with a spanned volume. Remember though, in a spanned volume, if one disk fails, all data on the volume is lost. In addition, a spanned volume cannot contain boot or system partitions. Therefore, you cannot extend your boot partitions by using another disk.
- When you want to shrink a volume, immovable files such as page files are not relocated. This means that you cannot reclaim space beyond the location where these files are on the volume. If you have the requirement to shrink a partition further, you need to delete or move the immovable files. For example, you can remove the page file, shrink the volume, and then add the page file back again.
- If bad clusters exist on the volume, you cannot shrink it.

Note: As a best practice for shrinking volumes, you should defragment the files on the volume before you shrink it. This procedure returns the maximum amount of free disk space. During the defragmenting process, you can identify any immoveable files.

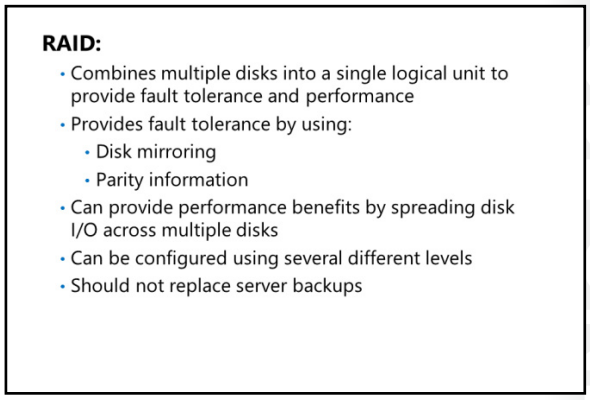
To modify a volume, you can use Disk Management, Diskpart.exe, or the **Resize-Partition** cmdlet in Windows PowerShell.

Additional Reading:

- For more information, refer to: "Extend a Basic Volume" at: http://aka.ms/sefpk3
- For more information, refer to: "Shrink a Basic Volume" at: http://aka.ms/H7pfnt

What is RAID?

RAID is a technology that you can use to configure locally attached storage or a storage system to provide high reliability and potentially, high performance. RAID implements storage systems by combining multiple disks into a single logical unit called a *RAID array*. Depending on the configuration, a RAID array can withstand the failure of one or more of the physical hard disks contained in the array, and in addition provide higher performance than is available by using a single disk.



RAID provides redundancy, which is an important component that you can use when planning and deploying Windows Server 2016 servers. In most organizations, it is important that the servers are available at all times. Most servers provide highly redundant components such as redundant power supplies and redundant network adapters. The goal of this redundancy is to ensure that the server remains available even if a single component on the server fails. By implementing RAID, you can provide the same level of redundancy for the storage system.

How RAID Works

RAID enables fault tolerance by using additional disks to ensure that the disk subsystem can continue to function even if one or more disks in the subsystem fail. RAID uses two options for enabling fault tolerance:

- Disk mirroring. With disk mirroring, all of the information that is written to one disk is also written to another disk. If one of the disks fails, the other disk is still available.
- Parity information. Parity information is used in the event of a disk failure to calculate the information that was stored on a disk. If you use this option, the server or RAID controller calculates the parity information for each block of data that is written to the disks, and then stores this information on another disk or across multiple disks. If one of the disks in the RAID array fails, the server can use the data that is still available on the functional disks along with the parity information to recreate the data that was stored on the failed disk.

RAID subsystems also can provide potentially better performance than single disks by distributing disk reads and writes across multiple disks. For example, when implementing disk striping, the server can read information from all hard disks in the stripe set. When combined with multiple disk controllers, this can provide significant improvements in disk performance.

Note: Although RAID can provide a greater level of tolerance for disk failure, you should not use RAID to replace traditional backups. If a server has a power surge or catastrophic failure and all of the disks fail, then you would need to rely on standard backups.

Hardware RAID vs. software RAID

You implement hardware RAID by installing a RAID controller in the server, and you then configure it by using the RAID controller configuration tool. When you use this implementation, the RAID configuration is hidden from the operating system. However, the operating system uses the RAID arrays as single disks. The only configuration that you need to perform in the operating system is to create volumes on the disks.

You can implement software RAID by using all of the disks that are available on the server. You then configure RAID from within the operating system. Windows Server 2016 supports the use of software RAID, and you can use Disk Management to configure several different RAID levels.

When choosing to implement hardware or software RAID, consider the following:

- Hardware RAID requires disk controllers that are RAID-capable. Most disk controllers shipped with new servers have this functionality.
- To configure hardware RAID, you need to access the disk controller management program. Normally, you can access this during the server boot process or by using a webpage that runs management software.
- Implementing disk mirroring with software RAID for a disk containing the system and boot volume can require additional configuration when a disk fails. Because the RAID configuration is managed by the operating system, you must configure one of the disks in the mirror as the boot disk. If that disk fails, you might need to modify the boot configuration for the server to start the server. This is not an issue with hardware RAID, because the disk controller accesses the available disk and exposes it to the operating system.
- In older servers, you might obtain better performance with software RAID when using parity, because the server processor can calculate parity more quickly than the disk controller can. This is not an issue with newer servers, where you could have better server performance because you can offload the parity calculations to the disk controller.

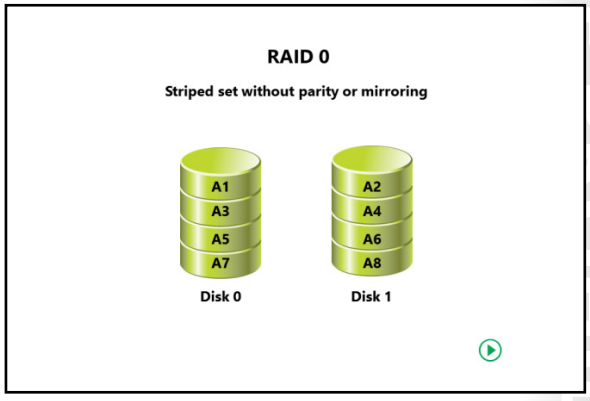
Level	Description	Performance	Space utilization	Redundancy	Comments
RAID 0	Striped set without parity or mirroring Data is written sequentially to each disk	High read and write performance	All space on the disk is available	A single disk failure results in the loss of all data	Use only in situations where you require high performance and can tolerate data loss
RAID 1	Mirrored set without parity or striping Data is written to both disks simultaneously	Good performance	Can only use the amount of space that is available on the smallest disk	Can tolerate a single disk failure	Frequently used for system and boot volumes with hardware RAID
RAID 2	Data is written in bits to each disk, with parity written to separate disk or disks	Extremely high performance	Uses one or more disks for parity	Can tolerate a single disk failure	Requires that all disks be synchronized
RAID 3	Data is written in bytes to each disk, with parity written to separate disk or disks	Very high performance	Uses one disk for parity	Can tolerate a single disk failure	Requires that all disks be synchronized Rarely used
RAID 4	Data is written in blocks to each disk, with parity written to a dedicated disk	Good read performance, poor write performance	Uses one disk for parity	Can tolerate a single disk failure	Rarely used
RAID 5	Striped set with distributed parity Data is written in blocks to each disk, with parity spread across all disks	Good read performance, poor write performance	Uses the equivalent of one disk for parity	Can tolerate a single disk failure	Commonly used for data storage where performance is not critical but maximizing disk usage is important
RAID 6	Striped set with dual distributed parity Data is written in blocks to each disk, with double parity written across all disks	Good read performance, poor write performance	Uses the equivalent of two disks for parity	Can tolerate two disk failures	Commonly used for data storage where performance is not critical but maximizing disk usage and availability are important

Level	Description	Performance	Space utilization	Redundancy	Comments
RAID 0+1	Striped sets in a mirrored set A set of drives is striped, and then the strip set is mirrored	Very good read and write performance	Only half the disk space is available due to mirroring	Can tolerate the failure of two or more disks provided that all failed disks are in the same striped set	Not commonly used
RAID 1+0 (or 10)	Mirrored set in a stripe set Several drives are mirrored to a second set of drives, and then one drive from each mirror is striped	Very good read and write performance	Only half the disk space is available due to mirroring	Can tolerate the failure of two or more disks provided that both disks in a mirror do not fail	Frequently used in scenarios where performance and redundancy are critical, and the cost of the required additional disks is acceptable
RAID 5+0 (or 50)	Striped set with distributed parity in a stripe set Drives are striped with RAID 5, and then striped without parity	Good read performance, better write performance than RAID 5	The equivalent of at least two disks is used for parity	Provides better fault tolerance than a single RAID level	This level is recommended for programs that require high fault tolerance, capacity, and random positioning performance Requires at least six drives

RAID levels

When implementing RAID, you need to decide what level of RAID to implement. The following table lists the features for each different RAID level.

Note: The most common RAID levels are RAID 1 (also known as *mirroring*), RAID 5 (also known as *striped set with distributed parity*), and RAID 1+0 (also known as *mirrored set in a stripe set*).



The following image illustrates the RAID 1 level.

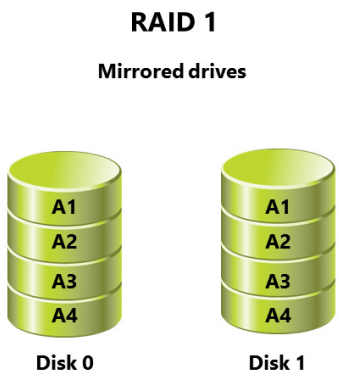


FIGURE 2.1: RAID 1

The following image illustrates the RAID 5 level.

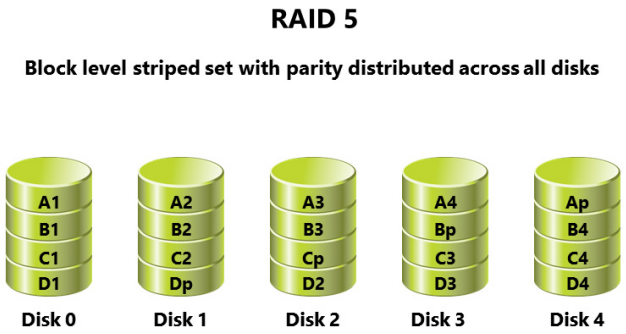
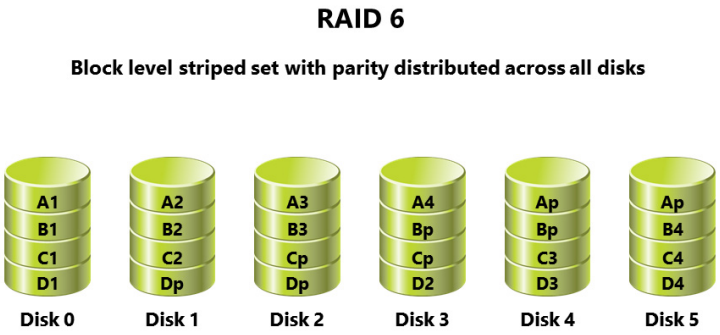
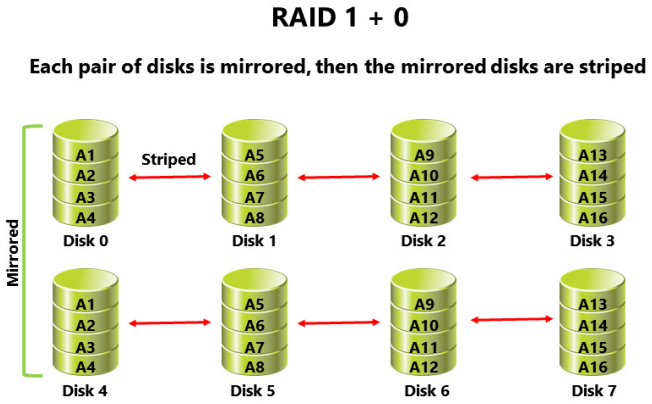


FIGURE 2.2: RAID 5

The following image illustrates the RAID 6 level.



The following image illustrates the RAID 1+ 0 level.



Question: Should you configure all disks with the same amount of fault tolerance?

Lab: Configuring local storage

Scenario

Your manager has asked you to add disk space to a file server that is running on a virtual machine. This virtual machine will potentially grow significantly in size in the upcoming months and you might need flexibility in your storage options. Your manager has asked you to optimize the cluster and sector size for virtual machines usage to accommodate large file sizes for storage on virtual machines. You need to assess the best options for storage and ease of expansion for potential future use.

Objectives

After completing this lab, you should be able to:

- Create and manage virtual hard disks.
- Resize volumes.

Lab Setup

Estimated Time: 40 minutes

Virtual machines: **20740A-LON-DC1**, **20740A-LON-SVR1**, and **20740A-LON-HOST1**

User name: **Adatum\Administrator**

Password: **Pa$$w0rd**

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

1. On the host computer, start **Hyper-V Manager**.
2. In **Hyper-V Manager**, click **20740A-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: **Administrator**
    - Password: **Pa$$w0rd**
    - Domain: **Adatum**
5. Repeat steps 2 through 4 for **20740A-LON-SVR1**.

Exercise 1: Creating and managing volumes

Scenario

In the test lab, you start by creating a number of volumes on the installed hard disks.

The main tasks for this exercise are as follows:

1. Create a hard disk volume and format for Resilient File System (ReFS).
2. Create a mirrored volume.

▶ Task 1: Create a hard disk volume and format for Resilient File System (ReFS)

1. On **LON-SVR1**, open **Windows PowerShell (Admin)**.
2. Create a new volume formatted for ReFS by using all the available disk space on Disk 1. Use the following Windows PowerShell cmdlets to complete this process:
   a. List all the available disks that have yet to be initialized:

```
Get-Disk | Where-Object PartitionStyle –Eq "RAW"
```

   b. Initialize disk 2:

```
Initialize-disk 2
```

   c. Review the partition table type:

```
Get-disk
```

   d. Create an ReFS volume by using all the available space on disk 1:

```
New-Partition -DiskNumber 2 -UseMaximumSize -AssignDriveLetter | Format-Volume -
NewFileSystemLabel "Simple" -FileSystem ReFS
```

3. Open **File Explorer**, and verify that the new drive is created and formatted. What is the drive letter?

▶ Task 2: Create a mirrored volume

1. Open **Disk Management**, and initialize all remaining disks.
2. Create a new volume on **Disk 3** and **Disk 4** with the following properties:
   - Disks: **Disk 3** and **Disk 4**
   - File system: **NTFS**
   - Quick format: **Yes**
   - Drive letter: **M**
   - Volume label: **Mirror**

Results: After completing this exercise, you should have successfully created several volumes.

Exercise 2: Resizing volumes

Scenario

You create a new volume, and then realize that you must resize it. You decide to use Diskpart.exe to complete this process.

The main tasks for this exercise are as follows:

1. Create a simple volume and resize it.
2. Shrink a volume.
3. Prepare for the next exercise.

▶ Task 1: Create a simple volume and resize it

1. Switch to **Windows PowerShell (Admin)** and create a new drive by running the following commands:
   - Initialize disk 5: **Initialize-disk 5**
   - Open diskpart: **diskpart**.
   - List available disks: **List disk**
   - Select the appropriate disk: **Select disk 5**
   - Make the disk dynamic: **Convert dynamic**
   - Create a simple volume on Disk 5: **Create volume simple size=10000 disk=5**
   - Assign the drive letter Z: **Assign letter=z**
   - Format the volume for NTFS: **Format**
2. In **Disk Management**, verify the presence of an NTFS volume on Disk 5 of size approximately **10** GB.
3. In the **Windows PowerShell (Admin)** window, run the following command:

```
Extend size 10000
```

4. In **Disk Management**, verify the presence of an NTFS volume on **Disk 5** of size approximately **20** GB.

▶ Task 2: Shrink a volume

1. In the **Windows PowerShell** (Admin) window, run the following command:

```
Shrink desired=15000
```

2. Switch to **Disk Management**.
3. Verify the presence of an NTFS volume on **Disk 5** of size approximately **5** GB.
4. Close the **Windows PowerShell (Admin)** window.

Results: After completing this exercise, you should have successfully resized a volume.

▶ Task 3: Prepare for the next exercise

1. On the host computer, start **Hyper-V Manager**.
2. In the **Virtual Machines** list, right-click **20740A-LON-DC1**, and then click **Revert**.
3. In the **Revert Virtual Machine** dialog box, click **Revert**.
4. Repeat steps 2 and 3 for **20740A-LON-SVR1**.
5. Restart your computer and select **20740A-LON-HOST1** when prompted.
6. Sign in as **Administrator** with the password **Pa$$w0rd**.

Exercise 3: Managing virtual hard disks

Scenario

You are required to create and configure virtual hard disks for use in a Windows Server 2016 server computer. The virtual hard disk is for the Sales department. You decide to use Windows PowerShell to achieve these objectives. First you must install the Windows PowerShell Hyper-V module.

The main tasks for this exercise are as follows:

1. Install the Windows PowerShell Hyper-V module.
2. Create a virtual hard disk.
3. Reconfigure the virtual hard disk.
4. Prepare for the next module.

▶ Task 1: Install the Windows PowerShell Hyper-V module

1. On your host computer, open **Server Manager** and install the Hyper-V server role and management tools.
2. Restart your computer and select **20740A-LON-HOST1** when prompted.

Note: Your computer might restart several times following installation of the Hyper-V components.

3. Sign in as **Administrator** with the password **Pa$$w0rd**.

▶ Task 2: Create a virtual hard disk

1. On your host computer, open **Windows PowerShell (Admin)**.
2. At the Windows PowerShell command prompt, type the following command, and then press Enter:

```
New-VHD -Path c:\sales.vhd -Dynamic -SizeBytes 10Gb | Mount-VHD -Passthru |Initialize-
Disk -Passthru |New-Partition -AssignDriveLetter -UseMaximumSize |Format-Volume -
FileSystem NTFS -Confirm:$false -Force
```

Note: If you get a Microsoft Windows pop-up dialog box prompting you to format the disk, you can close it and continue.

▶ Task 3: Reconfigure the virtual hard disk

Note: These steps are a duplicate of the detailed steps due to the complexity of the Windows PowerShell commands.

3. To dismount the virtual hard disk, at the Windows PowerShell command prompt, type the following command, and then press Enter:

```
Dismount-vhd C:\Sales.vhd
```

4. To check the properties of the virtual hard disk, at the Windows PowerShell command prompt, type the following command, and then press Enter:

```
Get-vhd C:\Sales.vhd
```

Question: What is the physical sector size?

5. To convert to a .vhdx file, at the Windows PowerShell command prompt, type the following command, and then press Enter:

```
Convert-VHD –Path C:\Sales.vhd –DestinationPath c:\Sales.vhdx
```

6. To change the sector size, at the Windows PowerShell command prompt, type the following command, and then press Enter:

```
Set-VHD –Path c:\Sales.vhdx –PhysicalSectorSizeBytes 4096
```

7. To check the properties of the .vhdx file, at the Windows PowerShell command prompt, type the following command, and then press Enter:

```
Get-vhd C:\Sales.vhdx
```

Question: What is the physical sector size?

8. To optimize the .vhdx file, at the Windows PowerShell command prompt, type the following command, and then press Enter:

```
Optimize-VHD –Path c:\Sales.vhdx –Mode Full
```

Results: After completing this exercise, you should have successfully created and managed virtual hard disks by using Windows PowerShell.

▶ Task 4: Prepare for the next module

- Restart your computer and when prompted, choose Windows Server 2012.

Question: In the lab, you used the Diskpart.exe command-line tool to create and resize volumes. What alternate Windows PowerShell cmdlets could you have used?

Question: Your current volume runs out of disk space. You have another disk available in the same server. What actions in the Windows operating system can you perform to help you add disk space?

Module Review and Takeaways

Review Questions

Question: What are the two disk types in Disk Management?

Question: What are the most important implementations of RAID?

Best Practices

The following list is of recommended best practices:

- If you want to shrink a volume, defragment the volume first so you can reclaim more space from the volume.
- Use the GPT partition table format for disks larger than 2 TB.
- For very large volumes, use ReFS.
- Do not use FAT or FAT32 on Windows Server operating system disks.

Tools

The following table lists the tools that this module references.

Tool	Use to	Where to find it
Disk Management	• Initialize disks • Create and modify volumes	In Server Manager on the **Tools** menu (part of Computer Management)
Diskpart.exe	• Initialize disks • Create and modify volumes from a command prompt	Command prompt
Mklink.exe	• Create a symbolic link to a file or folder	Command prompt
Chkdsk.exe	• Check a disk for an NTFS-formatted volume • Cannot be used for ReFS or virtual disks	Command prompt
Defrag.exe	• Disk defragmentation tool for NTFS-formatted volumes. • Cannot be used for ReFS or virtual disks	Command prompt

Module 3

Implementing enterprise storage solutions

Contents:

Module Overview

Storage is a key component that you must consider when planning and deploying your datacenter infrastructure. Most organizations require large amounts of storage, and this requirement is always increasing. Users work regularly with apps that create new files, which require storage in a central location. When users keep their files for longer periods, storage demands increase.

Storage options have expanded greatly over the last several years, with the introduction of new technologies and the expansion of existing ones. Therefore, as you plan your storage solutions, you must account for your current environment's technologies and the impact of introducing new technologies. Many organizations have standardized on a core group of hardware vendors and communication standards, and virtualization is driving many administrators to reevaluate those standards and begin thinking about next-generation storage solutions for heavily virtualized infrastructures. This module introduces you to various storage hardware and communication technologies. Technet24.ir

Objectives

After completing this module, you will be able to:

- Describe direct-attached storage (DAS), network-attached storage (NAS), and storage area networks (SANs).
- Compare Fibre Channel, Internet Small Computer System Interface (iSCSI), and Fibre Channel over Ethernet.
- Explain the use of Internet Storage Name Service (iSNS), Datacenter Bridging (DCB), and Multipath I/O (MPIO).
- Configure sharing in Windows Server.

Lesson 1
Overview of DAS, NAS, and SANs

When you are planning storage, you need to determine how your servers will access disks. In some cases, you can attach disks directly to the servers that require the storage. However, in enterprises, storage often is in NAS or SANs, which provide more flexibility. In this lesson, you will learn about the different methods that you can use to provide servers with storage access.

Lesson Objectives

After completing this lesson, you will be able to:

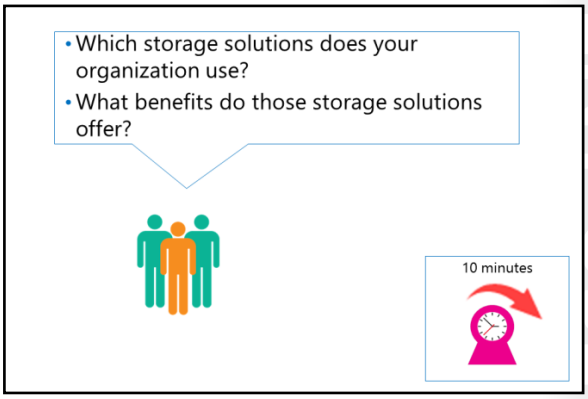
- Describe the storage solutions that are deployed in your environment.
- Describe DAS.
- Describe NAS.
- Describe SANs.
- Identify when you should use different storage types.
- List differences between block-level storage and file-level storage.

Discussion: Which storage solutions are deployed in your environment?

Organizations have a wide variety of storage options, such as DAS, NAS, and SANs. Each of these options is valid for different scenarios.

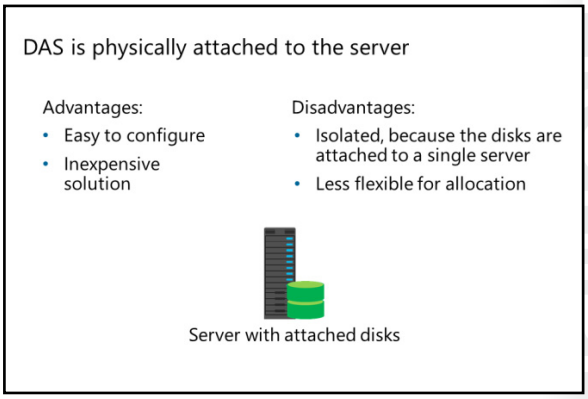
Question: Which storage solutions does your organization use?

Question: What benefits do those storage solutions offer?



What is DAS?

Almost all servers provide built-in storage, or *direct-attached storage* (*DAS*). DAS can include disks that are physically located inside the server or that connect directly with an external array, or disks that connect to the server with a universal serial bus (USB) cable or an alternative connector. However, because you connect DAS storage to the server physically, the storage is unavailable if the server fails. DAS comes in various disk types, such as Serial ATA (SATA), serial attached SCSI (SAS), or solid-state drive (SSD). These disk types all offer different speeds and performance levels, and have advantages *and* disadvantages.



Advantages of using DAS

A typical DAS system has a data-storage device that includes a number of hard-disk drives, which connect directly to a computer through a host bus adapter (HBA). There are no network devices—hubs, switches, or routers—between the DAS and the computer, but rather, the storage connects directly to the server that utilizes it. Therefore, DAS is the easiest storage system to deploy and maintain.

DAS typically is the least expensive storage that is available, and it is available widely in various speeds and sizes to accommodate different installations. Additionally, it is inexpensive and is very easy to configure. In most instances, you simply plug in the device, ensure that the running Windows operating system recognizes it, and then use the **Disk Management** feature to configure the disks.

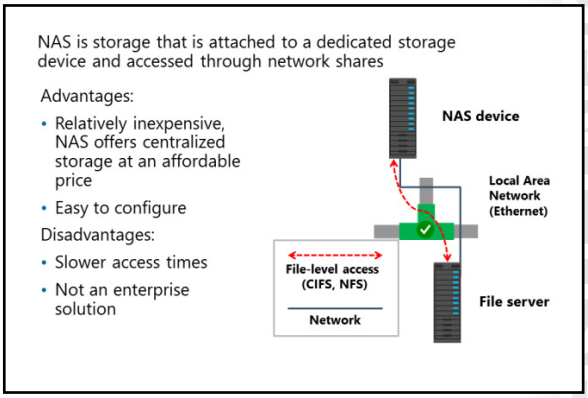
Disadvantages of using DAS

Storing data locally on DAS makes data centralization more difficult because the data is on multiple servers. This might make it more complex to back up data and users might find it more difficult to locate the data that they want to find. Furthermore, if any one device to which DAS connects suffers a power outage, the storage on that device becomes unavailable.

With DAS, allocating additional storage to servers can be more complex than with a SAN. With DAS, a physical disk needs to be installed in the server, whereas with a SAN, existing unallocated storage can be given to a server to expand storage without physically accessing the server.

What is NAS?

NAS is storage that connects to a dedicated storage device and is then accessed over the network. NAS differs from DAS because the storage does not attach directly to each individual server, but rather is accessible across a network to many servers. NAS has two distinct solutions: a low-end appliance (NAS only) and an enterprise-class NAS that integrates with a SAN.



Each NAS device has a dedicated operating system that solely controls data access on that device, which reduces the overhead associated with sharing the storage device with other server services. Windows Storage Server, a feature of Windows Server 2016, is an example of NAS software.

NAS devices typically provide file-level access to storage, which means that data in the storage is accessible only as files and folders, and you must use protocols such as Common Internet File System (CIFS), Server Message Block (SMB), or network file system (NFS) to access the files.

To enable NAS, you need a storage device. Frequently, these devices do not have any server interfaces, such as keyboards, mice, and monitors. To configure the device, you need to provide a network configuration, and then access the device across a network. You then can create shared folders on the device by using the name of the NAS and the share that you create. These shares then are accessible to the network's users.

Advantages of using NAS

NAS is an ideal choice for organizations that are looking for a simple and cost-effective way to achieve fast data access, at the file level, for multiple clients. NAS users benefit from performance and productivity gains, because a NAS device's processing power is dedicated solely to file distribution.

NAS also fits nicely into the market as a mid-priced solution. It is not expensive, but it suits more needs than DAS in the following ways:

- NAS storage typically is much larger than DAS.
- NAS typically includes RAID for data redundancy.
- NAS offers a single location for all critical files, rather than dispersing them on various servers by using DAS.
- NAS offers centralized storage at an affordable price.
- NAS units are accessible from any operating system. They often have multiple-protocol support and can serve up data via CIFS and NFS simultaneously. For example, Windows and Linux hosts can access a NAS unit simultaneously.

NAS also is a *Plug and Play (PNP) solution* that is easy to install, deploy, and manage, regardless of whether you have IT staff onsite.

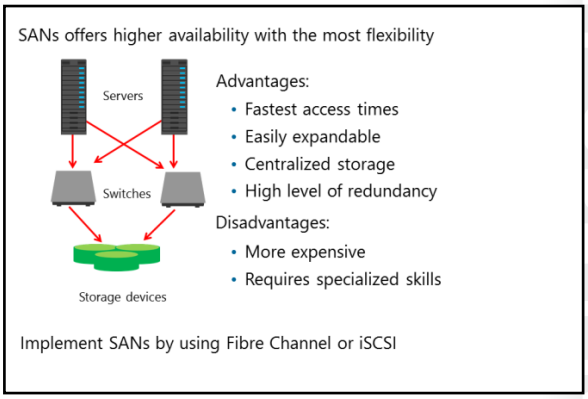
Disadvantages of using NAS

NAS is slower than SAN technologies. You typically access NAS by using Ethernet protocols, and it relies heavily on the network that is supporting the NAS solution. Therefore, NAS commonly is used as a file sharing/storage solution, but you cannot (and should not try to) use it with data-intensive programs such as Microsoft Exchange Server and Microsoft SQL Server.

NAS is affordable for small to mid-size businesses, but provides less performance and may be less reliable than a SAN. For this reason, most large enterprises use SANs rather than NAS.

What is a SAN?

The third type of storage is a SAN, which is a high□speed network that connects computer systems or host servers to high-performance storage subsystems. A SAN usually includes various components such as HBAs, special switches to help route traffic, and storage disk arrays with logical unit numbers (LUNs) for storage.



A SAN enables multiple servers to access a storage pool in which any server potentially can access any storage unit. However, because a SAN uses a network, you can use it to connect many different devices and hosts, and to provide access to any connected device from almost anywhere.

SANs provide block-level access. This means that rather than using a file-access protocol to access disk contents as files, SANs write blocks of data directly to the disks by using protocols such as Fibre Channel over Ethernet or Internet SCSI (iSCSI).

Today, most SAN solutions offer SAN and NAS together. The backend head units, disks, and technologies are identical, and the access method is the only thing that changes. Enterprises often provision block storage from the SAN to the servers by using Fibre Channel over Ethernet or iSCSI, while NAS services typically are available through CIFS and NFS.

Advantages of using SAN

SAN technologies read and write at block levels, which makes data access much faster. For example, with most DAS and NAS solutions, if you write a file of 8 gigabytes (GB), the entire file has to be read/written and its checksum calculated. However, with a SAN, the file is written to the disk based on the block size for which you configure the SAN. This speed is accomplished by using Fibre Channel and block-level writing, instead of reading/writing an entire file by using a checksum.

SANs also provide:

- Centralization of storage into a single pool, which enables storage resources and server resources to grow independently. They also enable dynamic storage assignment from the pool, when necessary. You can increase or decrease storage on a given server as necessary, without complex reconfiguration or recabling of devices.
- A common infrastructure for attaching storage, which enables a single common-management model for configuration and deployment.
- Storage devices that multiple systems share inherently.
- Data transfer directly from device to device without server intervention.
- A high level of redundancy. You deploy most SANs through a network with multiple network devices and paths. Additionally, the storage device contains redundant components, such as power supplies and hard disks.

Disadvantages of using SAN

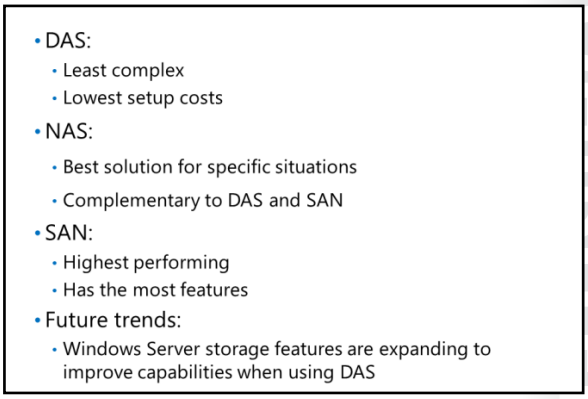
The main drawback to SAN technology is that you likely will need to use management tools and have expert skills because of its configuration complexities. Additionally, it is considerably more expensive than DAS or NAS. An entry-level SAN often costs as much as a fully loaded server with a DAS or NAS device, and that is without any SAN disks or configuration.

To manage a SAN, you must have a firm understanding of the underlying technology, including the LUN setup, the Fibre Channel network, the block sizing, and other factors. Additionally, each storage vendor often implements SANs by using different tools and features. Therefore, organizations often dedicate personnel to SAN deployment solely.

Note: You can implement SANs by using a variety of technologies, and the most common options are Fibre Channel and iSCSI.

Comparison and scenarios for usage

A good understanding of DAS, NAS, and SAN is the first step you must take in identifying the storage solution that best fits your requirements, and you should be aware that each of these storage technologies has expanded its available features and added flexibility. Often, you will not have a clear best choice, so this next topic examines the three topologies again, and compares them and explains which is the best solution for different scenarios.



DAS

You might consider using DAS because it typically is the least expensive and least complex solution. However, DAS might require more administrative overhead than NAS and SAN, especially if you deploy multiple DAS solutions. For example, imagine that your organization is deploying 15 Microsoft Hyper-V nodes in a failover cluster in Windows Server 2016. If you use NAS or SAN, a single highly-available storage solution can accommodate the failover cluster. However, if you use DAS, you might need 15 appliances. In such cases, DAS can create storage sprawl, which means that there are ever-increasing and expanding storage islands, which might be difficult to manage and maintain.

To combat this, the latest DAS solutions sometimes include some key SAN features, including multiple communication protocols, enterprise-management software, and easy expansion. You can use these features to add additional disk shelves. Entry-level DAS offerings provide only a single shelf in each appliance, and do not support expansion. These restrictions lead to storage sprawl. However, with high-end DAS systems, you can expand the disk shelves and disk count, and deploy solutions easily with hundreds of terabytes (TBs) of storage space. Therefore, these solutions can handle the Hyper-V failover cluster scenario that the section above describes.

In larger organizations, some database-management teams and messaging teams prefer to use DAS solutions to reduce their reliance on the organization's storage team. This gives them more control over their own storage.

NAS

A large majority of organizations use NAS, although many do not refer to their shared folder solutions as NAS. Third-party storage companies have introduced or expanded their NAS offerings, so it is common for SAN solutions to deliver NAS services via CIFS or NFS, as well. Therefore, in many organizations, SAN and NAS often share the same storage appliances, disk shelves, and supporting infrastructure.

NAS is so ubiquitous that it likely is not useful to compare it directly to DAS or SAN. DAS and SAN often compete directly with each other, but NAS typically plays a complementary role in systems that also incorporate DAS and SAN. Recently, some technologies have adopted support for NAS. One such example is Hyper-V, which now supports storing virtual machines on SMB 3.0 shares. If additional technologies begin to support NAS, then more-direct competition with DAS and SAN is likely in the future.

SAN

SAN solutions are known widely as the best enterprise storage solution. For a long time, SAN was the only solution for high-performance storage. Not only is it flexible and high performing, but you also can expand it more easily than DAS and NAS.

However, DAS and NAS have expanded their markets recently. DAS solutions can offer high-performance storage without the complexity of a SAN, because it utilizes the latest disk and SSD technologies. Countering that, SAN solutions can offer the same disk and SSD technologies on a much larger scale, and the scale is the key differentiator. Whereas the largest DAS solutions offer hundreds of TBs of storage space, the top SAN solutions offer thousands of TBs of storage space. Additionally, SAN solutions offer more spindles, which often lead to better performance.

Finally, SAN solutions offer:

- The best management tools. SAN management tools often provide a single management interface.
- The most enterprise features. For example, a common feature is an SSD cache in front of a huge spindle of spinning disks.
- The most flexibility. SANs provide SAN and NAS services in a single solution.

Future trends

With each new version of Windows Server, Microsoft is making Windows Server with DAS a more competitive option compared with SAN storage. Windows Server 2012 introduced storage spaces to provide redundancy for DAS, without requiring a Redundant Array of Independent Disks (RAID) controller. However, we recommend that you use caching controller for performance. Windows Server 2012 R2 introduced storage tiering to allow the most frequently accessed disk blocks to be automatically stored on SSD drives instead of spinning disks. High availability for shared folders was also available by implementing Scale-Out File Server. Windows Server 2016 also adds Storage Replica to provide block-level synchronous or asynchronous replication between two servers that are using DAS.

The storage features that Windows Server includes are expanding steadily to include those available only in SANs previously. Using Windows Server with DAS is often much less expensive than using it with a SAN, if the feature set meets your needs.

Scenarios for using DAS, NAS, or SAN

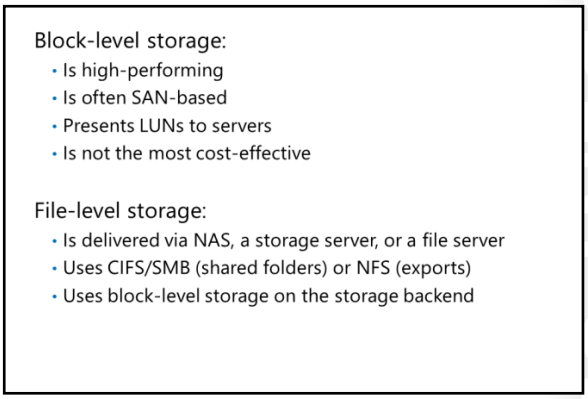
The following table highlights some common storage scenarios, and describes the capabilities of DAS, NAS, and SAN in each scenario.

Scenario	DAS	NAS	SAN
High performance storage for transactional databases	• Very good performance, and the lowest cost solution • Might add significant administrative overhead in large enterprise environments	Not a valid solution for most database servers	Excellent performance and features make this the best choice for transactional databases
User home folders	• Very good performance, but might expand into decentralized islands of storage • Enterprise management of many DAS installations adds administrative overhead	Best fit for user home folders because it offers CIFS access from any computing device without prohibitive costs	• Excellent performance and features, but more than required for user home folders • Home folders might need to be centralized • Might be cost-prohibitive
Storage of virtual machines	Very good performance but the administrative overhead is higher than SAN solutions	Supported for Hyper-V in Windows Server 2012 R2 or later, NAS is a good choice when trying to keep costs and complexity low	Excellent performance and features make this the best choice for most virtual environments
Branch office shared folders	• Easy to deploy and at a low cost • Often the best choice for general shared folders in branch offices because you do not need infrastructure at the branch offices	• Easy to deploy • Moderate cost • Often a good choice for branch offices that have a small infrastructure on site	Often cost-prohibitive and more features than what is required for a branch office

Scenario	DAS	NAS	SAN
Tiered storage for applications	Not as flexible as SAN, but viable for a small budget situation	Limited communication protocols compared to SAN, but some solutions are viable, such as a Scale-Out File Server with Storage Spaces and tiering	• Most flexible • Built-in tiering, caching, and other performance enhancements make SAN the best choice for applications
Microsoft Exchange database and log storage	Lowest cost, very good performance, and a very good alternative to SANs, especially for messaging teams that prefer to administer their own storage	Not a valid choice	Excellent performance and features make this a top choice

Block-level storage vs. file-level storage

You can arrange data on a disk in two ways: by blocks or by files. These ways of arranging data are block-level storage and file-level storage. Often, one arrangement or the other is the best solution in a particular scenario. Sometimes, however, they complement each other in a storage infrastructure. For example, it is common to use both types of storage in large enterprise environments.



You typically use block-level storage in conjunction with a SAN, and part or all of that storage is allocated to servers. You typically use file-level storage in conjunction with NAS, and NAS, a storage server or a file server allocates those chunks of storage by using file-level protocols, such as CIFS or NFS. Additionally, you typically place file-level storage on block-level storage.

Block-level storage

Block-level storage is delivered to servers via a SAN, most often by using one of the SAN communication protocols, such as iSCSI, Fibre Channel, or Fibre Channel over Ethernet. Storage administrators create storage volumes out of chunks of block-level storage. Inside the volumes, storage administrators create LUNs, which are virtual storage areas. You configure, or *present*, LUNs for use on one or more servers. Servers see the presented LUNs as physical hard drives, and administrators create volumes in Windows Server 2016 based on the LUNs. Volumes are formatted with a file system, such as the NTFS file system or Resilient File System (ReFS), and then accessed in the same manner as a physical or virtual hard disk. Block-level storage has the following characteristics:

- It is very flexible. For example, you can use it as an operating system volume, a data volume, or a storage location for shared folders.
- It is not tied to a specific operating system or a specific file system. All core operating systems and file systems support it.

- Operating systems can start from block-level storage LUNs. This means that your organization can deploy diskless physical servers. In such a scenario, the servers use Fibre Channel or iSCSI HBAs to connect to their boot LUN upon startup.
- You can present block-level storage directly to virtual machines to meet high-performance storage needs. In Hyper V, you can present block-level storage to virtual machines by using a pass-through disk or by using virtual Fibre Channel.

File-level storage

CIFS and NFS are the primary communication protocols that file-level storage uses. CIFS originally was an enhanced version of SMB. Today, however, the terms CIFS and SMB often are used interchangeably. Microsoft continues to make enhancements to CIFS with many major releases of the Windows Server operating system. File-level storage has the following characteristics.

- Access to file-level storage occurs over file-sharing protocols only.
- File-level storage sits on top of block-level storage and has a file system.
- Some applications support file-level storage, but others do not. In Windows Server 2012 R2, Hyper V began supporting virtual-machine storage in SMB 3.0 shared folders.
- File-level storage often is more economical than block-level storage.

Check Your Knowledge

Question	
Which type of storage typically has the lowest implementation costs?	
Select the correct answer.	
	DAS
	NAS
	SAN
	Block-level storage
	File-level storage

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

Statement	Answer
A SAN provides file-level storage.	

Lesson 2

Comparing Fibre Channel, iSCSI, and Fibre Channel over Ethernet

You can use multiple protocols to configure SANs, and the protocol that you select for a SAN typically is based on your organization's needs and the skills of your technical staff. Fibre Channel is the best performing solution for SANs, but it is the most complex and expensive system to implement. An iSCSI SAN is less expensive, because the equipment is less specialized, and is also simpler to implement and manage. In this lesson, you will learn about Fibre Channel and iSCSI.

Lesson Objectives

After completing this lesson, you will be able to:

- Describe Fibre Channel.
- List considerations for implementing Fibre Channel.
- Describe iSCSI.
- Identify components that are part of an iSCSI SAN.
- List considerations for implementing iSCSI.
- Describe physical-storage components.
- Configure an iSCSI target.

What is Fibre Channel?

Fibre Channel is a high-performance network technology that you use primarily to connect computers to SANs. It is a standard with a long history, and it was approved in 1994. Fibre Channel relies on the Fibre Channel protocol that transports SCSI commands over a network. A typical Fibre Channel implementation contains the following components:

Fibre Channel components include:
- A SAN
- A computer with an HBA card
- A Fibre Channel switch

Fibre Channel over Ethernet:
- Gives you the benefits of Fibre Channel while using an inexpensive, pre-existing Ethernet infrastructure

Fibre Channel layouts include:
- Arbitrated loop
- Point-to-point
- Switched fabric

- A SAN. In a Fibre Channel implementation, a SAN is the storage backend. It serves as a Fibre Channel target, which is the component that listens for requests from computers.
- A computer with an HBA card. In a Fibre Channel implementation, a computer with an HBA card is an *initiator,* because it initiates requests when it needs to access data on the SAN.
- A Fibre Channel switch. In a Fibre Channel implementation, you typically use Fibre Channel switches so that computers do not connect directly to a SAN. SANs often have a very limited number of target ports, and those ports almost always connect to Fibre Channel switches.

Fibre Channel over Ethernet is a newer implementation of Fibre Channel over a standard Ethernet network. It is becoming more popular, because it offers outstanding performance, particularly when you use it over your inexpensive, and often preexisting, Ethernet infrastructure. You can use Fibre Channel over Ethernet to converge all of your company's disparate communication mechanisms to Ethernet. There

are three main advantages to using Fibre Channel over Ethernet to merge your communication systems, including that:

- It is easier to manage a single network topology than a complex multitype network.
- You can use many of the standard network troubleshooting tools with Fibre Channel over Ethernet.
- Specialized training typically is not required.

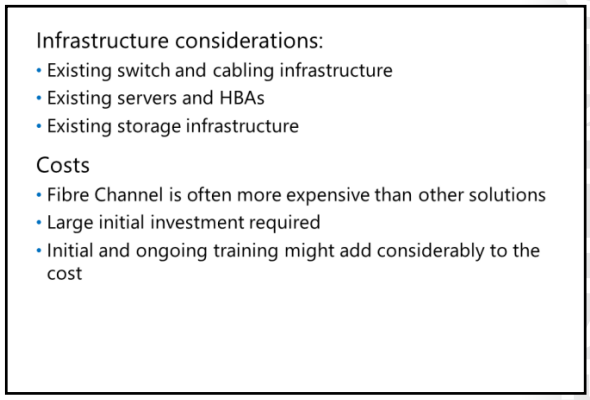
You can arrange a Fibre Channel network in one of three layouts:

- Arbitrated loop. In an arbitrated loop, Fibre Channel hosts and storage devices connect in a ring, and you do not need switches. This option was an inexpensive way to begin using Fibre Channel, when it was first introduced. However, it is quite rare today, because Fibre Channel and converged switches are very affordable.
- Point-to-point. In a point-to-point deployment, a Fibre Channel host connects directly to a storage device, and you do not need switches. However, organizations use this option rarely, because a very limited number of ports are available on storage devices.
- Switched fabric. This is the most common Fibre Channel deployment. Switched fabric environments use Fibre Channel switches. All Fibre Channel hosts connect to Fibre Channel switches, and the Fibre Channel switches connect to the backend storage.

Considerations for implementing Fibre Channel

You must consider several important factors when you decide whether to use Fibre Channel in a storage environment, including:

- Infrastructure requirements.
- Storage-bandwidth requirements.
- Connectivity reliability and security.
- Asset and administrative costs.



Infrastructure

The infrastructure requirements of Fibre Channel are often extensive for new storage deployments. When you use Fibre Channel, you typically install a specific and separate infrastructure for it. This dedicated infrastructure includes the following components:

- Fabric or network switches. In a network that uses only fiber optic cables, you might use Fibre Channel switches. However, many networks use more than one type of cable, and you also might combine separate networks that each are using a different type of cable. In these converged networks, switches must be able to handle multiple types of traffic and cables.
- HBAs. An HBA is an add-on card or functionality that is built into a computer's motherboard to enable communication over a Fibre Channel or Ethernet network.
- Additional cabling. Cabling is a critical component, and it typically consists of fiber optic or Ethernet cabling.
- Storage controllers. Storage controllers, or *storage heads*, manage communication to the backend storage.

A new Fibre Channel infrastructure typically requires switches that are dedicated solely to the storage environment. A dedicated network often provides better performance and security because the switches are only for storage-related traffic to and from the hosts and storage controllers. Fabric switches also generally require additional small form-factor pluggable transceivers that support Fibre Channel cabling. This increases the infrastructure's initial cost. Additionally, each host also requires at least one dedicated HBA, and often two HBAs for redundancy, which you must manage and cable separately from your production network traffic. Finally, the storage system that you are using also must support Fibre Channel.

You can use Fibre Channel with several cable types, the most common of which are:

- Single-mode fiber optic.
- Multi-mode fiber optic.
- Ethernet:
  - Fibre Channel over Ethernet.
  - Fibre Channel over IP.
- Ethernet over Copper

Dedicated Fibre Channel infrastructure uses fiber optic cabling in a variety of standards. Multi-mode fiber optic cabling is cheaper than single-mode fiber optic cabling and is suitable for most datacenters. The 128 Gbps standard for Fibre Channel supports multi-mode fiber at up to 100 meters and single-mode fiber at up to 2000 meters. Most organizations have no need for a 2000 meter distance, but when required, single-mode fiber provides the option.

Bandwidth

One of the most important benefits of using Fibre Channel to connect to a storage environment is the bandwidth and reliability that Fibre Channel can deliver. Currently, with bandwidth speeds up to 16 Gbps per port, Fibre Channel outperforms Ethernet on a per-port basis. This additional performance capability can be a major factor in deciding whether to use Fibre Channel. The most recent Fibre Channel standard is 32 Gbps.

Reliability and security

Fibre Channel provides good connectivity, reliability, and security, which are all important benefits. The Fibre Channel protocol is superior to the Ethernet protocol because it requires that frames are received in a specific order. This is not the case with Transmission Control Protocol (TCP)-based protocols, which can degrade performance and reliability. Additionally, because Fibre Channel deployments typically use a dedicated infrastructure, it is more secure and less susceptible to attack or degradation. In contrast to Fibre Channel, if a system's storage communication is shared with other network traffic, the storage operations of a host are vulnerable to the same attacks that can disrupt TCP communication. For example, a distributed denial of service (DDoS) attack in an environment with a converged infrastructure might prevent both TCP and storage communication. When you use a dedicated Fibre Channel infrastructure, this vulnerability is minimized. A middle ground in this scenario could be Fibre Channel over Ethernet, which provides the reliability of Fibre Channel over a typical Ethernet network.

Costs

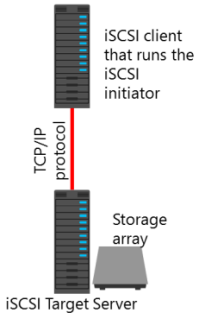
The personnel that manage the Fibre Channel solution require a specialized set of skills, which can make it more expensive than other storage solutions. In-house personnel might need additional training to initially deploy and manage the solution as well as ongoing training to stay current as the technology changes. If you use a third-party vendor to support your Fibre Channel solution, your costs might be the same or even higher than if you use your organization's staff.

What is iSCSI?

iSCSI is a protocol that supports access to remote, SCSI-based storage devices over a TCP/IP network. iSCSI carries standard SCSI commands over IP networks to facilitate data transfers, and to manage storage over long distances. You can use iSCSI to transmit data over local area networks (LANs), wide area networks (WANs), an intranet, or the Internet.

iSCSI transmits SCSI commands over IP networks

Component	Description
IP network	Network that provides high performance and redundancy
iSCSI targets	Servers that run on the storage device and enable access to the disks
iSCSI initiators	Software component or host adapter on the server that provides access to iSCSI targets
iSCSI IQN	Globally unique identifier that iSCSI uses to address initiators and targets on an iSCSI network



iSCSI relies on standard Ethernet networking architecture. You optionally can use specialized hardware, such as an HBA or network switches. iSCSI uses Transmission Control Protocol/Internet Protocol (TCP/IP), and specifically TCP port 3260. This means that iSCSI enables two hosts to negotiate and exchange SCSI commands by using an existing Ethernet network. Examples of what the two hosts negotiate include session establishment, flow control, and packet size. By doing this, iSCSI takes a popular, high-performance, local storage bus subsystem architecture and emulates it over networks, thereby creating a SAN.

Unlike some SAN protocols, iSCSI requires no specialized cabling. You can run it over an existing switching and IP infrastructure. However, to ensure performance, you should operate an iSCSI SAN deployment on a dedicated network. Otherwise, you may experience severely decreased performance.

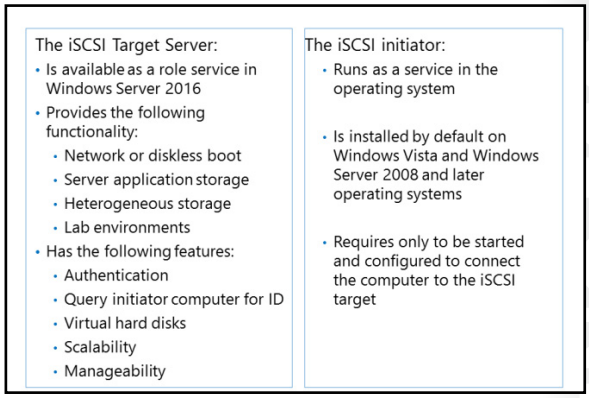
An iSCSI SAN deployment includes the following:

- IP network. You can use standard network interface adapters and standard Ethernet protocol network switches to connect servers to a storage device. To provide sufficient performance, the network should provide speeds of at least 1 Gbps, and should provide multiple paths to the iSCSI target. We recommend that you use a dedicated physical and logical network to achieve fast, reliable throughput.
- iSCSI targets. ISCSI targets present or advertise storage, similar to controllers for hard-disk drives of locally attached storage. However, servers access this storage over a network, rather than accessing it locally. Many storage vendors implement hardware-level iSCSI targets as part of their storage device's hardware. Other devices or appliances, such as Windows Storage Server devices, implement iSCSI targets by using a software driver and at least one Ethernet adapter. Windows Server 2016 provides the iSCSI Target Server, which is a driver for the iSCSI protocol, as a role service of the File and Storage Services role.
- iSCSI initiators. The iSCSI target displays storage to the iSCSI initiator, or *client*. The iSCSI initiator acts as a local disk controller for the remote disks. All Windows versions since Windows Server 2008 and Windows Vista include the iSCSI initiator and can connect to iSCSI targets.

iSCSI qualified name (IQN). IQNs are unique identifiers that iSCSI uses to address initiators and targets on an iSCSI network. When you configure an iSCSI target, you must configure the IQN for the iSCSI initiators that will connect to the target. iSCSI initiators also use IQNs to connect to iSCSI targets. However, if name resolution on the iSCSI network is a possible issue, you can identify iSCSI endpoints (both target and initiator) by their IP addresses.

iSCSI components

This topic discusses the two main components of iSCSI: an iSCSI Target Server and an iSCSI initiator.



iSCSI Target Server

The iSCSI Target Server role service provides for a software-based and hardware-independent iSCSI disk subsystem. You can use the iSCSI Target Server to create iSCSI targets and iSCSI virtual disks, and then use the Server Manager to manage these iSCSI targets and virtual disks.

The iSCSI Target Server that Windows Server 2016 includes provides the following functionality:

- Network or diskless boot. You can deploy diskless servers rapidly by using boot-capable network adapters or a software loader, and you can save as much as 90 percent of the storage space that you use for operating system images by using differencing virtual hard disks. This is ideal for large deployments of identical operating system images, such as on virtual machines that are running Hyper-V or in high-performance computing (HPC) clusters.
- Server application storage. Some applications, such as Microsoft Exchange Server, require block storage. The iSCSI Target Server can provide these applications with continuously available block storage. However, because the storage is accessible remotely, it also can combine block storage for central or branch-office locations.
- Heterogeneous storage. iSCSI Target Server supports iSCSI initiators that are not running Windows, so you can share storage on servers that are running Windows in mixed environments.
- Lab environments. The iSCSI Target Server role enables your Windows Server 2016 computer to be a network-accessible block-storage device. This is useful if you want to test applications before deploying them on SAN storage.

The features of the iSCSI Target Server in Windows Server 2016 include:

- Authentication. You can enable Challenge Handshake Authentication Protocol (CHAP) to authenticate initiator connections or enable reverse CHAP to allow the initiator to authenticate the iSCSI target.
- Query initiator computer for ID. To use this, you must use Windows 8 or Windows Server 2012 and newer operating systems.
- Virtual hard disk support. You create iSCSI virtual disks as virtual hard disks. Windows Server 2016 support both .vhd and .vhdx files, and .vhdx supports up to 64 TB capacity. You create new iSCSI virtual disks as .vhdx files, but you can import .vhd files.
- Scalability. The maximum number of iSCSI targets per target server is 256, and the maximum number of virtual hard disks per target server is 512.

Additional Reading: For more information, refer to: "iSCSI Target Server Scalability Limits" at: http://aka.ms/dfxgja

- Manageability. You manage the iSCSI Target Server by using Server Manager or Windows PowerShell. Windows Server 2016 uses the Storage Management Initiative Specification provider with Microsoft System Center 2012 Virtual Machine Manager and later versions to manage an iSCSI Target Server in a hosted and private cloud.

You could use the following Windows PowerShell cmdlets to manage the iSCSI Target Server:

```
Install-WindowsFeature FS-iSCSITarget-Server
New-IscsiVirtualDisk E:\iSCSIVirtualHardDisk\1.vhdx –size 1GB
New-IscsiServerTarget SQLTarget –InitiatorIds “IQN: iqn.1991-
05.com.Microsoft:SQL1.adatum.com”
Add-IscsiVirtualDiskTargetMapping SQLTarget E:\iSCSIVirtualHardDisk\1.vhdx
```

Additional Reading: For more information, refer to: “iSCSI Target Cmdlets in Windows PowerShell” at: http://aka.ms/j1iomo

When you enable the iSCSI Target Server to provide block storage, the iSCSI Target Server capitalizes on your existing Ethernet network. You need a dedicated network for iSCSI to ensure performance, or you can use Quality of Service (QoS) standards on your existing network. If high availability is important to your organization, you should configure a high-availability cluster. However, when you configure a high-availability cluster, you will need shared storage for the cluster. This storage can be hardware Fibre Channel storage or a serial attached SCSI storage array. You configure the iSCSI Target Server as a cluster role in the failover cluster. Windows Server 2016 introduces the Storage Spaces Direct feature, which uses unshared storage to make a high-availability cluster. It does this by using only local unshared storage and commodity hardware.

iSCSI initiator

The iSCSI initiator was introduced in Windows Server 2008 and Windows Vista, and it is installed by default. To connect your computer to an iSCSI target, you must start and configure the service.

You could use the following Windows PowerShell cmdlets to manage your iSCSI initiator:

```
Start-Service msiscsi
Set-Service msiscsi –StartupType “Automatic”
New-IscsiTargetPortal –TargetPortalAddress iSCSIServer1
Connect-IscsiTarget –NodeAddress “iqn.1991-05.com.microsoft:netboot-1-SQLTarget-target”
```

Considerations for implementing iSCSI

Before embarking on an iSCSI deployment, you should look at your infrastructure, staff, and customer requirements to ensure that you select the appropriate solution. The following are the primary considerations that you should take into account:

The primary factors to consider when planning on using iSCSI are:
- Network speeds and performance
- High availability
- Security
- Vendor information
- Infrastructure staff
- Application teams

Alternative solutions to iSCSI are Fibre Channel, Fibre Channel over Ethernet, and InfiniBand

- Network speed and performance. The network speed should be at least 1 Gbps, but in many cases, iSCSI networks in a datacenter now are 10 Gbps, 40 Gbps, or even 100 Gbps.
- High availability. The network infrastructure must be highly available because data is sent from the servers to the iSCSI storage over network devices and components.
- Security. The iSCSI solution should have an appropriate level of security. In situations where you need high security, you can use a dedicated network and iSCSI authentication. In situations with lower security requirements, you might not have to use a dedicated network and iSCSI authentication.

- Vendor information. Read the vendor-specific recommendations for different types of deployments and applications that use iSCSI storage, such as Exchange Server and SQL Server.
- Infrastructure staff. IT personnel who will design, configure, and administer the iSCSI storage must include IT administrators with different areas of specialization, such as Windows Server 2016 administrators, network administrators, storage administrators, and security administrators. This will help you design an iSCSI storage solution that has optimal performance and security. It also will help you create consistent management and operations procedures.
- Application teams. The design team for an iSCSI storage solution should include application-specific administrators, such as Exchange Server administrators and SQL Server administrators, so that you can implement the optimal configuration for the specific technology or solution.

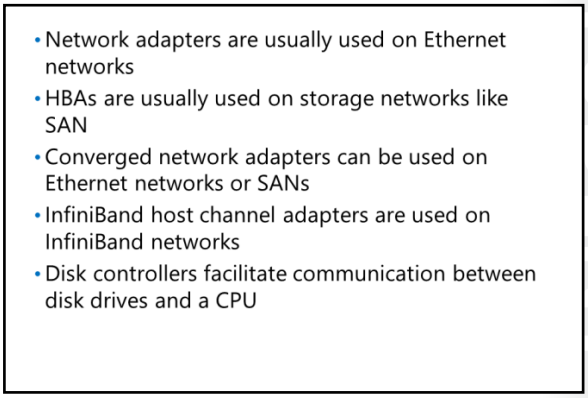
In addition to looking at the infrastructure and teams, you also need to investigate competitive solutions to see if they better meet your business requirements. The primary iSCSI competitors are Fibre Channel, Fibre Channel over Ethernet, and InfiniBand.

Core storage components

In a storage infrastructure, several types of adapters and controllers comprise a storage system's physical foundation, including:

- Network adapters
- HBAs
- Converged network adapters
- InfiniBand host channel adapters
- Disk controllers

This topic examines the characteristics of these components, and provides a high-level overview of scenarios for which each component is best suited.



Network adapters

Network adapters are composed of microchips and physical ports that are on a motherboard or an expansion card. Network adapters provide connectivity primarily to Ethernet networks. Network adapters communicate over a wired network by using an RJ-45 port or over wireless networks by using the 802.11 wireless network standard. Network adapters are the most cost-effective storage-connectivity solution.

Current network adapters operate at up to 100 Gbps per port, although 10 Gbps and 40 Gbps are more common.

You can configure teaming to achieve performance, failover, or both. When you use teaming, all network adapters that are part of a team combine to create a virtual network adapter, or *team network adapter*. You configure the settings on the team network adapter.

Note: Network teaming is a good high-availability option for general network connectivity. However, for specific use with iSCSI, you should consider using MPIO for redundancy across multiple network paths, instead of network teaming.

HBAs

Like network adapters, HBAs are made up of microchips and physical ports that can be embedded on a motherboard or on an expansion card. However, unlike network adapters, HBAs provide connectivity to a SAN. HBAs are more expensive than network adapters, although they are not the most expensive storage connectivity solution. Fibre Channel HBAs are uniquely identified on a Fibre Channel network by a World Wide Name (WWN). A WWN is a configurable 64-bit address that every Fibre Channel network component uses, although they do not apply to iSCSI HBAs.

Note: WWNs are configurable, so relying solely on WWNs is a security risk. Some attacks rely on *WWN spoofing*, which is the process of using another device's WWN without authorization to gain access to backend storage.

For performance, Fibre Channel HBAs offer speeds up to 16 Gbps per port, whereas iSCSI HBAs typically offer 1 Gbps or 10 Gbps per port. However, you can combine ports to achieve greater performance, which is similar to other storage-expansion cards. The industry offers theoretical Fibre Channel speeds up to 64 Gbps currently, by allow you to combine four 16-Gbps ports.

HBAs are load-balanced with software, and their speed is based on the total number of ports and optimized paths to the backend storage. In the real world, it is uncommon for a host to have more than two paths to a single SAN controller. Instead, companies generally opt to have paths going to more than one SAN controller, while using two HBAs. The industry has announced that upcoming solutions can meet a new standard of 32 Gbps per port performance. However, with the popularity of Fibre Channel over Ethernet and converged networking, Fibre Channel and Fibre Channel HBAs are beginning to lose market share to Ethernet and converged adapter solutions.

Converged network adapters

Converged network adapters are composed of microchips and physical ports, sometimes embedded on a motherboard and other times on an expansion card. You can configure converged network adapters to provide connectivity to an Ethernet network or SAN, or to both. Converged network adapters typically cost a little more than an HBA because they are built with multiport and multiprotocol support. Converged network adapters typically support multiple protocols simultaneously, which makes them the most flexible storage adapter that is available.

On the performance side, converged network adapters are capable of achieving the highest speed that a specific protocol can achieve. For example, if one of the ports is an Ethernet port, the converged network adapter can achieve speeds up to 10 Gbps. However, because converged network adapters usually provide multiple port types, they typically do not achieve the combined speed of a dedicated single-port solution.

Currently, converged network adapters are popular because of their flexibility, and organizations typically use them in modern datacenters.

InfiniBand host channel adapters

InfiniBand host channel adapters, similar to other storage connectivity cards, are composed of microchips and physical ports, typically on an expansion card. Host channel adapters provide connectivity over an InfiniBand network, and they provide the highest levels of performance available today. This high performance comes at a cost, however, because host channel adapters are the most expensive storage-connectivity adapters that are available. Some current host channel adapters operate at up to 56 Gbps. InfiniBand provides the lowest latency by having less communication overhead than competing solutions, such as Ethernet. However, organizations use InfiniBand rarely, typically because of high cost, the training that is necessary to use and manage it, and the competitive features of lower-cost solutions.

Disk controllers

Disk controllers are microchips that facilitate communication between hard disks and a central processing unit (CPU) over an associated bus. Early versions of disk controllers were embedded on dedicated expansion cards. Today, most disk controllers are embedded in a disk drive. Additionally, with the widespread adoption of virtualization, virtual disk controllers are quite common. Virtual disk controllers sometimes emulate physical disk controllers, although newer virtual controllers are written specifically for virtual implementations, and they do not rely on emulation.

Disk controllers have the following characteristics:

- Most servers offer built-in RAID capabilities and a specialized disk controller, or *RAID controller*, which facilitates the RAID capabilities.
- Another type of specialized disk controller, or *array controller*, facilitates communication between a server and a DAS appliance.
- Physical disk controllers typically operate over a serial ATA (SATA) or serial attached SCSI (SAS) interface.
- Virtual disk controllers typically emulate integrated drive electronics (IDE) or SCSI controllers.

Demonstration: Configuring an iSCSI target

In this demonstration, you will see how to:

- Add the iSCSI Target Server role service.
- Create two iSCSI virtual disks and an iSCSI target.
- Connect to the iSCSI target.
- Verify the presence of the iSCSI drive.

Demonstration Steps

Add the iSCSI Target Server role service

- On **LON-DC1**, use **Server Manager** to add the **iSCSI Target Server** role service in File and Storage Services.

Create two iSCSI virtual disks and an iSCSI target

1. On **LON-DC1**, in **Server Manager**, in **File and Storage Services**, browse to **iSCSI**.
2. Create a new iSCSI virtual disk with the following settings:
    - Name: **iSCSIDisk1**
    - Disk size: **5 GB**
    - iSCSI target: **New**
    - Target name: **LON-DC1**
    - Access servers: **172.16.0.21**
3. Create a second iSCSI virtual disk with the following settings:
    - Name: **iSCSIDisk2**
    - Disk size: **5 GB**
    - iSCSI target: **LON-DC1**

Connect to the iSCSI target

1. On **LON-SVR1**, open **Server Manager**, and open **iSCSI Initiator** from the **Tools** menu.
2. In the **iSCSI Initiator Properties** dialog box, configure the following:
   - Quick Connect: **LON-DC1**
   - Discover targets: **iqn.1991-05.com.microsoft:lon-dc1-lon-dc1-target**

Verify the presence of the iSCSI drive

1. On **LON-SVR1**, in **Server Manager**, open **Computer Management** from the **Tools** menu.
2. In the **Computer Management** console, in **Disk Management**, verify that the two 5 GB iSCSI disks are present.

Note: The new disks are added, but they all are currently offline and not formatted. These are listed as Disk 11 and Disk 12.

Question: Can you use your organization's internal TCP/IP network to provide iSCSI?

Question: When would you consider implementing diskless booting from iSCSI targets?

Lesson 3
Understanding iSNS, DCB, and MPIO

Enterprises often require storage features that smaller organizations do not need, and these advanced features typically simplify storage management. An iSNS server is a central directory of iSCSI targets. DCB helps ensure that QoS goals are met on high-speed converged networks that carry multiple types of data. Multipath I/O (MPIO) is used to identify multiple paths through a storage network for redundancy and performance.

Lesson Objectives

After completing this lesson, you will be able to:

- Describe iSNS.
- Describe DCB.
- Describe MPIO.
- Configure MPIO.

What is iSNS?

In complex IT systems, there are many storage devices and many devices that need access to storage. An iSNS server has a database with a collection of information about storage devices and where that storage has been allocated. This database and the associated iSNS protocol make it possible for devices that need storage to find allocated storage devices. That is, iSNS clients query the iSNS server to find storage allocated to them.

The iSNS Server service is a Windows feature that:

- Has three primary components: the iSNS server, iSNS client, and iSNS database
- Has several advantages, including that it:
  - Reduces administrative overhead by automating the configuration of iSCSI clients
  - Is compatible with iSCSI and Fibre Channel
  - Can make an IP network function like a SAN
  - Can integrate IP and Fibre Channel networks seamlessly
- Is not yet in widespread use

iSNS is a flexible protocol that uses few system resources, and iSNS servers and iSNS clients use the iSNS protocol to interact with one another. Clients can use iSNS to discover iSCSI storage devices automatically, and you can use iSNS to configure and manage iSCSI storage devices. iSNS also facilitates the same operations for Fibre Channel devices by using an Internet Fibre Channel protocol gateway.

However, because iSNS can perform storage discovery and configuration tasks, you can use iSNS to make an IP network function similar to a SAN. You also can use iSNS to integrate IP and Fibre Channel networks seamlessly because iSNS can emulate Fibre Channel fabric services, and manage both iSCSI and Fibre Channel devices. As a result, if iSCSI and Fibre Channel devices comprise your storage network, this is very valuable to your organization.

You can use iSNS to manage groups of devices instead of managing them individually, because after a device is registered in the iSNS database, it no longer requires manual configuration. iSNS serves as a central configuration point by which management stations can configure and manage the storage network.

iSNS components

iSNS has three primary components: clients, servers, and a database.

iSNS clients

When an iSNS client attempts to discover a storage device, it initiates communication with iSNS by using the iSNS protocol. iSNS clients are typically processes resident in the storage device. The iSNS client registers device attribute information, downloads information about other registered clients in a Discovery Domain, and receives asynchronous notification of events that occur in their Discovery Domain. A management station is a type of iSNS client that has access to Discovery Domains contained within iSNS.

iSNS servers

iSNS servers respond to iSNS protocol queries and requests. iSNS servers also initiate iSNS protocol state change notifications. Authenticated information submitted by a registration request is stored in the iSNS database.

iSNS database

iSNS servers use the iSNS database as an information repository. The iSNS database contains information about iSNS client attributes. It is possible to store iSNS client attributes in a Lightweight Direct Access Protocol (LDAP) directory by using a directory-enabled implementation of iSNS.

iSNS Functions

The four main functions of iSNS are:

- A name service. All entities in a storage network can use this service to register their names and other information in the database. All registered entities can then query the iSNS database to find other entities.
- A Discovery Domain and login control service. This service helps to divide storage nodes into groups. These groups are then used for administrative purposes and to control login activities.
- A state change notification service. The iSNS server uses this service to issue notifications about events on the network.
- Mapping information to an iSNS database. iSNS maps naming and discovery information about iSCSI and Fibre Channel devices to an iSNS database.

iSNS installation and configuration

The iSNS Server service is a Windows feature included in Windows Server 2016. You can install it by adding the feature in **Server Manager** or by using the **Add-WindowsFeature** cmdlet.

After installation, you can launch the iSNS Server from the **Tools** menu in **Server Manager**. You can then register iSCSI devices and group them into Discovery Domains and Discovery Domain Sets. When you are configuring the Windows iSCSI initiator, you specify which iSNS Server IP address or Domain Name System fully qualified domain name (DNS FQDN) to use. The initiator will query it to automatically discover all of the iSCSI targets present, essentially making manual configuration of portals unnecessary for your initiator.

To perform iSNS server registration, use the following Windows PowerShell commands, which manage Windows Management Instrumentation (WMI) objects:

To add an iSNS server, use the following command:

```
Set-WmiInstance -Namespace root\wmi -Class WT_iSNSServer -Arguments
@{ServerName="iSNS-server-name"}
```

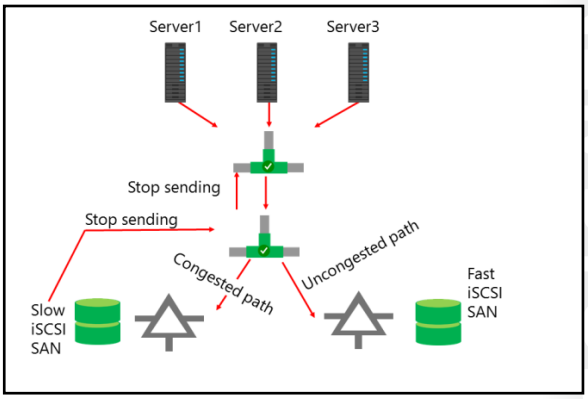
To view iSNS server settings, use the following command:

```
Get-WmiObject -Namespace root\wmi -Class WT_iSNSServer
```

To delete an iSNS server, use the following command:

```
Get-WmiObject -Namespace root\wmi -Class WT_iSNSServer -Filter “ServerName =’iSNS
-server-name’ | Remove-WmiInstance
```

What is DCB?



Most existing datacenters typically have several physical networks that accommodate different organizational needs. For example, system administrators and users might use an Ethernet network, data storage might use a separate physical Fibre Channel network, and high-performance computers might use an InfiniBand network. However, having separate networks increases costs and management overhead when you are building and maintaining the networks.

DCB, which was developed by an Institute of Electrical and Electronic Engineers (IEEE) 802.1 working group, provides a standard by which you can combine these networks into a single physical infrastructure that supports all of the above protocols and iSCSI. Typically, when you use a converged network adapter or a dedicated iSCSI HBA, the adapter vendor’s software includes the ability to configure hardware-based QoS and other features of DCB. Additionally, the network switches to which hosts connect must support DCB.

Features of DCB include:

- Congestion notification. You can use this to manage congestion for protocols that do not have built-in control mechanisms. The congestion notification can help the devices sending data to regulate the traffic that they are generating in order to avoid congestion.
- Priority-based flow control. This is a link-layer flow control mechanism that you can control based on the type of data being transmitted on the network. You can use this feature to target flow control instead of stopping data flow without regard for what is being transmitted. This last practice was a feature of the original Ethernet flow control.
- Enhanced transmission selection. This enables the system to reserve bandwidth for iSCSI and other network protocols. You can use enhanced transmission selection to set aside a specific amount of bandwidth for iSCSI as dictated by your requirements or usage. This helps to increase performance.
- Data Center Bridging Capabilities eXchange (DCBX) protocol. This enables devices such as the network adapters and switches to communicate and share capabilities and configuration information.

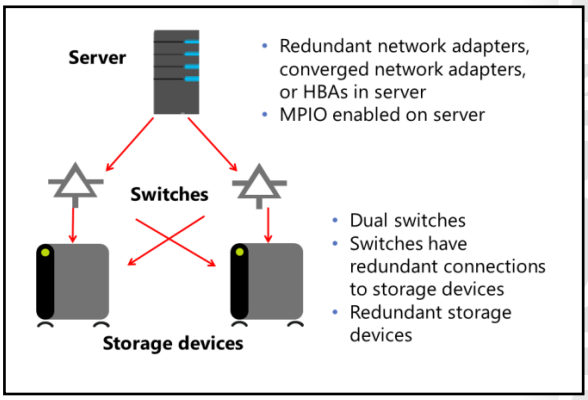
Installing and configuring DCB

DCB is a Windows Server 2016 feature that you can install from Windows PowerShell or by using Server Manager. To install DCB from Windows PowerShell, open a command prompt, type **Install-WindowsFeature "Data-Center-Bridging"**, and then press Enter.

Configuring DCB

You use Windows PowerShell to manage the QoS functionality in DCB. The cmdlets are in the **NetQos**, **DcbQos**, and **NetAdapter** modules. To view all cmdlets that relate to DCB QoS, run the **Get-Help *Qos*** command. Alternately, to retrieve the cmdlets that are available in each module, run the **Get-Command -Module DcbQos, NetAdapter, NetQos** command.

What is MPIO?



MPIO is a storage network enhancement that provides multiple physical paths from a computer to a block storage provider, regardless of whether the storage attaches directly to the storage provider or is available over a network. MPIO has been built into Windows Server since Windows Server 2008 and was available as a separate component for Windows Server 2003. In addition to this support built into Windows Server operating systems, many storage vendors offer their own MPIO software that can be installed on computers running Windows Server that connect to the backend storage. You use MPIO mainly in these situations:

- To create and/or maintain a highly available storage infrastructure. In this situation, MPIO is combined with other high-availability technologies, such as failover clustering, network load balancing, and datacenter availability. Datacenter availability specifically maintains power, cooling, and the network. Microsoft MPIO can handle up to 32 paths to the storage infrastructure.
- To maximize throughput for high-performance requirements. In this situation, MPIO uses MPIO load balancing to maximize the throughput to storage. In most deployments, high availability is still configured so that if a path fails, all traffic uses an alternate path, and throughput drops down to single path levels.

MPIO works in parallel with other software. One such piece of software is the device-specific module (DSM). A DSM is a storage vendor software component that facilitates efficient interaction with backend storage. The DSM software works in conjunction with the MPIO software for initialization events, I/O events, and other aspects of communication to backend storage. Similar to MPIO, storage vendors and Microsoft each provide their own DSM software.

Demonstration: Configuring MPIO

In this demonstration, you will see how to configure MPIO.

Demonstration Steps

1. On **LON-SVR1**, in **Server Manager**, add the **Multipath I/O** feature.
2. After installation is complete, restart **LON-SVR1** and sign in as **Adatum\Administrator** with the password **Pa$$w0rd**.
3. In **Server Manager**, open **MPIO** from the **Tools** menu.
4. In **MPIO Properties**, on the **Discover Multi-Paths** tab, add support for iSCSI devices and restart when prompted.

5. After restarting, sign in as **Adatum\Administrator** with the password **Pa$$w0rd**.
6. In **Server Manager**, open **MPIO** and verify that **MSFT2005iSCSIBusType_0x9** is listed as a device.

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

Statement	Answer
You can use iSNS for both iSCSI and Fibre Channel storage.	

Check Your Knowledge

Question	
What is the maximum number of paths that Microsoft MPIO can have?	
Select the correct answer.	
	4
	8
	16
	32

Lesson 4
Configuring sharing in Windows Server 2016

File sharing is a core service that is Windows Server 2016 provides. Each new version of Windows Server includes enhanced file-sharing capabilities for untraditional scenarios, such as storing virtual-machine files on a shared folder instead of a SAN or locally attached storage. You can use Server Manager to create SMB shares for Windows clients or NFS shares for Linux clients. In this lesson, you will learn how to create and manage shared folders.

Lesson Objectives

After completing this lesson, you will be able to:

- Describe the SMB file-sharing protocol.
- Identify configuration options for SMB shares.
- Configure SMB shares.
- Describe the NFS file-sharing protocol.
- Identify configuration options for NFS shares.
- Configure NFS shares.

What is SMB?

SMB is a client-server file-sharing protocol that was created in 1984. Microsoft modified the original SMB, and began using the name CIFS in 1996. Today, the terms SMB and CIFS are used interchangeably to refer to the same file-sharing protocol. This lesson uses the term SMB to refer to the technology.

- SMB is the file-sharing protocol that Windows client and server operating systems use
- Each new version has additional features
- SMB 3.0 introduced large performance benefits
- SMB 3.0.2 added:
  - Scale-Out File Server
  - Removable SMB 1.x
- SMB 3.1.1 added:
  - Pre-authentication integrity
  - SMB encryption improvements
  - Cluster dialect fencing

SMB is on multiple platforms, and an open-source version of SMB, named SAMBA, is supported on non-Windows platforms and is compatible with SMB.

There are multiple versions of SMB, and each new version has additional capabilities and enhancements. The version of SMB is incremented with the release of new operating systems. When two computers use SMB, they negotiate which version to use. If one computer is capable of SMB 2.0 and another is capable of SMB 3.0, then they use SMB 2.0. The following table lists the version of SMB that different Windows operating systems include.

Operating system	SMB version
Windows 10 and Windows Server 2016	SMB 3.1.1
Windows 8.1 and Windows Server 2012 R2	SMB 3.0.2
Windows 8 and Windows Server 2012	SMB 3.0
Windows 7 and Windows Server 2008 R2	SMB 2.1

Operating system	SMB version
Windows Vista and Windows Server 2008	SMB 2.0.2
Previous versions	SMB 1.x

Removing SMB 1.x

Current Windows versions do not have any dependencies on SMB 1.x. If your network no longer includes Windows XP or Windows Server 2003, then you should consider disabling SMB 1.x, by removing the SMB1 feature.

To ensure that your network does not have devices that are using SMB 1.x, you can enable auditing of SMB 1.x use on your servers. The events are stored in the **Microsoft-Windows-SMBServer/Audit** log. Enable SMB 1.x audit logging with the following Windows PowerShell command:

```
Set-SmbServerConfiguration -AuditSmb1Access $true
```

To disable SMB 1.x, use the following Windows PowerShell command:

```
Set-SMBServerConfiguration -EnableSMB1Protocol $false
```

SMB 3.x features

Each new SMB version provides additional functionality that supports new features in Windows Server. Some of the most significant enhancements started with the introduction of SMB 3.0, which offers significant performance improvements, including support for storage of SQL Server databases and Hyper-V virtual machines on SMB 3.0 shares.

SMB 3.0.2 provided the functionality that enabled you to implement the Scale-Out File Server feature for highly available file shares that store SQL Server databases and Hyper-V virtual machines. Additionally, it enables bandwidth limitations, and was the first version to allow you to disable SMB 1.x.

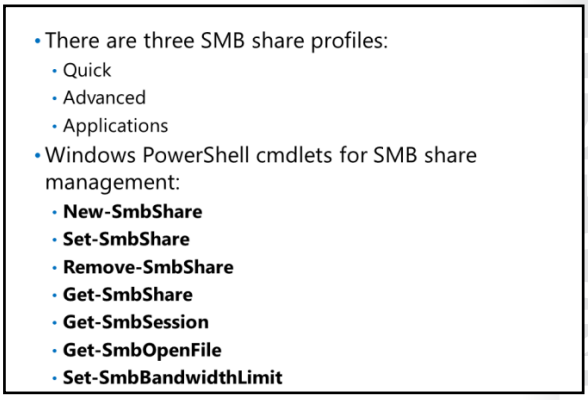
SMB 3.1.1 has the following new features:

- Pre-authentication integrity. Protects from man-in-the-middle attacks by using a Secure Hash Algorithm 512 (SHA-512) hash to verify packet contents during session setup.
- SMB encryption improvements. SMB encryption now defaults to use the AES-128-GCM encryption algorithm that has significantly better performance than AES-128-CCM, which was used in SMB 3.0.2.
- Cluster dialect fencing. To support rolling upgrades of Scale-Out File Server clusters, file shares in mixed mode use SMB 3.0.2. After all nodes in the cluster are upgraded, then file shares begin using SMB 3.1.1.

 **Additional Reading:** For more information, refer to: "What's New in SMB in Windows Server" at: http://aka.ms/Uthhq2

Configuring SMB shares

The creation and configuration of file shares has long been a core part of network administration. The ability to share files is one of the reasons that computer networks first became popular. Most administrators are aware that you can create shared folders from within File Explorer. However, in Windows Server 2016, you also can create shares by using Server Manager and Windows PowerShell. In Server Manager, the terms *file share* and *SMB* refer to the same component.



Share and NTFS permissions

The permissions a user has to access files on an SMB share are a combination of share permissions and NTFS permissions. The most restrictive set of permissions always applies. For example, if you give a user Full Control NTFS permissions, but he or she has only Read share permissions, the user's access is Read.

To simplify data access, when you use the **Quick** profile for creating an SMB share, the share permission is set to **Everyone Full Control**. Effectively this means that share permissions are not restricting access to the share and NTFS permissions are used to control access.

SMB share profiles

You can use Server Manager on Windows Server 2016 to create a new share. The built-in **New Share Wizard** offers three SMB file share profiles from which you can choose, including:

- **Quick**. This is the fastest method of sharing a folder on a network. With this method, you can select a volume or enter a custom path for the shared folder location. You can use the New Share Wizard to also configure additional options, such as access-based enumeration, share caching, encrypted data access, and permissions. You can configure these options and other options manually after you create the share.
- **Advanced**. This profile offers the same configuration options as the quick profile, and additional options such as folder owners, default data classification, and quotas. To create an advanced profile, you must install the File Server Resource Manager role service on at least one server that you are managing by using Server Manager.
- **Applications**. This specialized profile has appropriate settings for Hyper-V, databases, and other server applications. Unlike the quick and advanced profiles, you cannot configure access-based enumeration, share caching, default data classification, or quotas when you are creating an applications profile.

The following table identifies the configuration options that are available for each SMB share profile.

Share type	Access-based enumeration	Share caching	Encrypted data access	Default data classification	Quotas	Permissions
Quick	Yes	Yes	Yes	No	No	Yes
Advanced	Yes	Yes	Yes	Yes	Yes	Yes
Applications	No	No	Yes	No	No	Yes

Windows PowerShell cmdlets in the SmbShare module

The **SmbShare** module for Windows PowerShell contains 35 cmdlets in Windows Server 2016. This includes commonly used cmdlets such as **New-SmbShare**, **Set-SmbShare**, and **Remove-SmbShare**. If you use the **SmbShare** cmdlets, you can configure any share properties, even those that are not available in Server Manager.

If you want to identify the shares that exist on a server, and view the properties of those shares, you can use **Get-SmbShare**. The default output displays the **Name**, **ScopeName**, **Path**, and **Description**. **ScopeName** is only relevant when the server is part of a cluster and displays as ***** for unclustered file servers.

You can use **Get-SmbSession** to identify users that are connected to SMB shares. If the users have open files, then you can use **Get-SmbOpenFile** to identify open files.

If you are concerned about controlling the bandwidth allocated to SMB shares on a server, you can use **Set-SMBBandwidthLimit** to define a maximum throughput level that is allocated to SMB traffic on a server for different categories. This is useful for Hyper-V hosts to ensure that certain categories of traffic do not overwhelm the host and affect other categories, including:

- **Default**. This refers to all SMB traffic that does not relate to Hyper-V or Live Migration, such as standard file shares.
- **Hyper-V**. This refers to SMB traffic that you use for running virtual machines, such as accessing virtual hard disks on an SMB share.
- **Live Migration**. This refers to SMB traffic that generates when you perform a live migration from one Hyper-V host to another.

 **Note:** To explore all of the cmdlets in the **SmbShare** module, run the **Get-Command -Module SmbShare** command.

Demonstration: Configuring SMB shares by using Server Manager and Windows PowerShell

In this demonstration, you will see how to:

- Create an SMB share by using Server Manager.
- Create an SMB share by using Windows PowerShell.
- View SMB session information.

Demonstration Steps

Create an SMB share by using Server Manager

1. On **LON-SVR1**, in **Server Manager**, in **File and Storage Services**, browse to **Shares**.
2. Create a new share with the following settings:
   - File share profile: **SMB Share - Quick**
   - Server: **LON-SVR1**
   - Select by volume: **E:**

- Share name: **DemoShare**
- Enable access-based enumeration: selected
- Permissions: default

Create an SMB share by using Windows PowerShell

1. At the Windows PowerShell prompt, type the following command, and then press Enter:

```
Mkdir E:\Shares\DemoShare2
```

2. Type the following command, and then press Enter:

```
New-SmbShare -Name DemoShare2 -Path E:\Shares\DemoShare2 -FolderEnumerationMode
AccessBased
```

3. Type the following command, and then press Enter:

```
Get-SmbShare
```

4. Type the following command, and then press Enter:

```
Get-SmbShare DemoShare | FL *
```

View SMB session information

1. On **LON-DC1**, open **File Explorer**, and then browse to **\\LON-SVR1\DemoShare**.
2. On **LON-SVR1**, at the Windows PowerShell prompt, type the following command, and then press Enter:

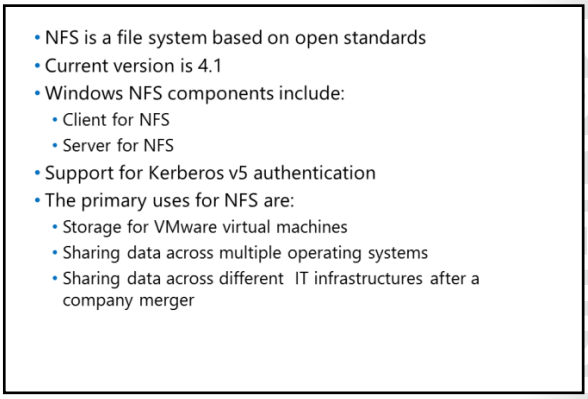
```
Get-SmbSession
```

3. Type the following command, and then press Enter:

```
Get-SmbSession -ClientUserName Adatum\Administrator | FL *
```

What is NFS?

NFS is a file-system protocol, which is based on open standards, and allows access to a file system over a network. NFS has been developed actively, and the current version is 4.1. The core releases and characteristics of the NFS protocol are:



- NFS version 1. Sun Microsystems developed Version 1 in 1984, and used it primarily internally. Initially, NFS was used on UNIX operating systems, but was subsequently supported on other operating systems, including Windows.
- NFS version 2. Request for Comments (RFC) 1094, "NFS: Network File System Protocol Specification" defines version 2. This version focused on improving performance. There is a file-size limit of 2 GB, because it was a 32-bit implementation.

- NFS version 3. RFC 1813, "NFS Version 3 Protocol Specification" defines version 3, and it introduced support for larger file sizes, because it was a 64-bit implementation. It also had performance enhancements, such as better protection from unsafe writes, and increased transfer sizes. It also included security enhancements, such as over-the-wire permission checks by the server.
- NFS version 4. RFC 3530, "Network File System (NFS) version 4 Protocol" defines version 4, which provided enhanced security and improved performance.
- NFS version 4.1. RFC 5661, "Network File System (NFS) Version 4 Minor Version 1 Protocol" defines version 4.1, which added support for clustering.

In UNIX, NFS works based on exports. Exports are similar to folder shares in Windows, because they are shared UNIX file-system paths.

Microsoft began supporting NFS by introducing the Microsoft Windows NT Services for the UNIX Add-On Pack in 1998. The product was used to integrate Windows-based computers with UNIX-based computers. One such integration feature was support for NFS. Microsoft continued to develop the product under the original name until 2004 when Microsoft Windows Services for UNIX 3.5 was released. At that time, the product was renamed Subsystem for UNIX-Based Applications (SUA) and the functionality was split as follows:

- The UNIX utilities and software development kit (SDK) became a free and optional download from the Microsoft Download Center.
- A portion of SUA, the Client for NFS component, and the Server for NFS component became Windows features. The SUA feature was deprecated in Windows Server 2012 and it is no longer available in Windows Server 2016. However, Client for NFS and Server for NFS are still supported and available as Windows features.

The two components for NFS support in Windows are:

- Client for NFS. This component enables a computer running a Windows operating system to access NFS exports on an NFS server, regardless of which platform the server runs on.
- Server for NFS. This component enables a Windows-based server to share folders over NFS. Any compatible NFS client can access the folders, regardless of which operating system the client is running. The vast majority of UNIX and Linux computers have a built-in NFS client.

Support for NFS has been improved and expanded with each iteration of the Windows Server operating system as follows:

- Windows Server 2008 R2 introduced support for Kerberos version 5 (v5) authentication in Server for NFS. Kerberos v5 authentication provides authentication before granting access to data, it also uses checksums to ensure that no data tampering has occurred.
- Windows Server 2012 introduced support for NFS version 4.1. This support included improved performance with the default configuration, native Windows PowerShell support, and faster failovers in clustered deployments.

Usage scenarios

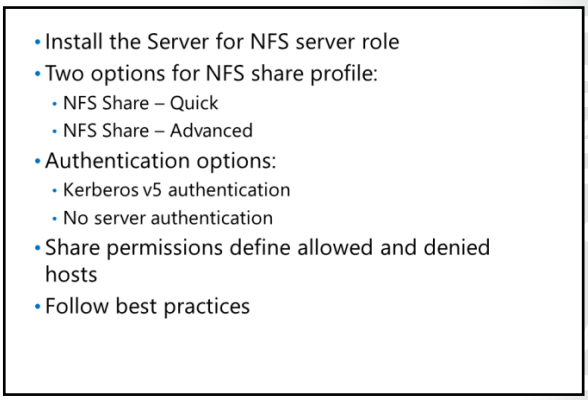
You can use NFS in Windows in many scenarios, and some of the most popular uses include for:

- VMWare virtual machine storage. In this scenario, VMWare hosts virtual machines on NFS exports. You can use Server for NFS to host the data on a Windows Server 2012 R2 server.
- Multiple-operating system environment. In this scenario, your organization uses a variety of operating systems, including Windows, Linux, and Mac. The Windows file-server system can use Server for NFS and the built-in Windows sharing capabilities to ensure that all of the operating systems can access shared data.

- Merger or acquisition. In this scenario, two companies are merging. Each company has a different IT infrastructure. Users from one company use Windows 8.1 client computers, and they must access data that the other company's Linux and NFS-based file servers are hosting. You can deploy Client for NFS to the client computers to allow the users to access the data.

Configuring NFS shares

The built-in **New Share Wizard** offers two NFS file share profiles from which you can choose:



- **Quick**. Creating a quick profile is the fastest way to create an NFS share, but it does not have some of the customizable share options that are available with advanced profiles. After you create a quick profile, you can configure the advanced sharing options manually, outside of the **New Share Wizard**.
- **Advanced**. The advanced profile is the most customizable way to create an NFS share. You can use it to set folder owners for access-denied assistance, configure default data classification, and to enable quotas. To create an advanced profile, you must install the File Server Resource Manager role service on the file server.

Installing NFS on the server

You can install NFS on the server by using Server Manager or Windows PowerShell. When you use Server Manager, you have to add the **File and Storage Services** role, and then install the **Server for NFS** role service. To use Windows PowerShell to install NFS on the server, run the following command:

```
Add-WindowsFeature FS-NFS-Service -IncludeManagementTools
```

Creating an NFS file share

After you install NFS on the server, you can create an NFS file share by using either Server Manager or Windows PowerShell. To create an NFS file share by using Windows PowerShell, run the following command to configure an NFS file share named Share1 for the directory located at d:\shares\share1:

```
New-NfsShare -Name Share1 -Path d:\shares\share1
```

Authentication for an NFS share can use Kerberos v5 authentication or No server authentication. When you use Kerberos v5 authentication, Active Directory Domain Services (AD DS) is used to authenticate the user account. When you use No server authentication, you can map user ID (UID) and group ID (GID) from a Linux system to AD DS accounts to assign permissions.

When you configure share permissions for an NFS share, you typically define hosts that are allowed to access the share. To allow all hosts, you can select **All Machines**. You also can allow and deny specify hosts.

Best Practices

You should consider several best practices before you implement NFS in your environment, including:

- Using the latest version of NFS servers and clients. Currently, NFS version 4.1 is the latest version and is supported on Windows Server 2012 and later and Windows 8 and later. By using the latest version of server and client operating systems, you can take advantage of the latest performance and security improvements, such as client/server negotiation and improved support for clustered servers.

- Using all available security enhancements. Since NFS version 3.0, NFS has offered Kerberos security options to strengthen NFS communication. You should use the following options when possible:
  - Kerberos v5 authentication protocol. This is the recommended authentication protocol to maintain the highest authentication security.
  - Kerberos v5 authentication and integrity. This adds integrity checking by using checksums to ensure that data has not been altered.
  - Kerberos v5 authentication and privacy. This adds encryption to the authentication traffic.
- Not allowing anonymous access. Although anonymous access is an option for NFS shares, you should not use it, because it reduces the security of your file-sharing environment.

NFS module for Windows PowerShell

Since Windows Server 2012, NFS has had its own Windows PowerShell module. To list all of the 42 cmdlets that are available in the module, run the **Get-Command -Module NFS** command.

Some of the most often used cmdlets from the NFS module are:

- **New-NfsShare**. This cmdlet creates an NFS file share.
- **Remove-NfsShare**. This cmdlet removes an NFS file share.
- **Get-NfsShare**. This cmdlet retrieves information about the configuration of an NFS file share.
- **Get-NfsSharePermission**. This cmdlet retrieves NFS file share permissions for a share.
- **Get-NfsClientConfiguration**. This cmdlet retrieves the NFS client configuration settings.
- **Get-NfsClientGroup**. This cmdlet retrieves the client groups configured on an NFS server.
- **New-NfsClientGroup**. This cmdlet creates a new client group on an NFS server.
- **Revoke-NfsSharePermission**. This cmdlet revokes NFS file share permissions from an NFS file share.
- **Set-NfsShare**. This cmdlet changes the configuration settings of an NFS share.
- **Set-NfsClientConfiguration**. This cmdlet changes the configuration settings of an NFS client.

Demonstration: Configuring an NFS share by using Server Manager

In this demonstration, you will see how to configure an NFS share by using Server Manager.

Demonstration Steps

1. On **LON-SVR1**, in **Server Manager**, in **File and Storage Services**, browse to **Shares**.
2. Create a new share with the following settings:
   - File share profile: **NFS Share - Quick**
   - Server: **LON-SVR1**
   - Select by volume: **E:**
   - Share name: **DemoNfsShare**
   - Authentication: **Kerberos v5 authentication(Krb5)**
   - Share permissions: **All Machines, Read / Write**
   - Permissions: default

Check Your Knowledge

Question	
Which version of SMB do Windows 10 and Windows Server 2016 use?	
Select the correct answer.	
	SMB 2.1
	SMB 3.0.2
	SMB 3.1.1
	SMB 3.2

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

Statement	Answer
You cannot use Kerberos authentication with NFS shares because they require AD DS.	

Lab: Planning and configuring storage technologies and components

Scenario

You are a Storage Administrator in A. Datum Corporation, and part of your job is to ensure that your data storage systems meet both short-term and long-term business needs that evolve regularly.

Objectives

After completing this lab, you will be able to:

- Plan storage requirements.
- Configure iSCSI storage.
- Configure and manage shares.

Lab Setup

Estimated Time: 60 minutes

Virtual machines: **20470A-LON-DC1** and **20470A -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 **20470A-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: **Administrator**
    - Password: **Pa$$w0rd**
    - Domain: **Adatum**
5. Repeat steps 2 through 4 for **20470A-LON-SVR1**.

Exercise 1: Planning storage requirements

Scenario

The A. Datum Corporation wants to design new storage solutions to support several recent changes. These changes include:

- External customers are using web applications more, and these customers need more and new business services.
- Internal users need more support and internal infrastructure services.
- Requirements for managing block-level storage and shared file access have expanded.
- A recently acquired company uses a different IT infrastructure than A. Datum. The IT department now needs to manage a mixed environment that includes remote geographical areas in London, New York, and Japan.

- The cost of storage has decreased significantly over recent years.
- The amount of data produced by A. Datum business groups has increased even faster.

Requirements

In general, the new system should be low-cost, have reasonable performance, and the storage administrators in A. Datum and the newly acquired company should be able to manage it easily.

The new storage system should include:

- Centralized management and control over the storage infrastructure.
- Support for applications that require large amounts of storage for SQL databases.
- An easy, inexpensive way to provision block-level storage that has minimal management overhead.
- The provisioning of VMWare ESX/ESXi virtual machines.
- The provisioning of Hyper-V virtual machines.
- Support for UNIX clients that require access to shared folders.
- Share access for older clients, if it is required.
    - As part of fulfilling this requirement, you will determine if older clients, including Windows XP and Windows Vista, need access to shares, and you then will remove any legacy shares that your users are not utilizing.

Proposals

As a senior server administrator at A. Datum, you are responsible for implementing the new file storage technologies for the organization. After reviewing the requirements, you propose a plan based on answers to the following questions:

- You plan to evaluate how iSCSI, Fibre Channel, and InfiniBand solutions meet the requirements. Which solution do you expect to select?
- Which storage—block-level storage or file-level storage—do you plan to implement for the SQL databases?
- How will your solution minimize administrative overhead for the storage administrators?
- Which server role(s) do you plan to use for the provisioning of VMWare ESX/ESXi virtual machines?
- Will you run the Hyper-V virtual machines on NFS or SMB?
- Which file sharing protocol will you use for UNIX clients that require access?
- How do you plan to disable legacy SMB access for existing SMB file shares?

The main tasks for this exercise are as follows:

1. Read the supporting documentation.
2. Record your planned course of action.

▶ Task 1: Read the supporting documentation

- Read the supporting documentation in the lab exercise scenario.

▶ Task 2: Record your planned course of action

Record your answers to the following questions:

1. You plan to evaluate how iSCSI, Fibre Channel, and InfiniBand solutions meet your requirements. Which solution do you expect to select?
2. Which storage type do you plan to implement for the SQL databases, block-level storage or file-level storage?
3. How will your solution minimize administrative overhead for storage administrators?
4. Which server role(s) do you plan to use for the provisioning of VMWare ESX/ESXi virtual machines?
5. Will you run the Hyper V virtual machines on NFS or SMB?
6. Which file sharing protocol will you use for UNIX clients that require access?
7. How do you plan to disable legacy SMB access for existing SMB file shares?

Results: After completing this exercise, you should have successfully planned a storage solution that will meet your organization's requirements.

Exercise 2: Configuring iSCSI storage

Scenario

You need to implement highly available iSCSI storage by using MPIO. There are two independent network paths between the file server and the iSCSI target. You will configure MPIO to use both paths to provide redundancy at the network level.

The main tasks for this exercise are as follows:

1. Enable network adapters.
2. Install the iSCSI target feature.
3. Create and configure an iSCSI target.
4. Configure MPIO.
5. Connect to the iSCSI target.
6. Initialize the iSCSI disks.

▶ Task 1: Enable network adapters

1. On **LON-DC1**, open a Windows PowerShell prompt.
2. Enable all network adapters by running the command **Get-NetAdapter | Enabled-NetAdapter**.
3. On **LON-SVR1**, open a Windows PowerShell prompt.
4. Enable all network adapters by running the command **Get-NetAdapter | Enable-NetAdapter**.

▶ Task 2: Install the iSCSI target feature

- On **LON-DC1**, in **Server Manager**, install the **iSCSI Target Server** role service in File and Storage Services.

▶ Task 3: Create and configure an iSCSI target

1. On **LON-DC1**, in **Server Manager**, in **File and Storage Services**, browse to **iSCSI**.
2. Create a new iSCSI virtual disk with the following settings:
   - Name: **iSCSIDisk1**
   - Disk size: **5 GB**
   - iSCSI target: **New**
   - Target name: **LON-DC1**
   - Access servers: **10.100.100.3**,**10.200.100.3**
3. Create a second iSCSI virtual disk with the following settings:
   - Name: **iSCSIDisk2**
   - Disk size: **5 GB**
   - iSCSI target: **LON-DC1**

▶ Task 4: Configure MPIO

1. On **LON-SVR1**, in **Server Manager**, add the **Multipath I/O** feature.
2. After installation is complete, restart LON-SVR1, and then sign in as **Adatum\Administrator** with the password **Pa$$w0rd**.
3. In **Server Manager**, open **iSCSI Initiator** from the **Tools** menu.
4. In the iSCSI Initiator, perform a quick connect to the target **10.100.100.2**.
5. In **Server Manager**, open **MPIO** from the **Tools** menu.
6. In **MPIO Properties**, on the **Discover Multi-Paths** tab, add support for iSCSI devices, and then restart when prompted.
7. After restarting, sign in as **Adatum\Administrator** with the password **Pa$$w0rd**.
8. In **Server Manager**, open **MPIO**, and then verify that **MSFT2005iSCSIBusType_0x9** is listed as a device.

▶ Task 5: Connect to the iSCSI target

1. On **LON-SVR1**, in **Server Manager**, open **iSCSI Initiator** from the **Tools** menu.
2. On the **Targets** tab, disconnect from all sessions.
3. Connect again, select the following options, and then enter the **Advanced** settings:
   - **Enable multi-path**
   - **Add this connection to the list of Favorite Targets**.
4. In the **Advanced Settings** dialog box, select the following settings:
   - Local adapter: **Microsoft iSCSI Initiator**
   - Initiator IP: **10.100.100.3**
   - Target Portal IP: **10.100.100.2 / 3260**

5. Connect a second time, select the following options, and then enter the **Advanced** settings:
   - **Enable multi-path**
   - **Add this connection to the list of Favorite Targets**.
6. In the **Advanced Settings** dialog box, select the following settings:
   - Local adapter: **Microsoft iSCSI Initiator**
   - Initiator IP: **10.200.100.3**
   - Target Portal IP: **10.200.100.2 / 3260**
7. On the **Volumes and Devices** tab, select the **Auto Configure** option.
8. On the **Targets** tab, select the **iqn.1991-05.com.microsoft:lon-dc1-lon-dc1-target** target, and then view the **Devices**.
9. For MPIO, verify that:
   - Load balance policy: **Round Robin**
   - The path details match the IP addresses you configure for source and destination addresses

▶ Task 6: Initialize the iSCSI disks

1. On **LON-SVR1**, in **Server Manager**, in **File and Storage Services**, browse to **Disks**.
2. Select an offline disk with a bus type of **iSCSI**, and then bring it online.
3. Right-click that disk, and then create a new volume with the following properties:
   - GPT disk
   - Drive letter: **J**
   - Volume label: **SMBShares**
   - Other settings: default
4. Select an offline disk with a bus type of **iSCSI**, and then bring it online.
5. Right-click that disk, and then create a new volume with the following properties:
   - GPT disk
   - Drive letter: **K**
   - File system: **NTFS**
   - Volume label: **NFSShares**
   - Other settings: default
6. Use **File Explorer** to verify that **SMBShares** and **NFSShares** are available in **This PC**.

Results: After completing this exercise, you should have successfully configured an iSCSI target that uses MPIO for redundancy.

Exercise 3: Configuring and managing the share infrastructure

Scenario

After configuring iSCSI storage for LON-SVR1, you need to create shares to support clients that are running both Windows and Linux operating systems.

The main tasks for this exercise are as follows:

1. Create an SMB share on iSCSI storage.
2. Create an NFS share on iSCSI storage.
3. Use Windows PowerShell to view share information.
4. Disable the legacy SMB1 protocol.
5. Prepare for the next module.

▶ Task 1: Create an SMB share on iSCSI storage

1. On **LON-SVR1**, in **Server Manager**, in **File and Storage Services**, browse to **Shares**.
2. Create a new share by using the following settings:
   - File share profile: **SMB Share – Quick**
   - Select by volume: **J:**
   - Share name: **Data**
   - **Enable access-based enumeration**
   - Add permission: **Domain Users, Modify**

▶ Task 2: Create an NFS share on iSCSI storage

1. On **LON-SVR1**, in **Server Manager**, in **File and Storage Services**, browse to **Shares**.
2. Create a new share with the following settings:
   - File share profile: **NFS Share – Quick**
   - Select by volume: **K:**
   - Share name: **LinuxData**
   - Authentication method: **Kerberos v5 authentication(Krb5)**
   - Add share permission: **All Machines, Read / Write**

▶ Task 3: Use Windows PowerShell to view share information

1. On **LON-DC1**, open **File Explorer**, and then browse to **\\LON-SVR1\Data**.
2. Create a new text file named **NewFile.txt**, and then open it in **Notepad**.
3. On **LON-SVR1**, open a Windows PowerShell prompt.
4. At the Windows PowerShell prompt, type the following command, and then press Enter:

```
Get-NfsShare
```

5. Type the following command, and then press Enter:

```
Get-NfsShare LinuxData | FL *
```

6. Type the following command, and then press Enter:

```
Get-SmbShare
```

7. Type the following command, and then press Enter:

```
Get-SmbShare Data | FL *
```

8. Type the following command, and then press Enter:

```
Get-SmbSession
```

9. Type the following command, and then press Enter:

```
Get-SMBSession -ClientUserName Adatum\Administrator | FL *
```

10. Type the following command, and then press Enter:

```
Get-SmbOpenFile
```

Note: There are two entries for **Adatum\Administrator**. File Explorer creates one, and Notepad creates the other. **NewFile.txt** is not included, because the file connection is maintained only for brief periods when you open the file initially or save it. If you do not see two entries, switch to **LON-DC1**, close Notepad and then double-click **NewFile.txt**. Then, on **LON-SVR1**, repeat step 10.

11. Leave the Windows PowerShell prompt open for the next task.

▶ Task 4: Disable the legacy SMB1 protocol

1. On **LON-SVR1**, at the Windows PowerShell prompt, type the following command, and then press Enter:

```
Set-SmbServerConfiguration -AuditSmb1Access $true
```

2. Type the following command, and then press Enter:

```
Get-SmbServerConfiguration | FL enable*
```

3. Type the following command, and then press Enter:

```
Set-SmbServerConfiguration -EnableSMB1Protocol $false
```

4. Type the following command, and then press Enter:

```
Get-WindowsFeature *SMB*
```

5. Type the following command, and then press Enter:

```
Remove-WindowsFeature FS-SMB1
```

Results: After completing this exercise, you should have successfully created SMB and NFS shares.

▶ Task 5: Prepare for the next module

After you finish the lab, revert the virtual machines to their initial state by completing the following steps:

1. On the host computer, switch to the **Hyper-V Manager** console.
2. In the **Virtual Machines** list, right-click **20740A-LON-DC1**, and then click **Revert**.
3. In the **Revert Virtual Machine** dialog box, click **Revert**.
4. Repeat steps 2 and 3 for **20740A-LON-SVR1**.

Question: Implementing MPIO for iSCSI is not as simple as installing MPIO. In this lab, what other steps did you perform to enable MPIO?

Question: When you use **Get-SmbOpenFile**, do all open files display?

Module Review and Takeaways

Review Questions

Question: If DAS provides similar performance to SAN, is it suitable to all storage needs?

Question: Which operating systems must you remove from your environment before you can disable SMB1?

Tools

Computer Management	Managing SMB shares Managing disks Viewing event logs	In Server Manager on the Tools menu
Disk Management	• Initializing disks • Creating and modifying volumes	In **Server Manager**, on the **Tools** menu, or within **Computer Management**
fsutil.exe	• Managing NTFS volumes; checking disk info, creating files of specific size, much more	Command prompt
File and Storage Services	• Performing basic storage management tasks • Examining storage configuration • Creating volumes	In **Server Manager**, under **File and Storage Services**

Module 4

Implementing Storage Spaces and Data Deduplication

Contents:

Module Overview

The Windows Server 2016 operating system introduces a number of storage technologies and improvements to existing storage technologies. You can use Storage Spaces, a feature of Windows Server 2016, to virtualize and provision storage based on storage pools and on virtual disks in which the physical storage is abstracted from the operating system. Data Deduplication is a feature that you can use to find and remove duplicate data while maintaining your data's integrity. This module describes how to use these two new features within your Windows Server storage architecture.

Objectives

After completing this module, you will be able to:

- Describe and implement the Storage Spaces feature in the context of enterprise storage needs.
- Manage and maintain Storage Spaces.
- Describe and implement Data Deduplication.

Lesson 1
Implementing Storage Spaces

Managing direct-attached storage (DAS) on a server can be a tedious task for administrators. To overcome this problem, many organizations use storage area networks (SANs) that group disks together. However, SANs are expensive because they require special configuration, and sometimes special hardware. To help overcome these storage issues, you can use Storage Spaces to pool disks together. Storage Spaces are then presented to the operating system as a single disk that can span multiple physical disks in a pool. This lesson explains how to implement Storage Spaces.

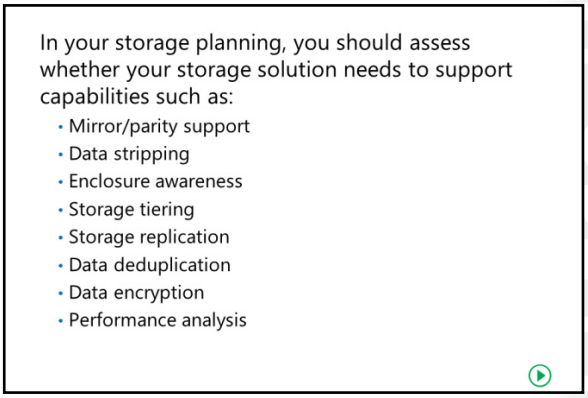
Lesson Objectives

After completing this lesson, you will be able to:

- Implement Storage Spaces as an enterprise storage solution.
- Describe the Storage Spaces feature and its components.
- Describe the features of Storage Spaces, including storage layout, drive allocation, and provisioning schemes such as thin provisioning.
- Describe changes to the Storage Spaces feature in Windows Server 2016.
- Describe common usage scenarios for storage spaces, and weigh their benefits and limitations.
- Compare using Storage Spaces to using other storage solutions.

Enterprise storage needs

In most organizations, discussions about storage needs can be straining. This is typically because storage costs are a major item on many Information Technology (IT) budgets. Despite the decreasing cost of individual units of storage, the amount of data that organizations produce continues to grow rapidly, so the overall cost of storage continues to grow.



Consequently, many organizations are investigating storage solutions that provide a cost-effective alternative to their existing solution, without sacrificing performance. A typical demand from organizations during storage planning is how to lower the costs and effort of delivering infrastructure as a service (IaaS) storage services. When planning your storage solution, you need to assess how well the storage solution scales. If your storage solution does not scale well, it will cost more. Additionally, you should consider deploying inexpensive networks and storage environments. This comes by deploying industry-standard server, network, and storage infrastructure to build highly available and scalable software-defined storage.

Finally, you should consider using disaggregated compute and storage deployments when planning how to lower the costs of delivering IaaS storage services. While many converged compute/storage solutions provide simpler management features, they also require scaling both components simultaneously. In other words, you might have to add compute power in the same ratio as previous hardware when expanding storage. To achieve lower costs of delivering IaaS storage service, you should consider independent management and independent scaling when planning your storage solution.

While your requirements might dictate which advanced features to consider during your storage planning, the primary drivers are typically capacity, performance, cost, and resiliency when assessing storage solutions. Although you could have lengthy discussions over each of these drivers separately, your storage solution needs to be a balanced storage deployment approach.

When planning your balanced storage deployment approach to meet your storage needs, you will need to assess your capacity and performance requirements in relation to your cost. For cost efficiency, your storage environment should utilize solid-state disks (SSDs) for highly active data (higher performance for the cost) and hard disk drives (HDDs) for data accessed infrequently (higher capacity for the cost).

If you deploy only HDDs, your budget constraints will prevent you from meeting your performance requirements; this is because HDDs provide higher capacity, but with lower performance. Likewise, if you deploy only SSDs, your budget constraints will prevent you from meeting your capacity requirements; this is because SSDs provide higher performance, but with lower capacity. As a result, your balanced storage deployment approach will most likely include a mix of HDDs and SSDs to achieve the best performance and capacity at the appropriate cost.

Included in your storage planning, you should consider whether your storage solution needs to support the common capabilities of most storage products, such as:

- Mirror/parity support
- Data stripping
- Enclosure awareness
- Storage tiering
- Storage replication
- Data deduplication
- Data encryption
- Performance analysis

 **Note:** This list is only meant to provide suggestions and is not an exhaustive list of the common capabilities of most storage products. The storage requirements of your organization might differ.

The growth in the size of data volumes, the ever-increasing cost of storage, and the need to ensure high availability of data volumes can be difficult problems for IT departments to solve. Windows Server 2016 provides a number of storage features that aim to address these important facets of storage management.

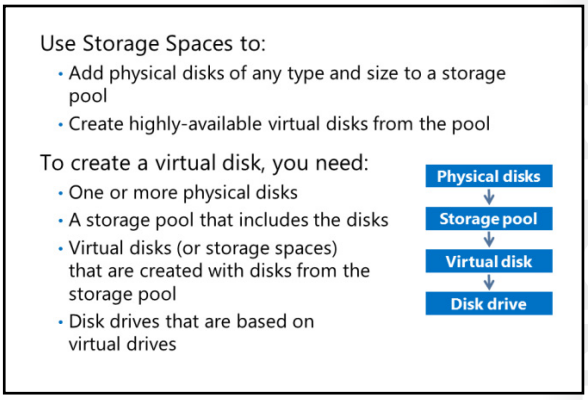
Question: Which factors should you consider when planning your enterprise storage strategy?

Question: What storage technologies does your organization use?

What are Storage Spaces?

Storage Spaces is a storage virtualization feature built into Windows Server 2016 and Windows 10.

The Storage Spaces feature consists of two components:



- Storage pools. Storage pools are a collection of physical disks aggregated into a single logical disk, allowing you to manage the multiple physical disks as a single disk. You can use Storage Spaces to add physical disks of any type and size to a storage pool.
- Storage spaces. Storage spaces are virtual disks created from free space in a storage pool. Storage spaces have attributes such as resiliency level, storage tiers, fixed provisioning, and precise administrative control. The primary advantage of storage spaces is that you no longer need to manage single disks. Instead, you can manage them as one unit. Virtual disks are the equivalent of a logical unit number (LUN) on a SAN.

Note: The virtual disks that you create with the Storage Spaces feature are not the same as the virtual hard disk files that have the .vhd and .vhdx file extensions.

To create a virtual disk, you need the following:

- Physical disks. Physical disks are disks such as Serial Advanced Technology Attachment (SATA) or serial-attached SCSI (SAS) disks. If you want to add physical disks to a storage pool, the disks must adhere to the following requirements:
  - One physical disk is required to create a storage pool.
  - At least two physical disks are required to create a resilient, mirrored virtual disk.
  - At least three physical disks are required to create a virtual disk with resiliency through parity.
  - At least five physical disks are required for three-way mirroring.
  - Disks must be blank and unformatted, which means no volumes can exist on the disks.
  - Disks can be attached using a variety of bus interfaces including SAS, SATA, SCSI, Non-Volatile Memory Express (NVMe), and universal serial bus (USB). If you plan to use failover clustering with storage pools, you cannot use SATA, SCSI, nor USB disks.
- Storage pool. A storage pool is a collection of one or more physical disks that you can use to create virtual disks. You can add one or more available, nonformatted physical disks to a storage pool, but you can attach a physical disk to only one storage pool.
- Virtual disk, or storage space. This is similar to a physical disk from the perspective of users and applications. However, virtual disks are more flexible because they include both fixed provisioning and thin provisioning, also known as just-in-time (JIT) allocations. They are also more resilient to physical disk failures with built-in functionality such as mirroring and parity. These resemble Redundant Array of Independent Disks (RAID) technologies, but Storage Spaces store the data differently than RAID.
- Disk drive. This is a volume that you can access from your Windows operating system, for example, by using a drive letter.

Note: When planning your Storage Spaces deployment, you need to verify whether the storage enclosure is certified for Storage Spaces in Windows Server 2016. For Storage Spaces to identify disks by slot and use the array's failure and identify/locate lights, the array must support SCSI Enclosure Services (SES) version 3.

Additional Reading: For more information about certified hardware, refer to: "Windows Server Catalog" at: http://aka.ms/Rdpiy8

You can format a storage space virtual disk with an FAT32 file system, New Technology File System (NTFS) file system, or Resilient File System (ReFS). You will need to format the virtual disk with NTFS if you plan to use the storage space as part of a Clustered Shared Volume (CSV), for Data Deduplication, or with File Server Resource Manager (FSRM).

Components and features of Storage Spaces

An important step when configuring storage spaces is planning virtual disks. To configure storage spaces to meet your requirements, you must consider the Storage Spaces features described in the following table before you implement virtual disks.

Features to use Storage Spaces optimally in your environment

Feature	Options
Storage layout	Simple Two-way or three-way mirrors Parity
Disk sector size	512 or 512e 4 KB
Drive allocation	Data-store Manual Hot spare
Provisioning schemes	Thin provisioning space Fixed provisioning space
Stripe parameters	Number of columns Interleave

Feature	Description
Storage layout	Storage layout is one of the characteristics that defines the number of disks from the storage pool that are allocated. Valid options include: • *Simple.* A simple space has data striping but no redundancy. In data striping, logically sequential data is segmented across several disks in a way that enables different physical storage drives to access these sequential segments. Striping can improve performance because it is possible to access multiple segments of data at the same time. To enable data striping, you must deploy at least two disks. The simple storage layout does not provide any redundancy, so if one disk in the storage pool fails, all data is lost unless you have a backup. • *Two-way and three-way mirrors*. Mirroring helps provide protection against the loss of one or more disks. Mirror spaces maintain two or three copies of the data that they host. Specifically, two-way mirrors maintain two data copies, and three-way mirrors maintain three data copies for three-way mirrors. Duplication occurs with every write to ensure that all data copies are always current. Mirror spaces also stripe the data across multiple physical drives. To implement mirroring, you must deploy at least two physical disks. Mirroring provides protection against the loss of one or more disks, so use mirroring when you are

Feature	Description
	storing important data. The disadvantage of using mirroring is that the data is duplicated on multiple disks, so disk usage is inefficient. • *Parity*. A parity space resembles a simple space because data is written across multiple disks. However, parity information is also written across the disks when you use a parity storage layout. The parity information can be used to calculate data if a disk is lost. Parity enables Storage Spaces to continue to perform read-and-write requests even when a drive has failed. The parity information is always rotated across available disks to enable I/O optimization. A storage space requires a minimum of three physical drives for parity spaces. Parity spaces have increased resiliency through journaling. The parity storage layout provides redundancy, but is more efficient in utilizing disk space than mirroring.  **Note:** The number of columns for a given storage space can also impact the number of disks.
Disk sector size	A storage pool's sector size is set the moment it is created. Its default sizes are set as follows: • If the list of drives being used contains only 512 and 512e drives, the pool sector size is set to 512e. A 512 disk uses 512-byte sectors. A 512e drive is a hard disk with 4,096-byte sectors that emulates 512-byte sectors. • If the list contains at least one 4-kilobyte (KB) drive, the pool sector size is set to 4 KB.
Cluster disk requirement	Failover clustering prevents work interruptions if there is a computer failure. For a pool to support failover clustering, all drives in the pool must support SAS.
Drive allocation	Drive allocation defines how the drive is allocated to the pool. Options are: • Data-store. This is the default allocation when any drive is added to a pool. Storage Spaces can automatically select available capacity on data-store drives for both storage space creation and JIT allocation. • Manual. A manual drive is not used as part of a storage space unless it is specifically selected when that storage space is created. This drive allocation property lets administrators specify particular types of drives for use only by certain storage spaces. • Hot spare. These are reserve drives that are not used in the creation of a storage space, but are added to a pool. If a drive that is hosting columns of a storage space fails, one of these reserve drives is called on to replace the failed drive.

Feature	Description
Provisioning schemes	You can provision a virtual disk by using one of two schemes: • Thin provisioning space. Thin provisioning enables storage to be readily allocated on a just-enough and JIT basis. Storage capacity in the pool is organized into provisioning slabs that are not allocated until datasets actually require the storage. Instead of the traditional fixed storage allocation method in which large portions of storage capacity are allocated but might remain unused, thin provisioning optimizes the use of any available storage by reclaiming storage that is no longer needed, using a process known as *trim*. • Fixed provisioning space. In Storage Spaces, fixed provisioned spaces also use flexible provisioning slabs. The difference is that the storage capacity is allocated up front, at the time that the space is created. You can create both thin and fixed provisioning virtual disks within the same storage pool. Having both provisioned types in the same storage pool is convenient, especially when they are related to the same workload. For example, you can choose to use a thin provisioning space for a shared folder containing user files, and a fixed provisioning space for a database that requires high disk I/O.
Stripe parameters	You can increase performance of a virtual disk by striping data across multiple physical disks. When creating a virtual disk, you can configure the *stripe* by using two parameters, *NumberOfColumns* and *Interleave*. • A *stripe* represents one pass of data written to a storage space, with data written in multiple stripes, or passes. • *Columns* correlate to underlying physical disks across which one stripe of data for a storage space is written. • *Interleave* represents the amount of data written to a single column per stripe. The *NumberOfColumns* and *Interleave* parameters determine the width of the stripe (e.g., *stripe_width = NumberOfColumns * Interleave*). In the case of parity spaces, the stripe width determines how much data and parity Storage Spaces writes across multiple disks to increase performance available to apps. You can control the number of columns and the stripe interleave when creating a new virtual disk by using the Windows PowerShell cmdlet **New-VirtualDisk** with the **NumberOfColumns** and **Interleave** parameters.

When creating pools, Storage Spaces can use any DAS device. You can use SATA and SAS drives (or even older integrated drive electronics [IDE] and SCSI drives) that are connected internally to the computer. When planning your Storage Spaces storage subsystems, you must consider the following factors:

- Fault tolerance. Do you want data to be available in case a physical disk fails? If so, you must use multiple physical disks and provision virtual disks by using mirroring or parity.

- Performance. You can improve performance for read and write actions by using a parity layout for virtual disks. You also need to consider the speed of each individual physical disk when determining performance. Alternatively, you can use disks of different types to provide a tiered system for storage. For example, you can use SSDs for data to which you require fast and frequent access and use SATA drives for data that you do not access as frequently.
- Reliability. Virtual disks in parity layout provide some reliability. You can improve that degree of reliability by using hot spare physical disks in case a physical disk fails.
- Extensibility. One of the main advantages of using Storage Spaces is the ability to expand storage in the future by adding physical disks. You can add physical disks to a storage pool any time after you create it to expand its storage capacity or to provide fault tolerance.

Demonstration: Configuring Storage Spaces

In this demonstration, you will see how to:

- Create a storage pool.
- Create a virtual disk and a volume.

Demonstration Steps

Create a storage pool

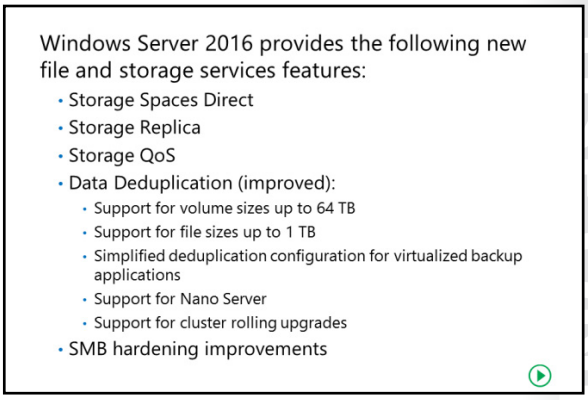
1. On **LON-SVR1**, in **Server Manager**, access **File and Storage Services** and **Storage Pools**.
2. In the **STORAGE POOLS** pane, create a **New Storage Pool** named **StoragePool1**, and then add some of the available disks.

Create a virtual disk and a volume

1. In the **VIRTUAL DISKS** pane, create a **New Virtual Disk** with the following settings:
   - Storage pool: **StoragePool1**
   - Disk name: **Simple vDisk**
   - Storage layout: **Simple**
   - Provisioning type: **Thin**
   - Size: **2 GB**
2. On the **View results** page, wait until the task completes, and then ensure that the **Create a volume when this wizard closes** check box is selected.
3. In the **New Volume Wizard**, create a volume with these settings:
   - Virtual disk: **Simple vDisk**
   - File system: **ReFS**
   - Volume label: **Simple Volume**
4. Wait until the task completes, and then click **Close**.

Changes to file and storage services in Windows Server 2016

File and storage services includes technologies that help you deploy and manage one or multiple file servers.



New features in Windows Server 2016

The following file and storage services features are new or improved in Windows Server 2016:

- Storage Spaces Direct. This feature enables you to build highly available storage systems by using storage nodes with only local storage. You will learn more about this feature later in this module.
- Storage Replica. This new feature in Windows Server 2016 enables replication—between servers or clusters that are in the same location or different sites—for disaster recovery. Storage Replica includes both synchronous and asynchronous replication for shorter or longer distance between sites. This enables you to achieve storage replication at a lower cost.
- Storage Quality of Service (QoS). With this feature, you can create centralized QoS policies on a Scale-Out File Server and assign them to virtual disks on Hyper-V virtual machines. QoS ensures that performance for the storage adapts to meet policies as the storage load changes.
- Data Deduplication. This feature was introduced in Windows Server 2012 and is improved in Windows Server 2016 in the following areas (more information about Data Deduplication is covered later in this module):
    - Support for volume sizes up to 64 terabytes (TB). The feature has been redesigned in Windows Server 2016 and is now multithreaded and able to utilize multiple CPU's per volume to increase optimization throughput rates on volume sizes up to 64 TB.
    - Support for file sizes up to 1 TB. With the use of new stream map structures and other improvements to increase optimization throughput and access performance, deduplication in Windows Server 2016 performs well on files up to 1 TB.
    - Simplified deduplication configuration for virtualized backup applications. In Windows Server 2016, the configuration of deduplication for virtualized backup applications is simplified when enabling deduplication for a volume.
    - Support for Nano Server. A new deployment option in Windows Server 2016, Nano Server fully supports Data Deduplication.
- Support for cluster rolling upgrades. You can upgrade each node in an existing Windows Server 2012 R2 cluster to Windows Server 2016 without incurring downtime to upgrade all the nodes at once.
- Server Message Block (SMB) hardening improvements. In Windows Server 2016, client connections to the Active Directory Domain Services default SYSVOL and NETLOGON shares on domain controllers now require SMB signing and mutual authentication (e.g., Kerberos authentication). This change reduces the likelihood of man-in-the-middle attacks. If SMB signing and mutual authentication are unavailable, a Windows Server 2016 computer won't process domain-based Group Policy and scripts.

Note: The registry values for these settings aren't present by default; however, the hardening rules still apply until they are overridden by Group Policy or other registry values.

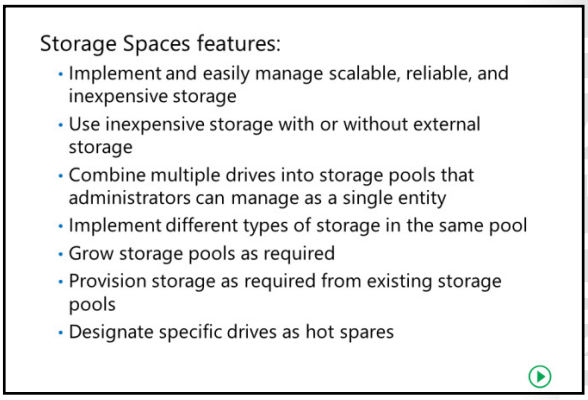
New features in Windows Server 2012 and Windows Server 2012 R2

Windows Server 2012 R2 and Windows Server 2012 offered several new and improved file and storage-services features over its predecessor, including:

- Multiterabyte volumes. This feature deploys multiterabyte NTFS file system volumes, which support consolidation scenarios and maximize storage use. NTFS volumes on master boot record (MBR) formatted disks can be up to 2 terabytes (TB) in size. Volumes on a globally unique identifier (GUID) partition table (GPT) formatted disks can be up to 18 exabytes.
- Data deduplication. This feature saves disk space by storing a single copy of identical data on the volume.
- iSCSI Target Server. The iSCSI Target Server provides block storage to other servers and applications on the network by using the iSCSI standard. Windows Server 2012 R2 includes also VHDX support and end-to-end management by using the Storage Management Initiative Specification.
- Storage spaces and storage pools. This feature enables you to virtualize storage by grouping industry standard disks into storage pools, and then create storage spaces from the available capacity in the storage pools. Storage spaces in Windows Server 2012 R2 enables you to create a tiered storage solution that transparently delivers an appropriate balance between capacity and performance that can meet the needs of enterprise workloads.
- Unified remote management of File and Storage Services in Server Manager. You can use the Server Manager to manage multiple file servers remotely, including their role services and storage.
- Windows PowerShell cmdlets for File and Storage Services. You can use the Windows PowerShell cmdlets for performing most administration tasks for file and storage servers.
- ReFS. The new Resilient File System (ReFS) introduced in Windows Server 2012 offers enhanced integrity, availability, scalability, and error protection for file-based data storage.
- Server Message Block (SMB) 3.0. SMB protocol is a network file-sharing protocol that allows applications to read and write to files and request services from server programs on a network.
- Offloaded Data Transfer (ODX). ODX functionality enables ODX-capable storage arrays to bypass the host computer and directly transfer data within or between compatible storage devices.
- Chkdsk. The new version of Chkdsk runs automatically in the background and monitors the health of the system volume; enabling organizations to deploy multiterabyte NTFS file system volumes without concern about endangering their availability. The Chkdsk tool introduces a new approach. It prioritizes volume availability and allows for the detection of corruption while the volume remains online and its data remains available to the user during maintenance.

Storage Spaces usage scenarios

When considering whether to use Storage Spaces in a given situation, you should weigh the following benefits and limitations. The Storage Spaces feature was designed to enable storage administrators to:



- Implement and easily manage scalable, reliable, and inexpensive storage.
- Aggregate individual drives into storage pools, which are managed as a single entity.
- Use inexpensive storage with or without external storage.
- Use different types of storage in the same pool (e.g., SATA, SAS, USB, SCSI).
- Grow storage pools as required.
- Provision storage when required from previously created storage pools.
- Designate specific drives as hot spares.
- Automatically repair pools containing hot spares.
- Delegate administration by pool.
- Use the existing tools for backup and restore and Volume Shadow Copy Service (VSCS) for snapshots.
- Management can be local or remote, by using Microsoft Management Console (MMC) or Windows PowerShell.
- Utilize Storage Spaces with Failover Clusters.

Note: While the list above mentions USB as a supported storage medium, using USB in a pool might be more practical on a Windows 8 client or while developing a proof of concept. Performance of this technology also depends on the performance capabilities of the storage you choose to pool together.

There are, however, inherent limitations in Storage Spaces. For example, in Windows Server 2016, the following are some of the limitations that you should consider when planning:

- Storage Spaces volumes are not supported on boot or system volumes.
- The contents of a drive are lost when you introduce that drive into a storage pool.
  - You should add only unformatted, or non-partitioned, drives.
- You must have at least one drive in a simple storage pool.
- Fault tolerant configurations have specific requirements:
  - A mirrored pool requires a minimum of two drives.
  - Three-way mirroring requires a minimum of five drives.
  - Parity requires a minimum of three drives.
- All drives in a pool must use the same sector size.

- Storage layers that abstract the physical disks are not compatible with Storage Spaces, including:
  - VHDs and pass-through disks in a virtual machine (VM).
  - Storage subsystems deployed in a separate RAID layer.
- Fibre Channel and iSCSI are not supported.
- Failover Clusters are limited to SAS as a storage medium.

Note: Microsoft Support provides troubleshooting assistance only in environments when Storage Spaces is deployed on a physical machine, not a virtual machine. In addition, just a bunch of disks (JBOD) hardware solutions that you implement must be certified by Microsoft.

When planning for reliability of a particular workload in your environment, Storage Spaces provide different resiliency types. As a result, some workloads are better suited for specific resilient scenarios. The following table depicts these recommended workload types.

Resiliency Type	Number of Data Copies Maintained	Workload Recommendations
Mirror	2 (two-way mirror) 3 (three-way mirror)	Recommended for all workloads
Parity	2 (single parity) 3 (dual parity)	Sequential workloads with large units of read/write, such as archival
Simple	1	Workloads which do not need resiliency, or provide alternate resiliency mechanism

Storage Spaces Direct deployment scenarios

Storage Spaces Direct removes the need for a shared SAS fabric, simplifying deployment and configuration. Instead it uses the existing network as a storage fabric, leveraging SMB 3.0 and SMB Direct for high-speed, low-latency CPU efficient storage. To scale out, you simply add more servers to increase storage capacity and I/O performance.

Storage Spaces Direct can be deployed in support of either primary storage of Hyper-V Virtual Machine (VM) file or secondary storage for Hyper-V Replica virtual machine files. In Windows Server 2016, both options provide storage for Hyper-V, specifically focusing on Hyper-V IaaS (Infrastructure as a Service) for service providers and enterprises.

In the *disaggregated* deployment scenario, the Hyper-V servers (compute component) are located in a separate cluster from the Storage Spaces Direct servers (storage component). The virtual machines are configured to store their files on the Scale-Out File Server (SOFS). The SOFS is designed for use as a file share for server application data and is accessed over the network using the SMB 3.0 protocol. This allows for scaling Hyper-V clusters (compute) and SOFS cluster (storage) independently.

In the *hyper-converged* deployment scenario, the Hyper-V (compute) and Storage Spaces Direct (storage) components are on the same cluster. This option does not require deploying a SOFS, because the virtual machine files are stored on the CSVs. This allows for scaling Hyper-V compute clusters and storage together and does not require configuring file server access and permissions. Once Storage Spaces Direct is configured and the CSV volumes are available, configuring and provisioning Hyper-V is the same process and uses the same tools that you use with any other Hyper-V deployment on a failover cluster.

Storage Spaces Direct can also be deployed in support of SQL Server 2012 or newer, which can store both system and user database files. SQL Server is configured to store these files on SMB 3.0 file shares for both stand-alone and clustered instances of SQL Server. The database server accesses the SOFS over the network using the SMB 3.0 protocol. This scenario requires Windows Server 2012 or newer on both the file servers and the database servers.

Note: Exchange Server workloads are currently not support on Storage Spaces.

Interoperability with Azure virtual machines scenarios

You can use Storage Spaces inside an Azure virtual machine to combine multiple virtual hard drives, creating more storage capacity or performance than is available from a single Azure virtual hard drive. There are three supported scenarios for using Storage Spaces in Azure virtual machines, but there are some limitations and best practices that you should follow, as described below.

- As high performance and/or capacity storage for a virtual machine.
- As backup targets for System Center Data Protection Manager.
- As storage for Azure Site Recovery.

Multi-tenant scenarios

You can provide delegation of administration of storage pools through access control lists (ACLs). You can delegate on a per-storage-pool basis, thereby supporting hosting scenarios that require tenant isolation. Because Storage Spaces uses the Windows security model, it can be fully integrated with Active Directory Domain Services.

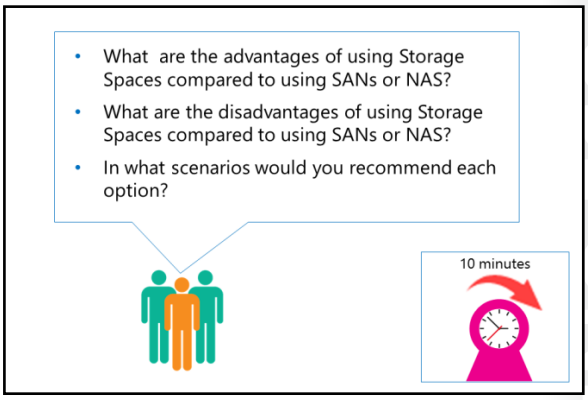
Storage Spaces can be made visible only to a subset of nodes in the file cluster. This can be used in some scenarios to leverage the cost and management advantage of larger shared clusters and to segment those clusters for performance or access purposes. Additionally, you can apply ACLs at various levels of the storage stack (for example, file shares, CSV, and storage spaces). In a multitenant scenario, this means that the full storage infrastructure can be shared and managed centrally and that dedicated and controlled access to segments of the storage infrastructure can be designed. You can configure a particular customer to have LUNs, storage pools, storage spaces, cluster shared volumes, and file shares dedicated to them, and ACLs can ensure only that the tenant has access to them.

Additionally, by using SMB Encryption, you can ensure all access to the file-based storage is encrypted to protect against tampering and eavesdropping attacks. The biggest benefit of using SMB Encryption over more general solutions, such as IPsec, is that there are no deployment requirements or costs beyond changing the SMB settings on the server. The encryption algorithm used is AES-CCM, which also provides data integrity validation.

Discussion: Comparing Storage Spaces to other storage solutions

Storage Spaces in Windows Server 2016 provides an alternative to using more traditional storage solutions, such as SANs and network-attached storage (NAS).

Consider the following questions to prepare for the class discussion:



Question: What are the advantages of using Storage Spaces compared to using SANs or NAS?

Question: What are the disadvantages of using Storage Spaces compared to using SANs or NAS?

Question: In what scenarios would you recommend each option?

Lesson 2
Managing Storage Spaces

Once you have implemented Storage Spaces, you must know how to manage and maintain them. This lesson explores how to use Storage Spaces to mitigate disk failure, to expand your storage pool, and to use logs and performance counters to ensure the optimal behavior of your storage.

Lesson Objectives

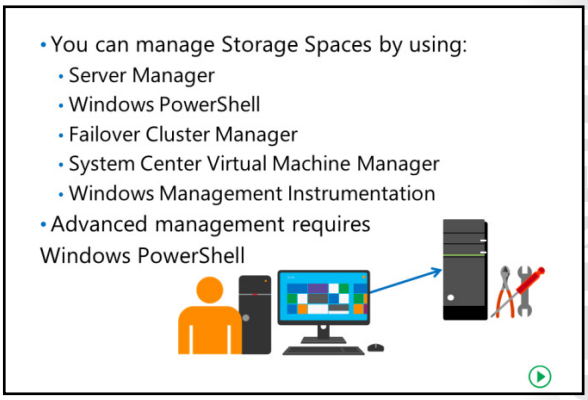
After completing this lesson, you will be able to:

- Describe how to manage Storage Spaces.
- Explain how use Storage Spaces to mitigate storage failure.
- Explain how to expand your storage pool.
- Describe how to use event logs and performance counters to monitor Storage Spaces.

Managing Storage Spaces

Storage Spaces is integrated with failover clustering for high availability, and integrated with cluster shared volumes (CSV) for SOFS deployments. You can manage Storage Spaces by using:

- Server Manager
- Windows PowerShell
- Failover Cluster Manager
- System Center Virtual Machine Manager
- Windows Management Instrumentation (WMI)



Manage using Server Manager

Server Manager provides you with the ability to perform basic management of virtual disks and storage pools. In Server Manager, you can create storage pools; add and remove physical disks from pools; and create, manage, and delete virtual disks. For example, in Server Manager you can view the physical disks that are attached to a virtual disk. If any of these disks are unhealthy, you will see an unhealthy disk icon next to the disk name.

Manage using Windows PowerShell

Windows PowerShell provides advanced management options for virtual disks and storage pools. Some examples of management cmdlets are listed in the following table.

Windows PowerShell cmdlet	Description
Get-StoragePool	Lists storage pools.
Get-VirtualDisk	Lists virtual disks.
Repair-VirtualDisk	Repairs a virtual disk.
Get-PhysicalDisk | Where {$_.HealthStatus -ne "Healthy"}	Lists unhealthy physical disks.
Reset-PhysicalDisk	Removes a physical disk from a storage pool.
Get-VirtualDisk | Get-PhysicalDisk	Lists physical disks that are used for a virtual disk.
Optimize-Volume	Optimizes a volume, performing such tasks on supported volumes and system SKUs as defragmentation, trim, slab consolidation, and storage tier processing.

 **Additional Reading:** For more information, refer to: "Storage Cmdlets in Windows PowerShell" at: http://aka.ms/po9qve

To use Storage Spaces cmdlets in Windows PowerShell, you must download the StorageSpaces module for use in Windows Server 2016. For more information, refer to: "Storage Spaces Cmdlets in Windows PowerShell" at: http://aka.ms/M1fccp

Monitoring storage tier performance

When planning for storage tiering, you should assess the workload characteristics of your storage environment so that you can store your data most cost-effectively depending on how you use it. In Windows Server 2016, the server automatically optimizes your storage performance by transparently moving the data that's accessed more frequently to your faster solid state drives (the SSD tier) and moving less active data to your less expensive, but higher capacity, hard disk drives (the HDD tier).

In many environments, the most common workload characteristics includes a large data set with a majority of the data that is typically cold. *Cold*, or *cool*, data is files that are accessed infrequently, and have a longer life span. In contrast, the most common workload characteristics also includes a smaller portion of the data that is typically hot. *Hot* data, commonly referred to as working set, is files that are currently being worked on; this part of the data set is highly active and changes over time.

 **Note:** The storage tiers optimization process moves data, not files; the data is mapped and moved at a sub-file level. For example, if only 30 percent of the data on a virtual hard disk is *hot*, only that 30 percent of the data is moved to your SSD tier.

Additionally, when planning for storage tiering, you should assess if there are situations in which a file works best when placed in a specific tier. For example, you need to place an important file in the fast tier, or you need to place a backup file in the slow tier. For these situations, your storage solution might have the option to assign a file to a particular tier, also referred to as pinning the file to a tier.

Before you create storage spaces, plan ahead and give yourself room to fine-tune the storage spaces after you observe your workloads in action. After observing input/output operations per second (IOPS) and latency, you will be able to more accurately predict the storage requirements of each workload. Here are some recommendations when planning ahead:

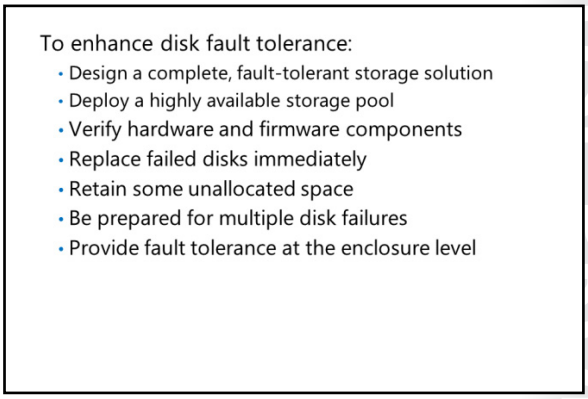
- *Don't allocate all available SSD capacity for your storage spaces immediately.* Keep some SSD capacity in the storage pool in reserve so you can increase the size of an SSD tier when a workload demands it.
- *Don't pin files to storage tiers until you see how well Storage Tiers Optimization can optimize storage performance.* When a tenant or workload requires a particular level of performance, you can pin files to a storage tier to ensure that all I/O activity is performed on that tier.
- *Do consider pinning the parent VHDX file to the SSD tier if you're providing pooled desktops through VDI*. If you have deployed a Virtual Desktop Infrastructure (VDI) to provide pooled desktops for users, you should consider pinning the master image that's used to clone users' desktops to the SSD tier.

You should use the Storage Tier Optimization Report when observing or monitoring your workloads. This report is used to check the performance of your storage tiers and identify the changes that might optimize their performance. As part of the performance analysis, the report provides data for answering questions such as, "How large is my working set?" and "How much do I gain by adding SSD capacity?"

Additional Reading: For more information, refer to: "Monitoring Storage Tiers Performance" at: http://aka.ms/Sz4zfi

Managing disk failure with Storage Spaces

Before deployment, you should plan Storage Spaces to handle disk and JBOD enclosure failures with minimal impact on service and minimal risk of data loss. With any storage solution, you should expect that hardware failure will occur; this is especially true in a large-scale storage solution. To help avoid problems caused by failing hardware, your storage plan should account for the types and number of failures, which might occur in your environment. You should also plan for how your solution should handle each fault without service interruption.



- Design a complete, fault-tolerant storage solution. For example, if you want your storage solution to be able to tolerate a single fault at any level, you need this minimum setup:
  - Two-way mirror or single-parity storage spaces.
  - A clustered file server.
  - Redundant SAS connections between each file server node and each JBOD.

  - Redundant network adapters and network switches.
  - Enough JBOD enclosures to tolerate an entire JBOD failing or becoming disconnected.
- Deploy a highly available storage pool. Using mirrored or parity virtual disks in Storage Spaces provides some fault tolerance and high availability to storage resources. However, because all physical disks connect to a single system, that system itself becomes a single point of failure. If the system to which the physical disks are connected fails, access to the storage resources ceases to exist. Storage Spaces in Windows Server 2016 supports creating a clustered storage pool when using mirror spaces, parity spaces, and simple spaces. To cluster Storage Spaces, your environment must meet the following requirements:
  - All storage spaces in the storage pool must use fixed provisioning.
  - Two-way mirror spaces must use three or more physical disks.
  - Three-way mirror spaces must use five or more physical disks.
  - All physical disks in a clustered pool must be connected by using SAS.
  - All physical disks must support persistent reservations and pass the failover cluster validation tests.

 **Note:** The SAS JBOD must be physically connected to all cluster nodes that will use the storage pool. Direct attached storage that is not connected to all cluster nodes is not supported for clustered storage pools with Storage Spaces.

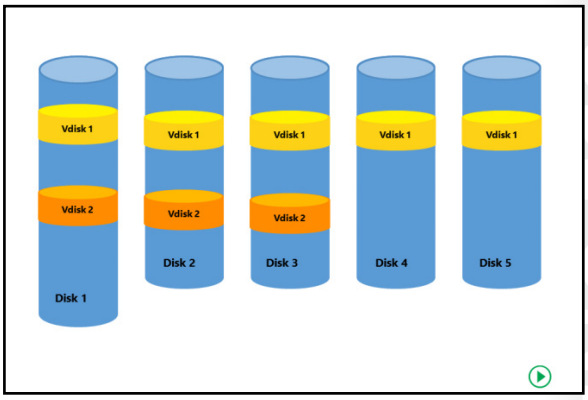
- Unless you deployed a highly available storage pool, import a storage pool on another server if the system fails. In Windows Server 2016, Storage Spaces writes the configuration about the storage pool directly to the disks. Therefore, if the single-point-of-failure system fails and the server hardware requires replacement or a complete reinstall, you can mount a storage pool on another server.
- Most problems with Storage Spaces occur because of incompatible hardware or because of firmware issues. To reduce problems, follow these best practices:
  - Use only certified SAS-connected JBODs. These enclosure models have been tested with Storage Spaces and enable you to easily identify the enclosure and slot for a physical disk.
  - Don't mix and match disk models within a JBOD. Use one model of solid-state drive SSD and one model of HDD for all disks in a JBOD (assuming that you are using storage tiers), and make sure that the disks are fully compatible with the JBOD model.
  - Install the latest firmware and driver versions on all disks. Install the firmware version that is listed as approved for the device in the Windows Server Catalog or is recommended by your hardware vendor. Within a JBOD, it's important that all disks of the same model have the same firmware version.
  - Follow the vendor's recommendations for disk placement. Install disks in the slots recommended by your hardware vendor. JBODs often have different requirements for placement of SSDs and HDDs, for cooling and other reasons.
- Unless you enabled hot spares, retire missing disks automatically. The default policy for handling a physical disk that goes missing from a storage pool (**-RetireMissingPhysicalDisks = Auto**) simply marks the disk as missing (**Lost Communication**), and no repair operation on the virtual disks takes place. This policy avoids potentially I/O-intensive virtual disk repairs if a disk temporarily goes offline, but the storage pool health will remain degraded, compromising resiliency if another disk fails before an administrator takes action. Unless you are using hot spares, we recommend that you change the

RetireMissingPhysicalDisks policy to **Always**, to initiate virtual disk repair operations automatically if a disk loses communication with the system, restoring the health of the pool and the dependent storage spaces as soon as possible.

- Always replace the physical disk before you remove the drive from the storage pool. Changing the storage pool configuration before you replace the physical disk in the enclosure can cause an I/O failure or initiate virtual disk repair, which can result in a "STOP 0x50" error and potential data loss.
- As a general rule, keep unallocated disk space in the pool for virtual disk repairs instead of using hot spares. In Windows Server 2016, you have the option to use available capacity on existing disks in the pool for disk repair operations instead of bringing a hot spare online. This enables Storage Spaces to automatically repair storage spaces with failed disks by copying data to multiple disks in the pool, significantly reducing the time it takes to recover from the failed disk when compared with using hot spares, and it lets you use the capacity on all disks instead of setting aside hot spares.
    - To correct a failed disk in a virtual disk or storage pool, you must remove the disk that is causing the problem. Actions such as defragmenting, scan disk, or using **chkdsk** cannot repair a storage pool.
    - To replace a failed disk, you must add a new disk to the pool. The new disk resynchronizes automatically when disk maintenance occurs during daily maintenance. Alternatively, you can trigger disk maintenance manually.
- When you configure column counts, make sure you have enough physical disks to support automatic virtual disk repairs. Typically, you should configure the virtual disk with 3-4 columns for a good balance of throughput and low latency. Increasing the column count increases the number of physical disks across which a virtual disk is striped, which increases throughput and IOPS for that virtual disk. However, increasing the column count can also increase latency. For this reason, you should optimize overall cluster performance by using multiple virtual disks with 3–4 columns (when using mirrors) or seven columns when using parity spaces. The performance of the entire cluster remains high because multiple virtual disks are used in parallel, making up for the reduced column count.
- Be prepared for multiple disk failures. If you purchased all of the disks in an enclosure at the same time, the disks are the same age, and the failure of one disk might be followed fairly quickly by other disk failures. Even if the storage spaces return to health after the initial disk repairs, you should replace the failed disk as soon as possible to avoid the risk of additional disk failures, which might compromise storage health and availability and risk data loss. If you want to be able to delay disk repairs safely until your next scheduled maintenance, configure your storage spaces to tolerate two disk failures.
- Provide fault tolerance at the enclosure level. If you need to provide an added level of fault tolerance, at the enclosure level, deploy multiple, compatible JBODs that support *enclosure awareness*. In an enclosure-aware storage solution, Storage Spaces writes each copy of data to a specific JBOD enclosure. As a result, if one enclosure fails or goes offline, the data remains available in one or more alternate enclosures. To use enclosure awareness with Storage Spaces, your environment must meet the following requirements:
    - JBOD storage enclosures must support SCSI Enclosure Services (SES).
    - Storage Spaces must be configured as a mirror.
    - To tolerate one failed enclosure with two-way mirrors, you need three compatible storage enclosures.
    - To tolerate two failed enclosures with three-way mirrors, you need five compatible storage enclosures.

Storage pool expansion

One of the main benefits of using Storage Spaces is the ability to expand your storage pool by adding additional storage. Occasionally, however, you must investigate the way in which storage is being used across the disks in your pool before you are able to extend the storage. This is because the blocks for your various virtual disks are distributed across the physical disks in the storage pool in a configuration that is based on the storage layout options that you selected when creating the pool. Depending upon the specifics, you might not be able to extend the storage, even if there is available space in the pool.



Example

Consider the following example:

In the first illustration, a storage pool consists of five disks, where disk1 is larger than the others. Space is consumed across all five disks by vdisk1, while vdisk2 consumes space only on disks 1 through 3.

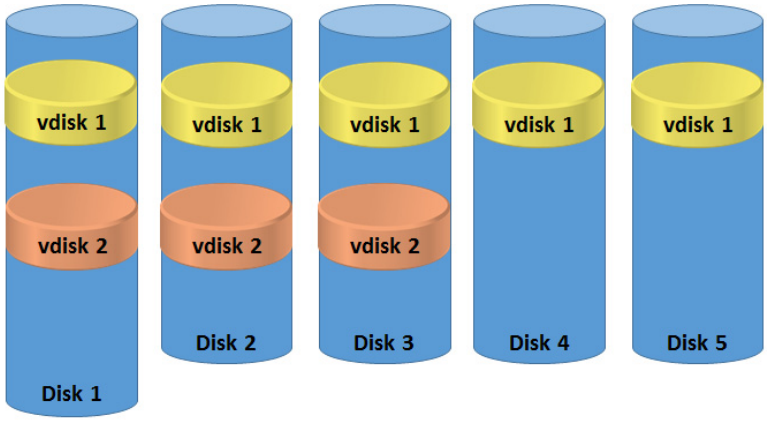


FIGURE 4.1: A STORAGE POOL CONSISTING OF FIVE DISKS

In the second illustration, a sixth disk has been added to the storage pool.

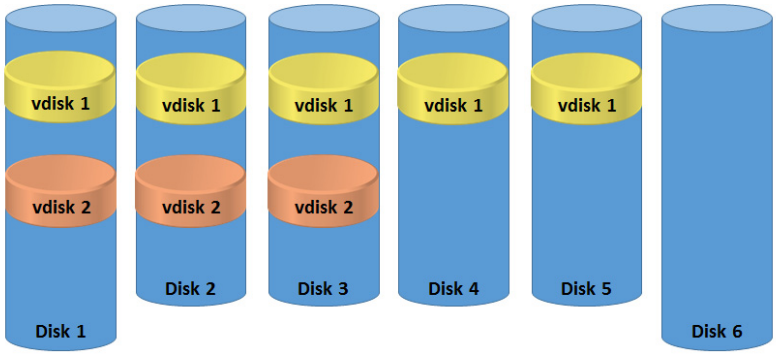


FIGURE 4.2: A STORAGE POOL CONSISTING OF SIX DISKS

- If you attempt to extend vdisk1, the maximum available space for that disk has already been used, even though more space is available within the pool on disk 6. This is because the layout required by vdisk1—due to the options chosen at creation (such as mirroring and parity) — needs five disks. Therefore, to expand vdisk1, you would need to add four additional disks.
- However, if you attempt to extend vdisk2, you can do so because that disk is currently distributed across three devices and there is available space across those three devices to extend it.

 **Note:** In Storage Spaces, blocked storage is arranged as columns. Therefore, in a pre-expanded state, vdisk1 uses five columns and vdisk2 uses three columns.

- Vdisk2 might just be a virtual disk that used two-way mirroring. This means that data on disk1 is duplicated on disk2 and disk3. If you wish to expand a virtual disk with two-way mirroring, it has to have the appropriate number of columns available to accommodate the needs of the virtual disk.

Determining Column Usage

Before you add storage to a storage pool, you must determine the current distribution of blocks across the devices by determining column usage. To do this, you can use the Windows PowerShell cmdlet **Get-VirtualDisk**.

 **Note:** To learn more about the **Get-Virtualdisk** cmdlet, refer to: "Storage Spaces Frequently Asked Questions (FAQ)" at: http://aka.ms/knx5zg

Expanding a storage pool

After you determine column usage where necessary, you can expand your storage pool using one of these options:

- Server Manager. Open **Server Manager**, select **File** and **Storage Services**, and then click **Storage Pools**. You can add a physical disk by right-clicking the pool, and then clicking **Add Physical Disk**.
- Windows PowerShell. You can use the Windows PowerShell cmdlet **Add-PhysicalDisk** to add a physical disk to the storage pool. For example:

```
Add-PhysicalDisk –VirtualDiskFriendlyName UserData –PhysicalDisks (Get-PhysicalDisk -
FriendlyName PhysicalDisk3, PhysicalDisk4)
```

Demonstration: Managing Storage Spaces by using Windows PowerShell

In this demonstration, you will see how to use Windows PowerShell to:

- View the properties of a storage pool.
- Add physical disks to a storage pool.

Demonstration Steps

View the Properties of a Storage Pool

1. On **LON-SRV1**, open **Windows PowerShell**.
2. View the current storage configuration in **Server Manager**.

3. Run the following commands:

   a. To return a list of storage pools with their current health and operational status, run the following command:

   ```
   Get-StoragePool
   ```

   b. To return more information about StoragePool1, run the following command:

   ```
   Get-StoragePool StoragePool1 | fl
   ```

   c. To return detailed information about your virtual disks, including provisioning type, parity layout, and health, run the following command:

   ```
   Get-VirtualDisk | fl
   ```

   d. To return a list of physical disks than can be pooled, run the following command:

   ```
   Get-PhysicalDisk | Where {$_.canpool –eq “true”}
   ```

Add Physical Disks to a Storage Pool

1. Run the following commands:

   a. To create a new virtual disk in StoragePool1, run the following command:

   ```
   New-VirtualDisk –StoragePoolFriendlyName StoragePool1 -FriendlyName Data -Size
   2GB
   ```

   You can see this new virtual disk in **Server Manager**.

   b. To add a list of physical disks that can be pooled to the variable, run the following command:

   ```
   $canpool = Get-PhysicalDisk –CanPool $true
   ```

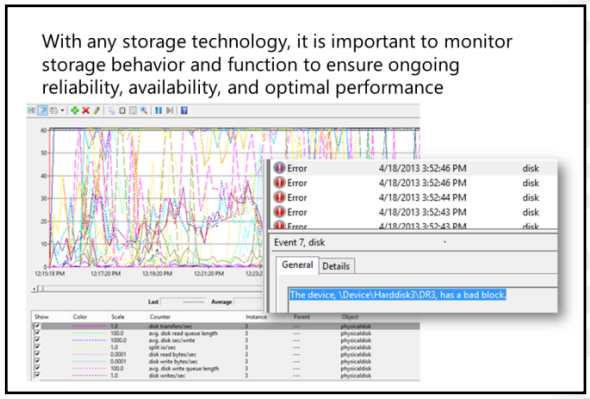
   c. To add the physical disks in the variable to StoragePool1, run the following command:

   ```
   Add-PhysicalDisk -PhysicalDisks $canpool -StoragePoolFriendlyName StoragePool1
   ```

2. View the additional physical disks in **Server Manager**.

Event logs and performance counters

With any storage technology, it is important that you monitor storage behavior and function to ensure ongoing reliability, availability, and optimal performance.



Using the Event Log

When problems are identified in the storage architecture, Storage Spaces generates errors, and then logs these errors to the Event Log. You can access these events by using the Event Log tool, or by accessing the recorded errors by using Server Manager or Windows PowerShell cmdlets. The

following table identifies common Event IDs associated with problematic storage.

Event ID	Message	Cause
100	Physical drive %1 failed to read the configuration or returned corrupt data for storage pool %2. As a result, the in-memory configuration might not be the most recent copy of the configuration. Return Code: %3.	A physical drive can fail to read the configuration or return corrupt data for a storage pool for the following reasons: • The physical drive might fail requests with device I/O errors. • The physical drive might contain corrupted storage pool configuration data. • The physical drive might contain insufficient memory resources.
102	Majority of the physical drives of storage pool %1 failed a configuration update, which caused the pool to go into a failed state. Return Code: %2.	A write failure might occur when writing a storage pool configuration to physical drives for the following reasons: • Physical drives might fail requests with device I/O errors. • An insufficient number of physical drives are online and updated with their latest configurations. • The physical drive might contain insufficient memory resources.
103	The capacity consumption of the storage pool %1 has exceeded the threshold limit set on the pool. Return Code: %2.	The capacity consumption of the storage pool has exceeded the threshold limit set on the pool.
104	The capacity consumption of the storage pool %1 is now below the threshold limit set on the pool. Return Code: %2.	The capacity consumption of the storage pool returns to a level that is below the threshold limit set on the pool.
200	Windows was unable to read the drive header for physical drive %1. If you know the drive is still usable, then resetting the drive health by using the command line or GUI might clear this failure condition and enable you to reassign the drive to its storage pool. Return Code: %2.	Windows was unable to read the drive header for a physical drive.
201	Physical drive %1 has invalid meta-data. Resetting the health status by using the command line or GUI might bring the physical drive to the primordial pool. Return Code: %2.	The metadata on a physical drive has become corrupt.
202	Physical drive %1 has invalid meta-data. Resetting the health status by using the command line or GUI might resolve the issue. Return Code: %2.	The metadata on a physical drive has become corrupt.

Event ID	Message	Cause
203	An I/O failure has occurred on Physical drive %1. Return Code: %2.	An I/O failure has occurred on a physical drive.
300	Physical drive %1 failed to read the configuration or returned corrupt data for storage space %2. As a result, the in-memory configuration might not be the most recent copy of the configuration. Return Code: %3.	A physical drive can fail to read the configuration or return corrupt data for the following reasons: • The physical drive might fail requests with device I/O errors. • The physical drive might contain corrupted storage space configuration data. • The physical drive might contain insufficient memory resources.
301	All pool drives failed to read the configuration or returned corrupt data for storage space %1. As a result, the storage space will not attach. Return Code: %2.	You can experience all physical drives failing to read their configuration or returning corrupt data for storage spaces for the following reasons: • Physical drives might fail requests with device I/O errors. • Physical drives might contain corrupted storage pool configuration data. • The physical drive might contain insufficient memory resources.
302	Majority of the pool drives hosting space meta-data for storage space %1 failed a space meta-data update, which caused the storage pool to go in failed state. Return Code: %2.	The majority of the pool drives hosting space metadata for a storage space can fail a metadata update for the following reasons: • Physical drives might fail requests with device I/O errors. • Insufficient number of physical drives have online storage space metadata. • The physical drive might contain insufficient memory resources.
303	Drives hosting data for storage space have failed or are missing. As a result, no copy of data is available. Return Code: %2.	This event can occur if a drive in the storage pool fails or is removed.
304	One or more drives hosting data for storage space %1 have failed or are missing. As a result, at least one copy of data is not available. However, at least one copy of data is still available. Return Code: %2.	One or more drives hosting data for a storage space have failed or are missing. As a result, at least one copy of data is not available. However, at least one copy of data is still available.

Event ID	Message	Cause
306	The attempt to map or allocate more storage for the storage space %1 has failed. This is because there was a write failure involved in the updating the storage space metadata. Return Code: %2.	The attempt to map or allocate more storage for the storage space has failed. More physical drives are needed.
307	The attempt to unmap or trim the storage space %1 has failed. Return Code: %2.	The attempt to unmap or trim the listed storage space has failed.
308	A repair attempt for storage space %1 was initiated by the driver. Return Code: %2.	A repair attempt for storage space was initiated by the driver. This is a normal condition. No further action is required.

Performance Monitoring

Most decisions that you make regarding the configuration of your storage architecture have an impact on the performance of your storage architecture. This is also true for using Storage Spaces to implement your storage architecture. Performance is better or worse because of the balance between multiple factors including cost, reliability, availability, power, and ease-of-use.

There are multiple components that handle storage requests within your storage architecture, including:

- File cache management.
- File system architecture.
- Volume management.
- Physical storage hardware.
- Storage Spaces configuration options.

You can use Windows PowerShell and Performance Monitor to monitor the performance of your storage pools. If you want to use Windows PowerShell, you must install the Storage Spaces Performance Analysis module for Windows PowerShell.

 **Note:** To download the "Storage Spaces Performance Analysis module for Windows PowerShell" module, go to: http://aka.ms/b1d52u

To use Windows PowerShell to generate and collect performance data, at a Windows PowerShell prompt, run the following cmdlet:

```
Measure-StorageSpacesPhysicalDiskPerformance -StorageSpaceFriendlyName StorageSpace1 -
MaxNumberOfSamples 60 -SecondsBetweenSamples 2 -ReplaceExistingResultsFile -
ResultsFilePath StorageSpace1.blg -SpacetoPDMappingPath PDMap.csv
```

This cmdlet:

- Monitors the performance of all physical disks associated with the storage space named StorageSpace1.
- Captures performance data for 60 seconds at two-second intervals.
- Replaces the results files if they already exist.
- Stores the performance log in the file named StorageSpace1.blg.
- Stores the physical disk mapping information in a file named PDMap.csv.

You can use Performance Monitor to view the data collected in the two files specified in the cmdlet above, named StorageSpace1.blg and PDMap.csv.

Lab A: Implementing Storage Spaces

Scenario

A Datum corporation has purchased a number of hard disk drives and SSDs and you have been tasked with creating a storage solution that can utilize these new devices to the fullest. With mixed requirements in A. Datum for data access and redundancy, you must ensure that you have a redundancy solution for critical data that does not require fast disk read and write access.

You decide to use Storage Spaces to meet the requirements.

Objectives

After completing this lab, you will be able to:

- Create a storage space.
- Enable and configure storage tiering.

Lab Setup

Estimated Time: **40 minutes**

Virtual machines: **20740A-LON-DC1** and **20740A-LON-SVR1**

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 **20740A-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: **Administrator**
    - Password: **Pa$$w0rd**
    - Domain: **Adatum**
5. Repeat steps 2 through 4 for **20740A-LON-SVR1**.

Exercise 1: Creating a Storage Space

Scenario

Your server does not have a hardware-based RAID card, but you have been asked to configure redundant storage. To support this feature, you must create a storage pool.

After creating the storage pool, you must create a redundant virtual disk. Because the data is critical, the request for redundant storage specifies that you must use a three-way mirrored volume. Shortly after the volume is in use, a disk fails, and you have to replace it by adding another disk to the storage pool.

The main tasks for this exercise are as follows:

1. Create a storage pool from six disks that are attached to the server.
2. Create a three-way mirrored virtual disk (need at least five physical disks).

3. Copy a file to the volume, and verify it is visible in File Explorer.
4. Remove a physical drive to simulate drive failure.
5. Verify that the file is still available.
6. Add a new disk to the storage pool and remove the broken disk.

▶ Task 1: Create a storage pool from six disks that are attached to the server

1. On **LON-SVR1**, open **Server Manager**.
2. In the left pane, click **File and Storage Services**, and then, in the **Servers** pane, click **Storage Pools**.
3. Create a storage pool with the following settings:
   - Name: **StoragePool1**
   - Physical disks: first 6 disks.

▶ Task 2: Create a three-way mirrored virtual disk (need at least five physical disks)

1. On **LON-SVR1**, in **Server Manager**, in the **VIRTUAL DISKS** pane, create a virtual disk with the following settings:
   - Storage pool: **StoragePool1**
   - Name: **Mirrored Disk**
   - Storage Layout: **Mirror**
   - Resiliency settings: **Three-way mirror**
   - Provisioning type: **Thin**
   - Virtual disk size: **10 GB**

   Note: If the three-way resiliency setting is unavailable, proceed to the next step in the lab.

2. In the **New Volume Wizard**, create a volume with the following settings:
   - Virtual disk: **Mirrored Disk**
   - Drive letter: **H**
   - File system: **ReFS**
   - Volume label: **Mirrored Volume**

▶ Task 3: Copy a file to the volume, and verify it is visible in File Explorer

1. On **LON-SVR**, open **Command Prompt**.
2. Type the following command, and then press Enter:

```
Copy C:\windows\system32\write.exe H:\
```

3. Open **File Explorer** from the taskbar, and then access **Mirrored Volume (H:)**. You should see write.exe in the file list.

▶ Task 4: Remove a physical drive to simulate drive failure

- On the host computer, in **Hyper-V Manager**, in the **Virtual Machines** pane, change the **20740A-LON-SVR1** settings to the following:
  - Remove the hard drive that begins with **20740A-LON-SVR1-Disk1**.

▶ Task 5: Verify that the file is still available

1. Switch to **LON-SVR1**.
2. Open **File Explorer**, and then go to **H:**.
3. Verify that **write .exe** is still available.
4. In **Server Manager**, in the **STORAGE POOLS** pane, on the menu bar, click **Refresh "Storage Pools"**.

   Note: Notice the warning that is visible next to Mirrored Disk.

5. Open the **Mirrored Disk Properties** dialog box, and then access the **Health** pane.

   Note: Notice that the Health Status indicates a warning. The Operational Status should indicate one or more of the following: Incomplete, Unknown, or Degraded.

6. Close the **Mirrored Disk Properties** dialog box.

▶ Task 6: Add a new disk to the storage pool and remove the broken disk

1. On **LON-SVR1**, in **Server Manager**, in the **STORAGE POOLS** pane, on the menu bar, click **Refresh "Storage Pools"**.
2. In the **STORAGE POOLS** pane, right-click **StoragePool1**, click **Add Physical Disk**, and then add the first disk in the list.
3. To remove the disconnected disk, open **Windows PowerShell**, and then run the following commands:

```
Get-PhysicalDisk
```

   Note: Note the FriendlyName for the disk that shows an OperationalStatus of Lost Communication. Use this disk name in the next command in place of *diskname*.

```
$Disk = Get-PhysicalDisk -FriendlyName 'diskname'
```

```
Remove-PhysicalDisk -PhysicalDisks $disk -StoragePoolFriendlyName StoragePool1
```

4. In **Server Manager**, refresh the storage pools view to see the warnings disappear.

Results: After completing this exercise, you will have successfully created a storage pool and added five disks to it. Additionally, you should have created a three-way mirrored, thinly-provisioned virtual disk from the storage pool. You also should have copied a file to the new volume and then verified that it is accessible. Next, after removing a physical drive, you should have verified that the virtual disk was still available and that you could access it. Finally, you should have added another physical disk to the storage pool.

Question: At a minimum, how many disks must you add to a storage pool to create a three-way mirrored virtual disk?

Question: You have a USB-attached disk, four SAS disks, and one SATA disk that are attached to a Windows Server 2012 server. You want to provide a single volume to your users that they can use for file storage. What would you use?

Lesson 3
Implementing Data Deduplication

Data Deduplication is a role service of Windows Server 2016. This service identifies and removes duplications within data without compromising data integrity. It does this to achieve the ultimate goals of storing more data and using less physical disk space. This lesson explains how to implement Data Deduplication in Windows Server 2016 storage.

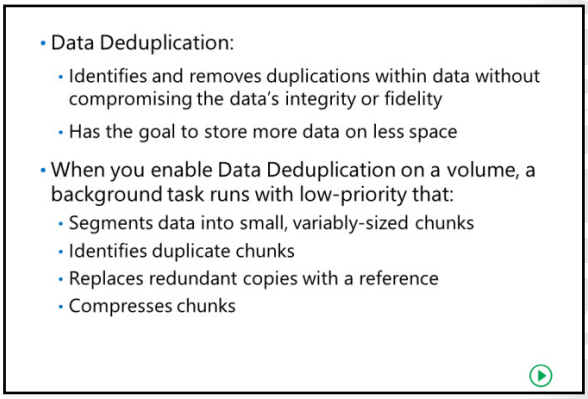
Lesson Objectives

After completing this lesson, you will be able to:

- Describe Data Deduplication in Windows Server 2016.
- Identify Data Deduplication components in Windows Server 2016.
- Explain how to deploy Data Deduplication.
- Describe common usage scenarios for data deduplication.
- Explain how to monitor and maintain data deduplication.
- Describe backup and restore considerations with Data Deduplication.

What is Data Deduplication?

To cope with data storage growth in the enterprise, organizations are consolidating servers and making capacity scaling and data optimization the key goals. Data Deduplication provides practical ways to achieve these goals, including:



- Capacity optimization. Data Deduplication stores more data in less physical space. It achieves greater storage efficiency as compared to features such as Single Instance Store (SIS) or NTFS compression. Data deduplication uses subfile variable-size chunking and compression, which deliver optimization ratios of 2:1 for general file servers and up to 20:1 for virtualization data.
- Scale and performance. Data Deduplication is highly scalable, resource efficient, and nonintrusive. While it can process up to 50 MB per second in Windows Server 2012 R2 and about 20 MB of data per second in Windows Server 2012, Windows Server 2016 is staged to perform significantly better, through the advancements in the Deduplication Processing Pipeline. In this latest version of Windows Server, Data Deduplication can run multiple threads in parallel by using multiple I/O queues on multiple volumes simultaneously without affecting other workloads on the server. Low impact on the server workloads is maintained by throttling the CPU and memory resources that are consumed; if the server is very busy, deduplication can stop completely. In addition, you have the flexibility to run Data Deduplication jobs at any time, set schedules for when data deduplication should run, and establish file selection policies.

- Reliability and data integrity. When Data Deduplication is applied to a volume on a server, the integrity of the data is maintained. Data Deduplication uses checksum results, consistency, and identity validation to ensure data integrity. Data Deduplication maintains redundancy, for all metadata and the most frequently referenced data, to ensure that the data is repaired, or at least recoverable, in the event of data corruption.
- Bandwidth efficiency with BranchCache. Through integration with BranchCache, the same optimization techniques are applied to data transferred over the WAN to a branch office. The result is faster file download times and reduced bandwidth consumption.
- Optimization management with familiar tools. Data Deduplication has optimization functionality built into Server Manager and Windows PowerShell. Default settings can provide savings immediately, or you can fine-tune the settings to see more gains. By using Windows PowerShell cmdlets, you can start an optimization job or schedule one to run in the future. Installing the Data Deduplication feature and enabling deduplication on selected volumes can also be accomplished by using the Unattend.xml file that calls a Windows PowerShell script and can be used with Sysprep to deploy deduplication when a system first boots.

The Data Deduplication process involves finding and removing duplication within data without compromising its fidelity or integrity. The goal is to store more data in less space by segmenting files into small variable-sized chunks (32–128 KB), identifying duplicate chunks, and maintaining a single copy of each chunk.

After deduplication, files are no longer stored as independent streams of data, and they are replaced with stubs that point to data blocks that are stored within a common chunk store. Because these files share blocks, those blocks are only stored once, which reduces the disk space needed to store all files. During file access, the correct blocks are transparently assembled to serve the data without the application or the user having any knowledge of the on-disk transformation to the file. This enables you to apply deduplication to files without having to worry about any change in behavior to the applications or impact to users who are accessing those files. Data Deduplication works best in storage scenarios with large amounts of data that are not modified frequently.

Enhancements to the Data Deduplication Role Service

Windows Server 2016 includes several important improvements to the way Data Deduplication worked in Windows Server 2012 R2 and Windows Server 2012, including:

- Support for volume sizes up to 64 TB. Data Deduplication in Windows Server 2012 R2 does not perform well on volumes greater than 10 TB in size (or less for workloads with a high rate of data changes), the feature has been redesigned in Windows Server 2016. Deduplication Processing Pipeline is now multithreaded and able to utilize multiple CPUs per volume to increase optimization throughput rates on volume sizes up to 64 TB. This is a limitation of VSS, on which Data Deduplication is dependent.
- Support for file sizes up to 1 TB. In Windows Server 2012 R2, very large files are not good candidates for Data Deduplication. However, with the use of the new stream map structures and other improvements to increase the optimization throughput and access performance, deduplication in Windows Server 2016 performs well on files up to 1 TB.
- Simplified deduplication configuration for virtualized backup applications. Although Windows Server 2012 R2 supports deduplication for virtualized backup applications, it requires manually tuning the deduplication settings. In Windows Server 2016, however, the configuration of deduplication for virtualized backup applications is drastically simplified by a predefined usage-type option when enabling deduplication for a volume.

- Support for Nano Server. Nano Server is a new deployment option in Windows Server 2016 that has a smaller system resource footprint, starts up significantly faster, and requires fewer updates and restarts than by using the Sever Core deployment option for Windows Server. In addition, Data Deduplication is fully supported on Nano Server.
- Support for cluster rolling upgrades. Windows servers in a failover cluster running deduplication can include a mix of nodes running Windows Server 2012 R2 and nodes running Windows Server 2016. This major enhancement provides full data access to all of your deduplicated volumes during a cluster rolling upgrade. For example, you can gradually upgrade each deduplication node in an existing Windows Server 2012 R2 cluster to Windows Server 2016 without incurring downtime to upgrade all the nodes at once.

 **Note:** Although both the Windows Server versions of deduplication can access the optimized data, the optimization jobs run only on the Windows Server 2012 R2 deduplication nodes and are blocked from running on the Windows Server 2016 deduplication nodes until the cluster rolling upgrade is complete.

Effectively, Data Deduplication in Windows Server 2016, allows you to efficiently store, transfer, and backup fewer bits.

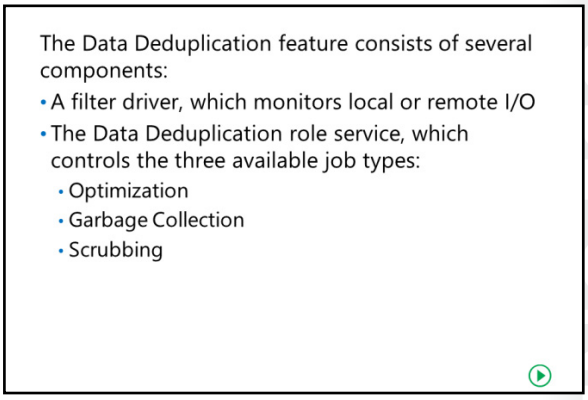
Volume requirements for Data Deduplication

After you install the role service, you can enable Data Deduplication on a per-volume basis. Data Deduplication includes the following requirements:

- Volumes must not be a system or boot volume. Because most files used by an operating system are constantly open, Data Deduplication on system volumes would negatively affect the performance because deduplicated data would need to be expanded again before the files could be used.
- Volumes might be partitioned by using master boot record (MBR) or GUID partition table (GPT) format and must be formatted by using the NTFS or ReFS file system.
- Volumes must be attached to the Windows Server and cannot appear as non-removable drives. This means that you cannot use USB or floppy drives for Data Deduplication, nor use remotely-mapped drives.
- Volumes can be on shared storage, such as Fibre Channel, iSCSI SAN, or SAS array.
- Files with extended attributes, encrypted files, files smaller than 32 KB, and reparse point files will not be processed for Data Deduplication.
- Data Deduplication is not available for Windows client operating systems.

Data Deduplication components

The Data Deduplication role service consists of several components. These components include:



- Filter driver. This component monitors local or remote I/O and handles the chunks of data on the file system by interacting with the various jobs. There is one filter driver for every volume.
- Deduplication service. This component manages the following job types:
  - Optimization. Consisting of multiple jobs, they perform both deduplication and compression of files according to the data deduplication policy for the volume. After initial optimization of a file, if the file is then modified and meets the data deduplication policy threshold for optimization, the file will be optimized again.
  - Garbage Collection. Data Deduplication includes garbage collection jobs to process deleted or modified data on the volume so that any data chunks no longer referenced are cleaned up. This job processes previously deleted or logically overwritten optimized content to create usable volume free space. When an optimized file is deleted or overwritten by new data, the old data in the chunk store is not deleted right away. While garbage collection is scheduled to run weekly, you might consider running garbage collection only after large deletions have occurred.
  - Scrubbing. Data Deduplication has built-in data integrity features such as checksum validation and metadata consistency checking. It also has built-in redundancy for critical metadata and for the most popular data chunks. As data is accessed or deduplication jobs process data, if these features encounter corruption, they record the corruption in a log file. Scrubbing jobs use these features to analyze the chunk store corruption logs and, when possible, to make repairs. Possible repair operations include using three sources of redundant data:
    - Deduplication keeps backup copies of popular chunks when they are referenced over 100 times in an area called the hotspot. If the working copy is corrupted, deduplication uses its own redundant copy in the case of soft corruptions such as bit flips or torn writes.
    - If using mirrored Storage Spaces, deduplication can use the mirror image of the redundant chunk to serve the I/O and fix the corruption.
    - If a file is processed with a chunk that is corrupted, the corrupted chunk is eliminated, and the new incoming chunk is used to fix the corruption.

    Note: Because of the additional validations that are built into deduplication, the deduplication subsystem is often the first system to report any early signs of data corruption in the hardware or file system.

  - Unoptimization. This job undoes deduplication on all of the optimized files on the volume. Some of the common scenarios for using this type of job include decommissioning a server with volumes enabled for Data Deduplication, troubleshooting issues with deduplicated data, or migration of data to another system that doesn't support Data Deduplication. Before you start this job, you should use the **Disable-DedupVolume** Windows PowerShell cmdlet to disable further data deduplication activity on one or more volumes. After you disable Data Deduplication, the volume remains in the deduplicated state and the existing deduplicated data

remains accessible; however, the server stops running optimization jobs for the volume and new data is not deduplicated. Afterwards, you would use the unoptimization job to undo the existing deduplicated data on a volume. At the end of a successful unoptimization job, all of the data deduplication metadata is deleted from the volume.

 **Note:** You should be cautious when using the unoptimization job, because all the deduplicated data will return to the original logical file size. As such, you should verify the volume has enough free space for this activity or move/delete some of the data to allow the job to complete successfully.

Data Deduplication Process

In Windows Server 2016, Data Deduplication transparently removes duplication without changing access semantics. When you enable Data Deduplication on a volume, a post-process, or target, deduplication is used to optimize the file data on the volume by performing the following actions:

- Optimization jobs, which are background tasks, run with low priority on the server to process the files on the volume.
- By using an algorithm, segment all file data on the volume into small, variable-sized chunks that range from 32 KB to 128 KB.
- Identifies chunks that have one or more duplicates on the volume.
- Inserts chunks into a common chunk store.
- Replaces all duplicate chunks with a reference, or stub, to a single copy of the chunk in the chunk store.
- Replaces the original files with a reparse point, which contains references to its data chunks.
- Compresses chunks and organizes them in container files in the **System Volume Information** folder.
- Removes primary data stream of the files.

The Data Deduplication process works through scheduled tasks on the local server, but you can run the process interactively by using Windows PowerShell. More information about this is discussed later in the module.

Data deduplication does not have any write-performance impact because the data is not deduplicated while the file is being written. Windows Server 2016 uses post-process deduplication, which ensures that the deduplication potential is maximized. The other advantage with this type of deduplication process is that all processing is offloaded from your application servers and client computers, which means less stress on the other resources in your environment. There is, however, a small performance impact when reading deduplicated files.

 **Note:** The three main types of data deduplication are source, target (or post-process deduplication) and in-line (or transit deduplication).

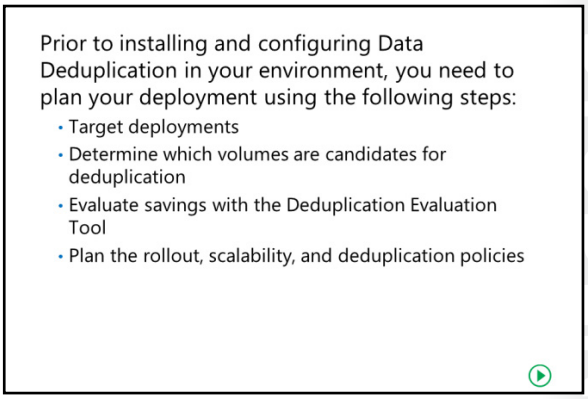
Data Deduplication potentially can process all of the data on a selected volume, except for files that are less than 32 KB in size, and files in folders that are excluded. You must carefully determine if a server and its attached volumes are suitable candidates for deduplication prior to enabling the feature. You should also consider backing up important data regularly during the deduplication process.

After you enable a volume for deduplication and the data is optimized, the volume contains the following elements:

- Unoptimized files. Includes files that do not meet the selected file-age policy setting, system state files, alternate data streams, encrypted files, files with extended attributes, files smaller than 32 KB, or other reparse point files.
- Optimized files. Includes files that are stored as reparse points that contain pointers to a map of the respective chunks in the chunk store that are needed to restore the file when it is requested.
- Chunk store. Location for the optimized file data.
- Additional free space. The optimized files and chunk store occupy much less space than they did prior to optimization.

Deploying Data Deduplication

Planning a Data Deduplication deployment



Prior to installing and configuring Data Deduplication in your environment, you must plan your deployment using the following steps:

- Target deployments. Data Deduplication is designed to be applied on primary – and not to logically extended – data volumes without adding any additional dedicated hardware. You can schedule deduplication based on the type of data that is involved and the frequency and volume of changes that occur to the volume or particular file types. You should consider using deduplication for the following data types:
  - General file shares. Group content publication and sharing, user home folders, and Folder Redirection/Offline Files.
  - Software deployment shares. Software binaries, images, and updates.
  - VHD libraries. Virtual hard disk (VHD) file storage for provisioning to hypervisors.
  - VDI deployments. Virtual Desktop Infrastructure (VDI) deployments using Hyper-V.
  - Virtualized backup. Backup applications running as Hyper-V guests saving backup data to mounted VHDs.
- Determine which volumes are candidates for deduplication. Deduplication can be very effective for optimizing storage and reducing the amount of disk space consumed – saving you 50 to 90 percent of your system's storage space when applied to the right data. Use the following considerations to evaluate which volumes are ideal candidates for deduplication:
  - *Is duplicate data present?*

File shares or servers which host user documents, software deployment binaries, or virtual hard disk files tend to have plenty of duplication, and yield higher storage savings from deduplication. More information on the deployment candidates for deduplication and the supported/unsupported scenarios are discussed later in this module.

- *Does the data access pattern allow for sufficient time for deduplication?*

  For example, files that frequently change and are often accessed by users or applications are not good candidates for deduplication. In these scenarios, deduplication might not be able to process the files, as the constant access and change to the data are likely to cancel any optimization gains made by deduplication. On the other hand, good candidates allow time for deduplication of the files.

- *Does the server have sufficient resources and time to run deduplication?*

  Deduplication requires reading, processing, and writing large amounts of data, which consumes server resources. Servers typically have periods of high activity and times when there is low resource utilization; the deduplication jobs work more efficiently when resources are available. However, if a server is constantly at maximum resource capacity, it might not be an ideal candidate for deduplication.

- Evaluate savings with the Deduplication Evaluation Tool. You can use the Deduplication Evaluation Tool, **DDPEval.exe**, to determine the expected savings that you would get if deduplication is enabled on a particular volume. DDPEval.exe supports evaluating local drives and mapped or unmapped remote shares.

  Note: When the deduplication feature is installed, the Deduplication Evaluation Tool (DDPEval.exe) is automatically installed to the \Windows\System32\ directory. For more information on this tool, refer to: http://aka.ms/sxzd2l

- Plan the rollout, scalability, and deduplication policies. The default deduplication policy settings are usually sufficient for most environments. However, if your deployment has any of the following conditions, you might consider altering the default settings:
  - Incoming data is static or expected to be read-only, and you want to process files on the volume sooner. In this scenario, change the **MinimumFileAgeDays** setting to a smaller number of days to process files earlier.
  - You have directories that you do not want to deduplicate. Add a directory to the exclusion list.
  - You have file types that you do not want to deduplicate. Add a file type to the exclusion list.
  - The server has different off-peak hours than the default and you want to change the Garbage Collection and Scrubbing schedules. Update the schedules using Windows PowerShell.

Installing and configuring Data Deduplication

After completing your planning, you need to use the following steps to deploy Data Deduplication to a server in your environment:

- Install Data Deduplication components on the server. Use the following options to install deduplication components on the server:
  - *Server Manager*. In Server Manager, you can install Data Deduplication by navigating to **Add Roles and Features Wizard** > under **Server Roles** > select **File and Storage Services** > select the **File Services** check box > select the **Data Deduplication** check box > click **Install**.

- *Windows PowerShell*. You can use the following command to install Data Deduplication:

```
Import-Module ServerManager
Add-WindowsFeature -Name FS-Data-Deduplication
Import-Module Deduplication
```

- Enable Data Deduplication**.** Use the following options to enable Data Deduplication on the server:
  - Server *Manager*. From the Server Manager dashboard:
    i. Right-click a data volume and select **Configure Data Deduplication**.
    ii. In the **Data deduplication** box, select the workload you want to host on the volume. For example, select **General purpose file server** for general data files or **Virtual Desktop Infrastructure (VDI) server** when configuring storage for running virtual machines.
    iii. Enter the minimum number of days that should elapse from the date of file creation before files are deduplicated, enter the extensions of any file types that should not be deduplicated, and then click **Add** to browse to any folders with files that should not be deduplicated.
    iv. Click **Apply** to apply these settings and return to the Server Manager dashboard, or click the **Set Deduplication Schedule** button to continue to set up a schedule for deduplication.
  - *Windows PowerShell*. Use the following command to enable deduplication on a volume:

```
Enable-DedupVolume –Volume VolumeLetter –UsageType StorageType
```

Note: Replace *VolumeLetter* with the drive letter of the volume. Replace *StorageType* with the value corresponding to the expected type of workload for the volume. Acceptable values include:

- *HyperV*. A volume for Hyper-V storage.
- *Backup*. A volume that is optimized for virtualized backup servers.
- *Default*. A general purpose volume.

Optionally, you can use the Windows PowerShell cmdlet **Set-DedupVolume** to configure additional options, such as the minimum number of days that should elapse from the date of file creation before files are deduplicated, the extensions of any file types that should not be deduplicated, or the folders that should be excluded from deduplication.

- Configure Data Deduplication jobs. With Data Deduplication jobs, you can run them manually, on demand, or use a schedule. The following list are the types of jobs which you can perform on a volume:
  - *Optimization*. Includes built-in jobs which are automatically scheduled for optimizing the volumes on a periodic basis. Optimization jobs deduplicate data and compress file chunks on a volume per the policy settings. You can also use the following command to trigger an optimization job on demand:

```
Start-DedupJob –Volume VolumeLetter –Type Optimization
```

- *Data Scrubbing*. Scrubbing jobs are automatically scheduled to analyze the volume on a weekly basis and produce a summary report in the Windows event log. You can also use the following command to trigger a scrubbing job on demand:

```
Start-DedupJob –Volume VolumeLetter –Type Scrubbing
```

- *Garbage Collection*. Garbage collection jobs are automatically scheduled to process data on the volume on a weekly basis. Because garbage collection is a processing-intensive operation, you may consider waiting until after the deletion load reaches a threshold to run this job on demand or schedule the job for after hours. You can also use the following command to trigger a garbage collection job on demand:

```
Start-DedupJob –Volume VolumeLetter –Type GarbageCollection
```

- *Unoptimization*. Unoptimization jobs are available on an as-needed basis and are not scheduled automatically. However, you can use the following command to trigger an unoptimization job on demand:

```
Start-DedupJob –Volume VolumeLetter –Type Unoptimization
```

Note: For more information on the Windows PowerShell cmdlet **Start-DedupJob**, refer to: http://aka.ms/o30xqw

- Configure Data Deduplication schedules. When you enable Data Deduplication on a server, three schedules are enabled by default: Optimization is scheduled to run every hour, and Garbage Collection and Scrubbing are scheduled to run once a week. You can view the schedules by using this Windows PowerShell cmdlet **Get-DedupSchedule**. These scheduled jobs run on all the volumes on the server. However, if you want to run a job only on a particular volume, you must create a new job. You can create, modify, or delete job schedules from the **Deduplication Settings** page in Server Manager, or by using the Windows PowerShell cmdlets: **New-DedupSchedule**, **Set-DedupSchedule**, or **Remove-DedupSchedule**.

Note: Data Deduplication jobs only support, at most, weekly job schedules. If you need to create a schedule for a monthly job or for any other custom time period, use Windows Task Scheduler. However, you will be unable to view these custom job schedules created with Windows Task Scheduler by using the Windows PowerShell cmdlet **Get-DedupSchedule**.

Demonstration: Implementing Data Deduplication

In this demonstration, you will see how to:

- Install the Data Deduplication role service.
- Enable Data Deduplication.
- Check the status of Data Deduplication.

Demonstration Steps

Install the Data Deduplication Role Service

- On **LON-SVR1**, in **Server Manager**, add the **Data Deduplication** role service.

Enable Data Deduplication

1. Open **File Explorer** and observe the available volumes and free space.
2. Return to **File and Storage Services**.
3. Click **Disks**.
4. Click the **1** disk, and then click the **E** volume.
5. Enable **Data Deduplication**, and then click the **General purpose file server** setting.
6. Configure the following settings:
   - Deduplicate files older than (in days): **1**
   - Enable throughput optimization
   - Exclude: **E:\shares**

Check the Status of Data Deduplication

1. Switch to **Windows PowerShell**.
2. Execute the following commands to verify Data Deduplication status:

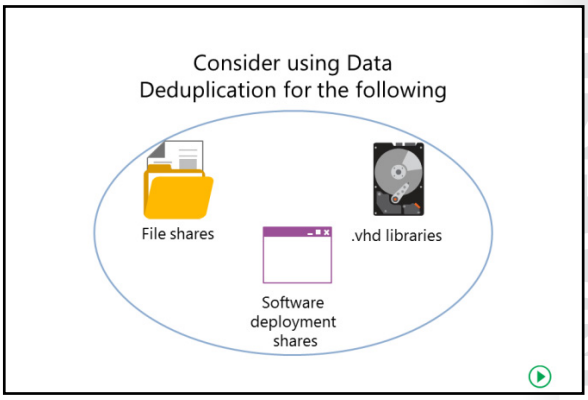
```
a. Get-DedupStatus
b. Get-DedupStatus | fl
c. Get-DedupVolume
d. Get-DedupVolume |fl
e. Start-DedupJob E: -Type Optimization –Memory 50
```

3. Repeat commands 2a and 2c.

Note: Because most the files on drive E are small, you may not notice a significant amount of saved space.

4. Close all open windows.

Usage scenarios for Data Deduplication



The following table highlights typical deduplication savings for various content types. Your data storage savings will vary by data type, the mix of data, and the size of the volume and the files that the volume contains. You should consider using the Deduplication Evaluation Tool to evaluate the volumes before you enable deduplication.

- User documents. This includes group content publication or sharing, user home folders (or MyDocs), and profile redirection for accessing offline files. Applying Data Deduplication to these shares might save you up to 30 to 50 percent of your system's storage space.
- Software deployment shares. This includes software binaries, cab files, symbols files, images, and updates. Applying Data Deduplication to these shares might be able to save you up to 70 to 80 percent of your system's storage space.
- Virtualization libraries. This includes virtual hard disk files (i.e., .vhd and .vhdx files) storage for provisioning to hypervisors. Applying Data Deduplication to these libraries might be able to save you up to 80 to 95 percent of your system's storage space.
- General file share. This includes a mix of all the types of data identified above. Applying Data Deduplication to these shares might save you up to 50 to 60 percent of your system's storage space.

Data Deduplication deployment candidates

Based on observed savings and typical resource usage in Windows Server 2016, deployment candidates for deduplication are ranked as follows:

- **Ideal candidates for deduplication**
  - Folder redirection servers
  - Virtualization depot or provisioning library
  - Software deployment shares
  - SQL Server and Exchange Server backup volumes
  - Scale-out File Servers (SoFS) CSVs
  - Virtualized backup VHDs (e.g., DPM)
  - VDI VHDs (only personal VDIs)

Note: In most VDI deployments, special planning is required for the boot storm, which is the name given to the phenomenon of large numbers of users trying to simultaneously log in to their VDI, typically upon arriving to work in the morning. In turn, this hammers the VDI storage system and can cause long delays for VDI users. However, in Windows Server 2016, when chunks are read from the on-disk deduplication store during startup of a virtual machine, they are cached in memory. As a result, subsequent reads don't require frequent access to the chunk store because they are intercepted by the cache; the effects of the boot storm are minimized because the memory is much faster than disk.

- **Should be evaluated based on content**
  - Line-of-business servers
  - Static content providers
  - Web servers
  - High-performance computing (HPC)
- **Not ideal candidates for deduplication**
  - Hyper-V hosts
  - WSUS
  - SQL Server and Exchange Server database volumes

Data Deduplication Interoperability

In Windows Server 2016, you should consider the following related technologies and potential issues when deploying Data Deduplication:

- BranchCache. Access to data over the network can be optimized by enabling BranchCache on Windows servers and clients. When a BranchCache-enabled system communicates over a WAN with a remote file server that is enabled for Data Deduplication, all of the deduplicated files are already indexed and hashed, so requests for data from a branch office are quickly computed. This is similar to preindexing or prehashing a BranchCache-enabled server.

  Note: BranchCache is a feature which can reduce wide area network (WAN) utilization and enhance network application responsiveness when users access content in a central office from branch office locations. When you enable BranchCache, a copy of the content that is retrieved from the web server or file server is cached within the branch office. If another client in the branch requests the same content, the client can download it directly from the local branch network without needing to retrieve the content by using the WAN.

- Failover Clusters. Failover clusters are fully supported in Windows Server 2016, which means deduplicated volumes will failover gracefully between nodes in the cluster. Effectively, a deduplicated volume is a self-contained and portable unit (i.e., all of the data and configuration information is contained on the volume) but requires that each node in the cluster that accesses deduplicated volumes must be running the Data Deduplication feature. When a cluster is formed, the Deduplication schedule information is configured in the cluster. As a result, if a deduplicated volume is taken over by another node, the scheduled jobs will be applied on the next scheduled interval by the new node.
- FSRM quotas. Although you should not create a *hard* quota on a volume root folder enabled for deduplication, using File Server Resource Manager (FSRM), you can create a *soft* quota on a volume root which is enabled for deduplication. When FSRM encounters a deduplicated file, it will identify the file's logical size for quota calculations. Consequently, quota usage (including any quota thresholds) does not change when a file is processed by deduplication. All other FSRM quota functionality, including volume-root soft quotas and quotas on subfolders, will work as expected when using deduplication.

  Note: File Server Resource Manager (FSRM) is a suite of tools for Windows Server 2016 that allows you to identify, control, and manage the quantity and type of data stored on your servers. FSRM enables you to configure hard or soft quotas on folders and volumes. A

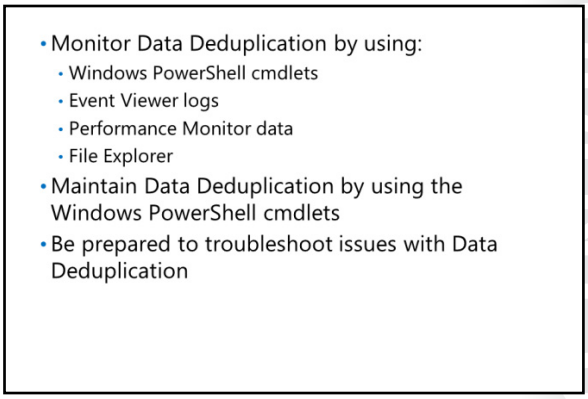
hard quota prevents users from saving files after the quota limit is reached; whereas, a soft quota does not enforce the quota limit, but generates a notification when the data on the volume reaches a threshold. When a hard quota is enabled on a volume root folder enabled for deduplication, the actual free space on the volume and the quota restricted space on the volume are not the same; this might cause deduplication optimization jobs to fail.

- DFS Replication. Data Deduplication is compatible with Distributed File System (DFS) Replication. Optimizing or unoptimizing a file will not trigger a replication because the file does not change. DFS Replication uses Remote Differential Compression (RDC), not the chunks in the chunk store, for over-the-wire savings. In fact, you can optimize the files on the replica instance by using deduplication if the replica is enabled for Data Deduplication.

Note: Single Instance Storage (SIS), a file system filter driver used for NTFS file deduplication, was deprecated in Windows Server 2012 R2 and completely removed in Windows Server 2016.

Monitoring and maintaining Data Deduplication

After you deploy Data Deduplication in your environment, it is important that you monitor and maintain the systems that are enabled for Data Deduplication and the corresponding data storage to ensure optimal performance. While Data Deduplication in Windows Server 2016 includes a lot of automation, including optimization jobs, the deduplication process requires that you verify the efficiency of optimization; make the appropriate adjustments to systems, storage architecture, and volumes; and troubleshoot any issues with Data Deduplication.



Monitoring and reporting of Data Deduplication

When planning for Data Deduplication in your environment, you will inevitably ask yourself, "What size should my configured deduplicated volumes be?" Although Windows Server 2016 supports Data Deduplication on volumes up to 64 TB, you must assess the appropriate size of the deduplicated volumes that your environment can support. For many, the answer to this question is that it depends on your hardware specifications and your unique workload. More specifically, it depends primarily on how much and how frequently the data on the volume changes and on the data access throughput rates of the disk storage subsystem.

Monitoring the efficiency of Data Deduplication in your environment is instrumental in every phase of your deployment, especially during your planning phase. As detailed earlier in the module, Data Deduplication in Windows Server 2016 performs intensive I/O and compute operations. In most deployments, deduplication operates in the background or on a daily schedule on each day's new or modified data (i.e., data churn); as long as deduplication is able to optimize all of the data churn on a daily basis, the volume size will work for deduplication. On the other hand, some organizations simply create a 64 TB volume, enable deduplication, and then wonder why they experience low optimization rates. Most likely in this scenario, deduplication is not able to keep up with the incoming churn from a dataset that is too large on a configured volume. Although Data Deduplication in Windows Server 2016

runs multiple threads in parallel using multiple I/O queues on multiple volumes simultaneously, the deduplication environment might require additional computing power.

You should consider the following when estimating the size of your volumes enabled for Data Deduplication:

- Deduplication optimization must be able to keep up with the daily data churn.
- The total amount of churn scales with the size of the volume.
- The speed of deduplication optimization significantly depends on the data access throughput rates of the disk storage subsystem.

Therefore, to estimate the maximum size for a deduplicated volume, you should be familiar with the size of the data churn and the speed of optimization processing on your volumes. You can choose to use reference data, such as server hardware specifications, storage drive/array speed, and deduplication speed of various usage types, for your estimations. However, the most accurate method of assessing the appropriate volume size is to perform the measurements directly on your deduplication system based on the representative samples of your data, such as data churn and deduplication processing speed.

You should consider using the following options to monitor deduplication in your environment and to report on its health:

- Windows PowerShell cmdlets. After you enable the Data Deduplication feature on a server, you can use the following Windows PowerShell cmdlets:
    - **Get-DedupStatus**. The most commonly used cmdlet, this cmdlet returns the deduplication status for volumes which have data deduplication metadata, which includes the deduplication rate, the number/sizes of optimized files, the last run-time of the deduplication jobs, and the amount of space saved on the volume.
    - **Get-DedupVolume**. This cmdlet returns the deduplication status for volumes that have data deduplication metadata. The metadata includes the deduplication rate, the number/sizes of optimized files, and deduplication settings such as minimum file age, minimum file size, excluded files/folders, compression-excluded file types, and the chunk redundancy threshold.
    - **Get-DedupMetadata**. This cmdlet returns status information of the deduplicated data store for volumes that have data deduplication metadata, which includes the number of data chunks in a container, the number of containers in the data store, the number of data streams in a container, number of containers in the stream map store, the number of hotspots in a container, the number of hotspots in the stream map store, and the number of corruptions on the volume.
    - **Get-DedupJob**. This cmdlet returns the deduplication status and information for currently running or queued deduplication jobs.

    One common scenario is to assess whether deduplication is keeping pace with the rate of incoming data. You can use the **Get-DedupStatus** cmdlet to monitor the number of optimized files compared with the number of in-policy files. This enables you to see if all the in-policy files are processed. If the number of in-policy files is continuously rising faster than the number of optimized files, you should examine your hardware specifications for appropriate utilization or the type of data on the volume usage type to ensure deduplication efficiency. However, if the output value from the cmdlet for **LastOptimizationResult** is 0x00000000, the entire dataset was processed successfully during the previous optimization job.

 **Note:** For more information about all the storage cmdlets in Windows Server 2016, refer to: http://aka.ms/po9qve

- Event Viewer logs. Monitoring the event log can also be helpful to understand deduplication events and status. To view deduplication events, in Event Viewer, navigate to **Applications and Services Logs**, click **Microsoft**, click **Windows**, and then click **Deduplication**. For example, Event ID 6153 will provide you with the elapsed time of a deduplication job and the throughput rate.
- Performance Monitor data. In addition to using the counters for monitoring server performance, such as CPU and memory, you can use the typical disk counters to monitor the throughput rates of the jobs that are currently running, such as: Disk Read Bytes/sec, Disk Write Bytes/sec, and Average Disk sec/Transfer. Depending on other activities on the server, you might be able to use the data results from these counters to get a rough estimate of the saving ratio by examining how much data is being read and how much is being written per interval. You can also use the Resource Monitor to identify the resource usage of specific programs/services. To view disk activity, in Windows Resource Monitor, filter the list of processes to locate **fsdmhost.exe** and examine the I/O on the files under the **Disk** tab.

   **Note:** Fsdmhost.exe is the executable file for the Microsoft File Server Data Management Host process, which is used by the Data Deduplication process in Windows Server 2016.

- File Explorer. While not the ideal choice for validating deduplication on an entire volume, you can use File Explorer to spot check deduplication on individual files. In viewing the properties of a file, you notice that **Size** displays the logical size of the file, and **Size on Disk** displays the true physical allocation of the file. For an optimized file, **Size on Disk** is less than the actual file size. This is because deduplication moves the contents of the file to a common chunk store and replaces the original file with an NTFS reparse point stub and metadata.

Maintaining Data Deduplication

With the data that is collected by monitoring, you can use the following Windows PowerShell cmdlets to ensure optimal efficiency of deduplication in your environment.

- **Update-DedupStatus**. Some of the storage cmdlets, such as **Get-DedupStatus** and **Get-DedupVolume**, retrieve information from the cached metadata. This cmdlet scans volumes to compute new Data Deduplication information for updating the metadata.
- **Start-DedupJob**. This cmdlet is used to launch ad hoc deduplication jobs, such as optimization, garbage collection, scrubbing, and unoptimization. For example, you might consider launching an ad hoc optimization job if a deduplicated volume is low on available space because of extra churn.
- **Measure-DedupFileMetadata**. This cmdlet is used to measure potential disk space on a volume. More specifically, this cmdlet returns how much disk space you can reclaim on a volume if you delete a group of folders and subsequently run a garbage collection job. Files often have chunks that are shared across other folders. The deduplication engine calculates which chunks are unique and would be deleted after the garbage collection job.
- **Expand-DedupFile**. This cmdlet expands an optimized file into its original location. You might need to expand optimized files because of compatibility with applications or other requirements. Ensure there is enough space on the volume to store the expanded file.

Troubleshooting adverse effects of Data Deduplication

When an application or access to a file is adversely impacted by Data Deduplication in Windows Server 2016, several options are available including:

- Use a different deduplication frequency by changing the schedule or opting for manual deduplication jobs.
- Use job options such as:
  - **StopWhenSystemBusy**, which halts deduplication if the job interferes with the server's workload.
  - **Preempt**, which causes the deduplication engine to move specific deduplication jobs to the top of the job queue and cancel the current job.
  - **ThrottleLimit**, which sets the maximum number of concurrent operations which can be established by specific deduplication jobs.
  - **Priority**, which sets the CPU and I/O priority for specific deduplication jobs.
  - **Memory**, which specifies the maximum percentage of physical computer memory that the data deduplication job can use.

 **Note:** While allowing deduplication to manage memory allocation automatically is recommended, you might need to adjust the maximum percentage in some scenarios. For most of these scenarios, you should consider a maximum percentage within a range of 15 to 50, and a higher memory consumption for jobs that you schedule to run when you specify the *StopWhenSystemBusy* parameter. For garbage collection and scrubbing deduplication jobs, which you typically schedule to run after business hours, you can consider using a higher memory consumption, such as 50.

- Use the **Expand-DedupFile** cmdlet to expand, or undeduplicate, specific files if needed for compatibility or performance.
- Use the **Start-DedupJob** cmdlet with the **Unoptimization** job type to disable deduplication on a volume.

Troubleshooting Data Deduplication corruptions

Data Deduplication in Windows Server 2016 provides functionality to detect, report, and even repair data corruptions. In fact, data integrity is considered highly important by deduplication, because a large number of deduplicated files might be referencing a single popular chunk, which gets corrupted. While there are a number of features built into deduplication to help protect against corruption, there are still some scenarios where deduplication might not recover automatically from corruption.

 **Additional Reading:** For more information, refer to: "Troubleshooting Data Deduplication Corruptions" at: http://aka.ms/Tdz13m

Some of the most common causes for deduplication to report corruption are:

- Incompatible Robocopy options used when copying data. Using Robocopy with the /MIR option on the volume root as the target wipes the deduplication store. To avoid this problem, use the /XD option to exclude the **System Volume Information** folder from the scope of the Robocopy command.

Note: For more information, refer to: "FSRM and Data Deduplication may be adversely affected when you use Robocopy /MIR in Windows Server 2012" at: http://aka.ms/W0ux7m

- Incompatible Backup/Restore program used on a deduplicated volume. You should verify whether your backup solution supports Data Deduplication in Windows Server 2016, as unsupported backup solutions might introduce corruptions after a restore. More information about this is covered later in this module.
- Migrating a deduplicated volume to a down-level Windows Server version. File corruption messages might be reported on files accessed from a deduplicated volume, which is mounted on an older version of Windows Server, but were optimized on a later version of the operating system. In this scenario, you should verify the version of the server accessing the deduplicated data is the same version level or higher than the version of the server that optimized the data on the volume. Although deduplicated volumes can be remounted on different servers, deduplication is backward compatible but not forward compatible; you can upgrade and migrate to a newer version of Windows Server, but data deduplicated by a newer version of Windows Server cannot be read on older versions of Windows Server and might report the data as corrupted when trying to read.
- Enabling compression on the root of a volume also enabled with deduplication. Deduplication is not supported on volumes that have compression enabled at the root. As a result, this might lead to the corruption and inaccessibility of deduplicated files.

Note: Deduplication of files in compressed folders is supported in Windows Server 2016 and should function normally.

- *Hardware issues*. Many hardware storage issues are detectable early by using the deduplication scrubbing job. Refer to the general corruption troubleshooting steps below for more information.
- *General corruption*. You can use the steps below to troubleshoot most general causes for deduplication to report corruption:

  1. *Check the Event Logs for details of corruption*. Check the deduplication Scrubbing Event logs for cases of early file corruption and attempted corruption fixes by the scrubbing job. Any corruption detected by deduplication is logged to the event log. The Scrubbing channel lists any corruptions that were detected and files that were attempted to be fixed by the job. The deduplication Scrubbing Event logs are located in the Event Viewer (under Application and Services > Microsoft > Windows > Deduplication > Scrubbing). In addition, searching for hardware events in the System Event logs and Storage Spaces Event logs will often yield additional information about hardware issues.

     Note: The potentially large number of events in the deduplication Scrubbing Event log might be difficult to parse through the Event Viewer. A publicly available script that generates an easy-to-read HTML which highlights detected corruptions and the results of any attempted corruption fixes from the Scrubbing job. For more information on **Get-DedupScrubbingReport**, refer to: "Microsoft TechNet Script Center" at: http://aka.ms/N75avw

2. Run **CHKDSK** in the read-only mode. While this command can repair some data corruption on volumes, running the command without any parameters will initiate a read-only scan.

   Note: For more information on CHKDSK in Windows Server 2016, refer to: http://aka.ms/Nep9wf

3. Run deep Scrubbing job to repair detected corruptions. A must for corruption investigations, a deep Scrubbing job should be used to ensure that all corruptions are logged in the deduplication scrubbing channel in the Event Logs. The scrubbing events will provide a breakdown of the corruptions, including corrupted chunks, affected files, the exact container offsets of the corruption, and the list of affected files (up to 10 K files).

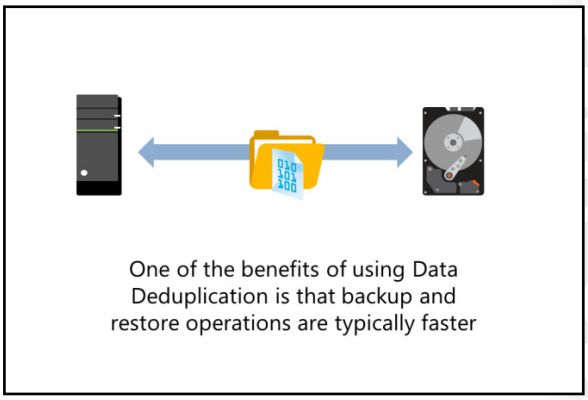
   You can use the following command in Windows PowerShell to initiate a deep Scrubbing job:

```
Start-DedupJob VolumeLetter -Type Scrubbing –Full
```

Note: Replace *VolumeLetter* with the drive letter of the volume.

Backup and restore considerations with Data Deduplication

One of the benefits of using Data Deduplication is that backup and restore operations are faster. This is because you have reduced the space used on a volume, meaning there is less data to back up. When you perform an optimized backup, your backup is also smaller. This is because the total size of the optimized files, non-optimized files, and data deduplication chunk store files are much smaller than the logical size of the volume.



Note: Many block-based backup systems should work with data deduplication, maintaining the optimization on the backup media. File-based backup operations that do not use deduplication usually copy the files in their original format.

The following backup and restore scenarios are supported with deduplication in Windows Server 2016:

- Individual file backup/restore
- Full volume backup/restore
- Optimized file-level backup/restore using VSS writer

On the other hand, the following backup and restore scenarios are not supported with deduplication in Windows Server 2016:

- Backup or restore of only the reparse points.
- Backup or restore of only the chunk store.

In addition, a backup application can perform an incremental optimized backup as follows:

- Back up only the changed files created, modified, or deleted since your last backup.
- Back up the changed chunk store container files.
- Perform an incremental backup at the sub-file level.

Note: New chunks are appended to the current chunk store container. When its size reaches approximately 1 GB, that container file is sealed and a new container file is created.

Restore Operations

Restore operations also can benefit from data deduplication. Any file-level, full-volume restore operations can benefit because they are essentially a reverse of the backup procedure, and less data means quicker operations. The method of a full volume restore is:

1. The complete set of data deduplication metadata and container files are restored.
2. The complete set of data deduplication reparse points are restored.
3. All non-deduplicated files are restored.

Block-level restore from an optimized backup is automatically an optimized restore because the restore process occurs under data deduplication, which works at the file level.

As with any product from a third-party vendor, you should verify whether the backup solution supports Data Deduplication in Windows Server 2016, as unsupported backup solutions might introduce corruptions after a restore. Here are the common methods on solutions which support Data Deduplication in Windows Server 2016:

- Some backup vendors support *unoptimized backup*, which rehydrates the deduplicated files upon backup; i.e., backs up the files as normal, full-size files.
- Some backup vendors support *optimized backup* for a full volume backup, which backs up the deduplicated files as-is; i.e., as a reparse point stub with the chunk store.
- Some backup vendors support both

The backup vendor should be able to comment on what their product supports, the method it uses and with which version.

Note: For more information, refer to: "Backup and Restore of Data Deduplication-Enabled Volumes" at: http://aka.ms/w8iows

Question: Can you enable Data Deduplication on a drive with storage tiering enabled?

Question: Can you enable Data Deduplication on ReFS formatted drives?

Question: Can you enable Date Deduplication on volumes in which virtual machines are running and apply it to those virtual machines?

Lab B: Implementing Data Deduplication

Scenario

After you have tested the storage redundancy and performance options, you decide that it also would be beneficial to maximize the available disk space that you have, especially on generic file servers. You decide to test Data Deduplication solutions to maximize storage availability for users.

New: After you have tested the storage redundancy and performance options, you now decide that it would also be beneficial to maximize the available disk space that you have, especially around virtual machine storage which is in ever increasing demand. You decide to test out Data Deduplication solutions to maximize storage availability for virtual machines.

Objectives

After completing this lab, you will be able to:

- Install the Data Deduplication role service.
- Enable Data Deduplication.
- Check the status of Data Deduplication.

Lab Setup

Estimated Time: **40 minutes**

Virtual machines**: 20740A-LON-DC1** and **20740A-LON-SVR1**

User name**: Adatum\Administrator**

Password**: Pa$$w0rd**

For this lab, you must use the available virtual machine environment. These should already be running from Lab A. If they are not, before you begin the lab, you must complete the following steps and then complete Lab A:

1. On the host computer, start **Hyper-V Manager**.
2. In **Hyper-V Manager**, click **20740A-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: **Administrator**
    - Password: **Pa$$w0rd**
    - Domain: **Adatum**
5. Repeat steps 2 through 4 for **20740A-LON-SVR1**.

Exercise 1: Installing Data Deduplication

Scenario

You decide to install the Data Deduplication role service on intensively used file servers by using Server Manager.

The main tasks for this exercise are as follows:

1. Install the Data Deduplication role service.
2. Check the status of Data Deduplication.
3. Verify the virtual machine performance.

▶ Task 1: Install the Data Deduplication role service

- On **LON-SVR1**, in **Server Manager**, add the **Data Deduplication** role service.

▶ Task 2: Check the status of Data Deduplication

1. Switch to **Windows PowerShell**.
2. To verify Data Deduplication status, run the following commands:

```
Get-DedupVolume
Get-DedupStatus
```

3. These commands return no results. This is because you need to enable it on the volume after installing it.

▶ Task 3: Verify the virtual machine performance

- On **LON-SRV1**, in **Windows PowerShell**, run the following command:

```
Measure-Command -Expression {Get-ChildItem –Path E:\ -Recurse}
```

Note: You will use the values returned from the previous command later in the lab.

Results: After completing this exercise, you should have successfully installed the Data Deduplication role service and enabled it on one of your file servers.

Exercise 2: Configuring Data Deduplication

Scenario

You determine that drive E is heavily used and you suspect it contains duplicate files in some folders. You decide to enable and configure the Data Deduplication role to reduce the consumed space on this volume.

The main tasks for this exercise are as follows:

1. Configure Data Deduplication.
2. Configure optimization to run now and view the status.
3. Verify if the file has been optimized.

4. Verify VM performance again.
5. Prepare for the next module.

▶ Task 1: Configure Data Deduplication

1. In **Server Manager**, click **File and Storage Services**.
2. Click **Disks**.
3. Click disk **1**, and then click the **E** volume.
4. Enable **Data Deduplication** for **General purpose file server** setting.
5. Configure the following settings:
   - Deduplicate files older than (in days): **0**
   - Enable **throughput optimization**.
   - Exclude: **E:\shares**

▶ Task 2: Configure optimization to run now and view the status

- On **LON-SRV1**, in **Windows PowerShell**, run the following commands:

```
Start-DedupJob E: -Type Optimization –Memory 50
Get-DedupJob –Volume E:
```

Note: Verify the status of the optimization job from the previous command. Repeat the previous command until the Progress shows as 100%.

▶ Task 3: Verify if the file has been optimized

1. On **LON-SVR1**, in **File Explorer**, navigate to the files in **E:\Labfiles\Mod04** and observe the following values from a few files properties: **Size** and **Size on disk**.
2. In **Windows PowerShell**, to verify Data Deduplication status, run the following commands:

```
Get-DedupStatus –Volume E: | fl
Get-DedupVolume –Volume E: |fl
```

Note: Observe the number of optimized files.

3. In **Server Manager**, click **File and Storage Services**, select **Disk 1**, and then select Volume **E**.
4. Refresh the display, and observe the values for **Deduplication Rate** and **Deduplication Savings**.

Note: Because most of the files on drive E are small, you might not notice a significant amount of saved space.

▶ Task 4: Verify VM performance again

- In **Windows PowerShell**, run the following command:

```
Measure-Command -Expression {Get-ChildItem –Path E:\ -Recurse}
```

Note: Compare the values returned from the previous command with the value of the same command earlier in the lab to assess if system performance has changed.

Results: After completing this exercise, you should have successfully configured Data Deduplication for the appropriate data volume on **LON-SVR1**.

▶ Task 5: Prepare for the next module

When you complete the lab, revert the virtual machines to their initial state.

1. On the host computer, start **Hyper-V Manager**.
2. In the **Virtual Machines** list, right-click **20740A-LON-SVR1**, and then click **Revert**.
3. In the **Revert Virtual Machine** dialog box, click **Revert**.
4. Repeat steps 2 and 3 for **20740A-LON-DC1**.

Question: Your manager is worried about the impact that using data deduplication will have on the write performance of your file servers' volumes. Is this concern valid?

Module Review and Takeaways

Review Questions

Question: You attach five 2-TB disks to your Windows Server 2012 computer. You want to simplify the process of managing the disks. In addition, you want to ensure that if one disk fails, the failed disk's data is not lost. What feature can you implement to accomplish these goals?

Question: Your manager has asked you to consider the use of Data Deduplication within your storage architecture. In what scenarios is the Data Deduplication role service particularly useful?

Common Issues and Troubleshooting Tips

Common Issue	Troubleshooting Tip
Some files cannot be read when the free disk space on a deduplicated volume approaches zero.	

Module 5

Installing and configuring Hyper-V and virtual machines

Contents:

Module Overview

Virtualization is a core technology used by large and small organizations for deploying servers. Server administrators need to understand how virtualization can be implemented and where it is appropriate to use.

The Hyper-V server role is how you can implement virtualization by using Windows Server 2016. This module describes how to implement Hyper-V and configure virtual machines.

Objectives

After completing this module, you will be able to:

- Describe Hyper-V and virtualization.
- Install Hyper-V.
- Configure storage on Hyper-V host servers.
- Configure networking on Hyper-V host servers.
- Configure Hyper-V virtual machines.
- Manage Hyper-V virtual machines.

Lesson 1
Overview of Hyper-V

Hyper-V was first introduced in Windows Server 2008. With each subsequent release of Windows Server, Hyper-V has been enhanced with new features. In this module, you will learn how Hyper-V can be used to implement virtualization, including some scenarios where it can be particularly useful. You will also learn about the new features for Hyper-V in Windows Server 2016. Finally, you will learn about Windows Server containers, a new virtualization technology.

Lesson Objectives

After completing this lesson, you will be able to:

- Describe Hyper-V.
- Identify when to use virtualization.
- Describe new Hyper-V features for hosts.
- Describe new Hyper-V features for virtual machines.
- Understand Windows Server Containers and Docker.

What is Hyper-V?

Hyper-V is the hardware virtualization role that is available in Windows Server 2016. Hardware virtualization allows the hardware capacity of a single physical computer to be subdivided and allocated to multiple virtual machines. Each virtual machine has an operating system that runs independently of the Hyper-V host and other virtual machines.

- Hyper-V is the hardware virtualization role in Windows Server 2016
- The hypervisor controls access to hardware
- Hardware drivers are installed in the host operating system
- Many guest operating systems are supported:
  - Windows Server 2008 SP2 or newer
  - Windows Vista SP2 or newer
  - Linux
  - FreeBSD

When you install Hyper-V, a software layer known as the hypervisor is inserted into the boot process. The hypervisor is responsible for controlling access to the physical hardware. Hardware drivers are installed only in the host operating system (also known as the parent partition). All of the virtual machines communicate only with virtualized hardware.

The operating systems running in virtual machines are referred to as guest operating systems. The following guest operating systems are supported for Hyper-V in Windows Server 2016:

- Windows Server 2008 with Service Pack 2 or later server operating systems.
- Windows Vista with Service Pack 2 or later client operating systems.
- Linux editions: CentOS, Red Hat Enterprise, Debian, Oracle, SUSE, and Ubuntu.
- FreeBSD.

Note: Some Hyper-V documentation refers to virtual machines as child partitions.

Additional Reading: For a current list of supported guest operating systems, refer to: Supported Windows guests" at: http://aka.ms/Geadun

New Hyper-V host features in Windows Server 2016

With each new release of Windows Server, Hyper-V is updated with new features and functionality. These new features and functionality provide you with options for supporting new workloads, increasing performance, and increasing security. The Hyper-V role in Windows Server 2016 has new and improved features as listed in the following table.

New features for Hyper-V hosts include:
- Host resource protection
- Hyper-V Manager improvements
- Nested virtualization
- Rolling Hyper-V cluster upgrades
- Shielded virtual machines
- Start order priority
- Storage QoS
- Windows PowerShell Direct

Feature	Description
Host resource protection	Prevents a virtual machine from monopolizing all of the resources on a Hyper-V host. This ensures that the Hyper-V host and other virtual machines have sufficient resources to function. This feature is not enabled by default.
Hyper-V Manager improvements	Improves manageability of Hyper-V hosts by allowing for alternate credentials when connecting to a Hyper-V host. Allows you to manage some previous versions of Hyper-V. Hyper-V Manager has been updated to use HTTP-based Web Services-Management (WS-MAN) for management instead of remote procedure calls (RPC) to simplify connectivity.
Nested virtualization	Allows you to enable the Hyper-V server role in a virtual machine running Windows Server 2016. This can be useful for test and education environments.
Rolling Hyper-V cluster upgrade	Allows you to upgrade a Windows Server 2012 R2 Hyper-V cluster to Windows Server 2016 by adding nodes to an existing cluster. Virtual machines can be moved between nodes running Windows Server 2013 R2 and Windows Server 2016 during co-existence.
Shielded virtual machines	Secures virtual machines from Hyper-V host administrators. The entire virtual machine is encrypted and is accessible only to the administrators of that virtual machine.
Start order priority	Improves Hyper-V host and virtual machine performance after restarts by identifying a specific startup order for virtual machines. This reduces resource contention and allows you to start the most important virtual machines first.
Storage Quality of Service (QoS)	Improves storage performance by allowing you to assign storage QoS policies on a Scale-Out File Server. Virtual hard disks stored on the Scale-Out File Server can be limited or can be guaranteed an amount of storage throughput.

Feature	Description
Windows PowerShell Direct	Allows you to run Windows PowerShell cmdlets on a virtual machine from the Hyper-V host. You do not need to configure any network connectivity to the virtual machine from the host.

New Hyper-V virtual machine features in Windows Server 2016

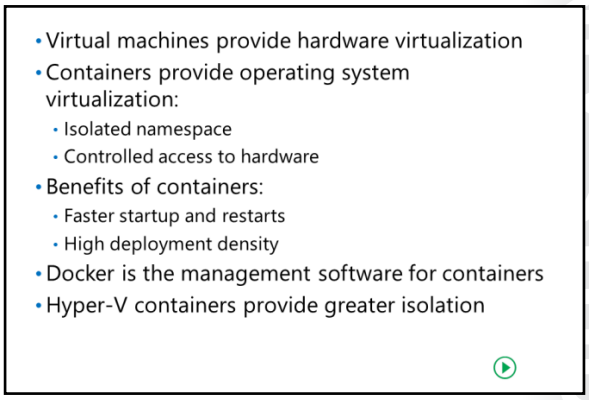
In addition to the improvements at the host level, Hyper-V has new features for virtual machines. New virtual machine-level features in Hyper-V for Windows Server 2016 are listed in the table below.

New features for virtual machines include:
- Discrete device assignment
- Hot add or remove for network adapters and memory
- Integration services delivered through Windows Update
- Linux Secure Boot
- Production checkpoints
- Virtual machine configuration file format
- Virtual machine configuration version

Feature	Description
Discrete device assignment	Allows virtual machines to directly access peripheral component interconnect express (PCIe) devices in the Hyper-V host. For some devices like a solid-state drive (SSD), this can provide increased performance.
Hot add or remove for network adapters and memory	Provides increased management flexibility to allocate resources as required to virtual machines. Network adapters and virtual memory can be added to a running virtual machine.
Integration services delivered through Windows Update	Simplifies management of virtual machines by delivering the most recent version of integration services through a standardized mechanism. Previously, integration services were distributed as an ISO image with Hyper-V and the software needed to be deployed to update it.
Linux Secure Boot	Increases security for Linux virtual machines. Secure Boot verifies digital signatures on files during the boot process to prevent malware. This feature was already available for Windows-based virtual machines.
Production checkpoints	Improves the functionality of checkpoints by ensuring that applications are in a consistent state when the checkpoint is created.
Virtual machine configuration file format	Increases efficiency of read and write operations to the virtual machine configuration file with a binary format instead of the previous XML format. This also prevents administrators from making manual changes to the configuration file.

Feature	Description
Virtual machine configuration version	Provides virtual machine compatibility with Windows Server 2012 R2. Any virtual machines migrated from Windows Server 2012 R2 (such as during a rolling cluster upgrade) are not automatically updated from configuration version 5 to 6 to retain backward compatibility. After you update a virtual machine to version 6, it can only be hosted on Windows Server 2016.

Windows Server Containers and Docker in Hyper-V



When you implement virtual machines, each virtual machine has its own operating system instance. The operating system in each virtual machine is completely independent. A problem in the operating system of one virtual machine does not cause errors in other virtual machines. This provides high levels of stability for the virtual machines. However, it also uses many resources because memory and processor resources are allocated to each individual operating system.

Windows Server containers are a new feature in Windows Server 2016 that allows you to run multiple applications independently within a single operating system instance. The kernel of the operating system is shared by multiple containers. This configuration is referred to as operating system virtualization. Just as a virtual machine presents hardware resources to an operating system, a container is presented with a virtual operating system kernel.

Each container gets its own namespace. The namespace includes a computer name, files, and network address. Access to hardware resources like memory and processor are throttled to ensure that one container does not monopolize resources on the host.

Containers have the following benefits over virtual machines:

- Faster startup and restarts because the operating system kernel is already started.
- Higher density on the same hardware because there is only one operating system instance.

Docker is the management software for containers. You can use Docker to retrieve containers from and store containers in a repository. In some cases, containers are layered together to provide an entire application. For example, there can be a container for the operating system, a container for the web server software, and then another container for the web-based app. In such a case, Docker can retrieve all containers required for the app from a repository and deploy them.

The storage for containers functions similarly to differencing drives in Hyper-V and you need to be aware of this if you update containers. If a lower layer container for an operating system is updated, it invalidates any upper layer containers that rely on it. Updating the lower layer forces you to also update the upper layers.

To provide greater stability for a container, there are also Hyper-V containers. Hyper-V containers use Hyper-V to provide a greater level of isolation for containers. Each Hyper-V container has its own operating system kernel and thus operates independently. In scenarios in which there are multiple tenants or untrusted groups, this isolation allows you to use containers for deployment but still have the isolation

benefits of virtual machines. For example, in a development environment, performance is more important than stability; therefore, Windows Server containers are used for app development. However, in production, where stability is critical, Hyper-V containers could be used. When development containers are judged to be stable, they can be moved into the production environment by using Hyper-V containers. No changes are required to the containers.

 **Additional Reading:** For more information about Windows Server containers, refer to: "Windows Containers" at: http://aka.ms/Kt23rj

Check Your Knowledge

Question	
Your organization has recently completed a security audit for the data center. One of the concerns raised by the auditors is the level of access that all of the server administrators have for the virtual machines. Which new Hyper-V feature in Windows Server 2016 can address this concern?	
Select the correct answer.	
	Shielded virtual machines
	Linux secure boot
	Discrete device assignment
	Nested virtualization
	Host resource protection

Question: A colleague has suggested that you should abandon virtual machines and begin using Windows Server containers instead. Explain why you should consider this carefully instead of implementing immediately.

Lesson 2
Installing Hyper-V

Before you can implement Hyper-V, you must ensure that your servers meet the prerequisites for installing Hyper-V; if they do not, you cannot install the Hyper-V server role. In some cases, you might want to implement nested virtualization where a virtual machine running on a Hyper-V host can also be configured as a Hyper-V host.

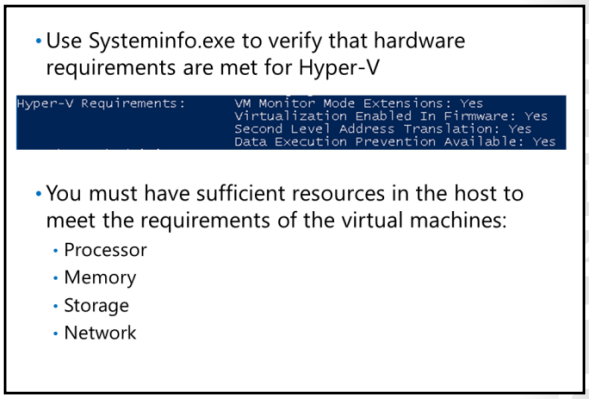
Lesson Objectives

After completing this lesson, you will be able to:

- Describe the prerequisites for installing Hyper-V.
- Install Hyper-V.
- Implement nested virtualization.

Prerequisites and requirements for installing Hyper-V

Deploying Hyper-V is a more complex process than simply installing the Hyper-V server role. To support virtual machines running production apps, you must carefully assess the capacity required for your virtual machines and plan your Hyper-V hosts accordingly. You also need to consider needs such as high availability. However, there are some basic hardware requirements for a Hyper-V host:



- A 64-bit processor with second-level address translation (SLAT).
- A processor with VM Monitor Mode extensions.
- A minimum of 4 gigabytes (GB) of memory.
- Intel Virtualization Technology (Intel VT) or AMD Virtualization (AMD-V) enabled.
- Hardware-enforced Data Execution Prevention (DEP) enabled (Intel XD bit, AMD NX bit).

The simplest way to verify that a system meets the requirements for Hyper-V is by running Systeminfo.exe. The output from this command has a Hyper-V section that identifies whether the requirements are met.

In addition to the hardware requirements for Hyper-V, you should ensure that the Hyper-V hosts have sufficient hardware resources for the virtual machines. The following is a list of necessary resources:

- Processor. Ensure that there are enough physical processor cores to support the virtual machines you plan to run.
- Memory. Ensure that there is enough memory in the Hyper-V host to support the number of virtual machines that you intend to run. The minimum 4 GB of memory is for the Hyper-V host operating system. You also must have memory for the virtual machines.

- Storage. Ensure that you have enough storage for the virtual hard disks used by your virtual machines. Also ensure that the storage subsystem has high throughput to support multiple virtual machines accessing the storage at the same time.
- Network. Ensure that there is enough network capacity in the Hyper-V host to allocate to the virtual machines. In some cases, you might need to allocate network adapters in the host for different purposes.

Demonstration: Installing the Hyper-V role

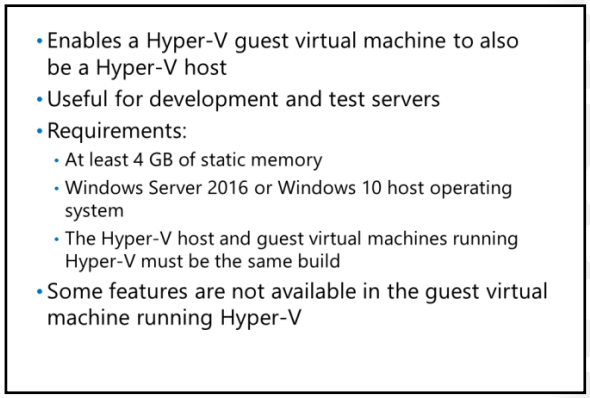
It is necessary to start a traditionally deployed server to run this demonstration or to configure a nested virtualization virtual machine host.

Demonstration Steps

1. On **LON-HOST1**, sign in as **Administrator** by using **Pa$$w0rd** as the password.
2. Use **Server Manager** to install the **Hyper-V** server role and all management tools.
3. After your computer restarts, sign in.
4. Wait for the **Hyper-V** installation to complete, and then start **Hyper-V Manager**.
5. In **Hyper-V Manager**, view the **Hyper-V Settings** for **LON-HOST1**.

Nested virtualization

Windows Server 2016 has introduced support for *nested virtualization*. Nested virtualization converts a Hyper-V guest virtual machine to a Hyper-V host so that it can host other guest virtual machines. This can be useful with development and test servers, in addition to some creative virtual-layered configurations in the future.



To enable nested virtualization, you need at least 4 GB of RAM and Windows Server 2016 or Windows 10 as the host operating system. Additionally, the virtual machine that is running Hyper-V must be the same build as the host.

Rather than providing detailed steps on how a virtual machine must be configured to support nested virtualization, Microsoft provides a script hosted on GitHub. This simplifies the deployment process for nested virtualization. The following command downloads the script and saves it in your user profile.

```
Invoke-WebRequest https://raw.githubusercontent.com/Microsoft/Virtualization-
Documentation/master/hyperv-tools/Nested/Enable-NestedVm.ps1 -OutFile ~/Enable-
NestedVm.ps1
```

When you run the script, you specify the name of the virtual machine to configure. It will confirm that several changes such as allowing media access control (MAC) address spoofing should be made. In the following command, "*DemoVM*" is the name of the virtual machine on which Hyper-V will be enabled.

```
~/Enable-NestedVm.ps1 -VmName "DemoVM"
```

After enabling nested virtualization, you can install Hyper-V on a virtual machine in the same way as you would a Hyper-V host. The following features are disabled or will fail after you enable nested virtualization:

- Virtual-based security.
- Device Guard.
- Dynamic Memory.
- Hot add Static Memory.
- Checkpoints.
- Live migration.
- Save or Restore state.

To allow the guest virtual machines to communicate on the external network, enable MAC spoofing. MAC spoofing must be configured on the virtual machine that is configured as a Hyper-V host. If you do not enable MAC spoofing, network packets from guest virtual machines are not recognized as legitimate and are blocked.

Question: Should nested virtualization be implemented by most organizations?

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

Statement	Answer
To install the Hyper-V server role in Windows Server 2016, your server hardware must support SLAT.	

Lesson 3
Configuring storage on Hyper-V host servers

Just as a physical computer has a hard disk for storage, virtual machines also require storage. When you create virtual hard disks for virtual machines, they can be in .vhd or the newer .vhdx format. There are also other types of virtual hard disks such as fixed-size and dynamically expanding. You need to know when it is appropriate to use the various formats and types of virtual hard disk. You also need to understand the various options for storing virtual hard disks so that you can select a storage option that meets your requirements for performance and high availability.

Lesson Objectives

After completing this lesson, you will be able to:

- Describe the storage options in Hyper-V.
- Identify considerations for selecting virtual hard disk formats and types.
- Describe Fibre Channel support in Hyper-V.
- Choose where to store virtual hard disks.
- Describe how virtual hard disks can be stored on Server Message Block (SMB) 3.0 shares.
- Manage storage in Hyper-V.

Storage options in Hyper-V

A virtual hard disk is a special file format that represents a traditional hard disk drive. Inside a virtual hard disk, you can configure partitions, files, and folders. Virtual machines use virtual hard disks for their storage.

- Virtual hard disk formats:
  - .vhd
  - .vhdx
  - .vhds
- Virtual hard disk types:
  - Fixed-size
  - Dynamically expanding
  - Pass-through
  - Differencing

You can create virtual hard disks by using:

- The Hyper-V Manager console.
- The Disk Management console.
- The Diskpart command-line tool.
- The New-VHD Windows PowerShell cmdlet.

Virtual hard disk formats

Windows Server 2008 and Windows Server 2008 R2 supported only the .vhd format for virtual hard disks. This format provided the necessary functionality for virtual machine storage but was limited to 2 terabytes (TB) in size and had limited performance.

Windows Server 2012 introduced the new .vhdx format for virtual hard disks. Compared to the .vhd format, the .vhdx format offers the following benefits:

- A .vhdx file can be as large as 64 TB.
- The .vhdx file structure minimizes the chance that a disk will become corrupted if the host server suffers an unexpected power outage.

- The .vhdx format supports better alignment when deployed to large-sector disks.
- A .vhdx allows larger block sizes for dynamically expanding and differencing disks, which provides better performance for these workloads.

Windows Server 2016 introduces the .vhds format, which is specific to shared virtual hard disks. This is a type of virtual hard disk that multiple virtual machines can access at the same time for high availability with clustering.

You can convert between virtual hard disk formats. When you do so, a new virtual hard disk is created and the contents of the existing virtual hard disk are copied into it, so ensure that you have sufficient disk space to perform the conversion.

Virtual hard disk types

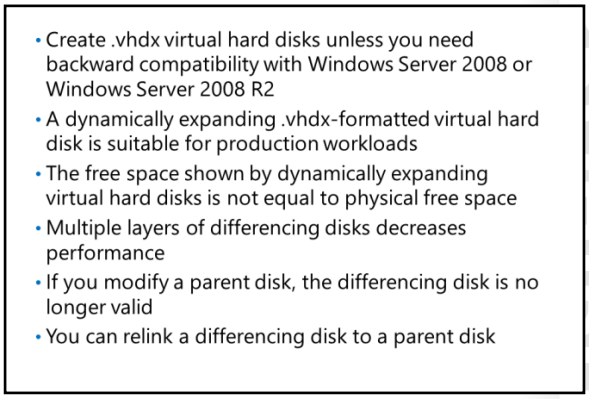
Windows Server 2016 supports multiple virtual hard disk types in addition to the different hard disk formats. Virtual hard disk types have varying benefits and drawbacks. The type of hard disk you select will vary depending on your needs. The virtual hard disk types are:

- Fixed-size. This type of virtual hard disk allocates all of the space immediately. This minimizes fragmentation, which, in turn, enhances performance.
- Dynamically expanding. This type of virtual hard disk allocates space as required, which is more efficient because there is no blank space in a virtual hard disk. If the virtual hard disk is .vhdx formatted and dynamically expanding, then it can also dynamically shrink when you remove data. Dynamic shrinking does not happen while the virtual machine is running, it occurs automatically when the virtual machine is shut down.
- Pass-through. This type of virtual hard disk provides direct access to a physical disk or Internet SCSI (iSCSI) logical unit number (LUN). In some cases, this offers better performance than storing data in a .vhd- or .vhdx-formatted virtual hard disk.
- Differencing. This type of dynamically expanding virtual hard disk stores data that has changed when compared to a parent disk. Differencing disks are typically used to reduce data storage requirements. For example, in a classroom, you could have 10 differencing disks based on the same parent disk that contains a sysprepped image of Windows Server 2016. The 10 differencing disks could then be used to create 10 different virtual machines.

Considerations for virtual hard disk formats and types

The following are some considerations for virtual hard disk types:

- Unless you are creating virtual hard disks that must be accessed on Windows Server 2008 or Windows Server 2008 R2, you should use .vhdx-formatted virtual hard disks.
- In the past, only fixed-size virtual hard disks were suitable for production, but for .vhdx-formatted virtual hard disks, dynamically expanding virtual hard disks offer almost the same level of performance and are supported for production workloads.

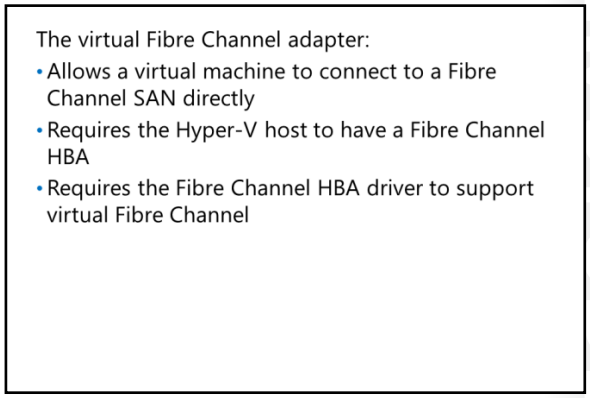


- Dynamically expanding virtual hard disks show the free space available based on the maximum size specified for the virtual hard disk rather than the actual physical space available. It is possible to physically run out of disk space on a Hyper-V host at the same time the dynamically expanding virtual hard disks show free space available.
- You can link multiple differencing disks, but, as the number of linked disks increases, performance tends to decrease.
- If you modify a parent virtual hard disk, a differencing disk is no longer valid.
- You can move a parent virtual hard disk, but you must relink it with the differencing disk.

Fibre Channel support in Hyper-V

Hyper-V virtual Fibre Channel is a virtual hardware component that you can add to a virtual machine; it enables a virtual machine to access Fibre Channel storage on storage area networks (SANs). To deploy a virtual Fibre Channel:

- You must configure the Hyper-V host with a Fibre Channel host bus adapter (HBA).
- The Fibre Channel HBA must have a driver that supports virtual Fibre Channel.
- The virtual machine must support virtual machine extensions.



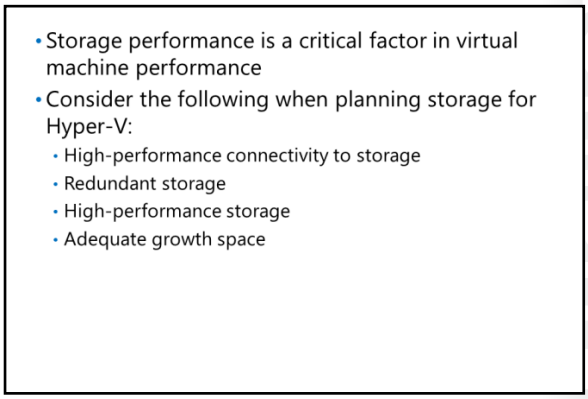
Virtual Fibre Channel adapters support port virtualization by exposing HBA ports in the guest operating system. This allows the virtual machine to access the SAN by using a standard World Wide Name that is associated with the virtual machine.

You can deploy up to four virtual Fibre Channel adapters on each virtual machine.

Note: For more information, refer to: "Hyper-V Virtual Fibre Channel Overview" at: http://aka.ms/gpv90h

Where to store VHDs?

A key factor when provisioning virtual machines is to ensure correct placement of virtual hard disks. Virtual hard disk performance can affect virtual machine performance dramatically. Servers that are otherwise well-provisioned with RAM and processor capacity can still experience poor performance if the storage system is overwhelmed. You can store virtual hard disks on local disks, a SAN, or SMB 3.0 file shares.

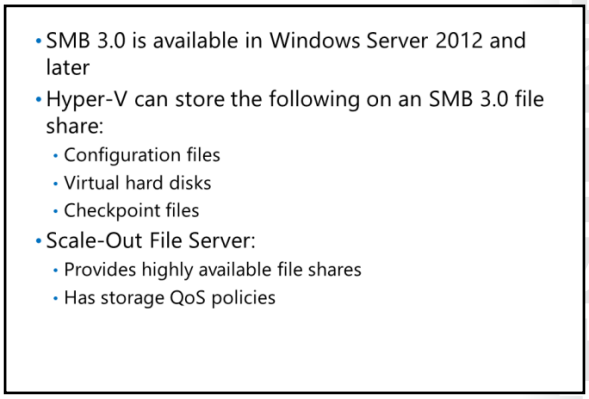


Consider the following factors when you plan the location of virtual hard disk files:

- High-performance connection to storage. You can locate virtual hard disk files on local or remote storage. When you locate them on remote storage, you need to ensure that there is adequate bandwidth and minimal latency between the host and the remote storage. Slow network connections to storage or connections where there is latency result in poor virtual machine performance.
- Redundant storage. The volume on which the virtual hard disk files are stored should be fault-tolerant, whether the virtual hard disk is stored on a local disk or on a remote SAN device. It is not uncommon for hard disks to fail. Therefore, the virtual machine and the Hyper-V host should remain in operation after a disk failure. Replacement of failed disks should not affect the operation of the Hyper-V host or virtual machines.
- High-performance storage. The storage device on which you store virtual hard disk files should have excellent I/O characteristics. Many enterprises use hybrid SSD drives in RAID 1+0 arrays to achieve maximum performance and redundancy. Multiple virtual machines that are running simultaneously on the same storage can place a tremendous I/O burden on a disk subsystem. Therefore, you must ensure that you choose high-performance storage. If you do not, virtual machine performance suffers.
- Adequate growth space. If you have configured virtual hard disks to grow automatically, ensure that there is adequate space into which the files can grow. In addition, carefully monitor growth so that you are not surprised when a virtual hard disk fills the volume that you allocated to host it.

Storing virtual machines on SMB 3.0 shares

Hyper-V supports storing virtual machine data such as virtual machine configuration files, checkpoints, and virtual hard disk files on SMB 3.0 file shares. The file share must support SMB 3.0. This limits placement of virtual hard disks to file shares that are hosted on Windows Server 2012 or later file servers. Older versions of Windows Server do not support SMB 3.0.



Note: We recommend that the bandwidth for network connectivity to the file share should be 1 gigabit per second (Gbps) or more.

SMB 3.0 file shares provide an alternative to storing virtual machine files on iSCSI or Fibre Channel SAN devices. When creating a virtual machine in Hyper-V on Windows Server 2012 or later, you can specify a network share when choosing the virtual machine location and the virtual hard disk location. You also can attach disks stored on SMB 3.0 file shares. You can use .vhd, .vhdx, and .vhds files with SMB 3.0 file shares.

When you use SMB 3.0 file shares for virtual machine storage, you are effectively creating a SAN using SMB 3.0. Like other SANs, you should segregate access to the file shares that store the virtual machine files. Client network traffic should not be on the same virtual LAN (VLAN).

To provide high availability for file shares storing virtual machine files, you can use Scale-Out File Server. Scale-Out File Server provides redundant servers for accessing a file share. This also provides faster performance than when you are accessing files through a single share, because all servers in the Scale-Out File Server are active at the same time. Windows Server 2016 now uses Storage QoS to manage QoS

policies for Hyper-V and Scale-Out File Servers. This allows deployment of QoS policies for SMB 3.0 storage.

Additional Reading: For more information, refer to: "Server Message Block Overview" at: http://aka.ms/obyww0

Demonstration: Managing storage in Hyper-V

In this demonstration, you will see how to create a differencing disk based on an existing disk by using both Hyper-V Manager and Windows PowerShell.

Demonstration Steps

1. Use **File Explorer** to create the following folders on the physical host drive:
   - **E:\Program Files\Microsoft Learning\20740\Drives\LON-GUEST1**
   - **E:\Program Files\Microsoft Learning\20740\Drives\LON-GUEST2**

Note: The drive letter for this path might vary depending on the configuration of the physical host.

2. Open a Windows PowerShell prompt and run the following command:

```
Set-VHD "E:\Program Files\Microsoft Learning\20740\Drives\20740A-BASE.vhd" -
ParentPath "E:\Program Files\Microsoft Learning\Base\Base16D-WS16-TP5.vhd"
```

3. In **Hyper-V Manager**, create a virtual hard disk with the following properties:
   - Disk Format: **VHD**
   - Disk Type: **Differencing**
   - Name: **LON-GUEST1.vhd**
   - Location: **E:\Program Files\Microsoft Learning\20740\Drives\LON-GUEST1**
   - Parent Location: **E:\Program Files\Microsoft Learning\20740\Drives\20740A-BASE.vhd**
4. In **Windows PowerShell**, run the following command:

```
New-VHD "E:\Program Files\Microsoft Learning\20740\Drives\LON-GUEST2\LON-GUEST2.vhd"
-ParentPath "E:\Program Files\Microsoft Learning\20740\Drives\20740A-BASE.vhd"
```

5. Inspect the **E:\Program Files\Microsoft Learning\20740\Drives\LON-GUEST2\LON-GUEST2.vhd** disk.
6. Verify that **LON-GUEST2.vhd** is configured as a differencing virtual hard disk with **E:\Program Files \Microsoft Learning\20740\Drives\20740A-BASE.vhd** as a parent.

Check Your Knowledge

Question	
When you create a virtual hard disk, which options are available? Select all that apply.	
Select the correct answer.	
	Pass-through
	Dynamic
	Differencing
	Fixed

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

Statement	Answer
To use a virtual Fibre Channel adapter in a virtual machine, the Hyper-V host must have a physical Fibre Channel adapter.	

Lesson 4
Configuring networking on Hyper-V host servers

Hyper-V supports a wide variety of network configurations. Each type of network is appropriate for specific types of scenarios. For example, an external network provides access to the physical network, but private networks are used to isolate hosts in a test environment. There are also new features for Hyper-V networking, such as switch-embedded teaming.

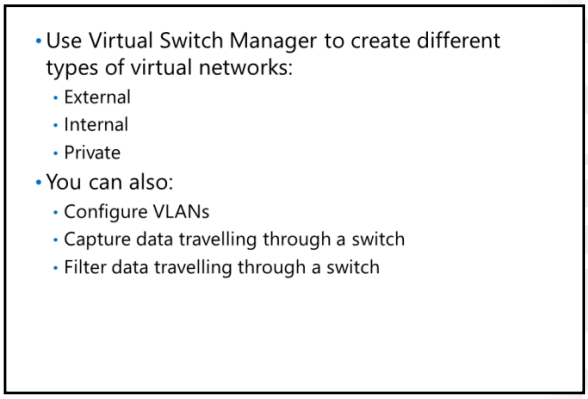
Lesson Objectives

After completing this lesson, you will be able to:

- Identify the types of Hyper-V networks.
- Configure Hyper-V networks.
- List best practices for configuring Hyper-V networks.
- Describe new features in Windows Server 2016 Hyper-V for networking.

Types of Hyper-V networks

Virtual switches are virtual devices that you can manage through the Virtual Switch Manager, which enables you to create three types of virtual switches. Virtual switches control how network traffic flows between virtual machines that are hosted on a Hyper-V server, in addition to how network traffic flows between virtual machines and the rest of the organizational network. There are some new features in Hyper-V networking.



Hyper-V on Windows Server 2012 and Windows Server 2016 supports three types of virtual switches, which the following table details.

Type	Description
External	You use this type of switch to map a network to a specific network adapter or network adapter team in the Hyper-V host. This provides virtual machines with access to a network that the host is connected to. Windows Server 2016 supports mapping an external network to a wireless network adapter if you have installed the Wireless LAN service on the host Hyper-V server and if the Hyper-V server has a compatible network adapter.
Internal	You use internal virtual switches to communicate between the virtual machines on a Hyper-V host and to communicate between the virtual machines and the Hyper-V host itself.
Private	You use private switches only to communicate between virtual machines on a Hyper-V host. You cannot use private switches to communicate between the virtual machines and the Hyper-V host.

When configuring an external or internal virtual network, you can also configure a virtual LAN (VLAN) ID for the management operating system to associate with the network. You can use this to extend existing VLANs on an external network to VLANs within the Hyper-V host's network switch. You can use VLANs to partition network traffic. VLANs function as separate logical networks. If traffic passes through a router, it can pass only from one VLAN to another.

You can configure the following extensions for each virtual switch type:

- Microsoft Network Driver Interface Specification (NDIS) Capture. This extension allows the capture of data that travels across a virtual switch.
- Microsoft Windows Filtering Platform. This extension allows filtering of data that travels across a virtual switch.

Demonstration: Configuring Hyper-V networks

In this demonstration, you will see how to create two types of virtual switches.

Demonstration Steps

1. In **Hyper-V Manager**, use the **Virtual Switch Manager** to create a new external virtual network switch with the following properties:
   - Name: **Corporate Network**
   - External Network: Mapped to the host computer's physical network adapter. Varies depending on the host computer.
2. In **Hyper-V Manager**, use the **Virtual Switch Manager** to create a new virtual switch with the following properties:
   - Name: **Private Network**
   - Connection type: **Private network**

Best Practices for configuring Hyper-V virtual networks

With respect to configuring virtual networks, best practices typically focus on ensuring that virtual machines are provisioned with adequate bandwidth. You do not want the performance of all virtual machines to be affected if a bandwidth-intensive operation, such as a large file copy or website traffic spike, occurs on one virtual machine on the same host.

When configuring virtual networks:
- Use NIC Teaming on the Hyper-V host to ensure connectivity to virtual machines if an adapter fails
- Enable bandwidth management to ensure that no single virtual machine is able to monopolize the network interface
- Use network adapters that support a VMQ
- Use network virtualization when you have to ensure that virtual machines keep their original IP addresses after migrating to a new host

The following general best practices apply while configuring virtual networks:

- Considerations for NIC Teaming. You should deploy multiple network adapters to a Hyper-V host and then configure those adapters as part of a team. This ensures that network connectivity will be retained if individual network adapters fail. Configure multiple teams with network adapters that are connected to different switches to ensure that connectivity remains if a hardware switch fails.

- Considerations for bandwidth management. You can use bandwidth management to allocate a minimum and a maximum bandwidth allocation on a per-virtual-network-adapter basis. You should configure bandwidth allocation to guarantee that each virtual machine has a minimum bandwidth allocation. This ensures that if another virtual machine that is hosted on the same Hyper-V server experiences a traffic spike, other virtual machines are able to communicate with the network normally.
- Considerations for virtual machine queue (VMQ). You should provision a Hyper-V host with an adapter that supports VMQ. VMQ uses hardware packet filtering to deliver network traffic directly to a virtual machine. This improves performance because the packet does not need to be copied from the host operating system to the virtual machine. When you do not configure virtual machines to support VMQ, the host operating system can become a bottleneck when it processes large amounts of network traffic.
- Considerations for network virtualization. Configuration of network virtualization is complicated, but it has an advantage over VLAN—it is not necessary to configure VLANs on all the switches that are connected to the Hyper-V host. You can perform all necessary configurations when you need to isolate servers on a Hyper-V host without needing to involve the network team. If you are hosting large numbers of virtual machines and need to isolate them, use network virtualization rather than VLANs.

New Hyper-V networking features in Windows Server 2016

Each new version of Windows Server includes enhancements for networking. In Windows Server 2012, software-defined networking was a major enhancement to networking for large scale deployments of Hyper-V. Windows Server 2016 provides additional improvements for software-defined networking and other features.

- QoS for software defined networking
- Virtual machine multi queues
- RDMA for virtual switches
- Switch embedded teaming:
  - Adapters must be identical
  - New-VMSwitch -Name "ExternalTeam" -NetAdapterName "NIC1","NIC2"
- NAT virtual switch:
  - New-VMSwitch -Name "NATSwitch" -SwitchType NAT -NATSubnetAddress 172.16.1.0/24

Quality of service

One of the new features for software-defined networking is QoS. There were QoS settings for Hyper-V networking previously, but they were not integrated into software-defined networking. QoS helps to ensure that all virtual machines are able to obtain a minimum level of network capacity when required.

Virtual machine multi queues

VMQ is a feature that enhances network performance for virtual machines. When it is enabled on the network card, VMQ passes network packets directly from the external network to virtual machines. Each virtual machine gets a queue for delivery of the packets. This feature was first available in Windows Server 2008 R2.

In Windows Server 2016, network performance has been enhanced by virtual machine multi queues (VMMQ). VMMQ improves on VMQ by allocating multiple queues per virtual machine and spreading traffic across the queues.

Remote direct memory access for virtual switches

Remote direct memory access (RDMA), also known as Server Message Block (SMB) Direct, is a feature that requires hardware support in the network adapter. A network adapter with RDMA functions at full speed with low resource utilization. Effectively, this means that there is higher throughput, which is important for busy servers with high-speed network adapters such as 10 Gbps.

In Windows Server 2012, RDMA could be used for network adapters in a Hyper-V host that accessed virtual hard disks over SMB. However, RDMA could not be used for adapters attached to a virtual switch, so virtual machines could not take advantage of RDMA for connectivity with clients. In Windows Server 2016, network performance for virtual machines is enhanced because RDMA can be used for network adapters that are attached to a Hyper-V switch.

Switch-embedded teaming

Windows Server 2012 introduced network teaming at the operating system layer. A network adapter team could be used to create a virtual switch in Hyper-V for high availability. One of the drawbacks of network teaming at the operating system level was that RDMA could not be used with a network adapter team.

In Windows Server 2016, switch-embedded teaming (SET) is a new way to implement network teaming for a virtual network that is compatible with RDMA. SET also works well with VMQ and other network features to provide high performance and high availability.

You can combine network adapters into a team by creating a virtual switch with up to 8 network adapters. All of the network adapters in a team must be identical with the same firmware version and driver. SET is automatically enabled when multiple network adapters are used. Unlike network adapter teaming, there is no name for the team.

To create a virtual switch with SET, use the following Windows PowerShell command:

```
New-VMSwitch -Name "ExternalTeam" -NetAdapterName "NIC1","NIC2"
```

 **Additional Reading:** For more information about RDMA and SET, refer to: "Remote Direct Memory Access (RDMA) and Switch Embedded Teaming (SET)" at: http://aka.ms/dzwmi9

NAT virtual switch

Network address translation (NAT) is often useful to control the use of IP addresses. This is particularly true if there are many virtual machines that require access to the Internet, but there is no requirement for communication to be initiated from the Internet back to the internal virtual machines. Windows Server 2016 includes a new NAT virtual switch type. This avoids the need to create a virtual machine that performs NAT.

To create NAT virtual switch, use the following Windows PowerShell command:

```
New-VMSwitch -Name "NATSwitch" -SwitchType NAT -NATSubnetAddress 172.16.1.0/24
```

Check Your Knowledge

Question	
You want to configure a network that allows multiple test systems using a private address space to access services on another network. What type of switch should you configure?	
Select the correct answer.	
	Internal
	Private
	External
	NAT

Check Your Knowledge

Question	
You are configuring a virtual switch that will be used for virtual machines that are accessed by clients. Which type of switch should you create?	
Select the correct answer.	
	Internal
	Private
	External
	NAT

Lesson 5
Configuring Hyper-V virtual machines

After the Hyper-V host has been installed and networks have been configured, you can begin to create virtual machines and configure them. When you move virtual machines from older Hyper-V hosts to Windows Server 2016, you must be aware of virtual machine configuration versions and how to update them. You also must be aware of the differences between Generation 1 and Generation 2 virtual machines. You should also understand new features in Hyper-V for Windows Server 2016, such as hot adding network adapters and memory. To enhance security for virtual machine data, you can implement shielded virtual machines.

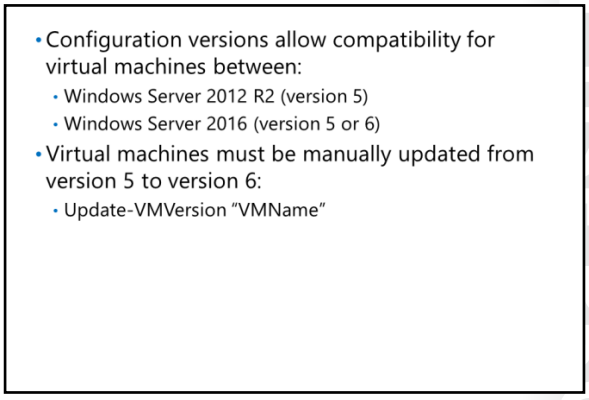
Lesson Objectives

After completing this lesson, you will be able to:

- Describe virtual machine configuration versions.
- Describe virtual machine generation versions.
- Create a virtual machine.
- Describe the hot adding feature.
- Identify the benefits of shielded virtual machines.
- List virtual machine settings.
- Identify best practices for configuring virtual machines.

What are virtual machine configuration versions?

Virtual machine configuration versions represent the Hyper-V compatibility settings for a virtual machine's configuration, saved states, and checkpoint files. In previous versions of Hyper-V, when you upgraded your host to a new operating system, the virtual machine would upgrade to the same configuration version as the host as soon as you moved the virtual machine.



With Windows Server 2016, a virtual machine's configuration version does not upgrade automatically. Instead, it is now a manual process. With rolling upgrades, it is highly likely that you might have a Hyper-V failover cluster that has both Windows Server 2012 R2 and Windows Server 2016. Windows Server 2012 R2 version 5.0 runs on both Windows Server 2012 R2 and Windows Server 2016 hosts. This allows administrators to leave virtual machines unchanged until the upgrade of all failover cluster nodes is completed.

After all hosts are upgraded or when you feel that you do not need to move your virtual machines to legacy hosts, you can shut down the virtual machine and upgrade the configuration version as needed.

Checking the virtual machine configuration version

To check a virtual machine's configuration version, run the following command in an elevated Windows PowerShell command prompt:

```
Get-VM * | Format-Table Name, Version
```

Updating a single virtual machine

To update the version of a single virtual machine, run the following command from an elevated Windows PowerShell command prompt:

```
Update-VMVersion "vmname"
```

Update all virtual machines on all cluster nodes

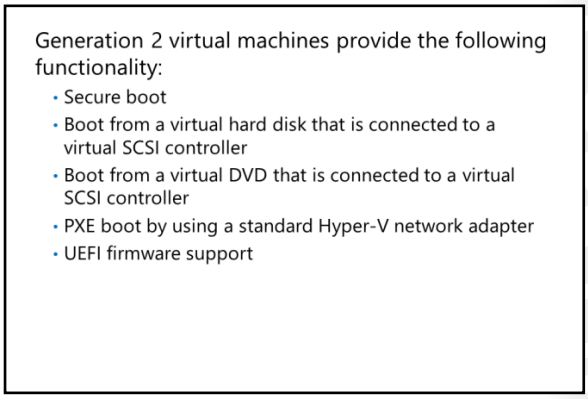
To update all virtual machines' versions on all cluster nodes, run the following command from an elevated Windows PowerShell command prompt:

```
Get-VM –ComputerName (Get-Clusternode) | Stop-VM
Get-VM –ComputerName (Get-Clusternode) | Update-Version –confirm $false
Get-VM –ComputerName (Get-Clusternode) | Start-VM
```

Note: New Hyper-V features in Windows Server 2016 are not available until the virtual machine configuration version has been upgraded to the Windows Server 2016 version. This includes hot add/remove of memory, production checkpoints, and live shared drive resizing.

Virtual machine generation versions

Windows Server 2012 R2 introduced a new type of virtual machine called a *Generation 2 virtual machine*. With this new name, all virtual machines that were created on platforms such as Windows Server 2012 and Windows Server 2008 R2 Hyper-V are termed *Generation 1 virtual machines*. Generation 2 virtual machines use a different hardware model and do not support many of the older devices that Generation 1 virtual machines supported, such as COM ports, the emulated floppy disk drive, and IDE controllers.



You select the generation of a virtual machine during virtual machine creation. After a virtual machine is created, you cannot migrate it from Generation 1 to Generation 2, or from Generation 2 to Generation 1.

With Windows Server 2016, it is a best practice to use Generation 2 virtual machines if the guest is a supported operating system.

Generation 2 virtual machines support the following functionality:

- Secure boot
- Boot from a virtual hard disk connected to a virtual SCSI controller
- Boot from a virtual DVD connected to a virtual SCSI controller

- PXE boot by using a standard Hyper-V (not legacy) network adapter
- Unified Extensible Firmware Interface (UEFI) firmware support

Because the guest operating systems must support booting from UEFI instead of BIOS, only the following guest operating systems are supported for Generation 2 virtual machines:

- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- x64 editions of Windows 10
- x64 editions of Windows 8.1
- x64 editions of Windows 8

Windows Server 2016 Hyper-V supports running Generation 1 and Generation 2 virtual machines concurrently.

Demonstration: Creating a virtual machine

In this demonstration, you will see how to create a virtual machine with the traditional method of using Hyper-V Manager. You also will see how you can automate the process by using Windows PowerShell.

Demonstration Steps

1. Use **Hyper-V Manager** to create a virtual machine with the following properties:
    - Name: **LON-GUEST1**
    - Location: **E:\Program Files\Microsoft Learning\20740\Drives\LON-GUEST1**
    - Generation: **Generation 1**
    - Memory: **1024 MB**
    - Use Dynamic Memory: **Yes**
    - Networking: **Private Network**
    - Connect Virtual Hard Disk: **E:\Program Files\Microsoft Learning\20740\Drives \LON-GUEST1\lon-guest1.vhd**
2. Open **Windows PowerShell**, import the **Hyper-V** module, and then run the following command:

```
New-VM –Name LON-GUEST2 –MemoryStartupBytes 1024MB –VHDPath “E:\Program
Files\Microsoft Learning\20740\Drives\LON-GUEST2\LON-GUEST2.vhd” –SwitchName “Private
Network”
```

3. Use the **Hyper-V Manager** console to edit the **LON-GUEST2** settings. Configure the following:
    - Automatic Start Action: **Nothing**
    - Automatic Stop Action: **Shut down the guest operating system**

The Hot Adding feature in Hyper-V

Many virtual machine settings cannot be modified while a virtual machine is running. Adding virtual hardware such as a processor is too disruptive to the virtual machine. For Generation 2 virtual machines, you can add memory and network adapters while a virtual machine is running.

- Hot adding requires Generation 2 virtual machines
- Memory:
  - Add memory to virtual machines with static memory while they are running
- Network adapter:
  - Add or remove network adapters to virtual machines while they are running

Hot add memory

Hot add memory provides flexibility for memory allocation to virtual machines that are not well suited to use dynamic memory. It provides the ability to change the memory allocated to a virtual machine while the virtual machine is running.

Dynamic memory allows you to configure Hyper-V so that a virtual machine is allocated as much memory as it needs. You can choose a minimum value, which will always be allocated to the virtual machine. You can choose a maximum value, which a virtual machine will not exceed even if more memory is requested. Virtual machines must support Hyper-V integration services through the deployment or inclusion of integration services components to be able to use dynamic memory.

Some workloads, such as Microsoft SQL Server or Exchange Server, are not well suited to dynamic memory because of how they use available memory for caching to optimize performance. In Windows Server 2016, you can modify the memory settings for servers that are configured with static memory while they are running.

Hot add network adapter

In previous versions of Hyper-V, you could change the virtual switch that a network adapter was connected to while the virtual machine was running. In Windows Server 2016, you can add or remove network adapters from a running virtual machine. This provides the flexibility to provide access to new networks without downtime.

Shielded virtual machines

In most Hyper-V deployments, the Hyper-V administrators have full access to all of the virtual machines. There might be application administrators that have access only to some virtual machines, but the administrators for the Hyper-V hosts have access to the entire system. This creates a risk where the contents of virtual machines could be accessed by an unauthorized Hyper-V administrator or someone who gains access to the Hyper-V host.

- A shielded virtual machine is:
  - Protected from anyone with access to the Hyper-V host
  - A Generation 2 virtual machine with a virtual TPM
  - Protected by BitLocker
- The Host Guardian Service has two attestation modes:
  - Admin-trusted attestation
  - TPM-trusted attestation

To enhance security for virtual machines, you can use shielded virtual machines. A shielded virtual machine must be a Generation 2 virtual machine and includes a virtual Trusted Platform Module (TPM). The virtual TPM is software-based and does not require a hardware TPM to be present in the server. You encrypt a shielded virtual machine by using BitLocker.

When you encrypt a virtual machine by using BitLocker, you protect the data inside it when the virtual machine is shut down. If someone copies a virtual hard disk and takes it offsite, it cannot be accessed. Hyper-V administrators can still perform maintenance on the Hyper-V hosts, but they no longer have access to the virtual machine data.

To implement shielded virtual machines, you implement a Guarded fabric, which requires a Host Guardian Service. The Host Guardian Service runs on a cluster of Windows Server and controls access to the keys that allow the shielded virtual machines to be started. A shielded virtual machine can be started only on authorized hosts.

There are two attestation modes that the Host Guardian Service can use to authorize hosts:

- Admin-trusted attestation. Computer accounts for trusted Hyper-V hosts are placed in an Active Directory Domain Services (AD DS) security group. This is simpler to configure but has a lower level of security.
- TPM-trusted attestation. Trusted Hyper-V hosts are approved based on their TPM identity. This provides a higher level of security but is more complex to configure. Hosts must have a TPM 2.0 and UEIF 2.3.1 with secure boot enabled.

Note: The attestation mode can be changed, which means that an initial deployment can use admin-trusted attestation, and TPM-trusted attestation can be introduced when all hosts have a TPM.

Additional Reading: For more information about shielded virtual machines, refer to: "Guarded Fabric and Shielded VMs" at: http://aka.ms/m83kd3

Virtual machine settings

Hyper-V virtual machines have many configuration options. You should be aware of what they are and how they work to ensure that you configure virtual machines properly for your environment.

- Integration services allow virtual machines to access Hyper-V services
- Smart paging allows disk to be used temporarily during virtual machine startup, when it is highly needed
- Resource metering monitors resource usage of virtual machines for planning
- Discrete device assignment allows direct access to PCIe devices
- Linux and FreeBSD Generation 2 virtual machines can use secure boot

Integration services

Integration services are software installed in guest operating systems to make them Hyper-V aware. When integration services are installed, the guest operating system has device drivers that are specific to Hyper-V. This allows the guest operating system to use the virtual hardware provided by Hyper-V. Without integration services, the guest operating system can use only emulated hardware, which has limited performance.

Guest operating systems with integration services installed also have access to services provided by Hyper-V. The services can be individually enabled and disabled. In most cases, all services will be enabled. In Windows-based guest operating systems, integration services are installed as services.

Smart Paging

Windows Server 2016 supports Smart Paging, which provides a solution to the problem of minimum memory allocation as it relates to virtual machine startup. Virtual machines can sometimes require more memory during startup than they would during normal operation. Before Windows Server 2012, it was necessary to allocate the minimum required memory for startup to ensure that startup occurred successfully, even if that value was more than what the virtual machine needed during normal operation.

Smart Paging uses disk paging for additional temporary memory when virtual machines are starting and need more memory than the host can allocate. For example, a virtual machine requires 3 GB of memory at startup, but only 1.5 GB of memory when it is running. If the host has 2 GB of memory available to allocate, Smart Paging will use 1 GB of disk space to allocate the necessary memory for the startup of the virtual machine. One drawback of Smart Paging is that there is a decrease in performance when the virtual machine is started. Having more memory available in the host is preferable.

Resource metering

Resource metering provides you with a way to measure the following parameters on individual Hyper-V virtual machines:

- Average CPU use.
- Average, minimum, and maximum memory use.
- Maximum disk allocation.
- Incoming and outgoing network traffic for a network adapter.

By measuring how much of these resources each virtual machine uses, an organization can bill departments or customers based on the resources their virtual machines use, rather than charging a flat fee per virtual machine. An organization with only internal customers can also use these measurements to see patterns of use and plan future expansions.

Discrete device assignment

Discrete device assignment is a method for allowing guest virtual machines to communicate directly with PCIe devices. The main purpose of discrete device assignment is to provide virtual machines with direct access to SSD drives, which are attached directly to the PCIe bus by using the Non-Volatile Memory Express (NVMe) standard. Graphics processing units (GPUs) can also be made available by using discrete device assignment, but it must be officially supported by the vendor.

 **Additional Reading:** For detailed information about enabling and configuring discrete device assignment, refer to: "Discrete Device Assignment - Description and background" at: http://aka.ms/Elnofg

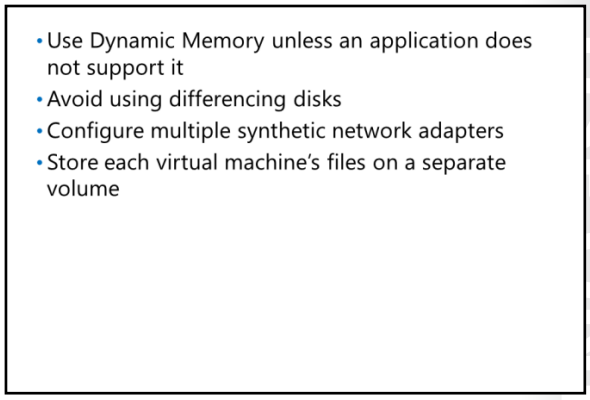
Secure boot for Linux and FreeBSD virtual machines

Hyper-V supports a variety of Linux distributions and FreeBSD as guest operating systems. For supported distributions, you can obtain Hyper-V integration services. In Windows Server 2012 R2, you could create Linux and FreeBSD virtual machines, but the secure boot option that verifies operating system files at start-up had to be disabled. In Windows Server 2016, secure boot can be used with Linux and FreeBSD.

 **Additional Reading:** For detailed information about supported distributions for Linux and FreeBSD, refer to: "Supported Linux and FreeBSD virtual machines for Hyper-V on Windows" at: http://aka.ms/Xa17y0

Best practices for configuring virtual machines

When creating new virtual machines, keep the following best practices in mind:



- Use dynamic memory. The only time you should avoid dynamic memory is if you have an application that does not support it. For example, Microsoft Exchange Server keeps requesting memory if it is available. In such cases, set static memory limits. You should monitor memory utilization and set the minimum memory to the server's minimum memory utilization. Also, set a maximum amount of memory. The default maximum is more memory than most host servers have available.
- Avoid differencing disks in production. Differencing disks reduce the amount of space required, but they decrease performance as multiple virtual machines access the same parent virtual hard disk file.
- Use multiple Hyper-V specific network adapters that are connected to different external virtual switches. Configure virtual machines to use multiple virtual network adapters that are connected to host network adapters, which in turn are connected to separate physical switches. This means that network connectivity is retained if a network adapter or a switch fails.
- Store virtual machine files on their own volumes if you are not using shared storage. This minimizes the chances of one virtual machine's virtual hard disk growth affecting other virtual machines on the same server.

  Question: You need to run guest virtual machines on both Windows Server 2012 R2 and Windows Server 2016 servers. What should you avoid doing until you no longer need to run these virtual machines on Windows Server 2012 R2?

Check Your Knowledge

Question	
Which virtual machine characteristics must be present to support hot adding a virtual network adapter? Choose all that apply.	
Select the correct answer.	
	Generation 1 virtual machine
	Generation 2 virtual machine
	Configuration version 5 (Windows 2012 R2)
	Guest Operating System Windows Server 2012 R2
	Guest Operating System Windows Server 2016

Lesson 6
Managing virtual machines

After virtual machines are created, there are command tasks for managing virtual machines. A virtual machine's state describes the current status of a virtual machine. Creating and managing checkpoints is an important skill for administrators, including the new production checkpoints. You can import and export virtual machines as part of the backup and migration processes. Finally, Windows PowerShell Direct is a new management option that can be used by virtual machines when there is no network connectivity to the virtual machine.

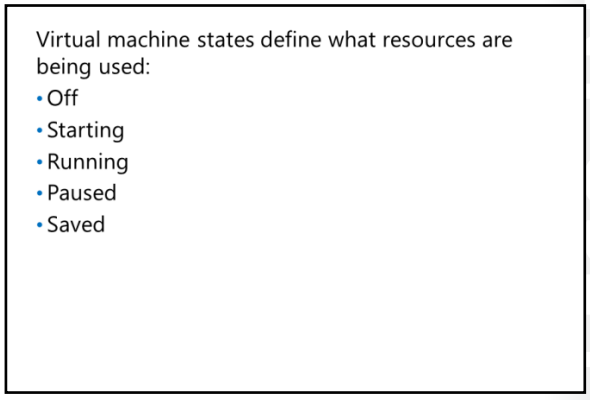
Lesson Objectives

After completing this lesson, you will be able to:

- Manage virtual machine state.
- Describe how to manage checkpoints.
- Create checkpoints.
- Import and export virtual machines.
- Describe Windows PowerShell Direct.
- Use Windows PowerShell Direct to manage virtual machines.

Managing virtual machine state

It is important to be clear about how the state of a virtual machine impacts the resources that it is using. This ensures that your Hyper-V host has sufficient resources to support the virtual machines that reside on it.

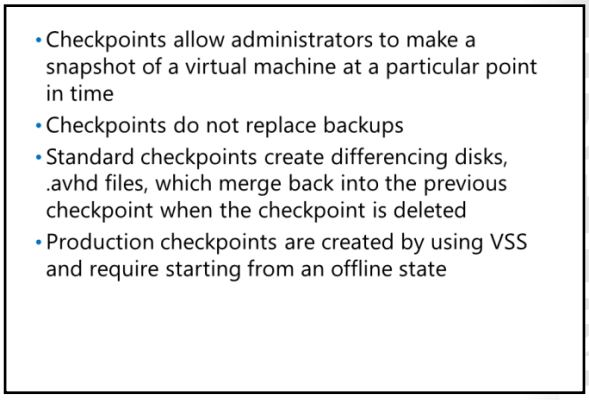


The states for a virtual machine are:

- Off. A virtual machine that is off does not use any memory or processing resources.
- Starting. A virtual machine that is starting verifies that resources are available before allocating those resources.
- Running. A virtual machine that is running uses the memory that has been allocated to it. It can also use the processing capacity that has been allocated to it.
- Paused. A paused virtual machine does not consume any processing capacity but does still retain the memory that has been allocated to it.
- Saved. A saved virtual machine does not consume any memory or processing resources. The memory state for the virtual machine is saved as a file and is read when the virtual machine is started again.

Managing checkpoints

Checkpoints are an important feature that allows administrators the ability to make a snapshot of a virtual machine at a specific time. Windows Server 2016 also provides production checkpoints and standard checkpoints, with the default being production checkpoints. It is important to know when to use a standard checkpoint and when to use a production checkpoint.



Note: Ensure that you use only checkpoints with server applications that support the use of checkpoints. Reverting to a previous checkpoint on a computer that hosts an application that does not support virtual machine checkpoints might lead to data corruption or loss. Some applications might only support production checkpoints.

Creating a checkpoint

You can create a checkpoint in the Actions pane of the Virtual Machine Connection window or in the Hyper-V Manager console. Each virtual machine can have a maximum of 50 checkpoints.

When creating checkpoints for multiple virtual machines that have dependencies, you should create them at the same time. This ensures synchronization of items such as computer account passwords. Remember that when you revert to a checkpoint, you are reverting to a computer's state at that specific time. If you take a computer back to a point before it performed a computer password change with a domain controller, you must rejoin that computer to the domain.

Checkpoints do not replace backups

Checkpoints are not a replacement for backups. Checkpoint data is stored on the same volume as the virtual hard disks. If the volume that hosts these files fails, both the checkpoint and the virtual hard disk files are lost. You can perform a virtual machine export of a checkpoint. When you export the checkpoint, Hyper-V creates full virtual hard disks that represent the state of the virtual machine when you created the checkpoint. If you choose to export an entire virtual machine, all checkpoints that are associated with the virtual machine are also exported.

Standard checkpoints

When you create a standard checkpoint, Hyper-V creates an .avhd file that stores the data that differentiates the checkpoint from either the previous checkpoint or the parent virtual hard disk. When you delete standard checkpoints, this data is discarded or merged into the previous checkpoint or parent virtual hard disk. For example, if you delete the most recent checkpoint of a virtual machine, the data is discarded. If you delete the second-to-last checkpoint of a virtual machine, the content of the differencing virtual hard disk merges with its parent, so that the earlier and latter checkpoint states of the virtual machine retain their integrity.

Production checkpoints

When you create a production checkpoint, Windows Server 2016 uses Volume Shadow Copy Service (VSCS) or File System Freeze for Linux. This places the virtual machine in a safe state to create a checkpoint that can be recovered in the same way as any VSCS or application backup. Unlike standard checkpoints that save all memory and processing in the checkpoint, production checkpoints are closer to a state backup. Production checkpoints require a virtual machine to start from an offline state to restore the checkpoint.

Managing checkpoints

When you apply a checkpoint, the virtual machine reverts to the configuration that existed at the time that it took the checkpoint. Reverting to a checkpoint does not delete any existing checkpoints. If you revert to a checkpoint after making a configuration change, you receive a prompt to create a checkpoint. Creating a new checkpoint is necessary only if you want to return to that current configuration.

It is possible to create checkpoint trees that have different branches. For example, if you create a checkpoint of a virtual machine on Monday, Tuesday, and Wednesday, apply the Tuesday checkpoint, and then make changes to the virtual machine's configuration, you create a new branch that diverts from the original Tuesday checkpoint. You can have multiple branches if you do not exceed the 50-checkpoint limit per virtual machine.

Demonstration: Creating checkpoints

In this demonstration, you will see how to create a production checkpoint and a standard checkpoint by using the traditional Hyper-V Manager method.

Demonstration Steps

1. In **Hyper-V Manager**, open the settings for **LON-GUEST1** and verify that the **Checkpoint Type** is set to **Production Checkpoints**.
2. Create a checkpoint for **LON-GUEST1**.
3. Open the settings for **LON-GUEST1** and change the **Checkpoint Type** to **Standard Checkpoints**.
4. Create a checkpoint for **LON-GUEST1.**
5. Delete the checkpoint subtree for **LON-GUEST1**.

Importing and exporting virtual machines

You can use Hyper-V import and export functionalities to transfer virtual machines between Hyper-V hosts and to create point-in-time backups of virtual machines.

- Import options:
  - Register the virtual machine in-place (use the existing unique ID)
  - Restore the virtual machine (use the existing unique ID)
  - Copy the virtual machine (create a new unique ID)
- Export options:
  - Export a checkpoint
  - Export a virtual machine including checkpoints
- Moving virtual machine storage:
  - Move all the virtual machine's data to a single location
  - Move the virtual machine's data to different locations
  - Move the virtual machine's virtual hard disks

Importing virtual machines

The virtual machine import functionality in Windows Server 2016 can identify configuration problems such as missing hard disks or virtual switches. This was more difficult to determine in older operating systems before Windows Server 2012.

In Windows Server 2016, you can import virtual machines from copies of virtual machine configurations, checkpoints, and virtual hard disk files rather than specially exported virtual machines. This is beneficial in recovery situations where an operating system volume might have failed but the virtual machine files remain intact.

When you perform an import, you have three options:

- Register the virtual machine in-place (use the existing unique ID). This option creates a virtual machine by using the files in the existing location.
- Restore the virtual machine (use the existing unique ID). This option copies the virtual machine files back to the location from which they were exported and then creates a virtual machine by using the copied files. This option effectively functions as a restore from backup.
- Copy the virtual machine (create a new unique ID). This option copies the virtual machine files to a new location that you can specify and then creates a new virtual machine by using the copied files.

Exporting virtual machines

When performing an export, you can select one of the following options:

- Export a checkpoint. This enables you to create an exported virtual machine because it existed at the point of checkpoint creation. The exported virtual machine will have no checkpoints.
- Export virtual machine with checkpoints. This exports the virtual machine and all checkpoints that are associated with the virtual machine.

Windows Server 2016 Hyper-V supports exporting virtual machines and checkpoints while a virtual machine is running.

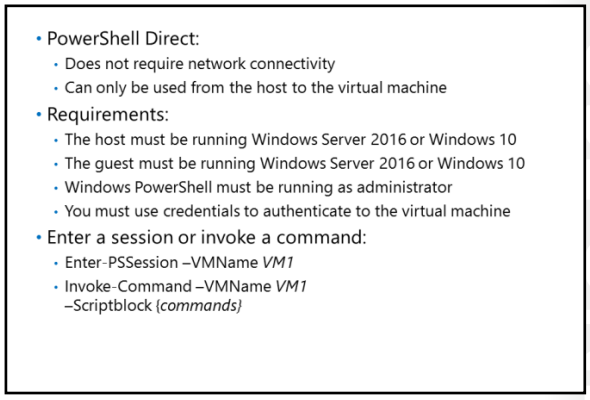
Moving virtual machines

You can perform two types of moves by using the Hyper-V move function: a live migration and a move of the actual virtual machine. You can move virtual machines from one Windows Server 2016 Hyper-V server to another if you have enabled live migrations. Live migration of virtual machines occurs when you move a virtual machine from one host to another while keeping the virtual machine online and available to clients.

You can use the move functionality to move some or all virtual machine files to a different location. For example, if you want to move virtual machines from one volume to an SMB 3.0 share while keeping the virtual machine hosted in the same location, you have the following options:

- Move all the virtual machine's data to a single location. This moves all configuration files, checkpoints, and virtual hard-disk files to the destination location.
- Move the virtual machine's data to different locations. This moves the virtual machine's configuration files, checkpoints, and virtual hard disks to separate locations.
- Move the virtual machine's virtual hard disks. This moves the hard disks to a separate location while keeping the checkpoint and configuration files in the same location.

Windows PowerShell Direct



Windows PowerShell has the ability to create remote sessions and run Windows PowerShell cmdlets on a remote host. The functionality is called PowerShell remoting and uses the WinRM service in Windows for connectivity. All connectivity is performed over a network.

In Windows Server 2016, PowerShell Direct has been added as an option for connecting to virtual machines and running Windows PowerShell cmdlets. PowerShell Direct does not require a network connection to do Windows PowerShell remoting from the Hyper-V host on which the virtual machine is running. This is useful if you want to run PowerShell cmdlets remotely in a virtual machine, but do not have network connectivity to that virtual machine. It also provides a way to easily script modifications to multiple virtual machines running on a Hyper-V host.

Requirements for PowerShell Direct are:

- The host operating system must be Windows Server 2016 or Windows 10.
- The guest operating system must be Windows Server 2016 or Windows 10.
- Windows PowerShell must be running as Administrator.
- You must use credentials to authenticate to the virtual machine.
- Virtual machine configuration version must be updated.

To enter a session on a virtual machine, use the following command:

```
Enter-PSSession -VMName VM1
```

To invoke a command on a virtual machine, use the following command:

```
Invoke-Command -VMName VM1 -ScriptBlock {Windows PowerShell commands}
```

Demonstration: Using Windows PowerShell Direct

In this demonstration, you will see how to use Windows PowerShell Direct,

Demonstration Steps

1. Complete setup of the guest operating system in **LON-GUEST1**.
2. Remove the network connection of the **LON-GUEST1** virtual machine.
3. Connect to **LON-GUEST1** and set the password for virtual machine.
4. Open a **Windows PowerShell** prompt as an Administrator and use **PowerShell Direct** to connect to **LON-GUEST1** by entering the following command:

```
Enter-PSSession –VMName “LON-GUEST1”
```

5. Restart **LON-GUEST1** by using **PowerShell Direct** with the following command:

```
Restart-Computer
```

6. Re-enable network connection for **LON-GUEST1**.

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

Statement	Answer
When restarting a virtual machine from a production checkpoint, the memory state is saved.	

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

Statement	Answer
You can use Windows PowerShell Direct from your workstation to access virtual machines running on a Hyper-V host.	

Lab: Installing and configuring Hyper-V

Scenario

IT management at A. Datum Corporation is concerned about the low utilization of many of the physical servers that are deployed in the London datacenter. A. Datum is also exploring options for expanding into multiple branch offices and deploying servers in public and private clouds. For this purpose, the company is exploring the use of virtual machines.

You will deploy the Hyper-V server role, configure virtual machine storage and networking, and deploy the virtual machines.

Objectives

After completing this lab, you will be able to:

- Verify the installation of the Hyper-V server role.
- Configure Hyper-V networks.
- Create and configure virtual machines.
- Enable nested virtualization.

Lab Setup

Estimated Time: **60 minutes**

Virtual machine: **20740A-LON-HOST1**

User name: **Administrator**

Password: **Pa$$w0rd**

1. Restart the classroom computer, and then, in **Windows Boot Manager**, select **20740A-LON-HOST1**.
2. Sign in to **LON-HOST1** with the following credentials:
    - User name: **Administrator**
    - Password: **Pa$$w0rd**

Exercise 1: Verifying installation of the Hyper-V server role

Scenario

The first step in migrating to a virtualized environment is to install the Hyper-V server role on a new server. You installed this role in Module 2. You must now verify the presence of the Hyper-V role.

The main task for this exercise is as follows:

1. Verify the presence of the Hyper-V server role.

▶ Task 1: Verify the presence of the Hyper-V server role

1. On **LON-HOST1**, sign in as **Administrator** by using **Pa$$w0rd** as the password.
2. Start **Hyper-V Manager** and verify the role is installed on **LON-HOST1**.

Results: After completing this exercise, you should have successfully verified the presence and configuration of the Hyper-V server role on a physical server.

Exercise 2: Configuring Hyper-V networks

Scenario

After installing the Hyper-V server role on the new server, you must configure the virtual networks. To see the differences between the different network types, you must create an external, internal, and private network.

The main tasks for this exercise are as follows:

1. Create an external network.
2. Create a private network.
3. Create an internal network.

▶ Task 1: Create an external network

Note: To perform this task, your computer must have physical network card (wired or wireless) and be connected to a network.

1. In **Hyper-V Manager**, open **Virtual Switch Manager**.
2. Create a new virtual network switch with the following settings:
   - Type: **External**
   - Name: **Physical Network**
   - Allow the management operating system to share this network adapter
3. In **Server Manager**, verify that the network adapter has been replaced with **vEthernet (Physical Network)**.

▶ Task 2: Create a private network

1. On **LON-HOST1**, in **Hyper-V Manager**, open **Virtual Switch Manager**.
2. Create a new virtual network switch with the following settings:
   - Name: **Isolated Network**
   - Connection type: **Private network**
3. In **Server Manager**, verify that there have been no changes to the network adapters.

▶ Task 3: Create an internal network

1. On **LON-HOST1**, in **Hyper-V Manager**, open **Virtual Switch Manager**.
2. Create a new virtual network switch with the following settings:
   - Type: **Internal network**
   - Name: **Host Internal Network**
3. In **Server Manager**, verify that a new network adapter named **vEthernet (Host Internal Network)** has been created.

Results: After completing this exercise, you should have successfully configured an external, internal, and private network.

Exercise 3: Creating and configuring virtual machines

Scenario

To view the differences between Generation 1 and Generation 2 virtual machines, you will create two new virtual machines. You will install the Generation 2 virtual machine from Windows Server 2016 installation media. You will create the Generation 1 virtual machine by using a differencing disk and a base image created for an earlier project.

The main tasks for this exercise are as follows:

1. Create a Generation 2 virtual machine.
2. Create a Generation 1 virtual machine.
3. Configure virtual machines.
4. Create checkpoints.
5. Enable host resource protection.
6. Export a virtual machine.

▶ Task 1: Create a Generation 2 virtual machine

1. Use **File Explorer** to create the following folders on the physical host drive:
   - **E:\Program Files\Microsoft Learning\20740\Drives\LON-GUEST1**
   - **E:\Program Files\Microsoft Learning\20740\Drives\LON-GUEST2**

   Note: The drive letter for this path might vary depending on the configuration of the physical host.

2. In **Hyper-V Manager**, create a new virtual machine with the following settings:
   - Name: **LON-GUEST2**
   - Location: **E:\Program Files\Microsoft Learning\20740\Drives\LON-GUEST2**
   - Generation: **2**
   - Memory: **1024MB**
   - Network: **Isolated Network**
   - Create a virtual hard disk:
     - Name: **LON-GUEST2.vhdx**
     - Location: **E:\Program Files\Microsoft Learning\Base\LON-GUEST2**
     - Size: **127 GB**
3. Open the **Settings** window for **LON-GUEST2** and add a new DVD drive attached to the SCSI controller.
4. Connect the new DVD drive to **E:\Program Files\Microsoft Learning\20740\Drives \WinServer2016_TP5.iso**.
5. In the **Firmware settings** tab, move **Network Adapter** to the end of the boot order.

6. Start **LON-GUEST2** and install **Windows Server 2016** by using all of the default settings:
   - I don't have a product key
   - Windows Server 2016 Datacenter Technical Preview 5 (Desktop Experience)
   - Custom: Install Windows only (advanced)
   - Password: **Pa$$w0rd**
7. When installation is complete, shut down **LON-GUEST2**.

Note: The installation of Windows requires an extended period of time. You can work on the next task while waiting for the installation to complete.

▶ Task 2: Create a Generation 1 virtual machine

1. Open a Windows PowerShell prompt and run the following command to link 20740A-BASE.vhd to the correct parent disk:

```
Set-VHD "E:\Program Files\Microsoft Learning\20740\Drives\20740A-BASE.vhd" -
ParentPath "E:\Program Files\Microsoft Learning\Base\Base16D-WS16-TP5.vhd"
```

2. In **Hyper-V Manager**, create a virtual hard disk with the following properties:
   - Disk Format: **VHD**
   - Disk Type: **Differencing**
   - Name: **LON-GUEST1.vhd**
   - Location: **E:\Program Files\Microsoft Learning\20740\Drives\LON-GUEST1**
   - Parent Location: **E:\Program Files\Microsoft Learning\20740\Drives\20740A-BASE.vhd**
3. Open a **Windows PowerShell** prompt and run the following command to create the new virtual machine:

```
New-VM –Name LON-GUEST1 –MemoryStartupBytes 1024MB –VHDPath "E:\Program
Files\Microsoft Learning\20740\Drives\LON-GUEST1\LON-GUEST1.vhd" –SwitchName
"Isolated Network"
```

▶ Task 3: Configure virtual machines

1. On **LON-HOST1**, in **Hyper-V Manager**, open the settings for **LON-GUEST1** and configure the following settings:
   - Maximum RAM: **4096 MB**
   - Enable Dynamic Memory
   - Number of virtual processors: **2**
   - Enable bandwidth management
   - Minimum bandwidth: **10 Mbps**
   - Maximum bandwidth: **100 Mbps**
   - Enable the Guest services integration service

Note: You must have completed the previous tasks in this exercise before you can continue. This includes shutting down **LON-GUEST2**.

2. Open the settings for **LON-GUEST2** and configure the following settings:
   - Review the Security settings
   - Verify that Enable dynamic memory is not selected
   - Number of virtual processors: **2**
   - For disk: **Enable Quality of Service management**
   - Minimum IOPS: **10**
   - Enable the Guest services integration service

▶ Task 4: Create checkpoints

1. On **LON-HOST1**, in **Hyper-V Manager**, create a checkpoint for **LON-GUEST2**.
2. Start **LON-GUEST2**.
3. Sign in to **LON-GUEST2** as **Administrator** by using **Pa$$w0rd** as the password.
4. In **Server Manager**, verify that there is only one network adapter.
5. On **LON-HOST1**, in **Hyper-V Manager**, open the settings for **LON-GUEST2** and add a network adapter.
6. On **LON-GUEST2**, in **Server Manager**, verify that a second network adapter has appeared.
7. On **LON-HOST1**, in **Hyper-V Manager**, create a checkpoint for **LON-GUEST2**.
8. After the checkpoint is created, apply the most recent checkpoint.
9. Verify that **LON-GUEST2** was stopped because it was a production checkpoint.

▶ Task 5: Enable host resource protection

- On **LON-HOST1**, at the **Windows PowerShell** prompt, type the following command, and then press Enter:

```
Set-VMProcessor LON-GUEST2 -EnableHostResourceProtection $true
```

▶ Task 6: Export a virtual machine

- On **LON-HOST1**, in **Hyper-V Manager**, export **LON-GUEST2** to **E:\Program Files \Microsoft Learning\20740\Drives\Guest2-Bak**.

Results: After completing this exercise, you should have successfully created and configured both a Generation 1 virtual machine and a Generation 2 virtual machine.

Exercise 4: Enabling nested virtualization for a virtual machine

Scenario

You are considering the use of nested virtualization for your development environment where you often have a need to test applications using failover clustering. With nested virtualization, many scenarios can be tested with a single physical host. Scripts are provided for creating the test environment.

The main tasks for this exercise are as follows:

1. Import LON-NVHOST2.
2. Enable nested virtualization.
3. Enable Hyper-V.
4. Prepare for the next module.

▶ Task 1: Import LON-NVHOST2

Note: Before beginning this task, verify the location of the base drives and 20740 course drives. You need the drive letter for both locations in this exercise. The exercise assumes that the drive letter **E:** is used for both, but substitute the correct drive letter as necessary.

1. On **LON-HOST1**, use **Windows PowerShell** to run the following script for creating virtual switches.

```
& 'E:\Program Files\Microsoft Learning\20740\Drives\CreateVirtualSwitches.ps1'
```

2. Run the following script for preparing virtual hard disks and importing the VMs:

```
& 'E:\Program Files\Microsoft Learning\20740\Drives\LON-HOST1_VM-Pre-Import-
20740A.ps1'
```

▶ Task 2: Enable nested virtualization

1. Run the following script to enable nested virtualization for **LON-NVHOST2**:

```
C:\Labfiles\Mod05\Enable-NestedVm.ps1 -vmName "20740A-LON-NVHOST2"
```

2. Accept all suggested changes.

▶ Task 3: Enable Hyper-V

1. On **LON-HOST1**, use **Windows PowerShell** to view the version number of the virtual machines by running the following command:

```
Get-VM | FT Name,Version
```

2. Update the version for **20740A-LON-NVHOST2** by running the following command:

```
Update-VMVersion 20740A-LON-NVHOST2
```

3. Start the **20740A-LON-NVHOST2** virtual machine by running the following command:

```
Start-VM 20740A-LON-NVHOST2
```

4. To view the activity on **LON-NVHOST2**, in **Hyper-V Manager**, connect to **20740A-LON-NVHOST2**.

5. Wait until **LON-NVHOST2** has started.
6. At the Windows PowerShell prompt, enter a **Windows PowerShell** session by using **PowerShell Direct**:

```
Enter-PSSession -VMName 20740A-LON-NVHOST2
```

7. When prompted, sign in as **Adatum\Administrator** by using **Pa$$w0rd** as the password.
8. Use **Windows PowerShell Direct** to install **Hyper-V on LON-NVHOST2**:

```
Install-WindowsFeature -Name Hyper-V -IncludeAllSubFeature -IncludeManagementTools -
Restart
```

9. Wait for **LON-NVHOST2** to restart. The virtual machine might restart several times.
10. Sign in to **LON-NVHOST2** as **Adatum\Administrator** by using **Pa$$w0rd** as the password.
11. Verify that **LON-NVHOST2** is listed in **Hyper-V Manager**.

Results: After completing this exercise, you should have successfully configured a virtual machine for nested virtualization.

▶ Task 4: Prepare for the next module

- Leave your host computer started as **LON-HOST1**.

Question: Do you need to download the script for enabling nested virtualization separately for each virtual machine?

Question: Why did adding a private network not create an additional virtual network adapter on LON-HOST1?

Module Review and Takeaways

Review Questions

Question: In which situations should you use static memory allocation rather than dynamic memory?

Question: When should you use the .vhdx format instead of .vhd format?

Question: You want to deploy a Hyper-V virtual machine's virtual hard disk on a file share. What operating system must the file server be running on to support this configuration?

Real-world Issues and Scenarios

You must ensure that virtual machines are provisioned with adequate memory. Having multiple virtual machines paging a hard disk drive because they are provisioned with inadequate memory decreases performance for all virtual machines on the Hyper-V host.

You should also monitor virtual machine performance carefully. One virtual machine that uses a disproportionate amount of server resources can adversely affect the performance of all other virtual machines that the Hyper-V server hosts.

Tools

The following table includes tools that are related to this module:

Tool	Used for	Where to find it
Sysinternals Disk2vhd	Converts physical hard disks to .vhd format.	**Additional Reading**: For more information, refer to: "Sysinternals Suite" at: http://aka.ms/kx5ojf
Microsoft System Center 2012 R2 - Virtual Machine Manager	• Manages virtual machines across multiple Hyper-V servers. • Performs online physical-to-virtual conversions; however, System Center 2012 R2 - Virtual Machine Manager does not support physical-to-virtual conversions.	**Additional Reading**: For more information, refer to: "Virtual Machine Manager" at: http://aka.ms/qc0v35

Module 6

Deploying and managing Windows and Hyper-V containers

Contents:

Module Overview

One of the important new features in Windows Server 2016 is the option to deploy containers. By deploying containers, you can provide an isolated environment for applications. You can deploy multiple containers on a single physical server or virtual server, and each container provides a complete operating environment for installed applications. This module introduces you to Windows and Hyper-V containers in Windows Server 2016, and it teaches you how to deploy and manage these containers.

Objectives

After completing this module, you will be able to:

- Describe containers in Windows Server 2016.
- Explain how to deploy containers.
- Explain how to install, configure, and manage containers using Docker.

Lesson 1
Overview of containers in Windows Server 2016

After completing this lesson, students will be able to explain the purpose of Windows Server and Hyper-V containers.

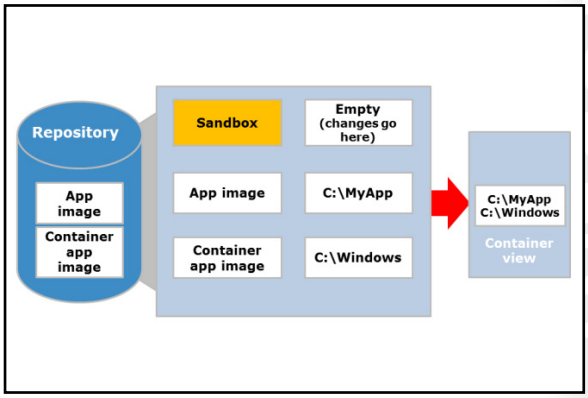
Lesson Objectives

After completing this lesson, you will be able to:

- Describe Windows Server containers.
- Describe Hyper-V containers.
- Describe scenarios for using containers
- Describe the installation requirements for containers.

Overview of Windows Server containers

Containers are an isolated operating environment that you can use to provide a controlled and portable space for an app. The container space provides an ideal environment for an app to run without affecting the rest of the operating system (OS) and without the OS affecting the app. Containers enable you to isolate apps from the OS environment.



In many ways, containers are the next evolution in virtualization. Containers are also referred to as *container-based OS virtualization*. Although containers run on the host OS, containers are isolated from one another. Isolated containers improve the security and the reliability of the apps that run within the containers. Containers provide a simulated environment for apps. For example, the local disk appears as a new copy of the OS files, while the memory appears to hold only files and data of the OS that recently started, and the only running component is the OS.

Windows Server 2016 supports two different types of containers, or *runtimes*, each offering different degrees of isolation with different requirements:

- Windows Server containers. These containers provide app isolation through process and namespace isolation technology. Windows Server containers share the OS kernel with the container host and with all other containers that run on the host. While this provides a faster startup experience, it does not provide complete isolation of the containers.
- Hyper-V containers. These containers expand on the isolation that Windows Server containers provide by running each container in a highly optimized virtual machine (VM). However, in this configuration, the OS kernel of the container host does not share with the Hyper-V containers.

Containers appear like a complete OS to an app. Therefore, in many respects, containers are similar to VMs because they run an OS, they support a file system, and you can be access them across a network like any other physical machine or VM. However, the technology and concepts behind containers are very different from that of VMs.

Container definitions

As you begin creating and working with containers in Windows Server 2016, it is helpful to learn the key concepts that make up the container architecture:

- *Container host*. This element consists of the physical or virtual computer that is configured with the Windows containers feature. The container host can run one or more Windows containers.
- *Container image*. As modifications are made to a containers file system or registry, these changes are captured in the container's sandbox. In many cases, you might want to capture the container image state so that the new containers that you create can inherit the container changes. After you stop the container, you can discard the sandbox, or you can convert it into a new container image. For example, you can install an app into a container and then capture the post-installation state. From this state, you can create a new container image that contains the app. The image will only contain the changes that the installation of the app made, with a layer on top of the container OS image.
- *Container OS image*. While containers are made from images, the container OS image is the first layer in potentially multiple image layers that make up a container. The container OS image provides the OS environment, and it is immutable.
- *Sandbox*. This layer consists of all the changes made to the container, including file system modifications, registry modifications, or software installations. You can keep or discard these changes as required.
- *Container repository*. Each time you make a container image, the container image and its dependencies are stored in a local repository. This allows you to reuse the image many times on the container host.

Finally, it is important to understand that you can manage containers by using the Windows PowerShell command-line interface or by using the open source Docker platform.

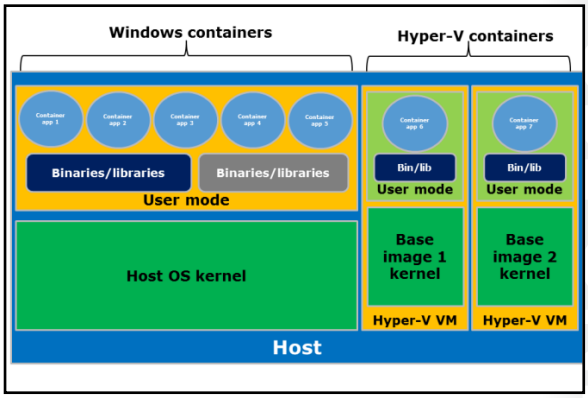
Windows Server containers

When you deploy a physical or virtual computer, the computer must have a single user mode that runs on top of a single kernel mode. Computers provide a boundary to allow multiple user modes so you can deploy multiple isolated apps. For example, Hyper-V offers child partitions, or VMs, which can each have their own Windows Server OS with the requisite kernel and user modes, and each app installs in each user mode, or each VM. Containers allow you to have more than one user mode per kernel mode, and they only require one computer per kernel mode.

As noted earlier, a computer deploys with the Windows Server OS with a kernel mode and a user mode. The user mode of the OS manages the container host, or the computer that is hosting the containers. A special stripped down version of the Windows OS, which is stored in a container repository as a container OS image, is used to create a container. This container only features a user mode—this is the distinction between Hyper-V and containers because a VM runs a guest OS with a user mode and a kernel mode. The Windows Server container's user mode allows Windows processes and app processes to run in the container, isolated from the user mode of other containers. When you virtualize the user mode of the OS, Windows Server containers allow multiple apps to run in an isolated state on the same computer, but they do not offer secure isolation.

Overview of Hyper-V containers

It is important to discuss VMs to help you understand Hyper-V containers. VMs also provide an isolated environment for running apps and services. However, a VM provides a full guest OS with kernel and user modes. For example, a computer with the Hyper-V role enabled includes a parent partition, or a management OS, isolated kernel and user modes, and it is responsible for managing the host. Each child partition, or hosted VM, runs an OS with a kernel mode and a user mode.



Similar to VMs, Hyper-V containers are the child partitions that are deployed. On the other hand, the guest OS in Hyper-V containers is not the normal, full Windows OS that we know; it is an optimized, stripped-down version of the Windows Server OS—this is not the same as Nano Server. The boundary provided by the Hyper-V child partition provides secure isolation between the Hyper-V container, other Hyper-V containers on the host, the hypervisor, and the host's parent partition.

Hyper-V containers use the base container image that is defined for the app, and they automatically create a Hyper-V VM by using that base image. When deployed, the Hyper-V container starts in seconds, which is much faster than a VM with a full Windows OS and is even faster than Nano Server. The Hyper-V container features an isolated kernel mode, a user mode for core system processes, and a container user mode, which is the same thing that runs in a Windows Server container. In fact, Hyper-V containers use the Windows containers within the VM to store the binaries, libraries, and the app.

Now that the Windows container is running inside a Hyper-V VM, this provides the app with kernel isolation and separation of the host patch and the version level. Because the app is containerized by using Windows containers, you can choose the level of isolation that is required during deployment by selecting a Windows or Hyper-V container. With multiple Hyper-V containers, you can use a common base image that does not require manual management of VMs; the VMs create and delete automatically.

Usage scenarios

Windows Server and Hyper-V container have several practical applications for enterprise environments.

Some common usage scenarios for Windows containers include:

- Windows Server containers for:
  - Hosting stateless apps
  - Rapid test deployment
- Hyper-V containers for:
  - Multiple tenants
  - Single tenants
  - Independent lifecycle management

Windows Server containers

While many similarities exist between Windows Server containers and Hyper-V containers, the differences in these virtualization technologies make one more suitable than the other based on your requirements. For example, Windows Server containers are preferred in scenarios where the OS trusts the apps that it hosts, and all the apps must trust each other. In other words, the host OS and apps are within the same trust boundary. This is true for many multiple-container apps, apps that compose a shared service of a larger app, and sometimes apps from the same organization.

You should ensure that the apps that you deploy in a container on a Windows Server 2016 host are stateless. This type of app does not store any state data in its container. Additionally, keep in mind that containers do not have a GUI. Based on the characteristics of a container, you will probably not run your accounting package in a container. On the other hand, some apps like games and websites render on local systems, not servers, so they make great examples of apps that are well suited for containers. In summary, stateless web apps, which do not have a GUI, and similar code are the most likely candidates for using Windows container technologies in Windows Server 2016.

Windows Server containers for rapid test deployment

Containers can be used to package and deliver distributed apps quickly. A custom app might require multiple deployments, either weekly or sometimes daily, to keep up with the changes.

Windows Server containers are an ideal way to deploy these apps because you can create packages by using a layered approach to building a deployable app. For example, you can create an image that hosts web sites that includes installed Internet Information Services (IIS) and the Microsoft ASP.NET software. Developers can then use that image multiple times to deploy apps without changing the underlying layers. Because Windows Server containers provide greater efficiency in startup times, faster runtime performance, and greater density than Hyper-V containers, developers can spend more time developing apps while requiring fewer resources.

 **Note:** While not unique to Windows Server containers, you can deploy the same package in your test environment to your production environment—it runs the same way it did for the developers and testers. As an added bonus, you also can deploy this container in Microsoft Azure without changing it.

Hyper-V containers

Hyper-V containers each have their own copy of the Windows OS kernel, and have memory assigned directly to them, which is a key requirement of strong isolation. Similar to VMs, you would use Hyper-V containers in scenarios that require central processing unit (CPU), memory, and I/O isolation, for example, a network and storage. The host OS only exposes a small, constrained interface to the container for communication and sharing of host resources. This very limited sharing means that Hyper-V containers are a bit less efficient in startup times and density than Windows Server containers, but they provide the isolation required to allow untrusted apps to run on the same host.

The trust boundary in Hyper-V containers provide secure isolation between the Hyper-V containers on the host, the hypervisor, and the host's other processes. For this reason, Hyper-V containers are the preferred virtualization model in multitenant environments.

Hyper-V containers for multiple tenants

In some situations, you might want to run apps that require different trust boundaries on the same host. For example, you might be deploying a multitenant platform as a service (PaaS) or SaaS offering where you allow your customers to supply their own code to extend the functionality of your service offering. However, you need to ensure that one customer's code does not interfere with your service or gain access to your other customers' data. Hyper-V containers provide the required components for the tenants, but they also ensure that one tenant's application cannot interfere with other applications.

In a typical usage scenario for cloud service providers that host Hyper-V containers, the service provider would have a cluster of Hyper-V hosts that run Windows Server 2016 for a portion of their cloud. This Hyper-V host cluster would host a group of VMs, and each VM would have Windows Server 2016 installed as its guest OS. When you use Windows container technology, each of these VMs would assume the role of a container host. Each container host, or VM, would then be assigned to a different tenant, and the tenant could then create as many containers as it needs on its dedicated container host. If malware or

malicious attack compromised one container host, or VM, the other VMs that belong to other customers would be unaffected.

Hyper-V containers for single tenants

Hyper-V containers might be useful even in a single-tenant environment. One common scenario is where one or more of the apps that you want to host in a Windows container have a dependency on the OS version level or the patch level of the underlying container host. In this scenario, you might consider provisioning a single Hyper-V host, or host cluster, and using Hyper-V containers instead of provisioning and configuring several systems as container hosts and using Windows Server containers.

Hyper-V containers for independent lifecycle management

The other scenario where isolation is very helpful is if you want to run a container with a different version of Windows Server. One of the challenges with Windows Server containers is that they share a significant portion of the OS between the base image and the container image. Consequently, if you upgrade the OS in the base image, then you also need to upgrade the container.

Alternatively, a Hyper-V container enables you to have different versions of base images that allow you to simultaneously host an OS *in* the container image. This feature is helpful for enterprises that want to have independent lifecycle management for patching, updating, and compliance reasons.

Installation requirements

When planning for Windows containers, you should be aware of the requirements for Windows Server 2016. You should also be familiar with the supported scenarios for Windows Server containers and Hyper-V containers in Windows Server 2016.

You should consider the following when planning for Windows containers:

- Windows container host requirements
- Virtualized container host requirements
- Supported scenarios

Host OS	Windows Server container	Hyper-V container
Windows Server 2016 Full UI	Server Core image	Nano Server image
Windows Server 2016 Core	Server Core image	Nano Server image
Windows Server 2016 Nano Server	Nano Server image	Nano Server image
Windows 10 Insider releases	Not available	Nano Server image

Windows container host requirements

When you are planning your deployment, the Windows container host has the following requirements:

- The Windows container role is only available on:
  - Windows Server 2016 Technical Preview 5 (TP5) (Full or Server Core) and newer.
  - Nano Server.
  - Windows 10 (build 14352 and newer).
- If Hyper-V containers are deployed, the Hyper-V role needs to be installed.
- Windows Server container hosts must have the Windows OS installed to **C:**. This restriction does not apply if only Hyper-V containers will deploy.

Virtualized container host requirements

If you deploy a Windows container host on a Hyper-V VM that is hosting Hyper-V containers, you need to enable nested virtualization. Nested virtualization has the following requirements:

- At least 4 gigabytes (GB) of memory available for the virtualized Hyper-V host.
- On the host system, you will need:
  - Windows Server 2016 TP5 and newer.
  - Windows 10 (build 10565 and newer).
- On the container host VM, you will need:
  - Windows Server TP5 (Full or Server Core).
  - Nano Server.
- A processor with Intel VT-x (this feature is currently only available for Intel processors).
- The container host VM requires at least two virtual processors.

Supported scenarios

Windows Server TP5 is offered with two container OS images: Windows Server Core and Nano Server. Not all configurations support both OS images, however. The following table lists the supported scenario.

Host OS	Windows Server container	Hyper-V container
Windows Server 2016 Full UI	Server Core image	Nano Server image
Windows Server 2016 Core	Server Core image	Nano Server image
Windows Server 2016 Nano Server	Nano Server image	Nano Server image
Windows 10 Insider releases	Not available	Nano Server image

Check Your Knowledge

Question	
In Windows Server 2016 containers, which of the following statements best describes a sandbox?	
Select the correct answer.	
	A sandbox is a computer that is configured with containers. This can be a physical computer or a virtual computer.
	A sandbox is the first layer of the container hierarchy.
	All changes that are made to a running container are stored in the sandbox.
	A sandbox is a management tool that you can use instead of the Windows PowerShell command-line interface to manage your containers.

Lesson 2
Deploying Windows Server and Hyper-V containers

Containers provide an isolated and portable operating environment for apps. From the app's perspective, a container appears as an isolated Windows OS with its own file system, devices, and configuration. Windows Server supports two types of containers: Windows Server containers and Hyper-V containers. Windows Server containers achieve isolation through namespace and process isolation, whereas Hyper-V containers encapsulate each container in a lightweight VM. To support your organization's app requirements, you should understand the fundamentals of how to enable and configure Windows Server to support containers.

Lesson Objectives

After completing this lesson, you will be able to:

- Explain how to deploy Windows Server containers.
- Explain how to deploy Hyper-V containers.
- Explain how to manage Windows Server and Hyper-V containers by using Windows PowerShell.
- Deploy Windows Server containers by using Windows PowerShell.

Deploying Windows Server containers

Before you can use containers in Windows Server 2016, you need to deploy a container host. You can choose to deploy containers on a physical host computer or within a VM. You can also choose to use Windows Server 2016, with or without Desktop Experience, or Nano Server. The procedure for deploying container hosts varies depending on the type of container.

- To prepare a Nano Server:
  - Create a Nano Server virtual hard disk (VHD) file for containers
  - Proceed with the steps below
- Use the following steps to prepare your Windows Server host for containers:
  1. Install the container feature*
  2. Create a virtual switch
  3. Configure NAT settings
  4. Configure MAC address spoofing
  5. Install container operating system images

* Step not required if you deploy to a Nano Server

Preparing a Nano Server

If you choose to deploy Windows Server containers on a Nano Server, use the high-level steps in the following table to prepare the server for Windows Server containers.

Deployment action	Details
Create a Nano Server virtual hard disk file for containers	Prepare a Nano Server virtual hard disk file with the container and Hyper-V capabilities. This requires that you build a Nano Server image by using the **-Compute** and **-Containers** switches. For example, you can type the following code, and then press Enter: `New-NanoServerImage -MediaPath $WindowsMedia -BasePath c:\nano -TargetPath C:\nano\NanoContainer.vhdx -GuestDrivers -ReverseForwarders -Compute -Containers`

After you deploy the Nano Server, you must then complete the steps listed in the following section.

Preparing the Windows Server host

Use the steps in the following table to prepare your Windows Server host for containers.

Deployment action	Details
Install the container feature*	This step enables the use of Windows Server and Hyper-V containers. You can install this feature by using **Server Manager**, or you can type the following Windows PowerShell cmdlet, and then press Enter: `Install-WindowsFeature Containers`
Create a virtual switch	All containers connect to a virtual switch for network communications. The switch type can be **Private**, **Internal**, **External**, or **NAT**. Type the following Windows PowerShell cmdlet to complete this task, and then press Enter: `New-VMSwitch -Name *Virtual Switch Name* -SwitchType *Type*` If the type is **NAT**, you must also use the **-NATSubnetAddress *172.16.0.0/12*** switch, substituting an appropriate subnet address for ***172.16.0.0/12***.
Configure network address translation (NAT)	If you want to use a virtual switch configured with NAT, you must configure the NAT settings. For example, you can type the following Windows PowerShell command, and then press Enter: `New-NetNat -Name ContainerNat -InternalIPInterfaceAddressPrefix "172.16.0.0/12"` Replace the subnet address with something appropriate for your network.
Configure media access control (MAC) address spoofing	If your container host is virtualized, you must enable MAC address spoofing. For example you can type the following Windows PowerShell command, and then press Enter: `Get-VMNetworkAdapter -VMName *Container Host VM* | Set-VMNetworkAdapter -MacAddressSpoofing On`

* This step is not required if you choose to deploy Windows Server containers to a Nano Server.

Deploying Windows Server containers

Use the high-level steps in the following table to deploy Windows Server containers.

Deployment action	Details

Install container operating system images.	Use the following Windows PowerShell commands to provide the base images for your container deployments:
	1. This installs the required Windows PowerShell module:
	`Install-PackageProvider ContainerProvider –Force`
	2. This lists the available images by name, version number, and description:
	`Find-ContainerImage`
	3. This installs the named image:
	`Install-ContainerImage -Name *ImageName* -Version *Number*`

Deploying Hyper-V containers

Before you can use containers in Windows Server 2016, you need to deploy a container host. You can choose to deploy containers either on a physical host computer or within a VM. You can also choose to use Windows Server 2016, with or without Desktop Experience, or Nano Server. The procedure for deploying container hosts varies depending on the type of container.

- To prepare a Nano Server:
  - Create a Nano Server virtual hard disk (VHD) file for containers
  - Proceed with the steps below
- Use the following steps to prepare your Windows Server host for containers:
  1. Install the container feature*
  2. Enable the Hyper-V role*
  3. Enable nested virtualization
  4. Configure virtual processors
  5. Create a virtual switch
  6. Configure NAT settings
  7. Configure MAC address spoofing
  8. Install container operating system images

* Step not required if you deploy to a Nano Server

Preparing a Nano Server

If you choose to deploy Hyper-V containers to a Nano Server, use the high-level steps in the following table to prepare the server for Hyper-V containers.

Deployment action	Details
Create a Nano Server virtual hard disk file for containers	Prepare a Nano Server virtual hard disk file with the container and Hyper-V capabilities. This requires that you build a Nano Server image by using the **-Compute** and **-Containers** switches, for example, type the following command, and then press Enter: `New-NanoServerImage -MediaPath $WindowsMedia -BasePath c:\nano -TargetPath C:\nano\NanoContainer.vhdx -GuestDrivers -ReverseForwarders -Compute -Containers`

You must then complete the steps listed in the next section.

Preparing the Windows Server host

Use the steps in the following table to prepare your Windows Server host for containers.

Deployment action	Details
Install the container feature*	You can install this feature by using **Server Manager** or by using the **Install-WindowsFeature Containers** Windows PowerShell cmdlet. You can then enable the use of Windows Server and Hyper-V containers.
Enable the Hyper-V role*	You can install this feature by using **Server Manager** or by using the **Install-WindowsFeature Hyper-V** Windows PowerShell cmdlet. This is required only if you deploy Hyper-V containers.
Enable nested virtualization	If your container host is a Hyper-V VM, you must enable nested virtualization. Type the following Windows PowerShell command, and then press Enter: Set-VMProcessor -VMName *Container Host VM* -ExposeVirtualizationExtensions $true
Configure virtual processors	If the container host is a Hyper-V VM, you must configure at least two virtual processors. You can type the following Windows PowerShell command, and then press Enter: Set-VMProcessor –VMName *Container Host VM* -Count 2
Create a virtual switch	All containers connect to a virtual switch for network communications. The switch type can be **Private**, **Internal**, **External**, or **NAT**. Type the following Windows PowerShell command, and then press Enter: New-VMSwitch -Name *Virtual Switch Name* -SwitchType *Type* If the type is **NAT**, you must also use the **-NATSubnetAddress *172.16.0.0/12*** switch, substituting an appropriate subnet address for ***172.16.0.0/12***.
Configure NAT	If you want to use a virtual switch configured with NAT, you must configure the NAT settings. For example, type the following Windows PowerShell command, and then press Enter: New-NetNat -Name ContainerNat -InternalIPInterfaceAddressPrefix "172.16.0.0/12" Replace the subnet address with something appropriate for your network.

Deployment action	Details
Configure MAC address spoofing	If your container host is virtualized, you must enable MAC address spoofing. For this task, type the following Windows PowerShell command, and then press Enter: `Get-VMNetworkAdapter -VMName *Container Host VM* | Set-VMNetworkAdapter -MacAddressSpoofing On`

* These steps are not required if you choose to deploy Hyper-V containers to a Nano Server.

Deploying Hyper-V containers

Use the high-level steps in the following table to deploy Hyper-V containers.

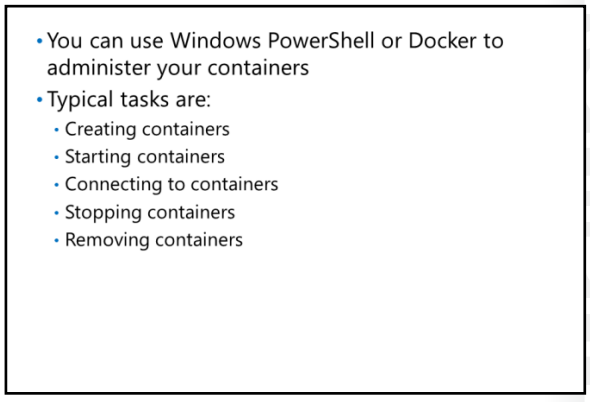
Deployment action	Details

Install container operating system images	Use the following Windows PowerShell commands to provide the base images for your container deployments:
	1. This installs the required Windows PowerShell module:
	`Install-PackageProvider ContainerProvider –Force`
	2. This lists the available images by name, version number, and description:
	`Find-ContainerImage`
	3. This installs the named image:
	`Install-ContainerImage -Name *ImageName* -Version *Number*`

Managing Windows Server and Hyper-V containers by using Windows PowerShell

After you have deployed a physical or virtual container host, you must create and configure your containers. You can use Windows PowerShell or Docker to administer your containers. Typical tasks include:

- Creating containers.
- Starting containers.
- Connecting to containers.
- Stopping containers.
- Removing containers.
- Configuring containers.



Note: This module covers how to use Docker to manage Windows containers later.

Creating containers

The first administrative task is to create containers. Start by determining the appropriate container base image. Open an elevated **Windows PowerShell Command Prompt** window, and then use the **Get-ContainerImage** cmdlet to perform this task; the cmdlet returns a list of available base images. Make a note of the container image's name and use the **New-Container** cmdlet to create an image. For example, type the following command to create a new container named **IIS** based on the **WindowsServerCore** container base image, and then press Enter:

```
New-Container -Name IIS -ContainerImageName WindowsServerCore
```

The previous command creates a Windows Server container by default. Alternatively, type the following command to create a new Hyper-V container named **IIS** based on the **WindowsServerCore** container base image, and then press Enter:

```
New-Container -Name IIS -ContainerImageName WindowsServerCore –RunTimeType HyperV
```

Note: Similar to the default method to create a Windows Server container, you can also use the **–RunTimeType** parameter with a value of **Default** to create a Windows Server container. For example type the following code, and then press Enter:
New-Container -Name IIS -ContainerImageName WindowsServerCore –RunTimeType Default

To start the container, you must complete the creation of the container. Additionally, you must enable a network adapter in your image. Use the following procedure to complete this task:

This cmdlet adds a network adapter to your **IIS** image:

```
Add-ContainerNetworkAdapter -ContainerName IIS
```

This cmdlet returns a list of available virtual switches; note the name of an appropriate VM switch:

```
Get-VMswitch
```

This cmdlet binds the network adapter to your preselected VM switch; substitute ***SwitchName*** with the value of your preselected switch:

```
Connect-ContainerNetworkAdapter -ContainerName IIS -SwitchName SwitchName
```

Starting containers

You can use the following procedure to start your container. The first cmdlet stores details about the **IIS** container in the **$container** variable, and the second cmdlet starts the **IIS** container. In Windows PowerShell, run the following cmdlets, and then press Enter:

```
$container = Get-Container -Name IIS
Start-container $container
```

Connecting to containers

You can use PowerShell Direct to connect to a container. This is useful when you must perform a task such as installing software or configuring or troubleshooting a container. Type the following cmdlet to connect to your **IIS** container, and then press Enter:

```
Enter-PSSession -ContainerName IIS –RunAsAdministrator
```

If you are successful in connecting, the Windows PowerShell command prompt changes to include the name of the container—in this case, **IIS**. You can now use any Windows PowerShell cmdlet to add or remove roles and features, to invoke scripts, or to install apps in the **IIS** container.

Stopping containers

You can use the following procedure to stop a container. The first cmdlet stores details about the **IIS** container in the **$container** variable, and the second cmdlet stops the **IIS** container. In Windows PowerShell, run the following cmdlets, and then press Enter:

```
$container = Get-Container -Name IIS
Stop-container $container
```

Removing containers

You can use the following procedure to remove a container. The first cmdlet stores details about the **IIS** container in the **$container** variable, and the second cmdlet removes the **IIS** container. In Windows PowerShell, run the following cmdlets, and then press Enter:

```
$container = Get-Container -Name IIS
Remove-container $container -Force
```

Configuring containers

As noted earlier, when you create a container in Windows PowerShell, the default container type that is created is a Windows Server container. If your intention is to create a Hyper-V container, one method to resolve this is to remove the container and create it again with the appropriate **-RunTimeType** parameter.

As an alternative to recreating the container, you can use the following procedure to reconfigure the container as the appropriate container type.

The following cmdlet stores details about the **IIS** container in the **$container** variable; you should run this prior to either of the next two cmdlets:

```
$container = Get-Container -Name IIS
```

The following cmdlet configures the **IIS** container from a Windows Server container to a Hyper-V container:

```
Set-Container $container –RunTimeType HyperV
```

The following cmdlet configures the **IIS** container from a Hyper-V container to a Windows Server container:

```
Set-Container $container –RunTimeType Default
```

Demonstration: Installing the containers feature and preparing for Docker

- In this demonstration, you will see how to prepare for managing containers using Docker.

Demonstration Steps

1. Open an elevated Windows PowerShell Command Prompt window, by clicking **Run as administrator**.
2. Run the following commands, and then press Enter:

```
Install-WindowsFeature Containers
Restart-Computer -Force
```

3. After the host computer **LON-HOST1** restarts, sign in as **Adatum\Administrator**, with the password **Pa$$w0rd**.
4. Open an elevated Windows PowerShell Command Prompt window, by clicking **Run as administrator** and run the following commands.

```
Invoke-WebRequest "https://get.docker.com/builds/Windows/x86_64/docker-1.12.0.zip" -
OutFile "$env:TEMP\docker-1.12.0.zip" -UseBasicParsing
Expand-Archive -Path "$env:TEMP\docker-1.12.0.zip" -DestinationPath $env:ProgramFiles
 [Environment]::SetEnvironmentVariable("Path", $env:Path + ";C:\Program
Files\Docker\", [EnvironmentVariableTarget]::Machine)
```

5. Close and then reopen the command prompt.
6. In the Windows PowerShell Command Prompt window, run the following commands:

```
dockerd.exe --register-service
Start-Service docker
docker pull microsoft/windowsservercore
```

Note: This will take some time to download the image.

Lesson 3

Installing, configuring, and managing containers by using Docker

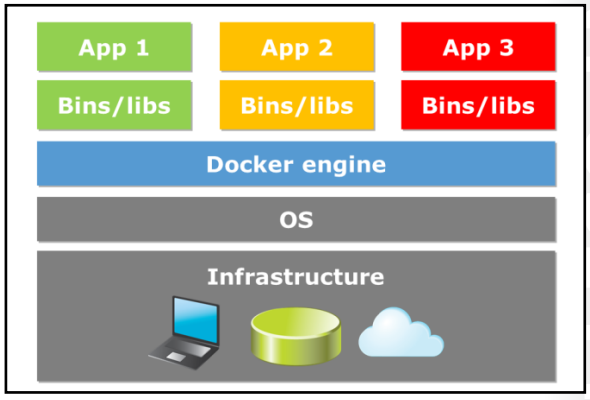
After completing this lesson, students will be able to install, configure, and manage containers by using Docker.

Lesson Objectives

After completing this lesson, you will be able to:

- Define Docker.
- Describe support for Docker on Windows Server 2016.
- Describe usage scenarios for Docker.
- Explain how to install and configure Docker.
- Describe management with Docker.
- Describe the Docker Hub.
- Describe how Docker integrates with Azure.
- Deploy Hyper-V containers by using Docker.

What is Docker?



Docker is a collection of open source tools, solutions, and cloud-based services that provide a common model for packaging, or *containerizing*, app code into a standardized unit for software development. This standardized unit, also called a *Docker container*, is software wrapped in a complete file system that includes everything it needs to run: code, runtime, system tools, and system libraries, or anything you can install on a server.

Supporting the Docker container is the core of the Docker platform, or the *Docker Engine*. This in-host daemon is a lightweight runtime environment that communicates with the *Docker client* to run commands to build, ship, and run Docker containers. This guarantees that the app always runs the same, regardless of the environment from which it is running.

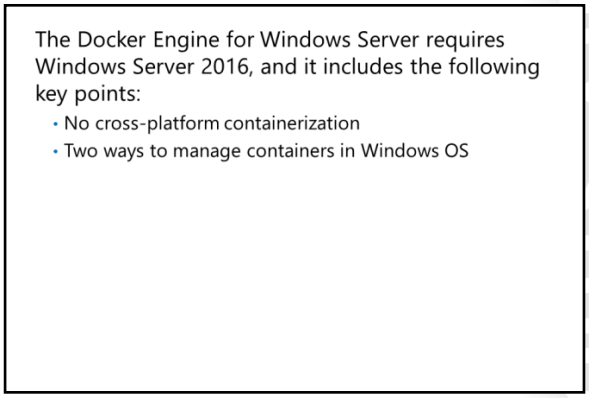
Docker containers have similar resource isolation and allocation benefits as VMs, but they use a different architectural approach that allows them to be more portable and efficient. These containers include the app and all of its dependencies, but share the kernel with other containers. Each Docker container runs as an isolated process in the user space on the host OS.

Docker containers are based on open standards that allow containers to run on all major Linux distributions and Microsoft OSs with support for every infrastructure. Because they are not tied to any specific infrastructure, Docker containers can run on any computer, on any infrastructure, and in any cloud.

To guarantee the packaging format remains universal, Docker recently organized the Open Container Initiative, aiming to ensure that container packaging remains an open industry standard with Microsoft as one of the founding members. Microsoft is collaborating with Docker with the aim of enabling developers to create, manage, and deploy both Windows Server and Linux containers by using the same Docker tool set. Developers who target Windows Server will no longer have to make a choice between using the vast range of Windows Server technologies and building containerized apps. By contributing to the Docker project, Microsoft supports using the Docker tool set to manage Windows Server containers and Hyper-V containers.

Docker support on Windows Server 2016

Until recently, it was not possible to use the Windows Server platform to host the Docker Engine without adding an additional layer of virtualization. This changed with the release of Windows Server 2016, which provides a built-in, native Docker daemon for Windows Server hosts. With this component in Windows Server 2016, you can use Docker containers, tools, and workflows in production Windows environments.



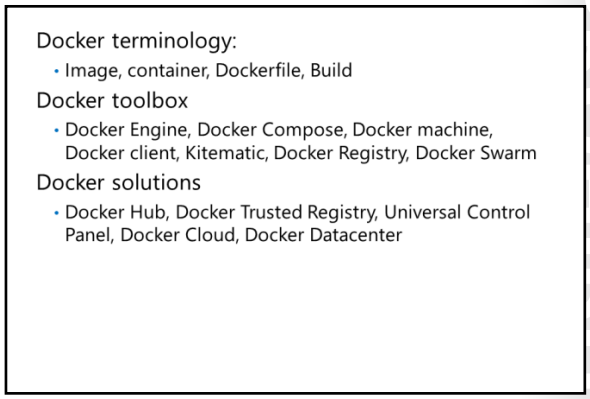
The Docker Engine for Windows Server requires Windows Server 2016, and it includes the following key points:

- No cross-platform containerization. There is currently no method to present the appropriate kernel to a container from another platform. In other words, Windows containers require a Windows Docker host, and Linux containers require a Linux Docker host.
- Two ways to manage containers in the Windows OS. You can create and manage Windows containers by using the Docker tool set or Windows PowerShell. However, containers that are created with Windows PowerShell cannot be managed with Docker, and containers that are created with the Docker tool set cannot be managed with Windows PowerShell.

Docker components

It is important to understand how Docker works and some basic Docker terminology; some of these are redefined from earlier to provide clarity that is specific to Docker:

- *Image*. A stateless collection of root file system changes in the form of layered file systems that are stacked on one another.
- *Container*. A runtime instance of an image, consisting of the image, its operating environment, and a standard set of instructions.



- *Dockerfile*. A text file that contains the commands that need to run to build a Docker image.
- *Build*. The process of building Docker images from a **Dockerfile** and any other files in the directory where the image is being built.

Docker toolbox

The Docker toolbox is a collection of Docker platform tools that make building, testing, deploying, and running Docker containers possible. These tools include:

- *Docker Engine*. This is a lightweight runtime environment for building and running Docker containers. The Docker Engine includes an in-host daemon (Linux service) that you communicate with by using the Docker client for building, deploying, and running containers.
- *Docker Compose*. This enables you to define a multiple-container app together with any dependencies so that you can run it with a single command. Docker Compose lets you specify the images your app will use with any necessary volumes or networks.
- *Docker Machine*. This enables you to provision Docker hosts by installing the Docker Engine on a computer in your datacenter or at a cloud provider. Docker Machine also installs and configures the Docker client so that it can talk with the Docker Engine.
- *Docker client*. This includes a command shell that is preconfigured as a Docker command-line environment.
- *Kitematic*. This GUI can help you to quickly build and run Docker containers and to find and pull images from the Docker Hub.
- *Docker Registry*. This open source app forms the basis for the Docker Hub and Docker Trusted Registry.
- *Docker Swarm*. This native clustering capability allows you to combine multiple Docker Engines into a single virtual Docker Engine.

You can download and install Docker software on various platforms, including Windows, Linux, and Mac OS X. After you install Docker software on your computer, you can then proceed to build images and tags and push or pull them to the Docker Hub.

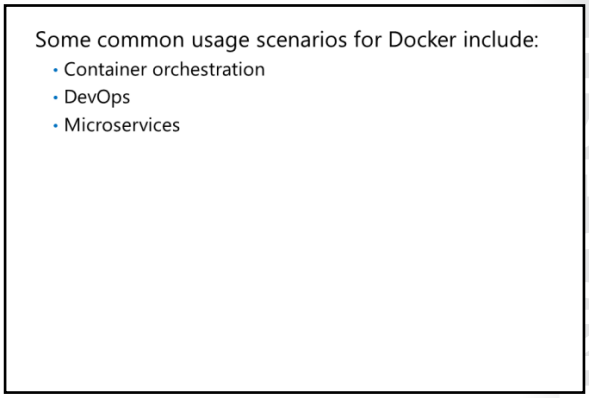
Docker solutions

The software in the Docker toolbox is not all the Docker platform has to offer. The following Docker solutions are also key parts of what makes Docker so powerful for DevOps:

- *Docker Hub*. This is a cloud-hosted service where you can register your Docker images and share them with others.
- *Docker Trusted Registry*. This private, dedicated image registry lets you store and manage images on-premises or in a virtual private cloud.
- *Universal Control Panel*. You can use this to manage Docker apps regardless of whether they are running on-premises or within a virtual private cloud.
- *Docker Cloud*. With this cloud-hosted service, you can directly deploy and manage your Docker apps.
- *Docker Datacenter*. The latest addition to the stable of Docker solutions, DDC is an integrated, end-to-end platform for deploying Containers as a Service on-premises or in a virtual private cloud. The self-service capabilities of DDC make it easy for developers to build, test, deploy, and manage agile apps.

Usage scenarios

As organizations adopt containers, they will discover the challenge of deploying dozens, hundreds, or thousands of containers that make up an app. Tracking and managing deployment requires advanced management and orchestration.



DevOps

The Docker platform provides developers with tools and services that they can use to:

- Build and share images through a central repository of images.
- Collaborate on developing containerized apps by using version control.
- Manage infrastructure for apps.

Docker helps developer teams to rapidly build, test, deploy, and run distributed apps and services at any scale. Because containerizing apps eliminates the problem of troubleshooting issues with software dependencies and differences between host environments, Docker increases developer productivity and lets you quickly move apps from development to test to production, and you can easily roll apps back if further remediation is necessary.

Another significant achievement is that Docker for Windows supports *volume mounting*, which means the container can see your code on your local device. To achieve this, the tool builds a connection between the container and the host. Effectively, this enables *edit and refresh* scenarios for development.

With Docker for Windows, you can now use Docker tools for Microsoft Visual Studio in the following scenarios:

- Docker assets for Debug and Release configurations are added to the project.
- A Windows PowerShell script is added to the project to coordinate the build and composition of containers, enabling you to extend them while keeping the Visual Studio designer experiences.
- With volume mapping configured, F5 in Debug config starts the Windows PowerShell script to build and run your **docker-compose.debug.yml** file.
- F5 in Release config starts the Windows PowerShell script to build and run your **docker-compose.release.yml** file, which allows you to verify and push an image to your Docker Registry for deployment to another environment.

Microservices

Another benefit of using Docker containers is that they can be individually scaled and updated. *Microservices* are an approach to app development where every part of an app deploys as a fully self-contained component. For example, the subsystem of an app that receives requests from the Internet might be separate from the subsystem that places the request into a queue for a backend subsystem that drops them into a database.

When an app is constructed by using microservices, each subsystem is a microservice. In a development or test environment on a single machine, microservices might each have one instance, but when the app runs in a production environment, each microservice can scale out to multiple instances, spanning across a cluster of servers based on resource demands.

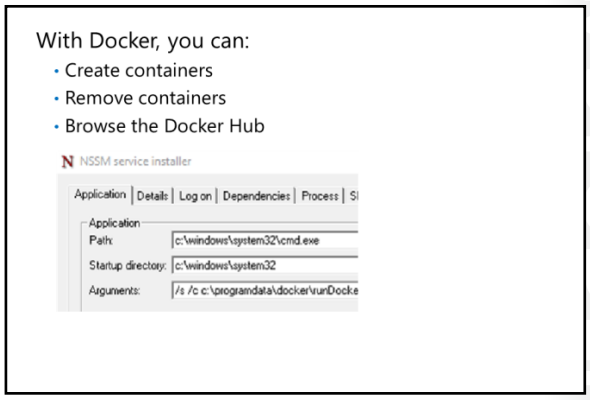
Some of the benefits of using Docker containers in this scenario include:

- Each microservice can quickly scale out to meet increased load.
- The namespace and resource isolation of containers also prevents one microservice instance from interfering with others.
- The Docker packaging format and app programming interfaces (APIs) unlock the Docker ecosystem for the microservice developer and app operator.

With a good microservice architecture, you can solve the management, deployment, orchestration, and patching needs of a container-based service with reduced risk of availability loss while maintaining high agility.

Installing and configuring Docker

Windows Server 2016 does not include the Docker Engine, and you to install and configure it separately. The steps to run the Docker Engine on the Windows OS vary from those on Linux. These instructions detail how to install and configure the Docker Engine on Windows Server 2016 and on Nano Server, in addition to instructions on how to install the Docker client. As a side note, the Docker Engine and the Docker client are now separate installations.



Note: You must enable the Windows container feature before Docker can create and manage Windows containers. For information on enabling this feature, refer to the instructions to deploy Windows containers earlier in this module.

Installing Docker on Windows Server 2016

Because Docker is not included with Windows Server 2016, you must download it from the Internet to deploy the software. At an elevated Windows PowerShell command prompt, use the following procedure to install Docker:

1. Download **Dockerd.exe** from **https://aka.ms/tp5/dockerd**, and place it in the ***%SystemRoot%*\System32** directory on your container host. For example type the following, and then press Enter:

```
Invoke-WebRequest -Uri “https://aka.ms/tp5/dockerd” -OutFile
“$env:SystemRoot\System32\dockerd.exe”
```

2. Create a directory named ***%ProgramData%*\Docker**, and then create a file named **runDockerDaemon.cmd** within this directory. For example, type the following, and then press Enter:

```
New-Item -ItemType File -Path %ProgramData%\Docker\runDockerDaemon.cmd -Force
```

3. Using a text editor, copy the following text into the **runDockerDaemon.cmd** file, and then press Enter:

```
@echo off
set certs=%ProgramData%\docker\certs.d
if exist %ProgramData%\docker (goto :run)
mkdir %ProgramData%\docker
:run
if exist %certs%\server-cert.pem (if exist %ProgramData%\docker\tag.txt (goto
:secure))
if not exist %systemroot%\system32\dockerd.exe (goto :legacy)
dockerd -H npipe://
goto :eof
:legacy
docker daemon -H npipe://
goto :eof
:secure
if not exist %systemroot%\system32\dockerd.exe (goto :legacysecure)
dockerd -H npipe:// -H 0.0.0.0:2376 --tlsverify --tlscacert=%certs%\ca.pem --
tlscert=%certs%\server-cert.pem --tlskey=%certs%\server-key.pem
goto :eof
:legacysecure
docker daemon -H npipe:// -H 0.0.0.0:2376 --tlsverify --tlscacert=%certs%\ca.pem--
tlscert=%certs%\server-cert.pem--tlskey=%certs%\server-key.pem
```

4. The NSSM installer creates and configures the Docker service. Download it from **https://nssm.cc/release/nssm-2.24.zip**. For example, type the following, and then press Enter:

```
Invoke-WebRequest -Uri “https://nssm.cc/release/nssm-2.24.zip” -OutFile
“$env:ALLUSERSPROFILE\nssm.zip”
```

5. Extract **Nssm.exe** from the contents of the compressed package. For example, type the following, and then press Enter:

```
Expand-Archive -Path $env:ALLUSERSPROFILE\nssm.zip $env:ALLUSERSPROFILE
```

6. Copy **nssm-2.24\win64\nssm.exe** from the extracted location into the ***%SystemRoot%*\System32** directory. For example, type the following, and then press Enter:

```
Copy-Item $env:ALLUSERSPROFILE\nssm-2.24\win64\nssm.exe $env:SystemRoot\system32
```

7. Run **Nssm.exe install** to configure the Docker service. For example, type the following, and then press Enter:

```
Start-Process nssm install
```

8. In the **NSSM service installer** dialog window, on the **App** tab, type the following data in the appropriate field:
   - Path: **C:\Windows\System32\cmd.exe**
   - **Startup Directory**: C:\Windows\System32
   - **Arguments**: /s /c C:\ProgramData\docker\runDockerDaemon.cmd
   - **Service Name**: Docker
9. On the **Details** tab, type the following data in the appropriate field:
   - **Display name**: Docker
   - **Description**: The Docker daemon provides management capabilities of containers for Docker clients.

10. On the **IO** tab, type the following data in the appropriate field:
    - **Output (stdout)**: C:\ProgramData\docker\daemon.log
    - **Error (stderr)**: C:\ProgramData\docker\daemon.log
11. Click **Install service**.

Note: The Docker daemon is now registered as a Windows service and will start when Windows Server starts. If you wish to enable remote Docker management, you also need to open the inbound TCP port 2376.

Installing Docker on Nano Server

Similar to Windows Server 2016, Docker is not included with Nano Server, and you must download it from the Internet to deploy the software. At an elevated Windows PowerShell command prompt, use the following procedure to install Docker:

1. Download **Docker.exe** from **https://aka.ms/tp5/dockerd**, and then place it in the ***%SystemRoot%*\System32** directory on your container host that is running Nano Server. Because Nano Server does not support the **Invoke-WebRequest** cmdlet, you will need to download the file to another computer, and then copy it to your container host.
2. Create a directory named ***%ProgramData%*\Docker**, and then create a file named **runDockerDaemon.cmd** within this directory. For example, type the following, and then press Enter:

```
New-Item -ItemType File -Path %ProgramData%\Docker\runDockerDaemon.cmd -Force
```

3. Using a text editor from another computer, copy the following text into the **runDockerDaemon.cmd** file, and then press Enter:

```
@echo off
set certs=%ProgramData%\docker\certs.d
if exist %ProgramData%\docker (goto :run)
mkdir %ProgramData%\docker
:run
if exist %certs%\server-cert.pem (if exist %ProgramData%\docker\tag.txt (goto
:secure))
if not exist %systemroot%\system32\dockerd.exe (goto :legacy)
dockerd -H npipe://
goto :eof
:legacy
docker daemon -H npipe://
goto :eof
:secure
if not exist %systemroot%\system32\dockerd.exe (goto :legacysecure)
dockerd -H npipe:// -H 0.0.0.0:2376 --tlsverify --tlscacert=%certs%\ca.pem --
tlscert=%certs%\server-cert.pem --tlskey=%certs%\server-key.pem
goto :eof
:legacysecure
docker daemon -H npipe:// -H 0.0.0.0:2376 --tlsverify --tlscacert=%certs%\ca.pem--
tlscert=%certs%\server-cert.pem--tlskey=%certs%\server-key.pem
```

4. Create a scheduled task, which will start the Docker daemon when the Nano Server starts. For example, type the following, and then press Enter:

```
# Creates a scheduled task to start docker.exe at computer start up.
$dockerData = "$($env:ProgramData)\docker"
$dockerDaemonScript = "$dockerData\runDockerDaemon.cmd"
$dockerLog = "$dockerData\daemon.log"
$action = New-ScheduledTaskAction -Execute "cmd.exe" -Argument "/c
$dockerDaemonScript > $dockerLog 2>&1" -WorkingDirectory $dockerData
$trigger = New-ScheduledTaskTrigger -AtStartup
$settings = New-ScheduledTaskSettingsSet -Priority 5
Register-ScheduledTask -TaskName Docker -Action $action -Trigger $trigger -Settings
$settings -User SYSTEM -RunLevel Highest | Out-Null
Start-ScheduledTask -TaskName Docker
```

Note: If you wish to enable remote Docker management, you also need to open the inbound TCP port 2376. You can use the **netsh** command to enable this port on Nano Server.

Installing the Docker client

The Docker client includes a command shell that is preconfigured as a Docker command-line environment (CLI), and it should install on the container host or any other system where you will run Docker CLI commands. At an elevated Windows PowerShell command prompt, use the following procedure to install the Docker client:

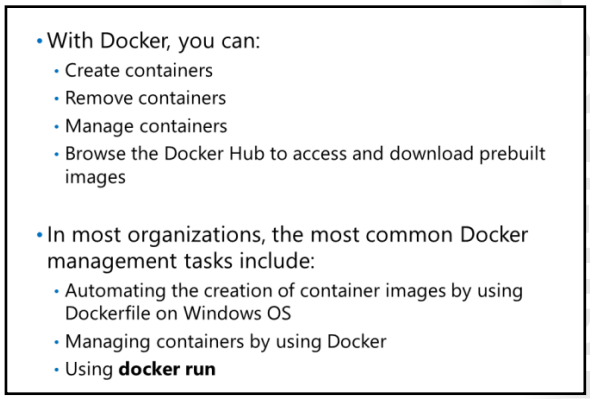
- Download **Docker.exe** from **https://aka.ms/tp5/docker**, and then place it in the ***%SystemRoot%*\System32** directory on your container host or another system for running the CLI. For example, type the following, and then press Enter:

```
Invoke-WebRequest -Uri “https://aka.ms/tp5/docker” -OutFile
“$env:SystemRoot\system32\docker.exe”
```

Note: While Nano Server does not support the **Invoke-WebRequest** cmdlet, you will need to download the file to another computer, and then copy it to your Nano Server container host.

Overview of management with Docker

As mentioned earlier in the module, you can choose to manage Windows containers by using Windows PowerShell or Docker. The advantage of using Docker on Windows Server is that Docker is an industry-standard container deployment and management tool that enables administrators with skills in container management on other OSs to manage your Windows containers.



With Docker, you can create containers, remove containers, manage containers, and browse the Docker Hub to access and download prebuilt images. In most organizations, the most common management tasks that use Docker include:

- Automating the creation of container images by using **Dockerfile** on Windows OSs.

- Managing containers by using Docker.
- Using **docker run**.

Automating the creation of container images by using Dockerfile on Windows

The Docker Engine includes tools for automating the creation of container images. While you can create container images manually, adopting an automated image creation process provides many benefits, including:

- Storing container images as code.
- Rapid and precise recreation of container images for maintenance and upgrade purposes.
- Continuous integration between container images and the development cycle.

The Docker components that drive this automation are the **Dockerfile** and the **docker build** command.

- **Dockerfile**. This text file contains the instructions needed to create a new container image. These instructions include identification of an existing image to use as a base, commands to run during the image creation process, and a command that will run when new instances of the container image deploy.
- **Docker build**. This Docker Engine command consumes a **Dockerfile**, and then triggers the image creation process. In its most basic form, a **Dockerfile** can be very simple.

The following example creates a new image, which includes IIS, and a "Hello world" site.

Dockerfile sample

```
# Indicates that the windowsservercore image will be used as the base image
FROM windowsservercore

# Metadata indicating an image maintainer.
MAINTAINER LJackman@adatum.com

# Uses dism.exe to install the IIS role.
RUN dism.exe /online /enable-feature /all /featurename:iis-webserver /NoRestart

# Creates an html file and adds content to this file.
RUN echo "Hello World - Dockerfile" > c:\inetpub\wwwroot\index.html

# Sets a command or process that runs each time a container is run from the new image.
CMD [ "cmd" ]
```

 **Additional Reading:** For more information on other examples of Dockerfiles for Windows, refer to: "Dockerfile for Windows Repository" at:: http://aka.ms/kq8gak

Dockerfile instructions provide the Docker Engine with the steps necessary to create a container image. These instructions perform in order, one by one.

 **Additional Reading:** For more information on the complete list of **Dockerfile** instructions, refer to: "Dockerfile reference" at: http://aka.ms/wrccuy

You can also specify Windows PowerShell commands to run in a **Dockerfile** by using the **RUN** operation. The following is a list of options for using Windows PowerShell commands in a **Dockerfile**:

- You can use Windows PowerShell and the **Invoke-WebRequest** command to gather information or files from a web service. For example, you could download the Python programming language from the vendor's website for installation in a new image.
- You can use Windows PowerShell to download files during the image creation process by using the .Net WebClient library. This method is shown to increase download performance.

Note: Nano Server does not currently support the .Net WebClient.

- You might consider it helpful to copy a Windows PowerShell script into the containers being used during the image creation process, and then run the script from within the container. For example, the following command copies a Windows PowerShell script from the build machine into the container by using the **ADD** instruction, and it then runs the script by using the **RUN** instruction. Type the following, and then press Enter:

```
FROM windowsservercore
ADD script.ps1 /windows/temp/script.ps1
RUN powershell.exe -executionpolicy bypass c:\windows\temp\script.ps1
```

After you create a **Dockerfile** and save it to disk, you can use **docker build** to create the new image. The **docker build** command takes several optional parameters and a path to the **Dockerfile**. For example, the following command creates an image named **IIS**:

```
docker build -t iis .
```

Additional Reading: For more information on **docker build**, including a list of all build options, refer to: "Docker Build" at: http://aka.ms/u29exr

Additional Reading: You can use several methods to optimize the Docker build process and the resulting Docker images. For more information on how the Docker build process operates and the tactics that you can use for optimal image creation with Windows containers, refer to: "Optimize Windows Dockerfiles" at: http://aka.ms/nrgyui

Managing containers by using Docker

You can use Docker to support a container environment. After you install Docker, use the following commands to manage your containers:

- **Docker images**. This lists the installed images on your container host. As you might recall, you use container images as a base for new containers. The Windows PowerShell cmdlet equivalent to this command is **Get-ContainerImage**.
- **Docker run**. This creates a container by using a container image. For example, the following command creates a container named **IIS** based on the Windows Server Core container image:

```
docker run --name IIS -it windowsservercore
```

The Windows PowerShell cmdlet equivalent to this command is **New-Container**.

- **Docker commit**. This commits the changes you made to the container and creates a new container image. For example, the following command creates a new container image named **WinSvrCoreIIS** based on the **IISBase** base image.

```
docker commit iisbase WINSVRCOREIIS
```

- **Docker stop**. This stops a container. The Windows PowerShell cmdlet equivalent to this command is **Stop-Container**.
- **Docker rm**. This removes a container. The Windows PowerShell cmdlet equivalent to this command is **Remove-Container**.

 **Additional Reading:** For more information about administering containers on Windows Server by using Docker, refer to: "Windows Containers Quick Start" at: http://aka.ms/xl3mdn

Using docker run

The **docker run** command is the most commonly used Docker command. As part of creating a container, you can use this command to define the container's resources at runtime.

Docker runs processes in isolated containers. These containers are simply a process that is running on a host. The host might be local or remote. When you run **docker run**, the container process that runs is isolated; for example, a separate file system, networking, and process tree from the host. During execution, the **docker run** command must specify an image from which to derive the container. When developing an image, you can define image defaults that relate to:

- Detached or foreground running.
- Container identification.
- Network settings.
- Runtime constraints on CPU and memory.

With **docker run**, you can add to or override the image defaults that were configured during image development. Additionally, you can override nearly all the defaults that the Docker runtime itself set. The ability to override image and Docker runtime defaults is why **docker run** has more options than any other Docker command.

The optional **cmd** switch opens an interactive session with the container to include a default command or other options. While you might have provided a default **COMMAND** by using the **Dockerfile CMD** instruction during image creation, you can override that **CMD** instruction when running a container from the image by specifying a new **COMMAND**. The Windows PowerShell cmdlet equivalent to this command is **Start-Container**. To end an interactive session with the container, type **exit**.

 **Note:** You can now use Windows PowerShell commands to install the required roles and features within a container. For example, **powershell.exe Install-WindowsFeature web-server** installs the IIS components within your container.

The Docker platform simplifies the experience of working across container options. An app that was developed by using Windows Server containers can deploy as a Hyper-V container without change. In fact, managing Hyper-V containers with Docker is almost identical to managing Windows Server containers with Docker. When you create a Hyper-V container by using **docker run**, you would include the **--isolation=hyperv** parameter.

For example, the following command starts a Windows Server container and hosts a long-running ping process:

```
docker run -d windowsservercore ping localhost –t
```

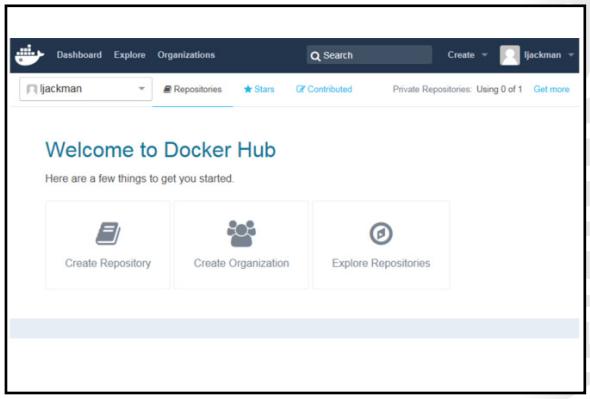
In contrast, this example also starts a Hyper-V container and hosts a long-running ping process:

```
docker run -d --isolation=hyperv nanoserver ping -t localhost
```

Additional Reading: For more information on using the **docker run** command to define a container's resources at runtime, refer to: "Docker run reference" at: http://aka.ms/Xjef2h

Overview of Docker Hub

Docker Hub is a cloud-based public registry service that the Docker company maintains for building and shipping app or service containers. It provides a centralized resource for container image discovery, distribution and change management, user and team collaboration, and workflow automation throughout the development pipeline.



Docker Hub features

Docker Hub provides the following major features and functions:

- Image repositories. Docker Hub contains images stored in repositories that you can find, manage, and push and pull images from community, official, and private image libraries to build containers. Specifically, repositories contain images, layers, and metadata about those images. The main concept of containerization is that you can build your own images based on existing images—this is known as *layers*.
- Organizations and teams. One useful aspect of private repositories is that you can share them with members of your organization or team only. Docker Hub lets you create organizations, or work groups that require user access, where you can collaborate with colleagues and manage private repositories.
- Automated builds. Automated builds automates the building and updating of images from GitHub or Bitbucket, directly on Docker Hub. It works by adding a commit hook to your selected GitHub or Bitbucket repository, triggering a build and update when you push a commit or when you make changes to the source repository.
- Webhooks. A webhook is a feature of automated builds that attaches to your repositories and allows you to trigger an event or action when an image or updated image successfully pushes to the repository. With a webhook, for example, you can specify a target URL and a JavaScript Object Notation (JSON) payload to deliver when you push the image.
- GitHub and Bitbucket integration. This allows you to add the Docker Hub and your Docker images to current workflows.

Working with image repositories

Docker Hub repositories provide a place to build and ship Docker images. These repositories enable you to share images with coworkers, customers, or the Docker community at large. You can configure Docker Hub repositories in two ways:

- Repositories. Repositories allow you to push images at will from your local Docker daemon to the Docker Hub. If you are building images internally, either on your own Docker daemon or by using your own continuous integration services, you can push them to a Docker Hub repository that you add to your Docker Hub user or organizational account.
- Automated builds. Automated builds allow you to configure GitHub or Bitbucket to trigger the Docker Hub to rebuild repositories when changes to the repository occur. If the source code for your Docker image is on GitHub or Bitbucket, you can use an Automated Build repository, which Docker Hub services build.

 **Note:** You can create public repositories that any other Docker Hub user can access, or you can create private repositories with limited access that you can manage.

Docker provides access to Docker Hub services by using four primary Docker Engine CLI commands: **docker login**, **docker search**, **docker pull**, and **docker push**.

Creating an account for sign-in

If you have not already done so, you will need to create a Docker ID to interact with your repositories on Docker Hub. To do this through Docker Hub, refer to: http://aka.ms/Hqfvqf. After you have a Docker ID, sign in to your account from the CLI. Type the following command, and then press Enter:

```
$ docker login
```

After signing in from the command line, you can use the other Docker Engine subcommands.

 **Additional Reading:** For more information on registering a Docker ID, refer to: "Your Docker ID" at: http://aka.ms/ya2hoo

Searching for images

You can search for public repositories and images that are available on the Docker Hub in two ways. You can use the **Search** feature on the Docker Hub website, or you can use the **docker search** command from the CLI. Both of these methods will show you a list of the currently available images that match the provided keywords from the public repositories on the Docker Hub.

 **Note:** Images from a private repository do not appear in the repository search results list. To see all the repositories that you can access and their status, view the dashboard on the Docker Hub website.

Image search results are based on criteria such as image name, user name, or description. Using the search criteria "CentOS" returns the following search results from all the repositories and images:

```
$ docker search centos
NAME                      DESCRIPTION                     STARS  OFFICIAL  AUTOMATED
centos                    The official build of CentOS.   1034   [OK]
ansible/centos7-ansible   Ansible on Centos7              43                [OK]
tianon/centos             CentOS 5 and 6, created wi...   13                [OK]
...
```

In the preceding example, your search returned three results: **centos**, **ansible/centos7-ansible**, and **tianon/centos**. The second and third results signal that they originate from public repositories named **ansible** and **tianon** respectively; the forward slash (/) character separates a user's repository name from the image name. On the other hand, the first result, **centos**, does not explicitly list a repository. In this latter scenario, this means that the image originates from the trusted, top-level namespace for Official Repositories from Docker Hub.

Docker Hub contains a number of *Official Repositories*. These are public, certified repositories from vendors and contributors to Docker that you can use to build apps and services. With Official Repositories, you know that you are using an optimized and up-to-date image that experts built to power your apps.

 **Additional Reading:** For more information on the Docker repositories that the Docker Hub supports and promotes, refer to: "Official Repositories on Docker Hub" at: http://aka.ms/f7zl0h

After you locate the image you want, you can download it with the **docker pull** command from the CLI. In the following example, you download the latest image from which you can run your containers:

```
$ docker pull centos
Using default tag: latest
latest: Pulling from library/centos
f1b10cd84249: Pull complete
c852f6d61e65: Pull complete
7322fbe74aa5: Pull complete
Digest: sha256:90305c9112250c7e3746425477f1c4ef112b03b4abe78c612e092037bfecc3b7
Status: Downloaded newer image for centos:latest
```

As noted earlier, image repositories contain images, layers, and metadata about those images. Part of this metadata is a tag that you can use to label an image. For example, you could use the following command to download version 5 of centos (**centos5** is the tag labeling an image in the centos repository for a version of CentOS):

```
docker pull centos:centos5
```

Contributing to Docker Hub

While anyone can download public images from the Docker Hub registry, you must register if you want to share your own images.

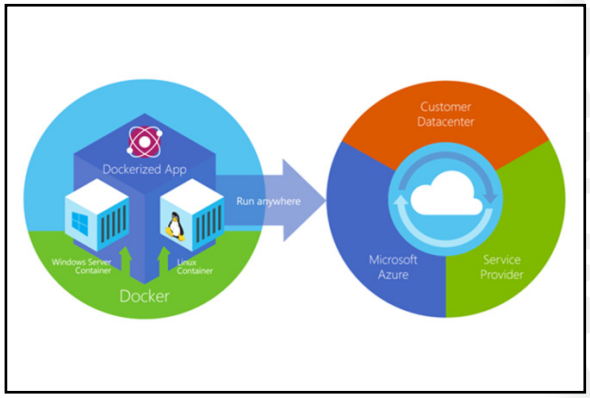
 **Additional Reading:** For more information on pushing a repository to the Docker Hub registry, refer to: "Build your own images" at: http://aka.ms/iyggmz

For example, you can push this repository and upload your image so that it is available for your teammates and the Docker Hub community to use:

```
$ docker push Docker ID/Image Name
```

Additional Reading: For more information on creating organizations and teams so that you can delegate access to colleagues for shared image repositories, refer to: "Organizations and teams" at: http://aka.ms/wzbstk

Docker with Azure



As an open source engine, Docker automates the deployment of any app as a portable, self-sufficient container that runs almost anywhere—including Azure. Typical VM images contain everything necessary to run, including the app, any dependencies, and the OS. In contrast, Docker containers include the app and some libraries, but the OS and common dependencies remain shared assets. Consequently, Docker containers are extremely lightweight compared with VM images. By making Docker containers significantly smaller than traditional VMs, more of them can run on a single host, they can start more quickly, and they are considerably more portable—these characteristics are ideal for PaaS like Azure.

With Azure, you have the flexibility to deploy Docker in a few different scenarios based on your needs:

- Docker Machine Azure driver to deploy Docker hosts within Azure.
- Azure Docker VM extension for template deployments.
- Deploy an Azure container service cluster.

Using Docker Machine Azure driver to deploy Docker hosts on Azure

You can use the Docker Machine Azure driver to deploy Docker hosts on Azure. Docker is one of the most popular virtualization approaches that use Linux containers rather than VMs as a way of isolating app data and computing on shared resources. One common scenario that uses this approach is when you need to prototype an app quickly.

You can create Docker host VMs on Azure by using the **docker-machine create** command with the **-d azure** Azure driver option. For example, you can use the following command for testing a web app; the command creates a new VM named **DockerVM**, opens port 80 to the Internet on the VM, and it enables ops as the sign-in user for Secure Shell (SSH):

```
docker-machine create -d azure \
  --azure-ssh-user ops \
  --azure-subscription-id Azure_Subscription_ID \
  --azure-open-port 80 \
  machine
```

Additional Reading: For more information on using Docker Machine to create new Docker host VMs in Azure for your Linux containers, refer to: "Use Docker Machine with the Azure Driver" at: http://aka.ms/wjudik

Using the Azure Docker VM extension for template deployments

For a template-based deployment, you can use the Docker VM extension for Azure VMs. This approach allows you to integrate with Azure Resource Manager template deployments and includes all of the related benefits such as role base access, diagnostics, and post-deployment configuration. The Azure Docker VM extension installs and configures the Docker daemon, the Docker client, and Docker Compose in your Linux VM.

You can also use the extension to define and deploy container apps by using Docker Compose. Azure Resource Manager templates enable you to deploy a solution throughout the development lifecycle and have confidence that your resources deployed in a consistent state. Using the Azure Docker VM extension is well suited for robust development or production environments because you have some additional control compared with simply using Docker Machine or manually creating a Docker host.

Using Azure Resource Manager, you can create and deploy templates that define the entire structure of your environment, such as the Docker hosts, storage, role-based access controls (RBACs), and diagnostics. The advantage of using Resource Manager templates over simply using Docker Machine is that you can define additional Docker hosts, storage, and access controls, and you can reproduce deployments as needed.

Additional Reading: For more information, refer to: "Azure Resource Manager overview" at: http://aka.ms/p35huz

Deploying an Azure Container Service cluster

The Azure Container Service provides rapid deployment of popular open source container clustering and orchestration solutions. With Azure Container Service, you can deploy clusters such as a Docker Swarm cluster by using Azure Resource Manager templates or the Azure portal. Docker Swarm clusters are ideal for production-ready, scalable deployments that take advantage of the additional scheduling and management tools that Docker Swarm provides.

Docker Swarm uses the native Docker API to provide an environment for deploying containerized workloads across a pooled set of Docker hosts. During the deployment of Docker Swarm clusters, you will use the Azure compute resource and Azure VM Scale Sets to manage a collection of VMs as a set.

Additional Reading: For more information on using the Azure Container Service to deploy Docker Swarm clusters, refer to: "Deploy an Azure Container Service cluster" at: http://aka.ms/F8azgy

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

Statement	Answer
Docker is a graphical management tool that you can use to manage Hyper-V containers in Windows Server 2016.	

Demonstration: Deploying Hyper-V containers by using Docker

The physical computer **20740A-LON-HOST1** is required to complete this demonstration. This should be running from the last demonstration.

Demonstration Steps

Install base OS images

- In an elevated **Windows PowerShell** window, type the following commands, and then press Enter:

```
Docker images
```

Download a prebuilt Microsoft and IIS Docker image

1. In the **Windows PowerShell** window, type the following command, and then press Enter:

```
Docker search Microsoft
```

2. In the **Windows PowerShell** window, type the following command, and then press Enter:

```
docker pull microsoft/iis
```

3. In the **Windows PowerShell** window, type the following commands, and then press Enter:

```
docker images
```

Deploy a new container with the prebuilt image

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

```
docker run -d -p 80:80 microsoft/iis ping -t localhost
```

Note: This command runs the IIS image as a background service (**-d**). It also configures networking such that port 80 of the container host maps to port 80 of the container.

Manage the container

- In the **Windows PowerShell** window, run the following command to view the running containers:

```
docker ps
```

Module Review and Takeaways

Review Questions

Question: When creating a virtual hard disk for Nano Server by using the **New-NanoServerImage** Windows PowerShell cmdlet, when do you use the **-Guestdrivers** switch?

Question: When using the Nano Server Recovery Console, which two fundamental components can you configure?

Question: When configuring Windows Server containers, what Windows PowerShell cmdlet do you use to create a container and what is the equivalent Docker command?

Module 7

Overview of high availability and disaster recovery

Contents:

Module Overview

IT solutions are a critical business tool in most organizations. Outages of even a few hours reflect poorly upon IT departments, and can result in sales losses or damage to business reputation. Providing high availability is important for any organization that wants to provide continuous services to its users. Failover clustering is one of the main technologies in Windows Server 2016 that can provide high availability for various applications and services. In this module, you will learn about failover clustering, failover clustering components, and implementation techniques.

Backing up Windows Server data on a regular basis is an essential part of your general Windows Server administration. Data backup enables you to restore the data at a later date, either in the event of data loss, corruption, or for test purposes. Backing up Windows Server 2016 is a relatively simple task, but factors such as backup hardware, backup windows durations, and restore constraints determine the backup regime. Service Level Agreements (SLAs) play a major part in determining backup regimes. For example, if your SLA for Windows Server specifies that operating system services must not be down for more than one hour during a disaster, you must design your backup regime to perform with this goal in mind.

This module describes the high-availability technology built into Windows Server 2016, and some of the outside factors that affect highly available solutions. Furthermore, the module describes backup and restore technologies for protecting data in Windows Server 2016.

Objectives

After completing this module, you will be able to:

- Define levels of availability.
- Plan high availability and disaster recovery solutions with Hyper-V virtual machines.
- Backup and restore data by using Windows Server Backup.
- Describe high availability with failover clustering in Windows Server 2016.

Lesson 1
Defining levels of availability

High availability helps ensure that Windows Server operating systems can survive the failure of a single server, or even multiple servers. When an application requires high availability, you must consider more than just the application components. All of the infrastructure and services that the application relies on also must be highly available. Consider the following additional components when planning for high availability.

For example, an organization might deploy multiple servers that run appropriate applications that provide high availability. However, if you connect all the servers to a single network switch, the network switch represents a single point of failure., If the switch is not operational, none of the client computers can connect to any of the servers, which makes the solution not highly available.

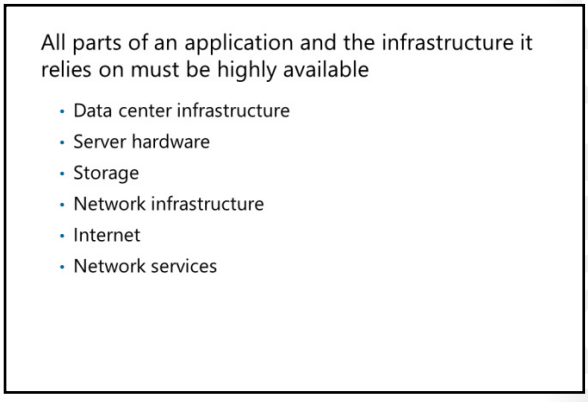
Lesson Objectives

After completing this lesson, you will be able to:

- Describe high availability.
- Describe continuous availability.
- Describe business continuity.
- Create a disaster recovery plan.
- Describe high availability for networking.
- Describe high availability for storage.
- Describe high availability computer or hardware functions.

What is high availability?

High availability for an IT solution describes components and technologies that need to be redundant so that the solution continues to work in a case of failure of any of the solution's components. IT consultants who design the solution have to ensure that the solution has "no single point of failure," which means that no matter which solution component fails, the solution continues to work, and data and services are available for the users.



Data center infrastructure

The room that stores the server must have sufficient power and cooling capacity, and that capacity also must be highly available. You can make power highly available by ensuring that an alternate power source, such as a battery or a generator, is available when the electrical utility experiences outages. You can make cooling capacity highly available by using multiple cooling units with sufficient capacity to keep the data center cool when one unit fails. In cases of catastrophic failure, you can use an alternate data center location.

Server hardware

For server hardware to be highly available, there must be redundant components. Redundant components can include power supplies, network adapters, processors, and memory. Error-correction code (ECC) memory helps to resolve minor memory errors.

Storage

To make storage highly available on a single server, you can use Redundant Array of Independent Disks (RAID). RAID uses parity information to ensure that a server can survive the loss of at least one hard drive, without losing any data. If multiple servers are available, you can replicate data between servers. This enables the data to survive the loss of an entire server, rather than just a hard drive.

Network infrastructure

To make a local area network (LAN) highly available, you must introduce redundant components. Within a LAN, this typically means redundant switches. Even moderately priced switches include redundant configurations. To make the network connectivity for any individual computer fault tolerant, you must configure redundant network interface cards on the computer. This is a standard feature in most mid-level and high-level servers. High availability for a wide area network (WAN) is typically the responsibility of the WAN service provider. However, if you are using private links for your WAN, you can create redundant paths through the WAN.

Internet connectivity

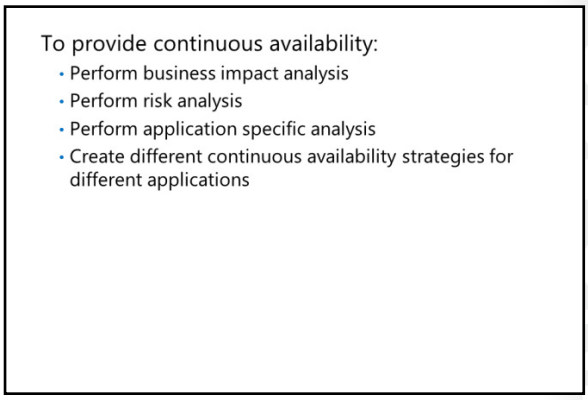
For highly available Internet access, you must have redundant Internet connectivity. Ideally, you should use two different Internet service providers (ISPs) and two different physical connectivity methods. For example, one ISP could be land based, and the other wireless. If you use these methods, it is unlikely that a problem affecting one ISP would affect the other. Many firewalls and routers are capable of using one connection for Internet connectivity and failing over to another if the primary service fails. For incoming email, you must use multiple mail exchange (MX) resource records, with one record pointing to the IP address allocated by each ISP.

Network services

Active Directory Domain Services (AD DS) and Domain Name System (DNS) service are the two services that must be highly available to support the infrastructure services in the organizations. To make AD DS servers highly available, you should have multiple domain controllers and global catalog servers. Depending on the size of a location, multiple domain controllers and global catalog servers may reside in a single location. To make internal DNS servers highly available, you must have multiple DNS servers with DNS information synchronized between them. By default, the DNS zones for AD DS are integrated and replicated among all DNS servers in the forest.

What is continuous availability?

Continuous availability results from technologies and procedures that ensure that an IT solution continues to work in a case of failure scenarios and planned maintenance downtime. Compared with high availability due to planned unavailability because of maintenance procedures, hardware upgrades, or updating an operating system, continuous availability means that a solution should continue to work during the planned downtime.



To provide continuous availability for your organization, you should devise strategies for implementing continuous availability by collecting data from:

- Business impact analysis. Business impact analysis determines an organization's critical business processes and the potential damage or loss that can result from their disruption or failure.
- Risk analysis. Risk analysis identifies risks and their probability of occurrence. Risk analysis also identifies single points of failure, such as an organization's disk drives, network switches, storage, or power supply.

There is a range of strategies for implementing continuous availability. Each strategy is specific for different applications. Continuous availability provides access to data and services during server maintenance tasks so the clients are not interrupted. Therefore, each administrator in the organization, such as the Exchange administrator, SQL Server administrator, and SharePoint administrator, must be involved in planning the continuous availability strategy by using procedures to maintain and update servers and applications without affecting the user experience.

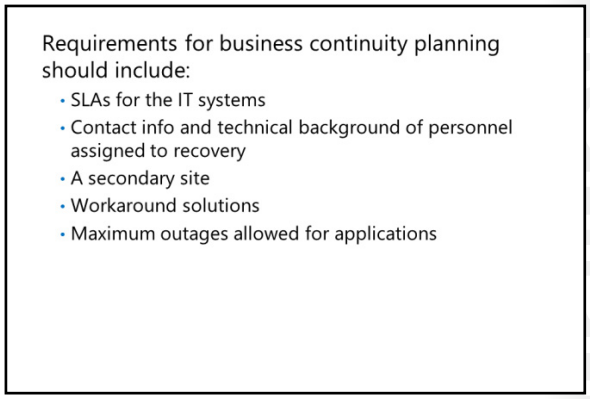
Note: Continuous availability requires a full-continuity provision strategy and often has a high cost. It is necessary where the impact and risks are great, and where the organization determines that continuous availability is business critical.

What is business continuity?

You plan for business continuity during an initial analysis phase. Business planning requirements differ depending on the organization's structure.

Here are several requirements that you should consider for your business continuity plan:

- SLAs for IT systems, both hardware and software.
- Contact information and technical details of backup administrators.
- A secondary site from which you can access critical applications and application data for critical business functions.



- Workaround solutions.
- Maximum outage time allowed for your applications.

Creating a solid list of requirements should involve not only IT staff, but also business managers and other high-level decision makers. Business managers should know the risks, and should understand how any failure can affect business. Business managers also need to decide which applications are critical for their business, and likely decide what recovery times must be to help define the appropriate backup and restore strategy.

Note: Organizations have different requirements, based on their business infrastructure and goals. The requirements for business continuity planning should not be static. Rather, you should evaluate and update them regularly, and you should reevaluate your planning every few months

To plan your strategies for implementing business continuity, you should collect data from:

- Business impact analysis. Business impact analysis determines an organization's critical business processes and the potential damage or loss that can result from their disruption or failure.
- Risk analysis. Risk analysis identifies possible risks and their probability. Also, risk analysis identifies the single points of failure, such as an organization's disk drives, network switches, storage, or power supply.

Business continuity strategies vary from organization to organization based on business requirements. Technologies that organizations use to achieve business continuity strategy can include:

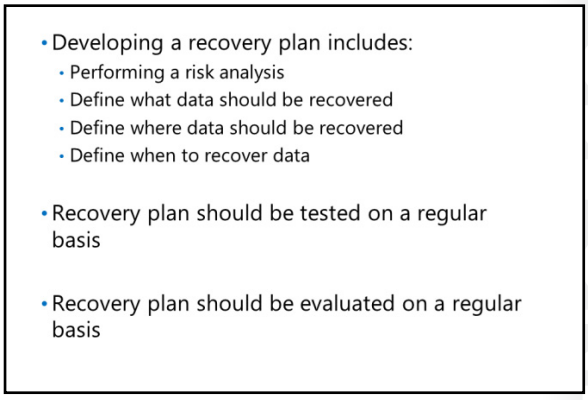
- Network Load Balancing (NLB).
- Failover clustering on physical or virtual machines.
- Application-aware high availability.
- Conventional data backups.
- Online backups.
- Virtual machine backups.

Organizations that have business-critical IT infrastructures might implement a full-continuity, high-cost strategy that includes different technologies. For example, to protect business-critical data some organizations could use NLB to provide high availability for web servers, use failover clustering to provide high availability for servers running Microsoft SQL Server, and perform data backups to tape, disk, and cloud backup services, such as Microsoft Azure Backup. Furthermore, organizations might deploy disaster recovery centers where data from the headquarters data center is replicated, providing site resilience.

Other organizations might decide to deploy a low-cost strategy that provides protection in situations where potential impacts are minimal, or the risk is acceptable. For example, organizations might perform a backup of critical data only, accepting the risk that servers might not be available for several hours or even a day.

Creating a disaster recovery plan

To ensure that your organization recovers from failure or disaster scenarios, you should create a disaster recovery plan to document all recovery procedures in an easy-to-follow manner. Additionally, a disaster recovery plan should ensure that you and your organization's personnel know exactly what steps to perform after a failure occurs.



Developing a recovery plan

When developing your recovery plan, ask yourself the following questions:

- Where should the recovered data be located?
- When should the recovery occur?
- What data should be recovered?

Selecting what data to recover

In most circumstances, you will recover everything that was backed up. In some circumstances, you might choose to perform only a partial recovery to meet business-continuity goals, leaving a full recovery for a later point. This is worth considering particularly if a full recovery would take a long time, whereas a partial recovery can get your users back up and working in a short amount of time.

Choosing a data-recovery location

Choosing where to recover is less complicated if your organization has replacement hardware, such as a replacement hard-disk drive or a full server chassis.

With the growth in virtualization, it is increasingly unnecessary to wait for specific hardware to become available when you need to perform a full server recovery. It is possible to perform a temporary recovery to a Hyper-V host, and enable it to host the recovered server virtually until such time as the replacement hardware arrives. This provides you with time to migrate from the virtual machine to a physical server.

Determining when to recover data

If a failure occurs, and your organization does not have an agreement with a hardware vendor for 24-hour replacement of components, you will have to wait until the components arrive. This could impact your RTO. Alternatively, you could perform a partial recovery to an alternate location. For example, if a remote branch-office file server fails, and it will be 72 hours before replacement components arrive, you might choose to host the file share temporarily on another file server. Alternatively, if you are using DFS with the shared files, you might create a new replica at the site, removing it after the original file server is back in operation.

Testing the recovery plan

Recovery plans should be planned and created carefully, because they include every single step needed to recover business critical and mission critical solutions in an organization. However, recovery plan must be tested in order that you are sure that recovery steps are valid and successful. Failing to test the recovery plan might result in failure during the recovery process. For example, during the creation of the recovery plan, administrator forgot to include a step for installing drivers on the server, which results in server not being able to discover the storage array during the operating system installation process. Furthermore, any delay in the recovery process will extend the time needed for recover the business critical systems, which might result in business loss or other types of loss for an organization.

Evaluating the recovery plan

IT infrastructure in every organization is dynamic. This means organizations during the year deploy new solutions, network devices, buy new servers and decommission old servers and devices. Recovery plans must follow the change in an organizations IT infrastructure. If not updated, recovery plan might become outdated and not correspond to the current configuration of the servers and applications in an organization. For example, an organization has updated their backup software with a new version which has slightly different steps for backup and restore. During the restore process, backup operator follows the recovery plan steps, and stops the recovery procedure because the interface on the backup software doesn't match the instructions in the recovery plan. As a result, there is a delay in the restore process, which might result in other types of loss for an organization.

Service Level Agreement (SLA)

An SLA document describes the responsibilities and specific objectives of a department, organization, or service provider. Specifically, the IT SLA describes the responsibilities of an IT department or IT service provider regarding the availability, performance, and protection of the organization's business critical IT solutions and data. Additionally, SLAs often specify how quickly a provider must restore services after a failure.

Some organizations have formal SLAs, while others have general guidelines. Typically, the performance of an IT department is measured against the objectives that an SLA spells out. These metrics form part of the IT department's performance evaluation, and can influence items such as budgets and salaries. SLAs are critical to the billing structure of managed services and cloud service providers. In other types of organizations, SLAs provide less formal guidelines. A successful SLA must be realistic and achievable.

An SLA might include the following elements:

- Hours of operation. The hours of operation define when the data and services are available to users, and how much planned downtime there will be due to system maintenance.
- Service availability. Service availability is a percentage of time, generally of a calendar year, that data and services are available to users. For example, a service availability of 99.9 percent per year means that data and services can have no more than 0.1 percent per year of unplanned downtime, or 8.75 hours per year on a 24/7 basis. However, organizations should also define maintenance windows, which represent the scheduled time when systems are offline for maintenance procedures, such as hardware upgrades or deploying software updates.
- Recovery point objective (RPO). A recovery point objective sets a limit on how much data you lose due to failure. RPOs are a contractually determined time. For example, if an organization sets an RPO of six hours, it is necessary to perform a backup every six hours or create a replication copy on different locations at six-hour intervals. Should a failure occur, an organization would use the most recent backup, which would be no more than six hours old.

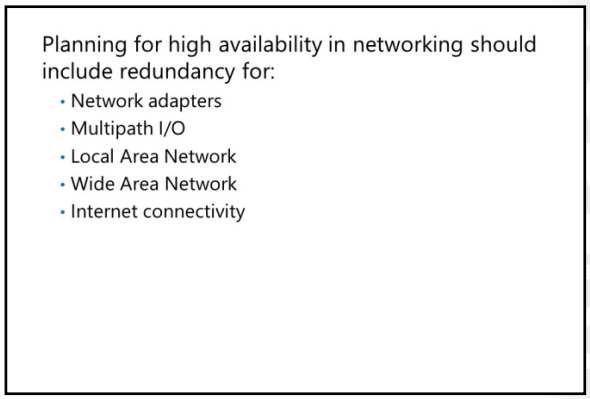
  You can configure backup software to perform backups every hour and provide a theoretical recovery point objective of 60 minutes. This means if any data loss occurs 60 minutes after the last backup, you will not be able to restore only the new data created within that hour. All other data created before the backup will be restored using the backup media. When calculating an RPO, consider the time that it takes to perform a backup. For example, suppose it takes 15 minutes to perform a backup, and you back up every hour. If a failure occurs during the backup process, your best possible RPO will be one hour and 15 minutes. A realistic RPO must balance your desired recovery time with your network infrastructure's realities. You should not aim for an RPO of two hours when a backup takes three hours to complete.

  An RPO also depends on the backup software technology that you are using. For example, when you use the snapshot feature in Windows Server Backup, or other backup software that uses Volume Shadow Copy Service (VSS), you are backing up to the time when the backup began.

- Recovery time objective (RTO). An RTO is the amount of time that it takes to recover from failure. The RTO varies depending on the type of failure. The loss of a motherboard on a critical server has a different RTO than the loss of a disk on a critical server because motherboard replacement takes significantly longer than disk replacement.
- Retention objectives. Retention objectives measure the length of time to store backed-up data. For example, you might need to recover data quickly from the previous month, but you must store data in some form for several years. The speed at which you agree to recover data in your SLA depends on the data's age. You should consider how quickly data is recoverable or whether you must recover it from your archives.
- System performance. System performance is an important SLA component, although it often does not relate directly to disaster recovery. Applications that an SLA includes should be available and should have acceptable response times to users' requests. If the system performance is slow, then business requirements might not be met.

Highly available networking

High availability in networking should be analyzed and planned to meet an organizations' business requirements for high availability and business continuity. Network administrators should evaluate each scenario where networks might be unavailable and propose a solution that will eliminate single points of failure in networking components.



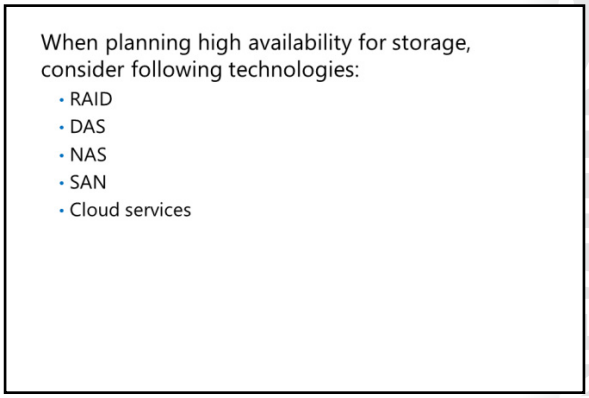
Planning for high availability in networking should include:

- Network adapters. Some applications have multiple network adapters installed for both high availability and improved network bandwidth. If one of the network adapters stops working, the other network adapters are still functional. However, you should verify the best practices recommended by the application vendors. For example, some applications do not support multiple network adapters, while others provide high availability with different technologies and recommend having just one network adapter per host. Furthermore, if you configure networking on a virtual machine, different recommendations apply depending on the application installed.
- Multipath I/O (MPIO) software. In a highly available IT environment, you can deploy nodes with multiple host bus adapters if supported by the application. Windows Server supports this scenario by using MPIO software. Implementing MPIO with multiple host adapters provides you with alternate paths to your storage devices. This provides the highest level of redundancy and availability. For Windows Server 2016, your multipath solution must be based on MPIO. Your hardware vendor usually supplies an MPIO device-specific module (DSM) for your hardware, although Windows Server 2016 includes one or more DSMs as part of the operating system.
- Local area networks (LANs). You connect an organizations' computers in LANs with network switches, routers, and wireless access points. Each of these devices represents a single point of failure if installed individually. Many networking equipment vendors provide options for configuring network equipment with a high availability configuration where you have installed redundant network equipment. If a single component fails, the redundant one continues to function normally.

- Wide area networks (WANs). Organizations that have multiple branch offices require high availability for their WAN networks and routers that connect branch offices to the corporate network. If a router fails, the second redundant router will continue to provide the connection. Organizations might consider having redundant WAN connections if they want branch offices to stay connected in a case of single WAN failure.
- Internet connectivity. Many organizations consider their Internet connectivity as a business-critical component. Therefore, we recommend that organizations consider deploying two Internet connections, preferably through two different ISPs. Although ISPs rarely have outages, having a secondary Internet connection through another ISP provides another level of redundancy. Furthermore, organizations should configure their routers in a redundant configuration. If a single router fails, the redundant router continues to provide Internet connectivity.

Highly available storage

Computer storage is one of the most critical components for every application. Stored data should be accessible at any time. To provide high availability for storage, organizations can choose between different storage solutions and configurations, depending on the business requirements.



RAID

RAID enables fault tolerance by using additional disks to ensure that the disk subsystem can continue to function even if one or more disks in the subsystem fail. RAID uses two options for enabling fault tolerance:

- Disk mirroring. With disk mirroring, all of the information that is written to one disk, is also written to another disk. If one of the disks fails, the other disk is still available.
- Parity information. RAID uses parity information in the event of a disk failure to calculate the information that was stored on a disk. The server or RAID controller calculates the parity information for each block of data written to the disks, and then stores this information on another disk or across multiple disks. If one of the disks in the RAID array fails, the server can use the data that is still available on the functional disks along with the parity information to recreate the data that was stored on the failed disk.

Direct-attached storage

Almost all servers provide some built-in storage or *direct-attached storage* (DAS). DAS can include disks that are physically located inside the server or connect directly with an external array. RAID technology should be used to provide high availability for the data in DAS. However, because DAS storage is connected to the server physically, the storage becomes unavailable if the server suffers a power failure.

Network-attached storage

Network-attached storage (NAS) is connected to a dedicated storage device and then accessed over the network. NAS is different from DAS in that the storage is not directly attached to each individual server, but rather is accessible across the network to many servers. You configure the storage in NAS devices in high available RAID arrays. Organizations benefit from performance gains because the processing power of the NAS device is dedicated solely to the distribution of the files. If one server fails, the data stored on NAS is still available, and you can access it from another server that is online at the moment.

Note: When planning for a NAS solution, ensure that all applications that store data on a NAS device are NAS supported. For example, Microsoft does not support the scenarios where Microsoft Exchange Server stores databases on NAS.

Storage area network

Storage area network (SAN) is a high‑speed network that connects computer systems or host servers to high-performance storage subsystems. A SAN usually includes components such as host bus adapters (HBAs), special switches to help route traffic, and storage disk arrays with logical unit numbers (LUNs). You configure SAN storage in highly available RAID arrays, where the SAN enables multiple servers to access a pool of storage that any server can potentially access. Because a SAN uses a network, a SAN can connect to many different devices and hosts, and provide access to any connected device. SANs also provide block level access. Rather than accessing the content on the disks as files by using a file access protocol, SANs write blocks of data directly to the disks using protocols such as Fibre Channel over Ethernet or Internet Small Computer System Interface (iSCSI).

Cloud storage services

Organizations that run their applications in a cloud environment, such as Microsoft Azure, benefit from storage that is already configured with high availability. Furthermore, organizations that use cloud services, such as Office 365, also benefit from storage and servers that are already running in high available configurations, where they do not require additional configuration. Applications that run in Office 365, such as Exchange Online, Skype for Business Online, and SharePoint online, are already configured for high availability.

Highly available compute or hardware functions

Windows Server 2016 operating system has functionalities that provide high availability for different types of applications. Some functionalities, such as failover clustering, are essential for high availability operations of many applications, such as SQL Server, Exchange Server, and Hyper-V. Other functionalities, such as Network Load Balancing (NLB), can be used, or you can deploy equivalent third-party devices instead.

- Consider using the high availability features that are built in to the operating system:
  - Failover clustering
  - Network Load Balancing
  - RAID
- Follow the best practice guidelines and recommendations for the specific application

When planning for high availability consider the following built-in Windows Server 2016 functionalities:

- Failover Clustering enables a group of independent servers to work together to increase the availability of applications and services. If a server cluster, or *node*, fails, then another node begins to provide services. This is *failover*, and it results in little or no disruption of service.
- NLB that enables a group of independent servers to distribute client requests between the servers where NLB is running. If one server becomes unavailable, then the remaining servers handle the requests.

- RAID functionalities are built into the Windows Server 2016 operating system and enable configuring a group of disks in RAID 1 or RAID 5 arrays, providing high availability for stored data. However, administrators might also consider using RAID software that is built into the DAS controllers. Furthermore, if you connect a server to NAS or SAN devices, it is recommended that you configure RAID arrays on NAS or SAN devices instead of on the operating system.

 **Note:** Before deciding which operating system or hardware high availability solution to deploy, always read the deployment guide and best practices recommendation for the particular application that requires high availability. Furthermore, pay attention to the configurations that particular application does not support.

Question: What should high availability provide for applications?

Question: What should continuous availability provide for applications?

Lesson 2

Planning high availability and disaster recovery solutions with Hyper-V virtual machines

One benefit of implementing server virtualization is the opportunity to provide high availability, both, for applications or services that have built-in high availability functionality and for applications or services that do not provide high availability in any other way. With the Windows Server 2016 Hyper-V technology and failover clustering, you can configure high availability by using several different options.

In this lesson, you will learn how to plan high availability for a virtual environment with failover clustering in a Hyper-V scenario.

Failover clustering is a Windows Server 2016 feature that enables you to make applications or services highly available. To make virtual machines highly available in a Hyper-V environment, you should implement failover clustering on the Hyper-V host computers.

This lesson summarizes the high availability options for Hyper-V-based virtual machines, and then focuses on how failover clustering works, and how to design and implement failover clustering for Hyper-V.

Lesson Objectives

After completing this lesson, you will be able to:

- Describe high availability considerations with Hyper-V virtual machines.
- Describe live migration.
- Describe live migration requirements.
- Describe high availability with storage migration.
- Describe Hyper-V Replica.
- Plan for Hyper-V Replica.
- Describe implementing Hyper-V Replica.

High availability considerations with Hyper-V virtual machines

Most organizations have some applications that are business critical and must be highly available. To make an application highly available, you must deploy it in an environment that provides redundancy for all components that the application requires. For virtual machines to be highly available, you can choose from several options. You can implement virtual machines as a clustered role, called host clustering, you can implement clustering inside virtual machines, called guest clustering; or you can use NLB inside virtual machines.

High availability options	Description
Host clustering	• Virtual machines are highly available • Does not require virtual machine operating system or application to be cluster aware
Guest clustering	• Virtual machines are failover cluster nodes • Virtual machine applications must be cluster aware • Requires iSCSI or virtual Fibre Channel interface for shared storage connections
NLB	• Virtual machines are NLB cluster nodes • Use for web-based applications

Host clustering

Host clustering enables you to configure a failover cluster by using the Hyper-V host servers. When you configure host clustering for Hyper-V, you configure the virtual machine as a highly available resource. You implement failover protection at the host-server level. This means that the guest operating system

and applications that are running within the virtual machine do not have to be cluster-aware. However, the virtual machine is still highly available.

Some examples of non-cluster aware applications are a print server or a proprietary network-based application, such as an accounting application. If the host node that controls the virtual machine unexpectedly becomes unavailable, the secondary host node takes control and restarts, or resumes, the virtual machine as quickly as possible. You can also move the virtual machine from one node in the cluster to another in a controlled manner. For example, you could move the virtual machine from one node to another, while patching the host management operating system.

The applications or services that are running in the virtual machine do not have to be compatible with failover clustering, and they do not have to be aware that the virtual machine is clustered. The failover is at the virtual machine level, therefore, there are no dependencies on software that you have installed in the virtual machine.

Guest clustering

Guest failover clustering is configured similarly to a physical-server failover clustering, except that the cluster nodes are virtual machines. In this scenario, you create two or more virtual machines and enable failover clustering within the guest operating system. You, then, enable the application or service for high availability between the virtual machines. Because failover clustering is implemented within each virtual machine node's guest operating system, you can locate the virtual machines on a single host. This configuration can be quick and cost-effective in a test or staging environment.

For production environments, however, you can better protect the application or service if you deploy the virtual machines on separate failover clustering-enabled Hyper-V host computers. When you implement failover clustering at both the host and virtual machine levels, the resource can restart regardless of whether the node that fails is a virtual machine or a host. This configuration is also known as a *Guest Cluster Across Hosts*. It is considered an optimal high-availability configuration for virtual machines running mission-critical applications in a production environment.

You should consider several factors when you implement guest clustering:

- The application or service must be failover cluster-aware. This includes any of the Windows Server 2016 services that are cluster-aware, and any applications, such as clustered Microsoft SQL Server and Microsoft Exchange Server.
- Hyper-V virtual machines can use Fibre Channel-based connections to shared storage. However, this is specific only to Microsoft Hyper-V Server 2012 and newer. Alternatively, you can implement iSCSI connections from the virtual machines to the shared storage. In Windows Server 2012 R2 and newer, you also can use the shared virtual hard disk feature to provide shared storage for virtual machines.

You should deploy multiple network adapters on the host computers and the virtual machines. Ideally, you should dedicate a network connection to the iSCSI connection if you use this method to connect to storage. You should also dedicate a private network between the hosts, and a network connection that the client computers use.

NLB

NLB works with virtual machines in the same manner that it works with physical hosts. It distributes IP traffic to multiple instances of a TCP/IP service, such as a web server that is running on a host within the NLB cluster. NLB transparently distributes client requests among the hosts, and it enables the clients to access the cluster by using a virtual host name or a virtual IP address. From the client computer's perspective, the cluster appears to be a single server that answers these client requests. As enterprise traffic increases, you can add another server to the cluster.

Therefore, NLB is an appropriate solution for resources that do not have to accommodate exclusive read or write requests. Examples of NLB-appropriate applications include web-based front ends, database applications, or Exchange Server Client Access services.

When you configure an NLB cluster, you must install and configure the application on all virtual machines that will participate in the NLB cluster. After you configure the application, you install the NLB feature in Windows Server 2016 within each virtual machine's guest operating system, not on the Hyper-V hosts, and then configure an NLB cluster for the application. Older versions of Windows Server also support NLB, so that the guest operating system is not limited to only Windows Server 2016; however, you should use the same operating system versions within one NLB cluster. Similar to a Guest Cluster Across Hosts, the NLB resource typically benefits from overall increased I/O performance when you locate the virtual machine nodes on different Hyper-V hosts.

Note: As with older versions of Windows Server, Windows Server 2016 NLB and failover clustering should not be implemented within the same operating system because the two technologies conflict with each other.

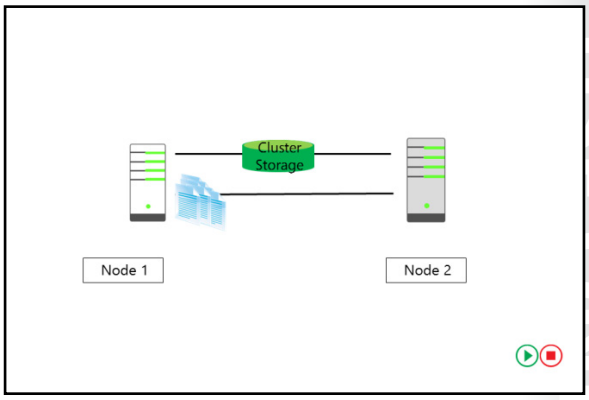
There are several scenarios in which you would want to migrate a virtual machine from one location to another. For example, you might want to move a virtual machine's virtual hard disk from one physical drive to another on the same host. In another example, you might move a virtual machine from one node in a cluster to another, or just move a computer from one host server to another host server without the hosts being members of a cluster. Compared with Windows Server 2008 R2, Windows Server 2012 and Windows Server 2016 enhance and simplify the procedures for this process.

In Windows Server 2016, you can perform migration of virtual machines by using these methods:

- Virtual Machine and Storage Migration. With this method, you move a powered-on virtual machine from one location to another or from one host to another by using the Move Virtual Machine Wizard in Hyper-V Manager. Virtual Machine and Storage Migration does not require failover clustering or any other high availability technology.
- Quick Migration. This method also is available in Windows Server 2008. It requires that you install and configure the failover clustering. During the migration process, when you use Quick Migration to move virtual machines between cluster nodes, a virtual machine is placed in a saved state. This causes some downtime until it copies the memory content to another node and restores the machine from the saved state.
- Live Migration. Live migration enables you to migrate a virtual machine from one host to another without experiencing downtime. In Windows Server, you also can perform Shared Nothing Live Migration, which does not require failover clustering. In addition, hosts do not have to share any storage for this type of migration to be performed.
- Exporting and importing virtual machines. This is an established method of moving virtual machines without using a cluster. You export a virtual machine on one host and then, move exported files physically to another host by performing an import operation. This is a very time-consuming operation. It requires that you turn off a virtual machine during export and import. Windows Server 2016 improved this migration method. You can import a virtual machine to a Hyper-V host without exporting it before import. Windows Server 2016 Hyper-V is now capable of configuring all necessary settings during the import operation.

  Question: Do you use any high availability solution for virtual machines in your environment?

Overview of Live Migration



Windows Server 2016 Hyper-V allows you to move virtual machines between physical Hyper-V nodes without the need to shut down the virtual machines. This process is called Live Migration, and you can perform it in a cluster or non-cluster environment. When used within a failover cluster, Live Migration enables you to move running virtual machines from one failover cluster node to another node. If used without a cluster, Live Migration performs as a Storage Migration, described in an earlier topic, and it is called *shared-nothing Live Migration*. With Live Migration, users should not experience any server outage when connected to the virtual machine.

Note: Although you also can perform Live Migration of virtual machines by using Virtual Machine and Storage Migration, as described earlier in this lesson, be aware that Live Migration is based on a different technology called failover clustering. Unlike the Storage Migration scenario, Live Migration is performed only if a virtual machine is highly available. Shared-nothing Live Migration does not use or depend on failover clustering. It moves virtual machines by copying them from one host to another.

You can start a Live Migration with one of the following:

- The Failover Cluster Management console.
- The Virtual Machine Manager (VMM) Administrator console, if you use VMM to manage your physical hosts.
- Windows Management Instrumentation (WMI) or a Windows PowerShell script.

Note: Live Migration enables you to reduce the perceived outage of a virtual machine significantly during a planned failover. During a planned failover, you start the failover manually. Live Migration does not apply during an unplanned failover, such as when the node that hosts the virtual machine fails.

The Live Migration process

The Live Migration process consists of four steps:

1. Migration setup. When the administrator starts the failover of the virtual machine, the source node creates a TCP connection with the target physical host. This connection transfers the virtual machine configuration data to the target physical host. Live Migration creates a temporary virtual machine on the target physical host, and allocates memory to the destination virtual machine. The migration preparation also checks to determine whether you can migrate a virtual machine.
2. Guest-memory transfer. The guest memory is transferred iteratively to the target host while the virtual machine is still running on the source host. Hyper-V on the source physical host monitors the pages in the working set. As the system modifies memory pages, it tracks and marks them as being modified. During this phase, the migrating virtual machine continues to run. Hyper-V iterates the memory copy process several times, and every time it copies a smaller number of modified pages to the destination physical computer. A final memory-copy process copies the remaining modified

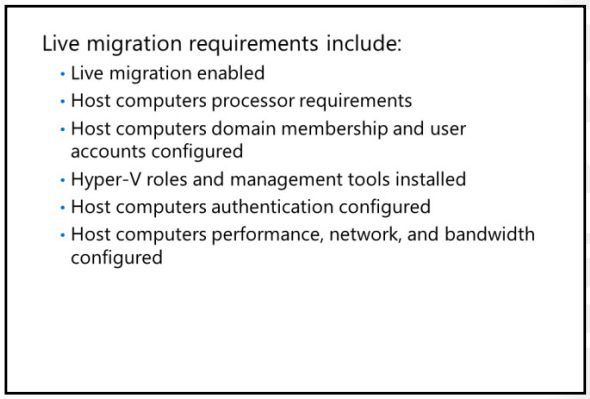
memory pages to the destination physical host. Copying stops as soon as the number of dirty pages drops below a threshold or after 10 iterations are complete.

3. State transfer. To migrate the virtual machine to the target host, Hyper-V stops the source partition, transfers the state of the virtual machine, including the remaining dirty memory pages, to the target host, and then restores the virtual machine on the target host. Hyper-V must pause the virtual machine during the final state transfer.
4. Cleanup. The cleanup stage finishes the migration by tearing down the virtual machine on the source host, terminating the worker threads, and signaling the completion of the migration.

Note: In Windows Server 2016, you can perform a virtual machine Live Migration by using server message block (SMB) 3.0 as a transport. This means that you can take advantage of key SMB features, such as traffic compression, SMB Direct (remote direct memory access), and SMB Multichannel, which provide high-speed migration with low CPU utilization.

Live migration requirements

To perform Live Migration, you must configure the host machines. Moreover, specific requirements must be met for Live Migration in Windows Server 2016:



- The live migration should be enabled; it is not enabled by default.
- The host computers should have identical processor architecture.
- User accounts must be a member of the local Hyper-V Administrators group, or the Administrators group on both hosts of the virtual machines.
- Both source and destination hosts must have the Hyper-V role installed.
- Both source and destination hosts must be members of the same domain, or members of different domains that trust each other.
- Hyper-V management tools should be installed on both source and destination hosts if you run the tools from source or destination hosts. Otherwise, management tools should be installed on a computer running Windows Server 2016 or Windows 10.
- You should configure authentication protocol for live migration traffic. You can choose from following authentication protocols:
    - Kerberos requires you to configure a constrained delegation. When Kerberos is enabled, there is no need for signing in to the server.
    - Credential Security Support Provider (CredSSP) does not require you to configure a constrained delegation, but it requires that administrator signs in to the server.
- You might choose to configure performance options for live migration to reduce network and CPU utilization, it might increase the speed of the live migration.

- You should perform live migration on a separate network, and you might use an encryption such as Internet Protocol security (IPsec) to protect the traffic between hosts in live migration.
- You can configure bandwidth limits for live migration to optimize network bandwidth during the live migration process by using the Windows PowerShell cmdlet **Set-SMBbandwidthlimit**.

Demonstration: Configuring live migration (optional)

In this demonstration, you will see how to enable and configure live migration.

Demonstration Steps

1. On **LON-HOST1**, open **Hyper-V Manager**.
2. In the **Hyper-V Manager Settings**, open **Live Migrations** and enable incoming and outgoing live migrations.
3. Specify the simultaneous number of live migrations if you want to use a different number than 2.
4. Review the option to use specific network connections to accept live migration traffic.
5. Select **Advanced Features** to demonstrate configuring Authentication protocol.
6. Perform steps 1 to 5 on **LON-NVHOST2**.

Providing high availability with storage migration

There are many cases in which an administrator might want to move the virtual machine files to another location. For example, if the disk where a virtual machine hard disk resides runs out of space, you must move the virtual machine to another drive or volume. Moving a virtual machine to another host is a very common procedure.

- Virtual Machine and Storage Migration technology enables you to move a virtual machine and its storage to another location without downtime
- During migration, the virtual machine hard disk is copied from one location to another
- Changes are written to both the source and destination drive
- You can move virtual machine storage to the same host, another host, or an SMB share
- Storage and virtual machine configuration can be in different locations

In older versions of Windows Server, such as Windows Server 2008 or Windows Server 2008 R2, moving a virtual machine resulted in downtime because the virtual machine had to be turned off. If you moved a virtual machine between two hosts, you also had to perform export and import operations for that specific machine. Export operations can be time consuming, depending on the size of the virtual machine hard disks.

In Windows Server 2012 and Windows Server 2016, Virtual Machine and Storage Migration enables you to move a virtual machine to another location on the same host or another host computer without turning off the virtual machine.

To copy a virtual hard disk, an administrator starts live storage migration by using the Hyper-V console or Windows PowerShell, and completes the Storage Migration wizard, or specifies parameters in Windows PowerShell. This creates a new virtual hard disk on the destination location, and the copy process starts.

During the copy process, the virtual machine is fully functional. However, all changes that occur during copying are written to both the source and destination location. Read operations are performed only from the source location.

As soon as the disk copy process is complete, Hyper-V switches virtual machines to run on the destination virtual hard disk. In addition, if you move the virtual machine to another host, the computer configuration is copied, and it associates the virtual machine with another host. If a failure were to occur on the destination side, you always have a fail-back option to run on the source directory. After the virtual machine is migrated to and associated with a new location successfully, the process deletes the source VHD/VHDX files and virtual machine configuration.

The time required to move a virtual machine depends on the source and destination location, the speed of hard disks or storage, and the size of the virtual hard disks. If the source and destination locations are on storage, and the storage supports Offloaded Data Transfer (ODX), the moving process is accelerated.

When you move a virtual machine's VHDs/VHDXs and configuration files to another location, a wizard presents three available options:

- Move all the virtual machine's data to a single location. You specify a single destination location, such as disk file, configuration, checkpoint, or smart paging.
- Move the virtual machine's data to a different location. You specify individual locations for each virtual machine item.
- Move only the virtual machine's virtual hard disk.: You move only the virtual hard disk file.

Demonstration: Configuring storage migration (optional)

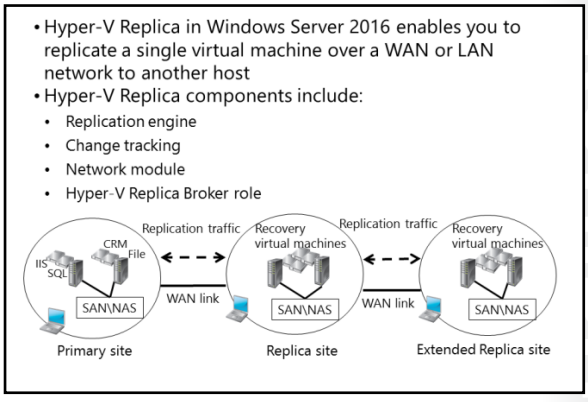
In this demonstration, you will see how to enable and configure storage migration

Demonstration Steps

1. On **LON-HOST1**, in **Hyper-V Manager**, open the **Hyper-V Settings** window for **LON-HOST1**.
2. Set the simultaneous number of storage migrations to **5**.
3. On **LON-HOST1** create a folder named **C:\VM**.
4. Start **Storage Migration** and show the options for moving the storage.
5. Move the **LON-SVR1-B** virtual machine to the **C:\VM** folder.

Overview of Hyper-V Replica

You might want to have a spare copy of one virtual machine that you can run if the original virtual machine fails. By implementing high availability, you have one instance of a virtual machine. High availability does not prevent corruption of software that is running inside the virtual machine. One way to address the issue of corruption is, periodically, to copy the virtual machine manually. You also can back up the virtual machine and its storage. Although this solution achieves the desired result, it is resource intensive and time-consuming. In addition, because you peform backups periodically, you never have the same copy as the running virtual machine.



To resolve this problem, and to enable administrators to have an up-to-date copy of a single virtual machine, Windows Server 2012 and newer implement *Hyper-V Replica*. This technology enables virtual machines running at a primary site, or a location or host, to be replicated efficiently to a secondary site (a location or host) across a WAN or a LAN link. Hyper-V Replica enables you to have two instances of a single virtual machine residing on different hosts, one as the primary, or live, copy and the other as a replica, or offline copy. These copies synchronize on a regular interval, which you can configure in the Windows Server 2016. You also can failover at any time.

In the event of a failure at a primary site caused by a natural disaster, power outage, or a server failure, an administrator can use Hyper-V Manager to execute a failover of production workloads to replica servers at a secondary location within minutes, thus incurring minimal downtime. Hyper-V Replica enables an administrator to restore virtualized workloads to a specific time depending on the Recovery History configuration settings for the virtual machine.

Hyper-V Replica technology consists of several components:

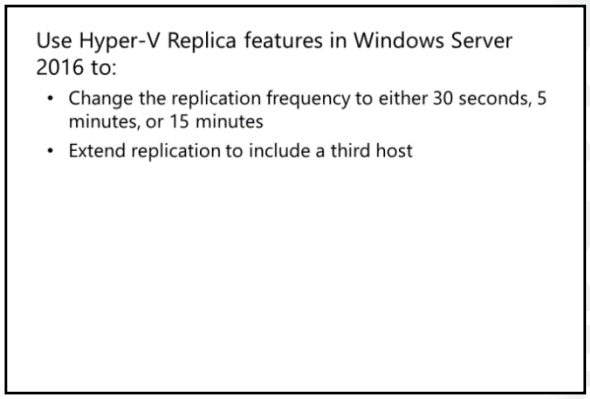
- Replication engine. This component is the core of Hyper-V Replica. It manages the replication configuration details and handles initial replication, delta replication, failover, and test-failover operations. It also tracks virtual machine and storage-mobility events, and takes the required appropriate actions. For example, the replication engine pauses replication events until migration events complete, and then resumes where these events left off.
- Change tracking. This component tracks changes that are happening on the primary copy of the virtual machine. It is designed to make the scenario work regardless of where the virtual machine VHD file or files reside.
- Network module. This module provides a secure and efficient way to transfer virtual machine replicas between the primary host and the replica host. Data compression is enabled by default. HTTPS and certification-based authentication secures this communication.
- Hyper-V Replica Broker role. This is a role implemented in Windows Server 2016. You configure this in failover clustering, and it enables you to have Hyper-V Replica functionality even when the virtual machine you are replicating is highly available and can move from one cluster node to another. The Hyper-V Replica Broker redirects all virtual machine-specific events to the appropriate node in the Replica cluster. The Broker queries the cluster database to determine which node should handle which events. This ensures that the Broker redirects all events to the correct node in the cluster, if you execute a Quick Migration, Live Migration, or Storage Migration process.

When you plan hardware configurations on the sites, you do not have to use the same server or storage hardware. It is important, however, to ensure that sufficient hardware resources are available to run the Hyper-V Replica virtual machine.

 **Note:** Hyper-V replica is not a high availability technology but a disaster recovery technology. It does not provide automatic failover.

Planning for Hyper-V Replica

With Windows Server 2016, administrators can benefit from the following new features that help optimize Hyper-V Replica and increase the availability of critical virtual machines.



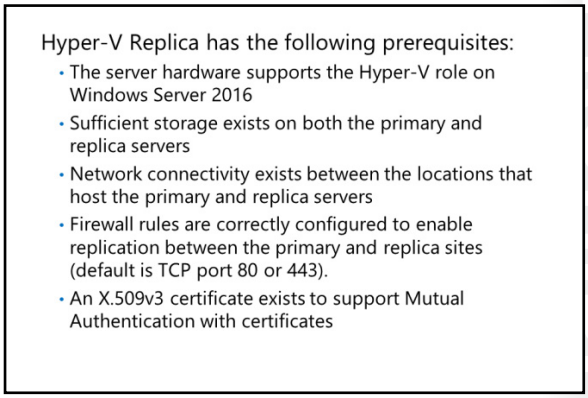
- Change the replication frequency. In earlier versions of Windows Server, Hyper-V Replica was to set to a five-minute replication interval, and you could not change this value. In Windows Server 2016, you can set the replication interval to 30 seconds, five minutes, or 15 minutes. This means that you can configure your replication traffic based on your real environment. However, keep in mind that a replica with a higher latency, for example, 15 minutes, will generate more traffic.
- Extended replication. With Windows Server 2012 and newer Windows Server operating systems, you can replicate a single virtual machine to a third server. Thus you can replicate a running virtual machine to two independent servers. However, the replication does not happen from one server to two other servers. The server that is running an active copy of the virtual machine replicates to the replica server, and the replica server then replicates to the extended replica server. You create a second replica by running the Extend Replication Wizard on a passive copy. In this wizard, you can set the same options that you chose when you configured the first replica.

Note: Hyper-V Replica now allows administrators to use a Microsoft Azure instance as a replica repository. This enables administrators to leverage Azure, rather than having to build out a Disaster Recovery site, or manage backup tapes off-site. To use Azure for this purpose, you must have a valid subscription. Note that this service might not be available in all world regions.

Question: Are there ways that extended replication could benefit your environment?

Implementing Hyper-V Replica

Before you implement Hyper-V Replica technology, ensure that you meet these prerequisites:



- The server hardware supports the Hyper-V role on Windows Server 2016.
- Sufficient storage exists on both the primary and replica servers to host the files that are used by replicated virtual machines.
- Network connectivity exists between the locations that host the primary and replica servers. This can be a WAN or LAN link.
- Firewall rules are correctly configured to enable replication between the primary and replica sites (default traffic is going over TCP port 80 or 443).
- An X.509v3 certificate exists to support Mutual Authentication with certificates if desired.

You do not have to install Hyper-V Replica separately because it is not a Windows Server role or feature. Hyper-V Replica is implemented as part of the Hyper-V role. It can be used on Hyper-V servers that are stand-alone, or on servers that are part of a failover cluster, in which case you should configure Hyper-V Replica Broker. Unlike failover clustering, a Hyper-V role does not depend on AD DS. You can use a Hyper-V role with Hyper-V servers that are stand-alone, or that are members of different Active Directory domains, except when servers that participate in Hyper-V replica are part of the same failover cluster.

To enable Hyper-V Replica technology, complete following steps:

- In the Replication Configuration group of options, enable the Hyper-V server as a replica server.
- Configure Hyper-V server settings. Select the authentication and port options, and configure the authorization options. You can choose to enable replication from any server that successfully authenticates. This is convenient in scenarios where all servers are part of the same domain, or you can type the fully qualified domain names (FQDNs) of servers that you accept as replica servers. Additionally, you must configure the location for replica files. You should configure these settings on each server that serves as a replica server.
- Specify both the replica server name and the connection options.
- Select which virtual hard disk drives you replicate, in cases where a virtual machine has more than one VHD, and you can also configure the Recovery History and the initial replication method. In Windows Server 2016, you can also configure replication interval, either for 30 seconds, five minutes (this is a default in Windows Server 2016) or 15 minutes.
- After you configure these options, you can start replication. After you make the initial replica in Windows Server 2016, you can also make an extended replica to a third physical or cloud-based instance running Hyper-V. The extended replica site is built from the first replica site, not from the primary virtual machine. It is possible to configure the different replication intervals for replica and extended replica instances of a virtual machine.

You can perform three types of failovers with Hyper-V Replica: test failover, planned failover, and failover. These three options offer different benefits and are useful in different scenarios.

Test failover

After you configure a Hyper-V Replica and after the virtual machines start replicating, you can perform a test failover. A test failover is a nondisruptive task that enables you to test a virtual machine on the replica server while the primary virtual machine is running, and without interrupting the replication. You can initiate a test failover on the replicated virtual machine, which creates a new checkpoint. You can use this checkpoint to select a recovery point, from which you create the new test virtual machine. The test virtual machine has the same name as the replica, but with "- Test" appended to the end. The test virtual machine is not started. It is disconnected by default to avoid potential conflicts with the running primary virtual machine.

After you finish testing, you can stop a test failover. This option is available only if a test failover is running. When you stop the test failover, it stops the test virtual machine and deletes it from the replica Hyper-V host. If you run a test failover on a failover cluster, you will have to remove the Test-Failover role from the failover cluster manually.

Planned failover

You can initiate a planned failover to move the primary virtual machine to a replica site, for example, before site maintenance or before an expected disaster. Because this is a planned event, there is no data loss, but the virtual machine will be unavailable for some time during its startup. A planned failover confirms that the primary virtual machine is turned off before the failover executes. During the failover, the primary virtual machine sends all the data that it has not yet replicated to the replica server. The planned failover process then fails over the virtual machine to the replica server, and starts the virtual machine on the replica server. After the planned failover, the virtual machine will run on the replica server,

and it does not replicate its changes. If you want to establish replication again, you should reverse the replication. You will have to configure settings similar to when you enabled replication, and it will use the existing virtual machine as an initial copy.

Failover

If there is a disruption to the primary site, you can perform a failover. You initiate a failover at the replicated virtual machine only if the primary virtual machine is either unavailable or turned off. A *failover* is an unplanned event that can result in data loss, because changes at the primary virtual machine might not have replicated before the disaster happened. The replication frequency setting controls how often changes are replicated. During a failover, the virtual machine runs on a replica server. If you start the failover from a different recovery point and discard all the changes, you can cancel the failover. After you recover the primary site, you can reverse the replication direction to reestablish replication. This also removes the option to cancel failover.

Demonstration: Implementing Hyper-V Replica (optional)

In this demonstration, you will see how to implement Hyper-V Replica.

Demonstration Steps

1. On **LON-HOST1** and **LON-NVHOST2**, configure each server to be a Hyper-V Replica server.
2. Use Kerberos (HTTP) for authentication.
3. Enable replication from any authenticated server.
4. Create and use the folder **C:\VMReplica** as a default location to store replica files.
5. Enable the firewall rule named **Hyper-V Replica HTTP Listener (TCP-In)** on both hosts.
6. On **LON-HOST1**, enable replication for the **20740A-LON-SVR1-B** virtual machine:
   - Use Kerberos (HTTP).
   - Allow 3 simultaneous storage migrations.
   - Select to have only latest recovery point available.
   - Set the replication frequency to 15 minutes.
   - Start replication immediately.
7. Wait for initial replication to finish, and ensure that the **20740A-LON-SVR1-B** virtual machine has appeared in the **Hyper-V Manager** console on **LON-NVHOST2**.
8. On **LON-HOST1**, view the replication health for **20740A-LON-SVR1-B**.
9. On **LON-HOST1**, shut down **20740A-LON-SVR1-B** and perform a planned failover to **LON-NVHOST2**. Verify that **20740A-LON-SVR1-B** is running on **LON-NVHOST2**.

Question: What are the migration options for virtual machines in Windows Server 2016?

Question: What is Hyper-V Replica?

Lab: Planning and implementing a high availability and disaster recovery solution

Scenario

A. Datum Corporation is looking to assess and configure the new high availability features and technologies that they can leverage. As the system administrator, you have been tasked with performing that assessment and implementation.

Objectives

After completing this lab, you will be able to:

- Configure a Hyper-V Replica.
- Configure a failover cluster for Hyper-V.
- Configure a highly available virtual machine.

Lab Setup

Estimated Time: 75 minutes

Virtual machines: **20740A-LON-DC1-B**, **20740A-LON-SVR1-B**

Host machines: **20740A-LON-HOST1**, **20740A-LON-NVHOST2**

User name: **Adatum\Administrator**

Password: **Pa$$w0rd**

To perform this lab, you should continue using the VM environment created in Module 2 and 5, which consists of physical host running **LON-HOST1** and nested host **LON-NVHOST2**. Before you start the preparation steps, you should import **LON-DC1-B** and **LON-SVR1-B** virtual machines, by performing following steps:

1. On **LON-HOST1**, open **Windows PowerShell**.

   Note: Before continuing on next task, verify the location of the base drives and 20740 course drives. You need the drive letter for both locations in this exercise. The exercise assumes that the drive letter **E:** is used for both, but substitute the correct drive letter as necessary.

2. At the **Windows PowerShell** prompt, type the following, and then press Enter:

   ```
   & 'E:\Program Files\Microsoft Learning\20740\Drives\LON-NVHOST2_VM-Pre-Import-20740A.ps1'
   ```

3. Type the drive letter for the base images, and then press Enter.
4. Type the drive letter for the course images, and then press Enter.
5. Press Enter to continue.
6. On the host computer, on the **Start** screen, click **Hyper-V Manager**.
7. In **Hyper-V Manager**, click **20740A**-**LON-DC1-B**, and then in the **Actions** pane, click **Start**.
8. In the **Actions** pane, click **Connect**. Wait until the virtual machine starts.

9. Sign in by using the following credentials:
    - User name: **Adatum\Administrator**
    - Password: **Pa$$w0rd**
10. Repeat steps 7 through 9 for **20740A-LON-NVHOST2** and **20740A-LON-SVR1-B** virtual machines.
11. On **LON-HOST1**, start **Server Manager**.
12. On **LON-HOST1**, in **Server Manager**, click **Local Server**.
13. In the details pane, click the **IPv4 address assigned by DHCP, IPv6 enabled** link for the vEthernet (Host Internal Network).
14. In **Network Connections**, right-click the **vEthernet (Host Internal Network)** adapter, and then click **Properties**.
15. Double-click **Internet Protocol Version 4 (TCP/IPv4)**.
16. Reconfigure the settings:
    - IP address: **172.16.0.160**
    - Subnet mask: **255.255.0.0**
    - Default gateway: **172.16.0.1**
    - Preferred DNS server: **172.16.0.10**
17. Click **OK** and then **OK**.
18. Disable and then enable the adapter. Disable any other adapters.
19. On **20740A-LON-DC1-B**, **20740A-LON-SVR1-B** and **20740A-LON-NVHOST2**, make sure that your VMs are configured with a **Host Internal Network (Internal Virtual Switch type)**.
20. On **LON-DC1-B**, open the **DNS Management** console and verify that IP addresses assigned to **20740A-LON-DC1-B**, **20740A-LON-SVR1-B** and **20740A-LON-NVHOST2** are the actual IP addresses of the virtual machines. If some of the IP addresses is missing, configure them according to the information in DNS Management console on **20740A-LON-DC1-B**. These should be as follows:
    - LON-DC1: **172.16.0.10**
    - LON-SVR1: **172.16.0.21**
    - LON-HOST1: **172.16.0.160**
    - NV-HOST2: **172.16.0.32**

 **Note:** You must have completed the labs in Module 2 and 5 to be able to complete this lab.

Exercise 1: Determine the appropriate high availability and disaster recovery solution

Scenario

A. Datum Corporation has its headquarters in New York. It is reviewing its current disaster recovery strategy after a recent fire in a remote office in London resulted in the loss of some data. It was also decided to review the current strategies around high availability. A. Datum is considering an upgrade to Windows Server 2016 and wants to determine if there are any Windows Server 2016 features that it can leverage. Budgets are also under pressure and management is looking to see if there are any cost savings that can be can realized to help offset the expenditure to replace existing legacy storage currently being used with a Hyper-V cluster. A. Datum has the following business requirements:

- Public facing financial transactions take place online.
- There are 1, 000 employees across Application/Product Development, HR, Finance, Customer Service, IT, and Sales.
- Finance cannot tolerate any downtime in their SQL and finance applications, which are running on Hyper-V.
- The finance team requires less than 1 min down time for their RTO and zero data loss as their RPO on their customer facing transactions.
- The finance division is also growing at a very fast rate and they expect increased demand for application and services.

The solution should:

- Allow for monthly patching with no downtime.
- Allow for existing legacy storage to be replaced without downtime to the Hyper-V cluster.
- Provide a disaster recovery strategy that allows for recovery of critical virtual machines should there be another disaster event in either office location.

The main task for this exercise is as follows:

1. Design the appropriate high availability and disaster recovery solution.

▶ Task 1: Design the appropriate high availability and disaster recovery solution

Question: What actions should you take and which technologies should you consider using?

Exercise 2: Implementing storage migration

Scenario

To balance the number of virtual machines running on both the existing hosts and the new hosts, you plan to move a virtual machine between Hyper-V hosts as it is running and without downtime. First, you will configure a destination Hyper-V host to allow live migration. Next, you will use the Move Wizard to move virtual machine storage, its virtual hard disk, and its checkpoints, to the Hyper-V host of your partner.

The main task for this exercise is as follows:

1. Configure and perform storage migration.

▶ Task 1: Configure and perform storage migration

1. On **LON-HOST1**, use **Hyper-V Manager** to confirm that **LON-SVR1-B** is running and configured with a locally stored VHD.
2. Use the **Move Wizard** to move the **20740A-LON-SVR1-B-Allfiles** virtual machine VHDs to **C:\VMs\LON-SVR1-B**. Do not move the other virtual disks.
3. Use **Hyper-V Manager** to confirm that the **20740A-LON-SVR1-B-Allfiles** virtual machine VHD is now stored under the **C:\VMs** folder structure.

Note: The VHD was moved while the virtual machine is running.

Results: After completing this exercise, you should have moved Hyper-V storage and virtual machines.

Exercise 3: Configuring Hyper-V Replicas

Scenario

Before you start with a cluster deployment, you have decided to evaluate the new technology in Hyper-V for replicating virtual machines between hosts. You want to be able to mount a copy of a virtual machine on to another host manually if the active copy or host fails.

The main tasks for this exercise are as follows:

1. Configure a replica on both host machines.
2. Configure replication for LON-SVR1-B virtual machine.
3. Validate a planned failover to the replica site.
4. Prepare for the next module.

▶ Task 1: Configure a replica on both host machines

1. On **LON-HOST1** and **LON-NVHOST2**, configure each server to be a Hyper-V Replica server.
   - Use Kerberos (HTTP) for authentication.
   - Enable replication from any authenticated server.
   - Create and use the folder **E:\VMReplica** as a default location to store replica files.
2. Enable the firewall rule named **Hyper-V Replica HTTP Listener (TCP-In)** on both hosts.

▶ Task 2: Configure replication for LON-SVR1-B virtual machine

1. On **LON-HOST1**, enable replication for the **20740A-LON-SVR1-B** virtual machine:
   - Use Kerberos (HTTP).
   - Set the replication frequency to 30 seconds.
   - Select to have only latest recovery point available.
   - Start replication immediately.
2. Wait for initial replication to finish, and ensure that the **20740A-LON-SVR1-B** virtual machine has appeared in **Hyper-V Manager** console on **LON-NVHOST2**.

▶ Task 3: Validate a planned failover to the replica site

1. On **LON-HOST1**, view replication health for **20740A-LON-SVR1**.
2. On **LON-HOST1**, shut down **20740A-LON-SVR1-B** and perform the planned failover to **LON-NVHOST2**.
3. Verify that **20740A-LON-SVR1-B** is running on **LON-NVHOST2**.

▶ Task 4: Prepare for the next module

1. Cancel Failover on **20740A-LON-SVR1-B** on **LON-NVHOST2**.
2. Remove the replica of **20740A-LON-SVR1-B** on both **LON-HOST1** and **LON-NVHOST2**.
3. Disable replication on both **LON-HOST1** and **LON-NVHOST2**.
4. On **LON-HOST1**, move the **20740A-LON-SVR1-B-Allfiles.vhd** back to **E:\Program Files \Microsoft Learning\20740\Drives\20740A-LON-SVR1-B\Virtual Hard Disks**.
5. Restart the host computer.
6. When you are prompted with the boot menu, select **Windows Server 2012**, and then press Enter.
7. Sign in to the host machine as directed by your instructor.

Results: After completing this exercise, you will have configured Hyper-V Replica.

Question: How can you extend Hyper-V Replica in Windows Server 2016?

Question: What is the difference between Live Migration and Storage Migration?

Lesson 3

Backing up and restoring by using Windows Server Backup

Data Protection describes the many technologies and methods that allow you to bring data, services, and servers back to an operational state after an unplanned event, such as data corruption, application failure, or the loss of a site through flooding or fire. An effective data protection strategy addresses the organization's needs without providing an unnecessary level of coverage. Although absolute protection might seem desirable, it is unlikely to be economically feasible. When you develop a data protection strategy, balance the cost to the organization of a particular type of data loss with the cost to the organization of protection from that data loss.

The software you use to perform backups also can influence your backup process. You can use Windows Server Backup in the Windows operating system or the Microsoft System Center Data Protection Manager (Data Protection Manager). You also can use third-party solutions for backing up Windows Server 2016.

Lesson Objectives

After completing this lesson, you will be able to:

- Describe Windows Server Backup
- Implement backup and restore

Overview of Windows Server Backup

Windows Server Backup is a feature in Windows Server 2016 that consists of a Microsoft Management Console (MMC) snap-in, the command **wbadmin**, and Windows PowerShell commands. You can use the wizards in Windows Server Backup to guide you through running backups and recoveries.

You can use Windows Server Backup to back up:

- A full server (all volumes), or just selected volumes.
- Individual files and folders.
- System state.
- Individual virtual machines on a Hyper-V host.
- Cluster Shared Volumes (CSVs).

Additionally, Windows Server Backup allows you to:

- Perform a bare-metal restore. A bare-metal backup contains at least all critical volumes, and 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.
- Restore system state. The backup contains all information to roll back a server to a specific time. However, you need to install an operating system before you can recover the system state.

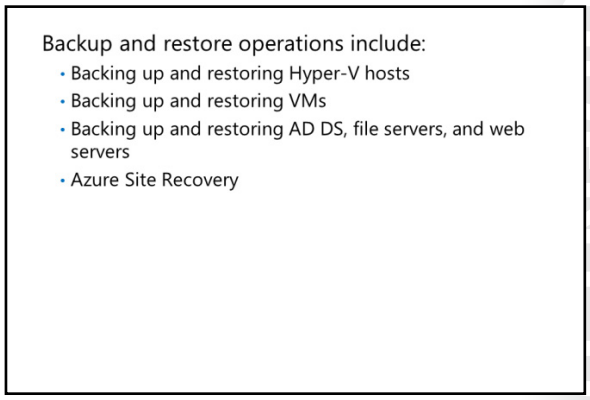
- Recover individual files and folders or volumes. The Individual files and folders option enables you to select to back up and restore specific files, folders, or volumes, or you can add specific files, folders, or volumes to the backup when you use an option such as critical volume or system state.
- Exclude selected files or file types. For example, you can exclude temporary files from the backup.
- Store backup on multiple storage locations. You can store backups on remote shares or non-dedicated volumes.
- Use the Microsoft Azure Online Backup. The Microsoft Azure Online Backup is a cloud-based backup solution for Windows Server 2016 that enables you to back up and recover files and folders off-site, using cloud services.

If events such as hard disk failures occur, 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.

Windows Server Backup is a single-server backup solution. You cannot use one instance of Windows Server Backup to back up multiple servers. You would need to install and configure Windows Server Backup on each server.

Implementing backup and restore

Backing up virtual machines



When creating a backup solution for virtual machines, you should consider the data that is being backed up. You can install Windows Server Backup on the host and perform a host-level backup or you can install Windows Server Backup inside a virtual machine to perform an in-guest backup. In many cases, you might want to use both host and in-guest backup. We recommended that you read the technical documentation and best practices on how to back up a specific application. For example, SQL Server, Exchange Server, and Skype for Business server have different best practices for backup. Furthermore, some applications support only in-guest backup.

You use a host-level backup when performing a full server backup where the data included in a backup includes virtual machines configurations, virtual machines associated snapshots, and virtual machines' virtual hard disks. When you restore data from backup, it is not necessary to recreate virtual machines or reinstall Windows Server roles. However, the backup does not include virtual networks settings, which need to be recreated and reattached to the virtual machines. For this purpose, you might create PowerShell scripts that automate the process of creating and attaching the virtual switches.

When you perform a backup within the guest operating system, the procedure is the same as performing a backup for a physical computer. When performing both a host-level backup and virtual machine backup, you should complete the backup within the guest operating system before performing a full backup on the host computer.

Backing up file servers and web servers

Consider a scenario where you want to provide a backup for a file or a web server. To provide fast recovery of individual files to a specific time, an in-guest backup is adequate.

If you want to back up a Remote Desktop Session host server, a host-level backup would most likely be more useful than an in-guest backup. The host-level backup enables you to recover the entire virtual

machine quickly, in its entirety, whereas the in-guest backup would require you to build a virtual machine and install Windows Server before you could attempt a recovery.

Backing up AD DS

Backing up the AD DS role is an important procedure that should be part of any backup and recovery process or strategy. You back up the AD DS role to restore data in different data loss scenarios, such as deleted data or a corrupted AD DS database.

When you back up AD DS, consider your backup schedule. Plan your AD DS backup schedule properly because you cannot restore from a backup that is older than 180 days, the deleted object lifetime. When a user deletes an object from AD DS, it keeps the information about that deletion for 180 days. If you have a backup that is newer than 180 days, you can restore the deleted object successfully. If your backup is older than 180 days, the restore procedure does not replicate the restored object to other domain controllers, which means the state of AD DS data will be inconsistent.

Understanding online and offline backups in virtual machines

You can perform online backups that do not incur virtual machine downtime, if the following conditions are met:

- The virtual machine being backed up has integration services installed and enabled.
- Each disk that the virtual machine uses is running NTFS file system basic disks.
- The VSS is enabled on all volumes within the virtual machine, and snapshots for each volume are stored on the same volume. For example, volume D: must store shadow copies on volume D:

 **Note:** In the Windows Server Backup Wizard in Windows Server 2012, when you select the Hyper-V virtual machines to back up, the backup types available are either Backup Using Saved State (Offline), or Backup Using Child Partition Snapshot (Online). This has been changed in Windows Server 2016 to Offline and Online.

 **Note:** During the backup procedure, you will see a warning that reminds you not to mix virtual volume backups with physical disk backups.

Advanced Settings

When you schedule or modify a backup by using the Backup Schedule Wizard, you can modify the following settings:

- Exclusions. You can exclude file types within specific folders and optionally their subfolders. For example, if you back up a Hyper-V host with several virtual machines, you may not want to back up any .iso files that have been attached.
- VSS backup. With VSS backup options, you can select either a VSS full back up or VSS copy backup. The full backup updates the backup history and clears the log file. However, if you use other backup technologies that also use VSS, you might want to choose the VSS copy backup, which retains the VSS writer log files.

Azure Site Recovery

Azure Site Recovery is a Microsoft Azure feature that provides replication of on-premises Hyper-V virtual machines and physical computers to Azure. Azure Site Recovery provides organizations with business continuity and disaster recovery services (BCDR) by performing replication, failover, and recovery of multiple virtual machines from a single location. You can use Azure Site Recovery for planned failovers for testing or maintenance, where failover is performed with zero data loss. You can also use Azure Site Recovery for unplanned outages, where, depending on replication frequency, you expect minimal data loss. You can perform both failover and failback operations and monitor and manage Azure Site Recovery operations for your virtual machines or physical computers by using a unified dashboard. Azure Site Recovery eliminates the need for an on-premises secondary datacenter for disaster recovery.

Question: Name several scenarios where you might use Windows Server Backup in your organization.

Question: Name several scenarios for backup and restore operations.

Lesson 4

High Availability with failover clustering in Windows Server 2016

Failover clusters in Windows Server 2016 provide a high-availability solution for many server roles and applications. By implementing failover clusters, you can maintain application or service availability if one or more computers in the failover cluster fail. Before you implement failover clustering, you should be familiar with general high-availability concepts. You must be familiar with clustering terminology, and understand how failover clusters work. It also is important to be familiar with new clustering features in Windows Server 2016.

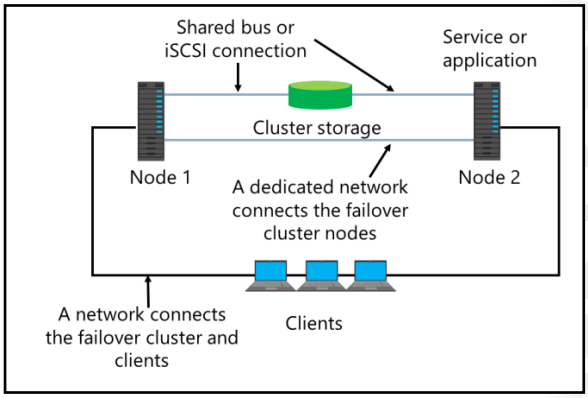
Lesson Objectives

After completing this lesson, you will be able to:

- Describe failover clustering
- Describe high availability with failover clustering
- Describe clustering terminology
- Describe clustering categories and types
- Describe failover clustering components
- Make technology redundancy comparison

What is failover clustering?

A cluster is a group of computers and storage devices that work together as a single organized system. You can use clusters to distribute servicing load or provide high availability of services. You can create many different types of clusters to provide these services. In a cluster, the component computers communicate with each other over a high-performance, reliable network. They may share one or more common storage devices. You use cluster configurations to address availability, scalability, and manageability.



A *failover cluster* is a group of independent computers that work together to increase the availability of applications and services. Physical cables and software connect the clustered servers, known as *nodes*. If one of the cluster nodes fails, another node begins to provide service. This process is known as *failover*. With failover, you can minimize service disruptions.

In a failover cluster, each node in the cluster has following properties:

- Has full connectivity and communication with the other nodes in the cluster.
- Is aware when another node joins or leaves the cluster.
- Is connected to a network through which client computers can access the cluster.
- Is connected through a shared bus or iSCSI connection to shared storage.

- Is aware of the services or applications that are running locally, and the resources that are running on all other cluster nodes.

Cluster storage usually refers to logical devices—typically drives or LUNs—that all the cluster nodes attach to through a shared bus. This bus is separate from the bus that contains the system and boot disks. The shared boot disks store resources such as applications and file shares that the cluster will manage.

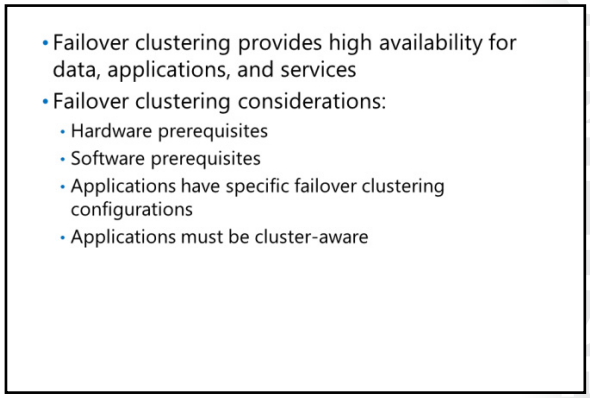
A failover cluster typically defines at least two data communications networks: one network enables the cluster to communicate with clients, and the second, isolated network enables the cluster node members to communicate directly with one another. If directly-connected shared storage is not being used, then a third network segment (for iSCSI or Fibre Channel) can exist between the cluster nodes and a data storage network.

Most clustered applications and their associated resources are assigned to one cluster node at a time. The node that provides access to those cluster resources is the active node. If the nodes detect the failure of the active node for a clustered application, or if the active node is offline for maintenance, the clustered application starts on another cluster node. To minimize the impact of the failure, client requests automatically redirect to an alternative node in the cluster as quickly as possible.

Question: Why do I need to implement a cluster if I can Live Migrate virtual machines from any location to another?

High availability with failover clustering

Failover clustering addresses organizations' business needs for high availability by providing that data, application, and services are available in different failure scenarios. However, a specific hardware configuration should be installed to meet the prerequisites for failover clustering. Furthermore, a specific operating system features and application components should be installed as prerequisites for failover clustering deployment.



Before you deploy a failover cluster for a specific technology, read the failover clustering planning and deployment guides and best practices document for that specific technology. High availability deployments for different applications can vary. For example, Microsoft Exchange Server uses failover clustering feature in the Windows Server operating system, however, you use Exchange server management tools to perform the process of high availability deployment and failover clustering installation completely., You must install the failover clustering feature from the Server Manager console or Windows PowerShell in the Windows Server operating system to deploy high availability for Hyper-V.

An application must be cluster-aware to user failover clustering. Failover clustering in Windows Server operating system provides high availability for the following applications and features:

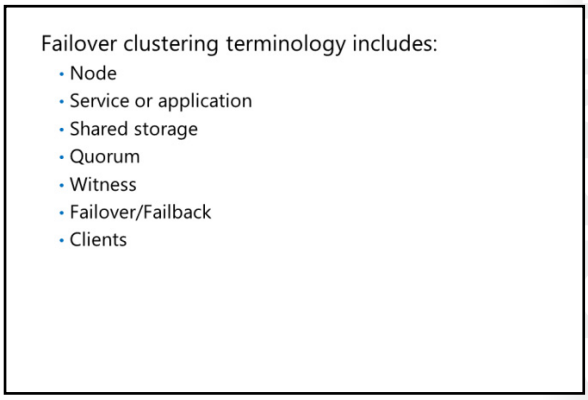
- DFS Namespace Server
- DHCP Server
- Distributed Transaction Coordinator (DTC)
- File Server
- Internet Storage Name Service (iSNS) Server

- Message Queuing
- Other Server
- Print Server
- Remote Desktop Connection Broker
- Virtual Machine
- WINS Server

Clustering terminology

To deploy failover clustering, you should understand clustering terminology. Failover clustering terminology is similar in both Windows Server and third party failover clustering products.

This table shows failover clustering terminology.

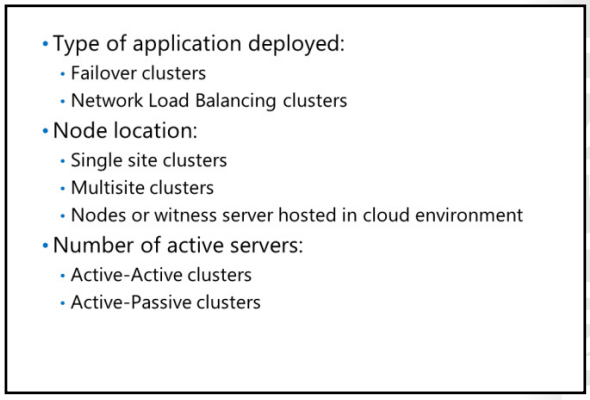


Term	Description
Node	A Windows Server 2016 computer that is part of a failover cluster, and has the failover clustering feature installed.
Service or application	A service that can be moved between cluster nodes (for example, a clustered file server can run on either node).
Shared storage	External storage that is accessible to all cluster nodes.
Quorum	The number of elements that must be online for a cluster to continue to run. The quorum is determined when cluster nodes vote.
Witness	A server that is participating in cluster voting when the number of nodes is even.
Failover	The process of moving cluster resources from the first node to the second node, as a result of node failure or administrator's action.
Failback	The process of moving cluster resources back from the second node to the first node, as a result of the first node going online again or an administrator's action. If the service or application fails over from Node1 to Node2, when Node1 is again available, the service or application will fail back to Node1.
Clients	Computers that connect to the failover cluster and are not aware which node the service is running on.

Note: You will learn failover clustering terminology in more detail in Module 8, "Implementing and managing failover clustering."

Clustering categories and types

Clustering technology includes different types of clusters, depending on the type of the application that you need to configure for high availability. Cluster deployment might differ depending on the location of the cluster nodes. Moreover, cluster functionality can differ according to the activity performed on each cluster member node.

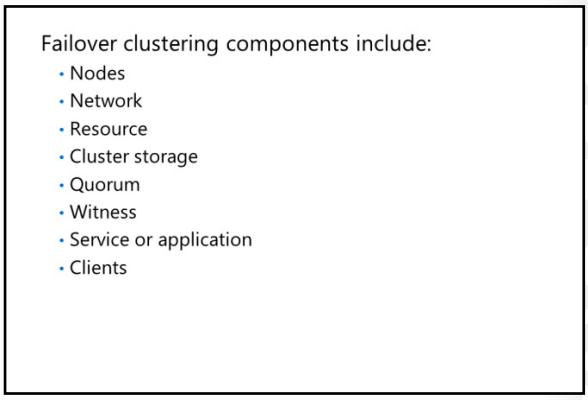


Consider deploying different categories and types of clustering depending on your organization's specific business requirements. Clustering categories and types include:

- Type of the clusters. For example, you achieve Hyper-V high availability by deploying failover clustering, whereas you achieve high availability for web servers with NLB clustering.
    - Failover clusters are deployed for stateful applications, such as SQL Server and Exchange Server. Stateful applications have long-running in-memory states, or have large, frequently updated data states. Other types of failover cluster applications include Hyper-V, file servers, and print servers.
    - NLB is deployed for stateless applications, such as web servers. Stateless applications do not have long-running in-memory states and work with data that is read-only or that does not change frequently. Stateless applications treat each client request as an independent operation, and they can load-balance each request independently. Stateless applications include web servers, virtual private networks (VPNs), File Transfer Protocol (FTP) servers, and firewall and proxy servers. NLB clusters support different TCP- or UDP-based services and applications.
- Single site clusters and multisite clusters. Cluster deployments could include a scenario where all nodes are located in single datacenter. However, some companies want to extend their application availability in case the main datacenter becomes unavailable. Therefore, organizations deploy stretch clusters, where they deploy nodes in multiple datacenters. Multiple site clusters can also include scenarios where organizations locate some of the cluster nodes, or the witness server, in the cloud environment, such as Azure.
- Active-Active and Active-Passive clusters. In Active-Active cluster configurations, such as Scale Out File Server Cluster, multiple nodes run cluster application resources and accept client connections. In Active–Passive cluster configurations, one node runs cluster applications, while other nodes are passive and do not accept client connections. If an active node fails for any reason, some of the remaining passive nodes become active and run the application, accepting client connections.

Failover clustering components

A failover clustering solution consists of several components listed in this table.

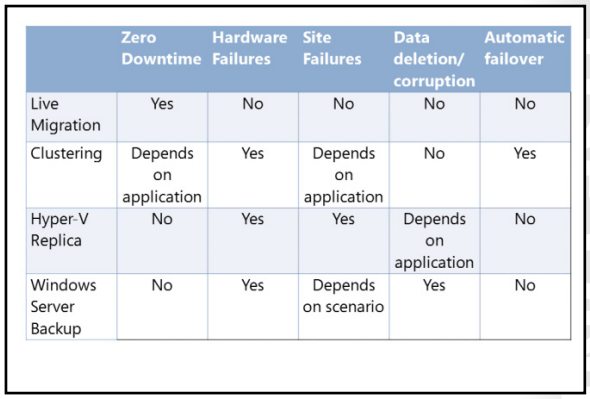


Component	Description
Nodes	Computers that are members of a failover cluster. These computers run the cluster service, and any resources and applications associated to the cluster.
Network	A network across which cluster nodes can communicate with one another and with clients. We discuss these networks in more detail in Module 8: Implementing and managing failover clustering.
Resource	A node hosts a resource. The cluster service manages the resource and can start, stop, and move it to another node.
Cluster storage	A storage system that cluster nodes share. In some scenarios, such as clusters of servers that run Exchange Server, you do not require shared storage.
Quorum	The number of elements that must be online for a cluster to continue to run. The quorum is determined when cluster nodes vote.
Witness	A witness can be a file share or disk, which you use to maintain quorum. Ideally the witness should be located on a network that is both logically and physically separate from those used by the failover cluster. However, the witness must remain accessible by all cluster node members.
Service or application	A software entity that Microsoft presents to clients and that clients use.
Clients	Computers (or users) that use the cluster service.

We discuss the failover clustering components in more detail in Module 8, "Implementing and managing failover clustering."

Technology redundancy comparison

Organizations deploy different technologies for data protection, high availability, site resilience and disaster recovery. However, none of the technologies can cover every failure or data loss scenario. Therefore, organizations should know what combination of technologies can protect them from different failure scenarios.



	Zero Downtime	Hardware Failures	Site Failures	Data deletion/ corruption	Automatic failover
Live Migration	Yes	No	No	No	No
Clustering	Depends on application	Yes	Depends on application	No	Yes
Hyper-V Replica	No	Yes	Yes	Depends on application	No
Windows Server Backup	No	Yes	Depends on scenario	Yes	No

For example, failover clustering protects organizations from server hardware failure, but it does not protect organizations from data loss caused by data deletion or data corruption. Windows Server Backup protects organizations from data loss caused by data deletion or data corruption, but it does not protect organizations from server hardware failure. As a result, organizations should choose to use failover clustering for protecting their applications from server hardware failures and also use Windows Server Backup to protect data from data deletion and corruption.

This table lists multiple Windows Server technologies and how they respond to different failure scenarios:

	Zero downtime	Hardware failures	Site Failures	Data deletion or corruption	Automatic failover
Live Migration	Yes	No	No	No	No
Clustering	Depends on application	Yes	Depends on application	No	Yes
Hyper-V Replica	No	Yes	Yes	Depends on application	No
Windows Server Backup	No	Yes	Depends on scenario	Yes	No

Some of the items are marked "Depends" because the specific capability depends on the application and scenario. For example, if you use failover clustering when Exchange Server is deployed, it provides zero downtime for clients, and you might also address site failures with a specific Exchange Server high availability configuration. However, other applications that use failover clustering, such as file server, might include some minimal downtime, after which the application, data, and services are restored.

Question: What are the properties of a failover clustering node?

Question: What are the failover clustering components of a failover clustering solution?

Module Review and Takeaways

Best Practices

- Develop standard configurations before you implement highly available virtual machines. You should configure the host computers as close to identical as possible. To ensure that you have a consistent Hyper-V platform, configure standard network names and use consistent naming standards for CSVs.
- Use new features in Hyper-V Replica to extend your replication to more than one server.
- Consider using Scale-Out File Server clusters as storage for highly available virtual machines.
- Implement VMM. VMM provides a management layer on top of Hyper-V and Failover Cluster Manager that can block you from making mistakes when you manage highly available virtual machines. For example, you can be blocked from creating virtual machines on storage that is inaccessible from all nodes in the cluster.

Common Issues and Troubleshooting Tips

Common Issue	Troubleshooting Tip
Virtual machine failover fails after you implement CSV and migrate the shared storage to CSV.	
A virtual machine fails over to another node in the host cluster, but loses all network connectivity.	
Four hours after restarting a Hyper-V host that is a member of a host cluster, there are still no virtual machines running on the host.	

Review Question

Question: In Windows Server 2016, must you implement CSV to provide high availability for virtual machines in VMM?

Tools

The tools for implementing failover clustering with Hyper-V include:

Tools	Where to Find	Use
Failover Cluster Manager	Administrative Tools	Failover clustering management
Hyper-V Manager	Administrative Tools	Virtual machine management
VMM Console	Start menu	Hyper-V hosts and virtual machine management

Module 8

Implementing failover clustering

Contents:

Module Overview

Planning, creating, and managing a failover cluster is very important for any organization that wants to provide continuous services to its users. Failover clustering is one of the main Windows Server 2016 technologies that can provide high availability for various applications and services. In this module, you will learn about failover clustering, failover-clustering components, and implementation techniques.

Objectives

After completing this module, you will be able to:

- Plan for a failover-clustering implementation.
- Create and configure a failover cluster.
- Maintain a failover cluster.
- Troubleshoot a failover cluster.
- Implement high availability and stretch clustering for a site.

Lesson 1
Planning a failover cluster

Planning a failover cluster is very important for a high-availability solution, because organizations depend on high-availability technologies to host their business-critical services and data. A solution that you plan properly results in you being able to deploy it faster, manage it more easily, test and verify failover and failback scenarios, and anticipate behaviors that results from failures. Planning a failover cluster includes multiple activities, such as:

- Gathering business requirements.
- Reading documentation about hardware, storage, network, and disk requirements to determine how you can implement best practices to ensure that a particular product is highly available, such as a file server, Microsoft SQL Server, or Microsoft SharePoint Server.
- Reading documentation about operating-system and software requirements to ensure that specific products are highly available.
- Analyzing different failure scenarios.
- Analyzing different failover and failback scenarios.
- Analyzing security considerations for failover clustering.

 **Note:** You always should read documentation about how specific products use failover clustering. Different Microsoft products provide high availability by using failover clustering differently. For example, when you compare high-availability configurations for Exchange Server, SQL Server, Skype for Business, and file-server roles, they are completely different.

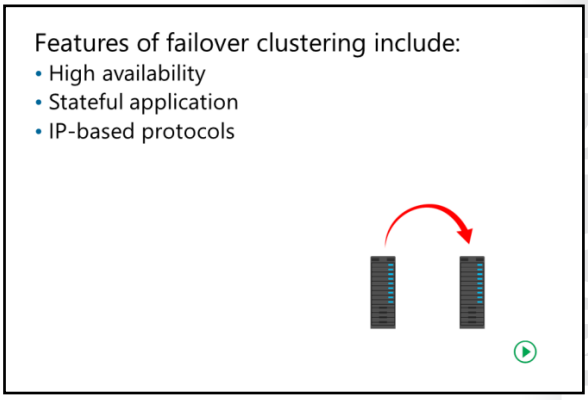
Lesson Objectives

After completing this lesson, you should be able to:

- Describe preparations for implementing a failover cluster.
- Describe how to plan for failover-cluster storage.
- Describe how to plan hardware requirements for failover-cluster implementation.
- Describe how to plan network requirements for failover-cluster implementation.
- Describe how to plan infrastructure and software requirements for a failover cluster.
- Identify the security considerations.
- Describe how to plan for quorum in Windows Server 2016.
- Describe how to plan for migrating and upgrading failover clusters.

Preparing to implement failover clustering

Before you implement a failover-clustering technology, you must identify services and applications that you want to make highly available. You cannot configure failover clustering equally to all applications.



Failover clustering is best for stateful applications that are restricted to a single data set, such as a database. You also can use failover clustering for Microsoft Hyper-V virtual machines (VMs) and for stateful applications that Hyper-V VMs implement.

Failover clustering uses only IP-based protocols, and therefore is suitable only for IP-based applications. Both IP version 4 (IPv4) and IP version 6 (IPv6) are supported.

Failover clustering allows the client to reconnect to an application automatically after failover. If the client does not reconnect automatically, the user must restart the client application.

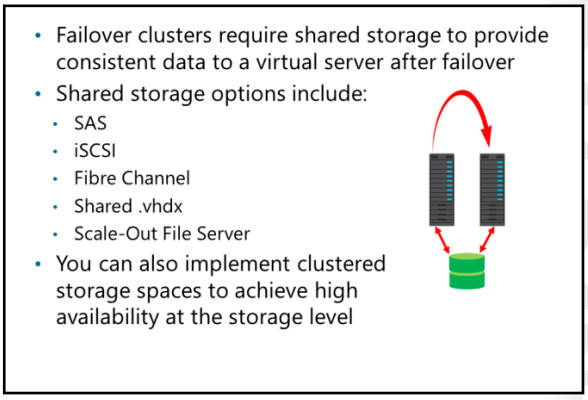
When you are planning node capacity in a failover cluster, you should:

- Configure distribution of highly-available applications from a failed node. When a node fails, a failed node's highly-available services or applications should distribute among the remaining nodes to prevent overloading a single node.
- Sufficient capacity for each node to service the highly-available services or applications that you allocate to it when another node fails. This capacity should be a sufficient buffer to avoid nodes that run at near capacity after a failure event. Failure to plan resource utilization adequately can result in performance decreases after node failure.
- Ensure that you use hardware that has similar capacity for all nodes in a cluster. This simplifies the failover planning process because the failover load will distribute evenly among the surviving nodes.

You also should examine all cluster-configuration components to identify single failure points. You can remedy many single failure points with simple solutions, such as adding storage controllers to separate and stripe disks, teaming network adapters, and by using multipathing software. These solutions reduce the probability that a single device's failure will cause a cluster failure. Typically, server-class computer hardware provides you with options to configure power redundancy by using multiple power supplies and for creating redundant array of independent disks (RAID) sets for disk-data redundancy.

Failover-cluster storage

Most failover-clustering scenarios require shared storage to provide consistent data to a highly-available service or application after failover. There are five shared-storage options for a failover cluster, including:



- Shared serial attached SCSI (SAS). Shared SAS is the lowest-cost option. However, it is not very flexible because the two cluster nodes must be close together physically. Additionally, the shared storage devices that support SAS have a limited number of connections for cluster nodes.
- iSCSI. iSCSI is a type of storage area network (SAN) that transmits SCSI commands over IP networks. Performance is acceptable for most scenarios when you use 1 gigabit per second (Gbps) or 10 Gbps Ethernet physical medium for data transmission. This type of SAN is inexpensive to implement because it does not require any specialized networking hardware. In Windows Server 2012 and newer, you can implement the Microsoft iSCSI Software Target on any server and present local storage over an iSCSI interface to clients.
- Fibre Channel. Fibre Channel SANs typically have better performance than iSCSI SANs, but they are significantly more expensive. Additionally, they require specialized knowledge and hardware to implement.
- Shared virtual hard disk. In Windows Server 2012 R2 and newer versions, you can use shared virtual hard disk as VM guest-clustering storage. You should locate a shared virtual hard disk on a Cluster Shared Volume (CSV) or Scale-Out File Server cluster, or you should connect to a SCSI or guest Fibre Channel interface so that you can add it to two or more VMs that are participating in the guest cluster.
- Scale-Out File Server. In Windows Server 2012 R2 and newer, you can utilize shared Server Message Block (SMB) storage as the shared location for some failover cluster roles, specifically SQL Server and Hyper-V. You then do not have to have local storage on nodes that are hosting the SQL Server or Hyper-V roles. All storage occurs over SMB 3.0 at the Scale-Out File Server.

Note: The Microsoft iSCSI Software Target is an integrated feature in Windows Server 2012 and newer. It can provide storage from a server over a TCP/IP network, including shared storage for applications that a failover cluster hosts. Additionally, you can configure a highly-available iSCSI Target Server as a clustered role by using Failover Cluster Manager or Windows PowerShell.

In Windows Server 2016, you can use storage as a cluster component and you also can implement clustered storage spaces, which provide high availability for storage components by using failover clustering. When you implement clustered storage spaces, you help to protect your environment from risks such as:

- Physical disk failures
- Data-access failures
- Data corruptions
- Volume unavailability
- Server-node failures

Reference Links: For more information, refer to: "Deploy Clustered Storage Spaces" at: http://aka.ms/b5cjdh

Storage requirements

You also should be aware of the following shared-storage requirements:

- If you want to use the native disk support that failover clustering includes, you should use basic disks, not dynamic disks.
- We recommend that you format the partitions with NTFS or Resilient File System (ReFS). For the disk witness, the partition must be NTFS or ReFS. Scale-Out File Servers do not support ReFS at this time.
- For the partition style of the disk, you can use either master boot record (MBR) or GUID partition table (GPT).
- Improvements in failover clusters require that storage responds correctly to specific SCSI commands, so storage must follow the SCSI Primary Commands-3 (SPC-3) standard. In particular, the storage must support persistent reservations, which the SPC-3 standard specifies.
- The miniport driver that you use for storage components must be compatible with the Microsoft Storport storage driver, which offers a higher-performance architecture and better Fibre-Channel compatibility in Windows Server operating systems.
- You must isolate storage devices, so that you have only one cluster per device. Servers from different clusters must be unable to access the same storage devices. In most cases, you should isolate a logical unit number (LUN) that one set of cluster servers uses from all other servers, by using LUN masking or zoning.
- Consider using Multipath I/O (MPIO) software. In a highly-available storage fabric, you can deploy failover clusters with multiple host-bus adapters by using an MPIO software application. This provides the highest level of redundancy and availability. For Windows Server 2016, you must base your multipath solution on MPIO. Your hardware vendor usually supplies an MPIO device-specific module (DSM) for your hardware, although Windows Server 2016 includes one or more DSMs as part of the operating system.
- If you use a shared virtual hard disk, you must have a CSV or a file server cluster on which you can store the virtual hard disk.

Reference Links: For more information, refer to: "Failover Clustering Hardware Requirements and Storage Options" at: http://aka.ms/kr8ahr

Hardware requirements for a failover-cluster implementation

When you select hardware for cluster nodes, you must understand the hardware requirements. To meet availability and support requirements, your failover clusters must satisfy the following hardware criteria, including that you:

- Should use hardware that is certified for Windows Server.
- Should install the same or similar hardware on each failover cluster node. For example, if you choose a specific model of network adapter, you should install this adapter on each of the cluster nodes. This helps you avoid compatibility and capacity issues.

The hardware requirements for a failover implementation include:

- You must use server hardware that is certified for Windows Server
- Server nodes should all have the same configuration and contain the same or similar components
- All servers must pass the tests in the **Validate a Configuration Wizard**

- Should ensure that if you use SAS or Fibre Channel storage connections, the mass-storage device controllers that you dedicate to the cluster storage are identical in all clustered servers. They also should use the same firmware version.
- Ensure that if you use iSCSI storage connections, each clustered server has one or more network adapters or host bus adapters that are dedicated to the cluster storage. You should not use the network that you use for iSCSI storage connections for nonstorage network communication. In all clustered servers, the network adapters that you use to connect to the iSCSI storage target should be identical, and we recommend that you use Gigabit Ethernet or faster adapters.
- Ensure that after you configure servers with hardware, the servers pass all tests in the **Validate a Configuration Wizard** before you consider the cluster a configuration that Microsoft supports.

Note: You will learn more about validating failover cluster configuration in the lesson "Creating and configuring a new failover cluster," under the topic "The Validation Wizard and the cluster support-policy requirements."

- Ensure that each node runs the same processor architecture. This means that each node must have the same processor family, which might be the Intel or Advanced Micro Devices (AMD) family of processors.

Network requirements for a failover-cluster implementation

Before you implement a failover cluster, you must ensure that your network components meet specific requirements and pass the tests in the **Validate a Configuration Wizard**, including that:

- Each node's network adapters should be identical and have the same IP protocol version, speed, duplex, and flow-control capabilities.

The network requirements for a failover implementation include:

- Your server should connect to multiple networks to ensure communication redundancy, or it should connect to a single network with redundant hardware, to remove single points of failure
- You should ensure that network adapters are identical and that they have the same IP protocol versions, speed, duplex, and flow-control capabilities
- Your network adapters should be compatible with RSS and RDMA

- The networks and network equipment to which you connect the nodes should be redundant, so that a single failure allows the nodes to continue communicating. You can provide single network redundancy by using network-adapter teaming. We recommend that you use multiple networks, so that you can provide multiple paths between nodes for internode communication. If you do not, a warning text will appear during the validation process.
- The network adapters in a cluster network should have the same IP address-assignment method, which means that they all use static IP addresses or they all use Dynamic Host Configuration Protocol (DHCP).
- Network settings and IP addresses match. When your network uses identical network adapters, you also should use identical communication settings on those adapters, such as speed, duplex mode, flow control, and media type. Additionally, compare the settings between the network adapter and the switch to which it connects, and ensure that there are no conflicts. Otherwise, network congestion or frame loss might occur, which could adversely affect how the cluster nodes communicate between each other, with clients, or with storage systems.
- You use unique subnets. If you have private networks that are not routed to your network infrastructure, you should ensure that each of these private networks uses a unique subnet. This is necessary even if you give each network adapter a unique IP address. For example, if you have a cluster node in a central office that uses one physical network, and another node in a branch office that uses a separate physical network, do not specify 10.0.0.0/24 for both networks, even if you give each adapter a unique IP address. This avoids routing loops and other network-communications problems if, for example, the segments are configured into the same collision domain inadvertently, because of incorrect virtual local area network (VLAN) assignments.
- You ensure your network adapters support RSS and RDMA. Receive side scaling (RSS) is a technology implemented in network drivers that allows distribution of network-receive processing across multiple central processing units (CPUs). Remote Direct Memory Access (RDMA) is a networking technology that provides high-throughput communication with minimum CPU usage. You can configure RDMA on network adapters that are bound to a Hyper-V Virtual Switch in Windows Server 2016. We recommend that your network adapters support RSS and RDMA. You can verify network adapter's RSS and RDMA compatibility by using the Windows PowerShell cmdlets **Get-NetAdapterRSS** and **Get-SMBServerNetworkInterface**.

 **Note:** If you connect cluster nodes with a single network, the network passes the redundancy requirement in the **Validate a Configuration Wizard**. However, the wizard's report includes a warning that the network should not have single points of failure.

Demonstration: Verify a network adapter's RSS and RDMA compatibility on an SMB Server

In this demonstration, you will learn how to verify a network adapter's RSS and RDMA compatibility on an SMB Server.

Demonstration Steps

1. Sign in to **LON-DC1** with username **Administrator** and password **Pa$$w0rd**, and then open Windows PowerShell.
2. In the **Windows PowerShell** console, run the following cmdlet:

```
Get-NetAdapterRSS –Name * | Format-List *
```

3. View the output, and then verify that the **RssOnPortsSupported** value for the network adapter is **True**.
4. In the **Windows PowerShell** console, run the following cmdlet:

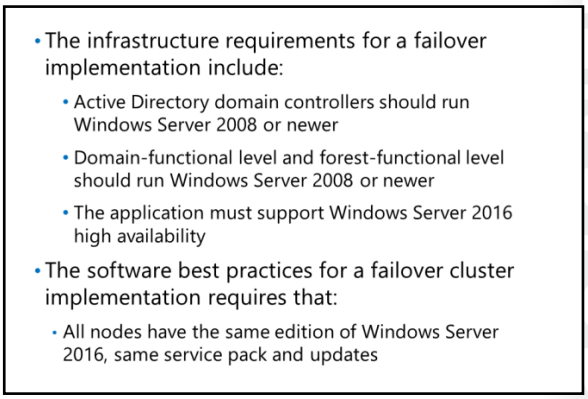
```
Get-SMBServerNetworkInterface
```

5. View the output, and then verify that the **RSS Capable** value for the network adapter is **True** and **RDMA Capable** value for the network adapter is **False**.

Infrastructure and software requirements for a failover cluster

When you select infrastructure for cluster nodes, you must ensure that your failover clusters satisfy the following hardware criteria so that they meet availability and support requirements, including that:

- You should run the supported version of Active Directory domain controllers, and they should use Windows Server 2008 or newer.
- Domain-functional level and forest-functional level should use Windows Server 2008 or newer.



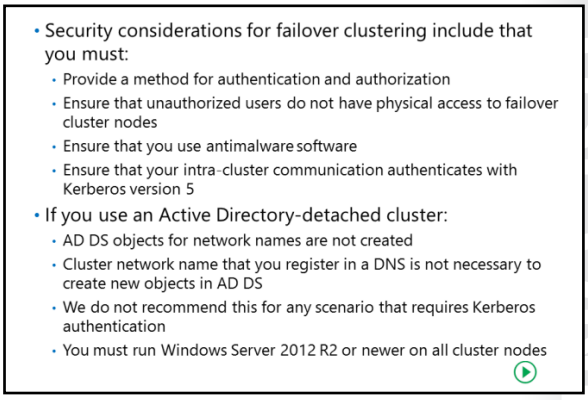
- You should run the supported version of Domain Name System (DNS) servers, and they should use Windows Server 2008 or newer.
- The application that you configure for high availability should support the Windows Server 2016 operating system.

We recommend that you run the same edition of Windows Server 2016 on each cluster node. The edition can be Windows Server 2016 Standard or Windows Server 2016 Datacenter. The nodes also must have the same software updates and service packs. Depending on which role you cluster, you also can utilize a Server Core or Nano installation of Windows Server 2016 to meet software requirements.

Note: With Windows Server 2016 and Cluster Operating System (OS) Rolling Upgrades, a cluster can have different operating systems. Therefore, we recommend that you have a cluster with the same operating system, edition, and updates. However, the cluster can run without this configuration, especially during an upgrade process.

Note: Windows Server 2012 and newer provides the Cluster-Aware Updating (CAU) technology, which you can use to maintain updates on cluster nodes. The Maintaining a failover cluster lesson discusses this feature in more detail.

Security considerations



Organizations typically deploy failover-clustering solutions because their business-critical systems must be highly available. If you want to deploy a failover cluster, you must plan and configure the failover clusters' security settings, because potential security issues might threaten the solution's high availability. For example, if you do not establish proper security for the file server that you configure with failover clustering, an unauthorized user might gain access to your cluster resources, and delete files or shut down cluster nodes. Therefore, you must plan and configure your security settings thoroughly to guard against unauthorized access to cluster resources. Furthermore, you must ensure that cluster nodes cannot be accessed physically by unauthorized users.

If the application that is highly available supports antimalware, the cluster nodes might be protected with that antimalware. However, if the application does not support installing antimalware software on cluster nodes, you should deploy the cluster nodes in a subnet that you protect with firewalls and intrusion-detection devices. If cluster nodes are domain members, same as in previous Windows Server versions, an administrator needs to create and configure a Cluster Named Object (CNO). Cluster nodes communicate by using Kerberos for authentication and NTLM for CNO authentication.

Windows Server 2012 R2 introduced *Active Directory-detached cluster*, which also is available in Windows Server 2016. Active Directory-detached cluster is a cluster that does not have dependencies in Active Directory Domain Services (AD DS) for network names. When you deploy clusters in the detached mode, you register the cluster network name and network names for clustered roles in a local DNS, but you do not have to create corresponding computer objects for cluster and clustered roles in AD DS.

Windows Server 2016 introduces several types of clusters, which you use depending on your domain-membership scenario, including:

- Single-domain clusters. In this type of cluster, cluster nodes are members of the same domain.
- Workgroup clusters. In this type of cluster, cluster nodes are not joined to the domain (workgroup servers).
- Multi-domain clusters. In this type of cluster, cluster nodes are members of the different domains.
- Workgroup and domain clusters. In this type of cluster, cluster nodes are members of domains and members that are not joined to the domain (workgroup servers).

There are ramifications to deploying Active Directory-detached clusters. Because you do not create computer objects, you cannot use Kerberos authentication when accessing cluster resources. However, despite using Kerberos authentication between cluster nodes, because you create their computer accounts and objects outside the cluster, you must use NTLM authentication. Therefore, we do not recommend that you deploy Active Directory-detached clusters for any scenario that requires Kerberos authentication.

To create an Active Directory-detached cluster, all cluster nodes must run Windows Server 2012 R2 or newer. You cannot configure an Active Directory-detached cluster by using the Failover Cluster Manager. You must use Windows PowerShell.

Quorum in Windows Server 2016

Windows Server 2016 includes the same quorum modes from Windows Server 2008 and newer operating systems, but there are changes to the process and recommendations for configuring quorum. However, a majority of votes still determines whether a cluster achieves quorum. Nodes can vote, as can a *disk witness* (disk in cluster storage), a *file share witness* (a file share)), or an Azure Cloud Witness, where appropriate.

Quorum mode	What has the vote?	When is quorum maintained?
Node majority	Only nodes in the cluster have a vote	When more than half of the nodes are online
Node and disk majority	The nodes in the cluster and a disk witness have a vote	When more than half of the votes are online
Node and file share majority	The nodes in the cluster and a file share witness have a vote	When more than half of the votes are online
No majority: disk only	Only the quorum-shared disk has a vote	When the shared disk is online
Dynamic quorum	Votes are dynamically assigned to always be odd	When half the votes are online

Before Windows Server 2012, there were only four quorum modes:

- Node Majority. Each node that is available and is in communication can vote. The cluster functions only with a majority, or more than half of votes. This model is preferred when the cluster consists of an odd number of server nodes and requires no witness to maintain or achieve quorum.
- Node and Disk Majority. Each node can vote, as can a designated disk in the cluster storage (the disk witness) when they are available and in communication. The cluster functions only with a majority (more than half) of votes. The basis for this model is that an even number of server nodes can communicate with each other and the disk witness.
- Node and File Share Majority. Each node can vote, as can a designated file share (file share witness) that an administrator creates, as long as they are available and in communication. The cluster functions only with a majority of votes. The basis for this model is that an even number of the cluster's server nodes can communicate with each other and the file share witness.
- No Majority: Disk Only. The cluster has quorum if one node is available and in communication with a specific disk in the cluster storage. Only the nodes that are in communication with that disk can join the cluster.

Dynamic quorum

In Windows Server 2012, a new mode was introduced called *dynamic quorum*, which refers to the dynamic adjustment of quorum votes on the basis of how many servers are online. For example, if you have a five-node cluster, and you place two of the nodes in a paused state, and one of the remaining nodes crashes, in any legacy configurations, your cluster would fail to achieve quorum and go offline. However, dynamic quorum would adjust the cluster's voting when the first two servers go offline, thereby making the cluster's quorum require two rather than three votes. The benefit is that a cluster with dynamic quorum stays online.

Windows Server 2012 R2 introduced *dynamic witness*, which builds on the dynamic quorum mode. Dynamic witness is a witness that dynamically has a vote, depending on the cluster's number of nodes. If there is an even number of nodes, the witness has a vote. If there are an odd number of nodes, the witness does not have a vote. The recommended configuration for a cluster was to create only a witness when you had an even number of nodes. However, with a dynamic witness's ability to remove voting, so that the cluster always has an odd number of votes, you should configure a witness for all clusters. This now is the default mode of configuration and is a best practice in most Windows Server 2016 and Windows Server 2012 R2 scenarios. In Windows Server 2016, the only suggested quorum mode is dynamic quorum, which is the default configuration.

In Windows Server 2016, you can choose whether to use file share witness, disk witness, or Azure Cloud Witness, as follows:

- Disk witness. Disk witness is the primary witness you would use for most scenarios, especially for local clustered scenarios. In this configuration, all nodes have access to a shared disk. One of the biggest benefits of this configuration is that the cluster stores a copy of the cluster database on the disk witness.
- File share witness. File share witness is ideal when shared storage is not available or when the cluster spans geographical locations. This option does not store a copy of the cluster database.
- Azure Cloud Witness. Azure Cloud Witness is new in Windows Server 2016, and it is the ideal option when you run Internet-connected stretched clusters. This technology does not require that you configure a file share witness at a third datacenter location or a cloud VM. Instead, this option is built into a failover cluster, and does not store a copy of the cluster database. Cloud Witness uses Microsoft Azure as the arbitration point. You can use the **Configure a Cluster Quorum Wizard** to configure a cloud witness as a quorum witness. Cloud Witness uses the publically available Microsoft Azure Blob Storage to read/write a blob file, which is then used as an arbitration point in case of split-brain resolution for eliminating the extra maintenance overhead of VMs hosted in a public cloud. You can use the same Microsoft Azure Storage Account for multiple clusters where one blob file is used per cluster and a blob file name is equal to the cluster unique id. Because Failover Cluster writes very small data per blob file during the cluster nodes' stat changes, Azure Cloud Witness does not create high cost for the Storage Account.

You also should consider the capacity of your cluster's nodes, and factor their ability to support the services and applications that might fail over to that node. For example, a cluster that has four nodes and a disk witness still has quorum after two nodes fail. However, if you deploy several applications or services on the cluster, each remaining cluster node might not have the capacity to provide services.

Planning for migrating and upgrading failover clusters

The upgrade steps for each node in the cluster include:

- Pause the cluster node and drain all cluster resources
- Migrate cluster resources to another node in the cluster
- Replace the cluster node operating system with Windows Server 2016 and add the node back to the cluster
- Upgraded all nodes to Windows Server 2016
- Run cmdlet **Update-ClusterFunctionalLevel**

Windows Server 2016 has a new process for upgrading a failover cluster named Cluster Operating System Rolling Upgrade. If you are performing cluster operating-system upgrades, you first upgrade the cluster operating system (OS) before you upgrade the cluster's functional level. For example, if you take a two-node cluster with Windows Server 2012 R2, you can upgrade it to Windows Server 2016 by draining the roles from one node, taking the node offline, and then removing it from the cluster. You then can upgrade that node to Windows Server 2016 and add the node back to the cluster. The cluster will continue to run on the Windows functional level of Windows Server 2012 R2. You can then drain the roles back to the Windows Server 2016 node. Then remove the Windows Server 2012 R2 node from the cluster, upgrade it, and add it back to the cluster. Finally, now that both nodes are running Windows Server 2016, you can upgrade the functional level by running the following Windows PowerShell command:

```
Update-ClusterFunctionalLevel
```

For example, let's assume that we need to upgrade a Hyper-V failover cluster. This task can be performed in Windows Server 2016 without downtime.

The upgrade steps for each node in the cluster include:

- Pause the cluster node and drain all the virtual machines that run on the node.
- Migrate the virtual machines that run on the node to another node in the cluster.
- Perform a clean installation to replace the cluster node operating system with Windows Server 2016.
- Add back the node now running the Windows Server 2016 operating system to the cluster.
- Next, upgrade all nodes to Windows Server 2016.
- Finally, use the Windows PowerShell cmdlet **Update-ClusterFunctionalLevel** to upgrade the cluster functional level to Windows Server 2016.

Note: In the scenario where cluster nodes are running Windows Server 2012 R2 or Windows Server 2016 operating systems, the cluster is running in mixed mode, however all nodes run in Windows Server 2012 R2 functional mode. In this mode, Windows Server 2016 new features are not available. Some examples of the failover clustering features that are not available in mixed mode include:

Site-aware Failover Clusters, Workgroup and Multi-domain Clusters, Virtual Machine Node Fairness, Virtual Machine Start Order, Simplified SMB Multichannel, and Multi-NIC Cluster Networks.

Question: What quorum configuration do you recommend for Windows Server 2016 failover clusters?

Question: Describe the steps for Cluster Operating System Rolling Upgrade.

Lesson 2
Creating and configuring a new failover cluster

After you configure a clustering infrastructure, you should configure specific roles or services that you want to be highly available. You cannot cluster all roles. Therefore, you should first identify the resource that you want to place in a cluster, and then verify if the resource can be clustered. In this lesson, you will learn how to configure roles and applications in clusters, and configure cluster settings.

Lesson Objectives

After completing this lesson, you will be able to:

- Describe the **Validate a Configuration Wizard** and cluster support-policy requirements.
- Explain the process for creating a failover cluster.
- Describe the process for configuring roles.
- Explain how to manage cluster nodes.
- Describe the process for configuring cluster properties.
- Describe the process of configuring failover and failback.
- Describe the process of configuring storage.
- Describe the process of configuring networking.
- Describe the process of configuring quorum options.

The Validation Wizard and the cluster support-policy requirements

The Validation Wizard performs multiple tests for different failover-cluster hardware configurations and settings. You can run the wizard before *and* after you configure the failover cluster, and it verifies whether every component of the failover cluster node meets the hardware, network, infrastructure, and software requirements. The wizard must certify each of the cluster node components for Windows Server 2016 failover clustering.

- Validation wizard performs multiple types of tests, such as:
  - Cluster
  - Inventory
  - Network
  - Storage
  - System
- You can perform validation from the **Validate a Configuration Wizard** or with the **Test-Cluster** Windows PowerShell cmdlet

The Validation Wizard helps you performs multiple types of tests, such as:

- Cluster
- Inventory
- Network
- Storage
- System.

Additionally, it helps you:

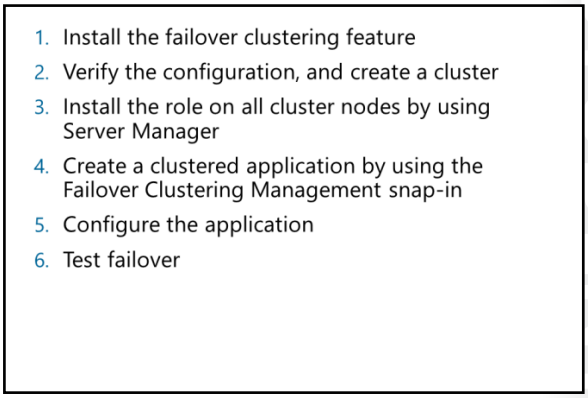
- Detect any issues with hardware or configuration settings.
- Validate changes to a cluster's hardware or configuration settings.
- Perform diagnostic tests on a cluster.

You also can run validation tests by using the **Test-Cluster** cmdlet. Some of the tests require that you perform administrative action before the tests start. For example, before you run storage tests on the disks or storage pools that a clustered role uses, you have to run the **Stop-ClusterGroup** cmdlet to stop the clustered role. After the tests are complete, you can restart clustered roles.

If there are any issues and errors during the validation, use the report that the Cluster Validation Wizard generates to analyze and perform troubleshooting. You also can send the report to the product support team.

The process for creating a failover cluster

You must install the failover clustering feature before you configure any failover cluster role. To implement clustering for a server role, perform the following procedure:



1. Install the failover clustering feature. Use Server Manager or Windows PowerShell to install the failover clustering feature on all computers that will be cluster members.
2. Verify the configuration, and create a cluster with the appropriate nodes. Use the Failover Cluster Management snap-in to validate the configuration, and then to create a cluster with the selected nodes.
3. Install the role on all cluster nodes. Use Server Manager to install the server role that you want to use in the cluster.
4. Create a clustered role by using the Failover Clustering Management snap-in.
5. Configure the cluster role. Configure options on the application that the cluster uses.
6. Test failover. Use the Failover Cluster Management snap-in to test failover by intentionally moving the service from one node to another.

Note: If the cluster is a mixed domain or workgroup cluster, you must use Windows PowerShell to configure the cluster. As of Windows Server 2016 Technical Preview 4, the Failover Clustering Management snap-in is not supported.

After you create the cluster, you can monitor its status by using the **Failover Cluster Management** console, and manage available options.

Demonstration: Creating a failover cluster

In this demonstration, you will learn how to create a failover cluster.

Demonstration Steps

Configure the iSCSI targets

1. On **LON-SVR1**, sign in as **Adatum\Administrator** with the password **Pa$$w0rd**.
2. Open **Server Manager**.
3. In **Server Manager**, go to **File and Storage Services**, and then go to **iSCSI**.
4. Create an iSCSI virtual disk with the following values:
   - Storage location: **C:**
   - Disk name: **iSCSIDisk1**
   - Size: **5 GB**
5. Create a new iSCSI target with the following values:
   - Target name: **lon-svr1**
   - Two iSCSI initiators with the following IP addresses:
     - IP Address: **172.16.0.22**
     - IP Address: **172.16.0.23**
6. Repeat step 4 and 5 to create two more iSCSI virtual disks with disk names **iSCSIDisk2** and **iSCSIDisk3**.

Connect nodes to the iSCSI targets

1. On **LON-SVR2**, open **Server Manager**, start the **iSCSI Initiator**, and configure **Discover Portal** with the IP address **172.16.0.21**.
2. In the **Targets** list, connect to the discovered target.
3. Repeat steps 1 and 2 on **LON-SVR3**.
4. On **LON-SVR2**, open **Disk Management**.
5. Bring the three new disks online, and then initialize them. These are disks 4 through 6.
6. Create a simple volume on each disk, and format it with the NTFS file system. Label the disks **Data1**, **Data2**, and **Data3** respectively.
7. On **LON-SVR3**, open **Disk Management**, and then bring the three new disks online.

Install the Failover Clustering feature

1. On **LON-SVR2**, install the Failover Clustering feature by using Server Manager.
2. On **LON-SVR3**, install the Failover Clustering feature by using Server Manager.

Demonstration: Reviewing the Validation Wizard

The **Validate a Configuration Wizard** runs tests that confirm if the hardware and hardware settings are compatible with failover clustering. You can use this wizard to run the complete set of configuration tests or a subset of tests. We recommend that you run the tests on your servers and storage devices before you configure the failover cluster, and again after you make any major changes to the cluster. You can access the test results in the **%windir%\cluster\Reports** directory.

In this demonstration, you will learn how to validate and configure a failover cluster.

Demonstration Steps

1. On **LON-SVR2**, open the **Failover Cluster Manager** console.
2. Open the **Validate a Configuration Wizard**.
3. Use **LON-SVR2** and **LON-SVR3** as nodes for test.
4. Run all tests.
5. There should be no errors, but some warnings are expected.

Configuring roles

Failover clustering supports clustering several Windows Server roles, such as File Services, DHCP, and Hyper-V. After you install the failover clustering feature on the servers that you plan to configure as failover-cluster nodes, you should install a clustered role by using Cluster Manager or Windows PowerShell.

- Configuring a cluster role includes:
  - Choosing a clustering role
  - Installing the role
  - Verifying the status (Running) on all cluster nodes
- You can configure a cluster role by using:
  - The **Cluster Manager** console
  - The **New-Cluster** Windows PowerShell cmdlet

The following table lists the clustered roles that you can configure on failover cluster nodes and the components that each role requires that you install:

Clustered Role	Role or feature prerequisite
DFS Namespace Server	DFS Namespaces (part of File Server role)
DHCP Server	DHCP Server role
Distributed Transaction Coordinator (DTC)	None
File Server	File Server role
Generic Application	Not applicable
Generic Script	Not applicable
Generic Service	Not applicable
Hyper-V Replica Broker	Hyper-V role
iSCSI Target Server	iSCSI Target Server (part of File Server role)

Clustered Role	Role or feature prerequisite
iSNS Server	iSNS Server Service feature
Message Queuing	Message Queuing Services feature
Other Server	None
Virtual Machine	Hyper-V role
WINS Server	WINS Server feature

To configure a cluster node in Cluster Manger, you should expand the cluster name, right-click **Roles**, click **Configure Role**, and then follow the steps in the wizard. After you complete the installation, you should ensure that the role has a **Running** status on all nodes in the **Failover Clustering** console.

Demonstration: Creating a general file-server failover cluster

In this demonstration, you will see how to cluster a file server role.

Demonstration Steps

Create a failover cluster

- Create a cluster with following parameters:
  - Servers: **lon-svr2** and **lon-srv3**
  - Cluster Name: **Cluster1**
  - Address: **172.16.0.125**

Add a file-server application to the failover cluster

1. On **LON-SVR2**, open the **Failover Cluster Manager** console.
2. In the **Storage** node, click **Disks**, and then verify that three cluster disks are online.
3. Add **File Server** as a cluster role. Select the **File Server for general use** option.
4. Specify **AdatumFS** as **Client Access Name**, use **172.16.0.130** as the address and **Cluster Disk 2** as the storage.
5. Close the **Failover Cluster** window.

Managing failover clusters

You can perform several failover-cluster management tasks, ranging from adding and removing cluster nodes to modifying quorum settings. Some of the most frequently used configuration tasks include:

The most common management tasks include:
- Managing nodes
- Managing networks
- Managing permissions
- Configuring cluster-quorum settings
- Migrating services and applications to a cluster
- Configuring new services and applications
- Removing the cluster

- Managing cluster nodes. For each node in a cluster, you can stop the cluster service temporarily, pause it, initiate a remote desktop session to the node, or evict the node from the cluster. You also can choose to drain the nodes in the cluster, such as if you want to perform maintenance or install updates. This functionality is part of the infrastructure that enables CAU for patching a cluster's nodes.
- Managing cluster networks. You can add or remove cluster networks, and you can configure networks that you will dedicate solely to intercluster communication.
- Managing permissions. If you manage permissions, you delegate rights to administer a cluster.
- Configuring cluster quorum settings. If you configure quorum settings, you determine how quorum is achieved and who can vote in a cluster.
- Migrating services and applications to a cluster. You can implement existing services to a cluster and make them highly available.
- Configuring new services and applications to work in a cluster. You can implement new services in a cluster.
- Removing a cluster. You might remove a cluster if you are removing or moving a service to a different cluster. However, you first must remove the service that you are clustering.

You can perform these administrative tasks by using the **Failover Cluster Management** console, or Windows PowerShell.

Configuring cluster properties

Cluster nodes are mandatory for each cluster. After you create a cluster and move it into production, you might need to configure cluster properties, which you can do by using the **Failover Cluster Manager** console.

The three aspects of managing cluster nodes include:
- Adding nodes after you create a cluster
- Pausing nodes, which prevents resources from running on that node
- Evicting nodes from a cluster, which removes the node from the cluster configuration

Configuration tasks are available in:
- The **Actions** pane of the **Failover Cluster Management** console
- Windows PowerShell

You can configure cluster properties by right-clicking the cluster object in Failover Cluster Manager, and then clicking **Properties**. The tabs available in the properties window include:

- **General**. Displays the name of the cluster, and manages cluster group properties. In Cluster Group properties, you can select preferred owners for the core cluster resource group, and configure failover and failback settings.
- **Resource Types**. Allows you to manage current cluster resource types and add new cluster resource types.

- **Balancer**. Allows you configure virtual machine balancing
- **Cluster Permissions**. Allows you configure cluster security permissions.

There are three aspects of managing cluster nodes:

- Add a node. You can add a node to an established failover cluster by selecting **Add Node** in the **Actions** pane of the **Failover Cluster Management** console. The **Add Node Wizard** prompts you for information about the additional node.
- Pause a node. You can pause a node to prevent resources from failing over or moving to that node. You typically pause a node when it is undergoing maintenance or troubleshooting.
- Evict a node. You can evict a node, which is an irreversible process for a cluster node. After you evict the node, you must add it back to the cluster. You evict nodes when a node is damaged beyond repair or is no longer needed in the cluster. If you evict a damaged node, you can repair or rebuild it, and then add it back to the cluster by using the **Add Node Wizard**.

Each of these configuration actions is available in the **Actions** pane of the **Failover Cluster Management** console and in Windows PowerShell.

Configuring failover and failback

Failover transfers responsibility for providing access to a cluster's resources from one node to another. Failover can occur when one node experiences unplanned downtime because of hardware failure or service failure on an active node can initiate failover to another node. A failover also can occur when an administrator intentionally moves resources to another node for maintenance.

- During failover, the clustered instance and all associated resources move from one node to another
- Failover occurs when:
  - The node that hosts the instance becomes inactive for some reason
  - One of the resources within the instance fails
  - An administrator performs a failover
- The Cluster service can fail back after the offline node becomes active again
- Failover can be planned or unplanned

A failover attempt consists of the following steps:

1. The Cluster service takes all of the instance's resources offline in the order determined by the instance's dependency hierarchy. The dependent resources go offline first, and then the resources on which they depend go offline. For example, if an application depends on a physical-disk resource, the Cluster service takes the application offline first, which enables the application to write changes to the disk before the disk goes offline.
2. The Cluster service attempts to transfer the instance to the node that is next on the instance's list of preferred owners. This occurs after *all* resources are offline.
3. If the Cluster service moves the instance to another node successfully, it attempts to bring all resources online. It begins in reverse order of the dependency hierarchy. In this example, the Cluster service attempts to bring the disk back online first, and then the application. Failover is complete when all resources are online on the new node.

There are exceptions to this rule. One exception is that when failing over Hyper-V Servers that are running Windows Server 2012 R2 or newer, the role does not go offline. Instead, it writes to the source location and the resource owner's destination until the failover is complete. It then moves the I/O to the new failover cluster node.

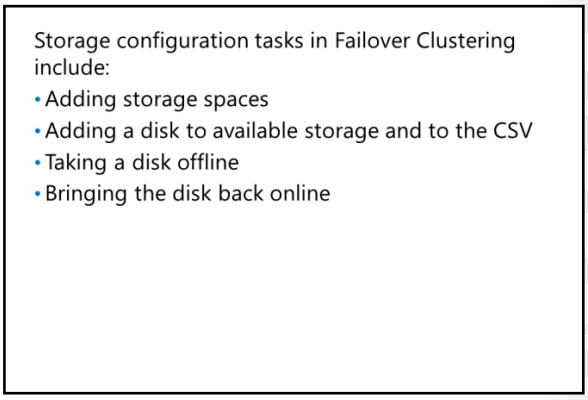
You can preconfigure the Cluster service to fail back instances, which were hosted originally on an offline node, after that offline node becomes active again. When the Cluster service fails back an instance, it uses the same procedures that it performs during failover, which means that the Cluster service takes all of the instance's resources offline, moves the instance, and then brings all the resources in the instance back online.

Planned vs. unplanned failover

The steps discussed previously occur when a failover cluster completes in a planned failover. For an unplanned failover, the failback steps are the same as for a planned failover. However, an unplanned failover usually occurs when one node goes offline without any planning. Therefore, the services abruptly shut down on the node that owns them. This causes the Failover Cluster Manager to skip to step three, and then nodes attempt to bring the offline services back online as quickly as possible.

Configuring storage

Failover clustering uses different storage configurations depending on the cluster role that you deploy. For the clustering roles that are available in failover cluster manager, you should know what storage solution is necessary for the failover clustering role and how to perform storage-configuration tasks.



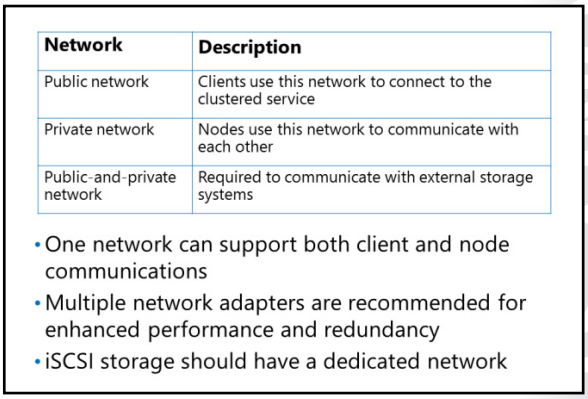
In a failover clustering, storage-configuration tasks include:

- Adding storage spaces. To add storage spaces, configure storage spaces first. After you configure storage spaces, you create clustered storage spaces in the Failover Cluster Manager by performing the following steps:
  - In the **Failover Cluster Manager** console, expand **Cluster Name**, expand **Storage**, right-click **Pools**, and then click **New Storage Pool**.
  - Follow the wizard instructions to include physical disks in the storage pool. You will need at least three physical disks for each failover cluster.
  - As you proceed through the wizard's steps, you must choose resiliency options and virtual disk size.
- Adding a disk. Use the **Failover Cluster Manager** console to add a disk by performing the following steps:
  - Right-click **Failover Cluster Manager**, click **Manage a Cluster**, and then select the cluster to which you want to add a disk.
  - Right click **Storage**, click **Add a disk** and then add the disks from the storage system.
  - If you need to add a disk to a CSV, you should follow the procedure for adding a disk, but then also add a disk to the **CSV** on the cluster.
- Taking a disk offline. In some scenarios, such as for maintenance, you might need to take cluster disk offline by performing the following steps:
  - In the **Failover Cluster Manager** console, right-click the appropriate disk, and then click **Take Offline**.

- Bringing a disk online. After you complete maintenance on the disk, you should bring the disk online by performing the following steps:
    - In the **Failover Cluster Manager** console, right-click the appropriate disk, and then click **Bring Online**.

Configuring networking

Networking and network adapters are important parts of every cluster implementation. You cannot configure a cluster without configuring the networks that the cluster will use. A network can perform one of three roles in a cluster, including that it can be a:



- Private network. A private network carries internal cluster communication. When you use this type of network, cluster nodes exchange heartbeats and check for another node or nodes. The failover cluster authenticates all internal communication. However, administrators who are concerned about security might want to restrict internal communication to networks that are secure physically.
- Public network. A public network provides client computers with access to cluster-application services. Failover Clustering application creates IP address resources on the network that provides clients with access to the Cluster service.
- Public-and-private network. A public-and-private network, or *mixed network*, carries internal cluster communication and connects clients to cluster application services.

When you configure networks in failover clusters, you also must dedicate a network to connect to the shared storage. If you use iSCSI for your shared storage connection, the network will use an IP-based Ethernet communications network. However, you should not use this network for node or client communication. Sharing the iSCSI network in that way might result in contention and latency issues for users and the resource that that the cluster provides.

You can use the private and public networks for both client and node communications. Preferably, you should dedicate an isolated network for the private node communication. The reason is similar to using a separate Ethernet network for iSCSI to avoid resource bottleneck and contention issues. You configure the public network to allow client connections to the failover cluster. Although the public network can provide backup for the private network, a better design is to define alternative networks for the primary private and public networks, or you should team the network adapters that you use for these networks.

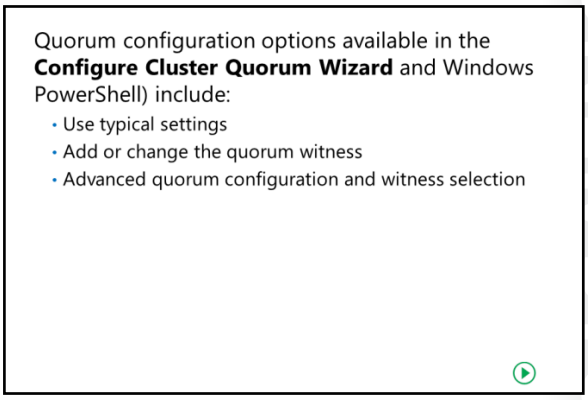
The networking features in failover clusters include the following:

- The nodes transmit and receive heartbeats by using User Datagram Protocol (UDP) unicast, instead of UDP broadcast, which was used in legacy clusters. The messages are sent on port 3343.
- You can include clustered servers on different IP subnets, which reduces the complexity of setting up multisite clusters.
- The Failover Cluster Virtual Adapter is a hidden device that is added by the installation process to each node when you install the failover clustering feature. The installation process assigns to the adapter a media access control (MAC) address based on the MAC address that is associated with the node's first enumerated physical network adapter.

- Failover clusters support IPv6 fully for node-to-node and node-to-client communication.
- You can use DHCP to assign IP addresses or assign static IP addresses to all of the cluster's nodes. However, if some nodes have static IP addresses and you configure others to use DHCP, the **Validate a Configuration Wizard** will display an error. The cluster IP address resources are obtained based on the configuration of the network adapter supporting that cluster network.

Configuring quorum options

Cluster quorum is a critical resource in the failover cluster, because if the quorum is lost, the cluster nodes will not respond to client requests. Therefore, you must configure cluster quorum correctly. Proper cluster configuration ensures that cluster resources will be online during the cluster membership changes, such as planned or unplanned node shutdown, network issues, or any other failure scenarios.



To modify the quorum configuration in a Windows Server 2016 failover cluster, you can use the **Configure Cluster Quorum Wizard** or Windows PowerShell cmdlets. There are three quorum configuration options that are available:

- **Use typical settings**. When you use this option, the failover cluster automatically assigns a vote to each node and dynamically manages the node votes. If hardware configuration includes cluster shared storage, the cluster will select a disk witness. In this scenario, the failover cluster software will automatically choose a quorum and witness configuration that provides the highest availability for the specific cluster configuration.
- **Add or change the quorum witness**. When you use this option, you can add, change or remove a witness resource. A witness resource can be a file share or a disk. In this scenario, the failover cluster software will automatically assign a vote to each node and dynamically manage the node votes.
- **Advanced quorum configuration and witness selection**. This option is needed only when there are specific requirements by the application or by the site location for quorum configuration. In this scenario you will manually modify the quorum witness and add or remove node votes. You might also choose that that cluster dynamically manages node votes. By default, the votes are assigned to all nodes, and the node votes are managed dynamically.

After you choose the quorum configuration option, the cluster will have one of the following quorum modes:

- Node majority (no witness).
- Node majority with witness (disk of file share).
- No majority (disk witness only).

One of the advanced quorum configuration options is to choose dynamic quorum management by cluster. In this scenario, the failover cluster dynamically manages the vote assignment to nodes, where decisions are made based on the state of each node. For example, whenever a node is leaving an active cluster membership, the cluster removes the vote from that node, and whenever a node rejoins the cluster, a vote is automatically assigned to that node.

Dynamic quorum management allows for a cluster to run on the last surviving cluster node, because the cluster can continue to work even in sequential node shutdowns by dynamically adjusting the quorum majority requirement. If you want to verify the cluster-assigned dynamic vote of a node, you can run the **Get-ClusterNode** Windows PowerShell cmdlet and check the **DynamicWeight** property. If the **DynamicWeight** property is **0**, the node does not have a quorum vote. However, if the **DynamicWeight** property is **1**, the node has a quorum vote. By running the **Validate Cluster Quorum** validation test, you can verify the vote assignment for all cluster nodes. However, dynamic quorum management cannot allow the cluster to survive a simultaneous failure of a majority of voting nodes, because the cluster must always have a quorum majority at the time of a node shutdown or failure. Furthermore, if you explicitly remove a vote from a node, the cluster cannot dynamically add or remove that vote.

Before deploying the cluster into production, we recommend that you verify detailed cluster configuration by using the **Validate a Configuration Wizard**, or the **Test-Cluster** Windows PowerShell cmdlet. Furthermore, we do not recommend that you change the quorum configuration unless you determine that the change is appropriate for specific scenarios, such as adding or evicting nodes; when nodes or witnesses fail and you cannot recover them quickly; or if you need to recover a cluster in a multisite disaster-recovery scenario.

Demonstration: Configuring the quorum

In this demonstration, you will learn how to configure a quorum.

Demonstration Steps

Determine the current quorum model

1. On **LON-SVR2**, open **Failover Cluster Manager** and **Windows PowerShell**.
2. In the **Windows PowerShell** console, run the following command:

```
get-clusterquorum | Get-Member
```

3. Review the command's output to determine the viable options that you can configure.
4. In the **Windows PowerShell** console, run the following command:

```
Get-ClusterQuorum | Select Cluster, QuorumResource, QuorumType
```

5. Review the command's output.

Create a file share on LON-SVR1

- On **LON-SVR1**, in **File Explorer**, create a shared folder called **C:\FSW**. Use **Share with specific people**, and assign **Everyone** Read/Write access.

Convert from Disk Witness to File Share Witness

- On **LON-SVR2**, in the **Windows PowerShell** console, run the following command:

```
Set-ClusterQuorum -NodeAndFileShareMajority "\\LON-SVR1\fsw"
```

Validate quorum change

1. On **LON-SVR2**, in the **Windows PowerShell** console, run the following command:

```
Get-ClusterQuorum | Select Cluster, QuorumResource, QuorumType
```

2. Review the command's output.

   Question: In Failover Cluster Manager what are some of the Windows Server 2016 roles that you can configure?

Sequencing Activity

Question: The following are the steps for clustering server roles. Arrange them in the correct order by numbering each step.

	Steps
	Install the failover clustering feature. Use Server Manager or Windows PowerShell to install the failover clustering feature on all computers that will be cluster members.
	Verify the configuration, and create a cluster with the appropriate nodes. Use the Failover Cluster Management snap-in to validate the configuration and to create a cluster with the selected nodes.
	Install the role on all cluster nodes. Use Server Manager to install the server role that you want to use in the cluster.
	Create a clustered application by using the Failover Clustering Management snap-in.
	Configure the application. Configure the options on the application that the cluster uses.
	Test failover. Use the Failover Cluster Management snap-in to test failover by intentionally moving the service from one node to another.

Lab A: Implementing failover clustering

Scenario

A. Datum Corporation is looking to ensure that its critical services, such as file services, have better uptime and availability. You decide to implement a failover cluster with file services to provide better uptime and availability.

Objectives

After completing this lab, you will be able to:

- Create a failover cluster.
- Verify quorum settings and that you added a node.
- Configure CAU on the failover cluster.

Lab Setup

Estimated Time: **45 minutes**

Virtual machines: **20740A-LON-DC1**, **20740A-LON-SVR1**, **20740A-LON-SVR2**, **20740A-LON-SVR3**, **20740A-LON-SVR5**, and **20740A-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 **20740A-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 through 4 for **20740A-LON-SVR1**, **20740A-LON-SVR2**, **20740A-LON-SVR3**, and **20740A-LON-CL1**.
6. Repeat steps 2 and 3 for **20740A-LON-SVR5**.

Exercise 1: Creating a failover cluster

Scenario

A. Datum has important applications and services that they want to make highly available. Therefore, you decide to implement failover clustering by using iSCSI storage. You will configure iSCSI storage to support your failover cluster, and then configure a failover cluster.

To configure a failover cluster, you plan to implement the core components for failover clustering, validate the cluster, and then create the failover cluster. After you create a cluster infrastructure, you plan to configure a highly available file server, and then implement settings for failover and failback. Additionally, you also will perform failover and failback tests.

The main tasks for this exercise are as follows:

1. Connect cluster nodes to iSCSI shared storage.
2. Install the Failover Cluster feature.
3. Validate the servers for failover clustering.
4. Create the failover cluster.
5. Add the file-server application to the failover cluster.
6. Add a shared folder to a highly-available file server.
7. Configure failover and failback settings.
8. Validate the highly available file-server deployment.
9. Validate the failover and quorum configuration for the File Server role.

▶ Task 1: Connect cluster nodes to iSCSI shared storage

Configure the iSCSI targets

1. On **LON-SVR1**, open the **Server Manager**.
2. In **Server Manager**, go to **File and Storage Services**, and then go to **iSCSI**.
3. Create an iSCSI virtual disk with the following values:
   - Storage location: **C:**
   - Disk name: **iSCSIDisk1**
   - Size: **5 GB**
4. Create a new iSCSI target with the following values:
   - Target name: **lon-svr1**
   - Two iSCSI initiators with the following IP addresses:
     - IP Address: **172.16.0.22**
     - IP Address: **172.16.0.23**
5. Repeat step 4 and 5 to create two more iSCSI virtual disks with disk names **iSCSIDisk2** and **iSCSIDisk3**.

Connect nodes to the iSCSI targets

1. On **LON-SVR2**, open **Server Manager**, start the **iSCSI Initiator**, and then configure **Discover Portal** with the IP address **172.16.0.21**.
2. In the **Targets** list, connect to the discovered target.
3. Repeat steps 1 and 2 on **LON-SVR3**.
4. On **LON-SVR2**, open **Disk Management**.
5. Bring the three new disks online, and then initialize them. These are disks 4 through 6.
6. Create a simple volume on each disk, and format it with NTFS. Label the disk **Data1**, **Data2**, and **Data3** respectively.
7. On **LON-SVR3**, open **Disk Management**, and then bring the three new disks online.

▶ Task 2: Install the Failover Cluster feature

1. On **LON-SVR2**, install the Failover Clustering feature by using Server Manager.
2. On **LON-SVR3**, install the Failover Clustering feature by using Server Manager.

▶ Task 3: Validate the servers for failover clustering

1. On **LON-SVR2**, open the **Failover Cluster Manager** console.
2. Open the **Validate a Configuration Wizard**.
3. Use **LON-SVR2** and **LON-SVR3** as nodes for test.
4. Run all tests.
5. There should be no errors, but you may receive some warning messages.

▶ Task 4: Create the failover cluster

- Create a cluster with the following parameters:
  - Servers: **LON-SVR2** and **LON-SVR3**
  - Cluster Name: **Cluster1**
  - Address: **172.16.0.125**

▶ Task 5: Add the file-server application to the failover cluster

1. On **LON-SVR2**, open the **Failover Cluster Manager** console.
2. In the **Storage** node, click **Disks**, and verify that three cluster disks are online.
3. Add **File Server** as a cluster role. Select the **File Server for general use** option.
4. Specify **AdatumFS** as **Client Access Name**, use **172.16.0.130** as the address, and **Cluster Disk 2** as the storage.
5. Close the **Failover Cluster** window.

▶ Task 6: Add a shared folder to a highly-available file server

1. On **LON-SVR3**, from **Server Manager**, open the **Failover Cluster Manager** console.
2. Open the **New Share Wizard**, and add a new shared folder to the AdatumFS cluster role.
3. Specify the File share profile as **SMB Share – Quick**.
4. Accept the default values on the **Select the server and the path for this share** page.
5. Name the shared folder **Docs**.
6. Accept the default values on the **Configure share settings** and **Specify permissions to control access** pages.
7. At the end of the **New Share Wizard**, create the share.

▶ Task 7: Configure failover and failback settings

1. On **LON-SVR3**, in the **Failover Cluster Manager** console, open the **Properties** for the AdatumFS cluster role.
2. Enable failback between 4 and 5 hours.
3. Select both **LON-SVR2** and **LON-SVR3** as the preferred owners.
4. Move **LON-SVR3** to the first space in the preferred owners list.

▶ Task 8: Validate the highly available file-server deployment

1. On **LON-DC1**, open **File Explorer**, and then attempt to access the **\\AdatumFS** location. Verify that you can access the **Docs** folder.
2. Create a text document inside this folder named **test.txt**.
3. Verify the current owner of **AdatumFS**.

Note: The owner will be **LON-SVR2** or **LON-SVR3**.

4. On **LON-SVR2**, in the **Failover Cluster Manager** console, move **AdatumFS** to the second node.
5. On **LON-DC1**, in File Explorer, verify that you can still access the **\\AdatumFS** location.

▶ Task 9: Validate the failover and quorum configuration for the File Server role

1. On **LON-SVR2**, determine the current owner for the **AdatumFS** role.
2. Stop the **Cluster** service on the node that is the current owner of the **AdatumFS** role.
3. Try to access **\\AdatumFS** from **LON-DC1** to verify that **AdatumFS** has moved to another node and that the **\\AdatumFS** location is still available.
4. Start the **Cluster** service on the node in which you stopped it in step 2.
5. Browse to the **Disks** node, and take the disk marked as **Disk Witness in Quorum** offline.
6. Verify that **AdatumFS** is still available by trying to access it from **LON-DC1**.
7. Bring the disk witness online.
8. Open **Cluster Quorum Settings**.
9. Choose to perform advanced configuration.
10. Change the witness disk to **Cluster Disk 3**. Do not make any other changes.

Results: After completing this exercise, you should have created a failover cluster successfully, configured a highly available file server, and tested the failover scenarios.

Exercise 2: Verifying quorum settings and adding a node

Scenario

As A. Datum's business grows, it is becoming increasingly important that many of the applications and services on the network have increased scalability and remain high available at all times. Your responsibility is to increase the number of cluster nodes in the current cluster, and to evaluate and suggest a new quorum model.

The main tasks for this exercise are as follows:

1. Remotely connect to a cluster.
2. Check the assigned votes in the Nodes section.
3. Verify the status of the disk witness.

4. Add a node in the cluster.
5. Verify the assigned votes.
6. Prepare for the next lab.

▶ Task 1: Remotely connect to a cluster

- On **LON-CL1**, remotely connect to the **AdatumFS** failover cluster by using **Failover Cluster Manager** in Remote Server Administration Tools RSAT.

▶ Task 2: Check the assigned votes in the Nodes section

1. On **LON-SVR2**, in **Windows PowerShell**, run following cmdlet to check the assigned votes:

```
Get-ClusterNode | select name, nodeweight, ID, state
```

2. Verify that **NodeWeight** property of a cluster node has value **1**, which means that the quorum vote of the node is assigned and that the cluster is managing it.

▶ Task 3: Verify the status of the disk witness

- On **LON-SVR2**, in the **Windows PowerShell** console, run the following command to verify the disk witness status:

```
Get-ClusterQuorum | Select Cluster, QuorumResource, QuorumType
```

▶ Task 4: Add a node in the cluster

1. On **LON-SVR2**, in **Failover Cluster Manager**, add the **LON-SVR5** node in the **Cluster1** failover cluster.
2. Perform validation of the cluster by using default values. You do not need to view the validation report.

▶ Task 5: Verify the assigned votes

1. On **LON-SVR2**, in **Windows PowerShell** console, run following cmdlet to check the assigned votes:

```
Get-ClusterNode | select name, nodeweight, ID, state
```

2. Verify that **NodeWeight** property of a cluster node has value **1**, which means that the quorum vote of the node is assigned and that the cluster is managing it.

Results: After completing this exercise, you should have added another node in the cluster successfully, and changed the quorum to the witness disk.

▶ Task 6: Prepare for the next lab

- When you finish the lab, leave the virtual machines running for the subsequent lab.

Question: What information do you need for planning a failover-cluster implementation?

Question: After running **Validate a Configuration Wizard**, how can you resolve the network communication's single point of failure?

Question: In which situations might it be important to enable failback of a clustered application during a specific time?

Lesson 3
Maintaining a failover cluster

Once you have your cluster infrastructure running, you should establish monitoring procedures to prevent possible failures. Additionally, you should have backup and restore procedures for cluster configuration. In Windows Server 2016, CAU allows you to update cluster nodes without downtime. In this lesson, you will learn how to monitor, backup and restore, and update cluster nodes.

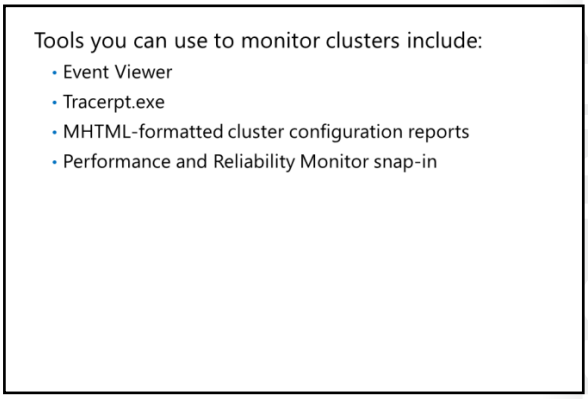
Lesson Objectives

After completing this lesson, you will be able to:

- Describe how to monitor failover clusters.
- Describe how to back up and restore failover cluster configurations.
- Describe how to maintain failover clusters.
- Describe how to manage failover clusters.
- Describe cluster aware updating.

Monitoring failover clusters

Many tools are available to help you monitor failover clusters. You can use standard Windows Server operating system tools such as Event Viewer and the Performance and Reliability Monitor snap-in to review cluster event logs and performance metrics. You also can use the Tracerpt.exe tool to export data for analysis. Additionally, you can use the Multipurpose Internet Mail Extension Hypertext Markup Language (MHTML)-formatted cluster configuration reports and the **Validate a Configuration Wizard** to troubleshoot problems with the cluster configuration and hardware changes.



Event Viewer

If problems arise in a cluster, you can use the Event Viewer to view events with a Critical, Error, or Warning severity level. Additionally, you can view informational-level events in the Failover Clustering Operations log, which you can access in the Event Viewer in the **Applications and Services Logs\Microsoft\Windows** folder. Informational-level events typically are common cluster operations, such as cluster nodes leaving and joining the cluster, or resources going offline or coming online.

In earlier Windows Server versions, event logs were replicated to each node in the cluster. This simplified cluster troubleshooting because you could review all event logs on a single cluster node. Windows Server 2012 and newer does not replicate the event logs between nodes. However, the Failover Cluster Management snap-in has a **Cluster Events** option that allows you to view and filter events across all cluster nodes. This feature is helpful in correlating events across cluster nodes.

The Failover Cluster Management snap-in also provides a **Recent Cluster Events** option that queries all the Error and Warning events from all the cluster nodes in the last 24 hours.

You can access additional logs, such as the Debug and Analytic logs, in the Event Viewer. To display these logs, modify the view on the top menu by selecting the **Show Analytic and Debug Logs** options.

Event tracing for Windows

Event tracing for Windows is a kernel component that is available early after startup, and late into shutdown. It allows fast tracing and delivery of events to trace files and to consumers. However, because its design makes it fast, it allows only basic in-process filtering of events on the basis of event attributes.

The event trace log contains a comprehensive accounting of the failover-cluster actions. To view the data, use Tracerpt.exe to access the information in the event trace log. Tracerpt.exe parses the event trace logs only on the node on which it runs. All of the individual logs are collected in a central location. To transform the XML file into a text file, or into an HTML file that you can open in Microsoft Edge or Internet Explorer, you can parse the XML-based file by using the Microsoft XSL parsing command-prompt tool Msxsl.exe and an XSL-style sheet.

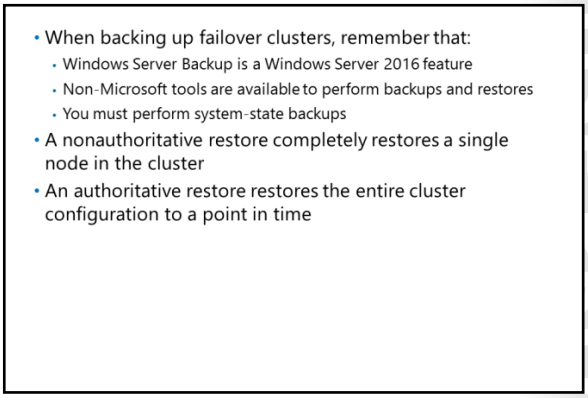
Performance and Reliability Monitor snap-in

You also can use the Performance and Reliability Monitor snap-in to help monitor failover clusters. The Performance and Reliability Monitor snap-in allows you to:

- Monitor the performance baseline on application-performance on each node. To determine how an application is performing, you can view and trend specific information on system resources that each node is using.
- Monitor the performance baseline on application-failures and stability on each node. You can pinpoint when application failures occur, and match the application failures with other events on the node.
- Modify trace log settings. You can start, stop, and adjust trace logs, including their size and location.

Backing up and restoring failover-cluster configuration

Configuring clusters can be a time-consuming and detail-oriented process. To avoid having to repeat the process, you should ensure that you back up cluster configurations. You can use Windows Server Backup or a non-Microsoft backup tool to perform a backup and restore of cluster configurations.



Backing up a cluster

When you back up your cluster configuration, be aware of the following:

- You must test your backup and recovery process before you put a cluster into production.
- You must add the Windows Server Backup feature, if you decide to use it. You can do this by using Server Manager.

Windows Server Backup is the built-in backup and recovery software for Windows Server 2016. To complete a backup successfully, you should remember that:

- For a backup to succeed in a failover cluster, the cluster must be running and must have quorum. In other words, enough nodes must be running and communicating that the cluster achieves quorum. To do this, you could utilize a witness disk or witness file share, depending on your quorum's configuration.
- You must back up all clustered applications. If you cluster a SQL Server database, you must have a backup plan for the databases and configuration outside the cluster configuration.
- If you must back up the application data, the disks on which you store the data must be available to the backup software. You can achieve this by running the backup software from the cluster node that owns the disk resource, or by running a backup against the clustered resource over the network.
- The cluster service keeps track of which cluster configuration is the most recent, and it replicates that configuration to all cluster nodes. If the cluster has a witness disk, the Cluster service also replicates the configuration to the witness disk.

Restoring a cluster

When restoring a cluster, there are two types of restore methods that are available to you:

- Nonauthoritative restore. Use a nonauthoritative restore when a single node in the cluster is damaged or rebuilt, and the rest of the cluster is operating correctly. Perform a nonauthoritative restore by restoring the system recovery (system state) information to the damaged node. When you restart that node, it joins the cluster and receives the latest cluster configuration automatically.
- Authoritative restore. Use an authoritative restore when you must roll back the cluster configuration. For example, you would use an authoritative restore if an administrator accidentally removed clustered resources or modified other cluster settings, and you need to revert the cluster to a previous point in time. To perform authoritative restore, stop the cluster resource on each node, and then perform a system recovery (system state) on a single node by using the command-line Windows Server Backup interface. After the restored node restarts the cluster service, the remaining cluster nodes also can start the cluster service.

Maintaining failover clusters

Although cluster validation in Windows Server 2016 failover clustering prevents misconfigurations and nonworking clusters, you still might have to perform cluster troubleshooting. To troubleshoot a failover cluster, use the following guidelines:

- Use the **Validate a Configuration Wizard** to identify configuration issues that might cause cluster problems.
- Review cluster events and trace logs to identify application or hardware issues that might cause an unstable cluster.

Failover cluster troubleshooting techniques include:

- Using the **Validate a Configuration Wizard**
- Reviewing events in logs (cluster, hardware, storage)
- Defining a process for troubleshooting failover clusters
- Reviewing storage configuration
- Checking for group and resource failures

- Review hardware events and logs to help pinpoint specific hardware components that might cause an unstable cluster.
- Review SAN components, switches, adapters, and storage controllers to help identify any potential problems.

When troubleshooting failover clusters, you must:

- Identify the perceived problem by collecting and documenting the problem's symptoms.
- Identify the problem's scope so that you can understand what it affects and what impact that effect has on the application and the clients.
- Collect information so that you can understand and pinpoint the possible problem accurately. After you identify a list of possible issues, you can prioritize them by probability, or by a repair's potential impact. If you cannot identify the problem, you should attempt to recreate the problem.
- Create a schedule for repairing the problem. For example, if the problem only affects a small subset of users, you can delay the repair to an off-peak time so that you can schedule downtime.
- Complete and test each repair one at a time so that you can identify the fix.

To troubleshoot SAN issues, start by checking physical connections, and by reviewing each of the hardware component logs. Next, run the **Validate a Configuration Wizard** to verify that the current cluster configuration is supported. When you run the **Validate a Configuration Wizard**, ensure that the storage tests that you select can run on an online failover cluster. Several of the storage tests cause loss of service on the clustered disk when the tests run.

Troubleshooting group and resource failures

To troubleshoot group and resource failures:

- Use the Dependency Viewer in the Failover Cluster Management snap-in to identify dependent resources.
- Review the Event Viewer and trace logs for errors from the dependent resources.
- Determine whether the problem happens only on a specific node or nodes by trying to recreate the problem on different nodes.

Managing cluster-network heartbeat traffic

Cluster-network heartbeat traffic is very important for determining node health in Windows Server Failover Clustering. If one node cannot communicate with another over a network, the communicating nodes will initiate a recovery action to bring applications, services, and data online.

Windows Failover Clustering health-monitoring configuration has default settings that are optimized for different failure scenarios. However, you can modify those settings to meet requirements for a specific type of configuration or high-availability scenarios.

- Types of network monitoring:
  - Aggressive
  - Relaxed
- Network-monitoring parameter settings:
  - **Delay**
  - **Threshold**
- Windows PowerShell cmdlet examples:

```
Get-Cluster | fl *subnet*
(Get-Cluster).SameSubnetThreshold=10
```

There are two types of network monitoring in failover-clustering scenarios:

- Aggressive monitoring. Aggressive monitoring provides the fastest detection of server failure and also provides fast recovery, which means this type of monitoring provides the highest level of availability. However, this type of monitoring initiates a failover procedure even if a short transient network outage occurs, which does not always indicate that a server has failed.
- Relaxed monitoring. Relaxed monitoring provides more tolerance in network-failure detection, which means that in some cases of very short network outage, a cluster's nodes do not initiate a failover procedure. However, in this scenario, if node fails, it takes longer for other nodes to initiate a failover procedure.

Parameter settings that define network-health monitoring include:

- **Delay**. This is the frequency of the cluster heartbeats, such as the number of seconds before the next heartbeat is sent. Parameters for delay that you can configure are:
  - **SameSubnetDelay**. A parameter that controls the delay between heartbeats measured in milliseconds, for nodes located on the same subnet.
  - **CrossSubnetDelay**. A paremeter that controls the time interval, measured in milliseconds, that the cluster network driver waits between sending Cluster Service heartbeats across subnets.
  - **CrossSiteDelay**. A parameter that controls the delay between heartbeats, measured in milliseconds, for nodes located in different sites.
- **Threshold**. This is the number of missed heartbeats before the cluster initiates a failover procedure. Parameters for threshold that you can configure are:
  - **SameSubnetThreshold**. A parameter that controls how many heartbeats can be missed by the nodes located on the same subnet, before the network route is declared as unreachable.
  - **CrossSubnetThreshold**. A parameter that controls how many Cluster Service heartbeats can be missed by nodes located in different subnets before a node in one site determines that the Cluster Service on a node in a different site has stopped responding.
  - **CrossSiteThreshold**. A parameter that controls the number of missed heartbeats between nodes in different sites before a node in one site determines that the network interface on a node in a different site is considered down.

For example, if you configure **CrossSubnetDelay** parameter to **3** seconds and **CrossSubnetThreshold** to **10** heartbeats missed before initiating failover, the cluster will have a total network tolerance of 30 seconds before it initiates a failover procedure.

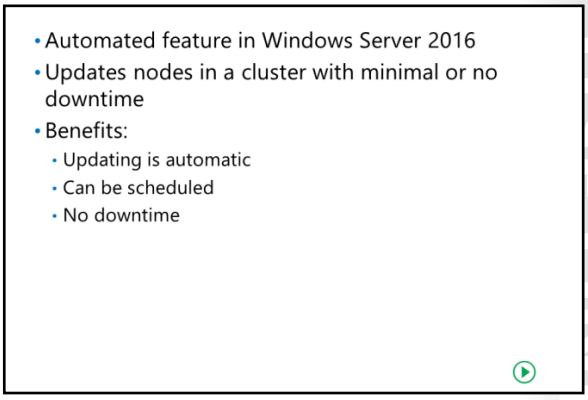
To view the configuration of your network-health monitoring, you can use **Get-Cluster** Windows PowerShell cmdlet. For example, to list **Delay**, **Treshold CrossSubnet** and **SameSubnet** parameters, you should type the following at a command prompt, and then press Enter:

```
Get-Cluster | fl *subnet*
```

To configure **SameSubnetTreshold** parameter with value **10**, you should type the following at a command prompt, and then press Enter:

```
(Get-Cluster).SameSubnetThreshold = 10
```

What is cluster-aware updating?



You must be careful when applying operating-system updates to a cluster's nodes. In earlier Windows Server versions, you can provide zero downtime for a clustered role, but you must update cluster nodes manually and one at a time. Additionally, you must move resources manually from the node that you are updating to another node. This procedure can be very time consuming. In Windows Server 2012, Microsoft implemented CAU, a feature for automatic updating of cluster nodes.

CAU is a feature that allows administrators to update cluster nodes automatically with little or no loss in availability during the update process. During an update procedure, CAU transparently takes each cluster node offline, installs the updates and any dependent updates, performs a restart if necessary, brings the node back online, and then moves to update the next node in a cluster.

For many clustered roles, this automatic update process triggers a planned failover, and it can cause a transient service interruption for connected clients. However, for continuously available workloads in Windows Server 2016, such as Hyper-V with live migration or file server with SMB Transparent Failover, CAU can orchestrate cluster updates with no effect on the service availability.

How CAU works?

CAU orchestrates complete cluster updating in one of the following two modes:

- Remote updating mode. In this mode, you configure a computer that runs Windows Server 2012 R2, Windows 8.1 or newer as a CAU orchestrator. To configure a computer as a CAU orchestrator, you must install the failover-clustering administrative tools. The orchestrator computer should not be a member of the cluster that you are updating. From the orchestrator computer, the administrator triggers on-demand updating by using a default or custom Updating Run profile. Remote-updating mode is useful for monitoring real-time progress during the Updating Run and for clusters that run on Server Core installations of Windows Server 2016.
- Self-updating mode. In this mode, you configure the CAU clustered role as a workload on the failover cluster that you are updating, and then you define an associated update schedule. In this scenario, CAU does not have a dedicated orchestrator computer. The cluster updates itself at scheduled times by using a default or custom Updating Run profile. During the Updating Run, the CAU orchestrator process starts on the node that currently owns the CAU clustered role, and the process performs updates sequentially on each cluster node.

  In the self-updating mode, CAU can update the failover cluster by using a fully automated, end-to-end updating process. An administrator also can trigger updates on-demand in this mode or use remote updating. In the self-updating mode, an administrator can access summary information about an Updating Run in progress by connecting to the cluster and then running the Windows PowerShell **Get-CauRun** cmdlet.

To use CAU, you must install the failover clustering feature in Windows Server 2016, and then create a failover cluster. The components that support CAU functionality then install automatically on each cluster node.

You also must install the CAU tools, which the Failover Clustering Tools include. These tools also are part of the Remote Server Administration Tools (RSAT). The CAU tools consist of the CAU GUI tools and the Windows PowerShell cmdlets. When you install the failover-clustering feature, the Failover Clustering Tools install by default on each cluster node. You also can install these tools on a local or a remote computer that runs Windows Server 2016 or Windows 10, and that has network connectivity to the failover cluster.

Demonstration: Configuring CAU

In this demonstration, you will learn how to configure CAU.

Demonstration Steps

1. Install the **Failover Clustering Tools** feature on **LON-DC1**.
2. Run **Cluster-Aware Updating** on **LON-DC1**, and configure it to connect to **CLUSTER1**.
3. Start the process to **Generate Update Preview List**, and then click **Cancel** to cancel the update process because the virtual machines are not connected to the Internet.

Note: In a real-world scenario, you should wait until the update preview list generates.

4. Review the available options under the **Cluster Actions** pane on the right side of **Cluster Aware Updating** window for the Updating Run Profile.
5. Review the options for **Apply updates to this cluster**, and then cancel the application of updates.
6. Configure **Cluster self-updating options** on **LON-SVR2**.

Question: What are some of the troubleshooting techniques for failover clusters?

Question: You have an eight-node cluster that is running Windows Server 2016 Hyper-V. How would you update each node on a schedule without downtime?

Lesson 4
Troubleshooting a failover cluster

Failover clustering provides high availability for business-critical applications. Therefore, you need to learn how to troubleshoot the failover-clustering feature in Windows Server 2016 so that you can help prevent potential downtime of business-critical applications.

Lesson Objectives

After completing this lesson, you will be able to:

- Describe how to detect communication issues.
- Explain how to repair the cluster name object in AD DS.
- Describe how to start a cluster with no quorum.
- Describe how to review a Cluster.log file.
- Describe how to monitor performance with failover clustering.
- Describe how to use Event Viewer with failover clustering.
- Explain how to interpret the output of Windows PowerShell troubleshooting cmdlets.

Communication issues

A network is one of the most critical resources that cluster nodes use to communicate and to determine which nodes are up and running. A healthy network with fast performance ensures healthy cluster applications. Therefore, proper network configuration of cluster nodes, network infrastructure, and network devices is essential for healthy applications that run in failover clustering.

- The following might cause communications issues in failover clustering:
  - Network latency
  - Network failures
  - Network-adapter driver issues
  - Firewall rules
  - Security software
- You can use **Get-ClusterLog** cmdlet to generate the **Cluster.log** file for troubleshooting located in **C:\Windows\Cluster\Reports**

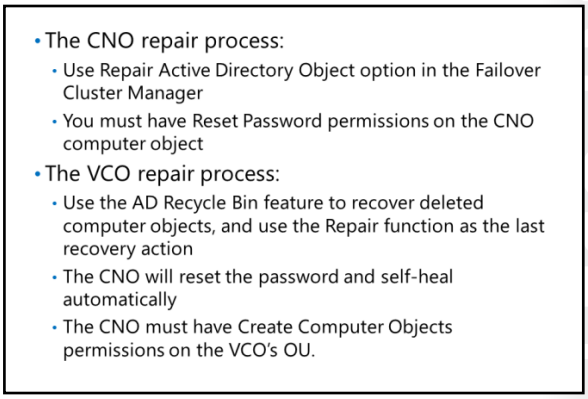
Network issues that can potentially threaten failover clustering include:

- Network latency. Cluster nodes might interpret network latency as the network being unavailable, which might failovers or loss of quorum. While latency should not appear in local area networks (LANs), it might appear in communication between different sites. Organizations might sign a service-level agreement (SLA) with the network provider, who guarantees an appropriate latency level that is acceptable.
- Network failures. Different types of network failures might cause cluster nodes to fail over or loose quorum even when all the cluster nodes are running and healthy. Therefore, the networking team must ensure that there are no network failures in the LAN. However, it can be challenging to ensure that there are no network failures between different sites in a stretch-cluster scenario, particularly if a third party provides network communications. In that scenario, an organization might sign an SLA with a network provider who guarantees an appropriate level of network availability.
- Network cards drivers. If network adapters on cluster nodes do not have the correct network driver, issues might occur in network traffic that cause communication issues between cluster nodes, and therefore cause frequent failovers or even quorum loss. Therefore, network adapters must have tested and approved the installed network drivers.

- Firewall rules. In some organizations, the administrators responsible for server clustering might not communicate clearly with the networking team about the type of the ports and port numbers that failover clustering is using, and for applications that are using the failover-clustering technology. Therefore, the firewall might block network communication between the cluster nodes, which causes a cluster to quit functionality correctly. Issues also might occur if the networking team reconfigures the firewalls or replaces the existing firewall infrastructure with the new firewalls, without first verifying the complete list of ports that must be open.
- Antimalware or intrusion detection software. Many organizations install different types of security software, such as antimalware and intrusion-detection software, to protect from various security threats. However, security software might block some network communication between cluster nodes and cause issues in cluster functionality. Therefore, you should read best practices and technical documentation from security software vendors so that you ensure that you configure security software on cluster nodes correctly.

One of the troubleshooting steps that you can use is to analyze the **Cluster.log** file, which by default is in the **C:\Windows\Cluster\Reports** folder. You can generate the **Cluster.log** file on each server by using the **Get-ClusterLog** cmdlet in Windows PowerShell. The **Cluster.log** file includes details about the cluster objects, such as resources, groups, nodes, networks, network adapters, and volumes, and you can use this information to troubleshoot cluster issues. The **Cluster.log** file in Windows Server 2016 also includes a new verbose log that exists alongside the diagnostic channel for failover clustering, and you can find it under the diagnostic verbose section. Furthermore, in Windows Server 2016, you can include other event channels, such as the system-event log channel.

Repairing the cluster name object in AD DS



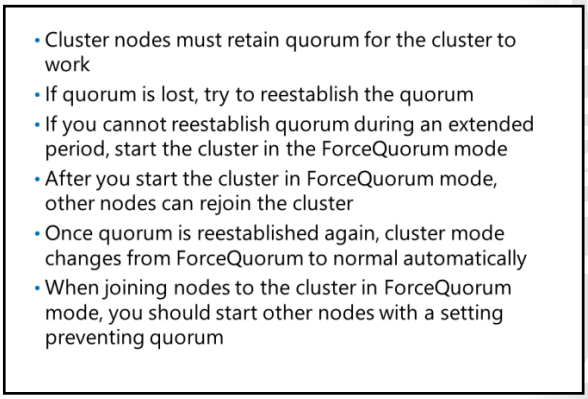
CNO represents a cluster name resource in AD DS, and it changes its associated computer object's password in AD DS, by default, every 30 days. In some scenarios, the computer object password does not match the password that is in the cluster database; for example, when an administrator mistakenly deletes the CNO, or an administrator runs a script that deletes the CNO. Since the CNO password doesn't match the password that is in the cluster database, the cluster service cannot sign in to the computer object, which causes the network name to go offline. If the network name is not online, Kerberos protocol will start generating errors because it cannot register in a secure DNS zone. Furthermore, if you perform a live migration, it will fail. In this scenario, you resynchronize the password for cluster computer objects by using the Repair **Active Directory Object** option in the Failover Cluster Manager. During the repair process, the administrator who is signed in currently will use his own credentials to reset the computer objects password. If you need to run a repair task, you must have the Reset Password permissions on the CNO computer object.

The CNO also is responsible for password management of all other virtual computer objects (VCOs) for the cluster's other cluster network names. If the VCO password fails to synchronize, the CNO resets the password and repairs automatically, so you will not need to reset the VCO password. The automatic repair procedure checks if the associated VCO computer object exists in AD DS. If it has been deleted, you can perform the repair process to recreate the missing computer object. However, the automatic-recovery process for VCOs might interfere with some applications. Therefore, we recommend that you use the AD Recycle Bin feature to recover deleted computer objects, and use the Repair function only if the

AD Recycle Bin feature does not recover your VCO. However, please note that the CNO cannot recreate VCO computer accounts if it does not have Create Computer Objects permissions on the VCO's organizational unit (OU).

Starting a cluster with no quorum

In a failover-clustering configuration, cluster nodes must retain quorum to continuing working. If any failures occur, and the cluster loses quorum, the cluster will not have enough quorum votes to start. Therefore, in any failure scenario that includes quorum loss, you should check the cluster-quorum configuration and perform troubleshooting if the cluster no longer has quorum. You also can verify quorum information in the Event Viewer system log, where the Event ID 1177 will appear.



During the cluster-recovery process, we recommend that you first try to reestablish a quorum and start the cluster nodes. However, there are situations in which reestablishing quorum is not possible in a specific time period. For example, if an organization has a stretched cluster in which one of the sites has a majority of the nodes, and it loses power for an extended period, administrators and business owners might decide to bring the cluster online forcibly and without quorum in the site that has the smaller number of nodes. This allows continued functioning in comparison to waiting several days until power is restored in the site where a majority of the nodes reside. If you run the Windows PowerShell cmdlet: **Start-ClusterNode** with the **–FQ switch**, it forces the cluster to override the cluster quorum configuration and starts in ForceQuorum mode. After a cluster starts in the ForceQuorum mode, you can bring the majority of nodes that were down back online to rejoin the cluster. When a majority of the nodes rejoins the cluster, the cluster will change its mode automatically from ForcedQuorum to normal, which means you do not need to restart it.

The cluster node that starts the cluster by force uses its configuration and replicates the configuration to other available nodes. While the cluster is running in ForceQuorum mode, it ignores quorum-configuration settings until a majority of the nodes are online again. After you start the first cluster node in the ForceQuorum mode, you must start the other nodes with a setting to prevent quorum by running the Windows PowerShell cmdlet **Start-ClusterNode** with the **–PQ switch**. When you start a node with a setting that prevents quorum, the cluster service joins an existing running cluster. If you do not start a node with a setting that prevents quorum, the cluster service creates a *split cluster*, which is new cluster instance. Therefore, we recommend that after you start a cluster in ForceQuorum mode, you must start the remaining nodes with a setting to prevent quorum.

Demonstration: Reviewing the Cluster.Log file

In this demonstration, you will learn how to review a **Cluster.log** file.

Demonstration Steps

1. Switch to **LON-SVR3**.
2. In Windows PowerShell, run the following cmdlet:

```
Get-ClusterLog
```

3. Open **File Explorer**, go to **C:\Windows\Cluster\Reports**, and then open **Cluster.log** file.
4. Review the **Cluster.log** file.
5. Search the **Cluster.log** file for the words **heartbeat** and **NETFT** for network related entries.
6. Search the **Cluster.log** file for the word **ACCEPT** so that you can locate entries that pertain to accepted inbound connections from remote endpoints.
7. Search the **Cluster.log** file for the word **SV** for entries that pertain to securing a route between nodes.

Monitoring performance with failover clustering

Monitoring cluster parameters will help administrators learn which system resources a cluster is using and will provide detailed information on cluster scalability and performance. Furthermore, monitoring helps with troubleshooting in many failure scenarios.

Some of the failover clustering performance counters include:
- Cluster Network Messages
- Cluster Network Reconnections
- Global Update Manager
- Database
- Resource Control
- API
- Cluster Shared Volumes

Some of the network-performance counters for failover clustering that you should monitor by using Performance Monitor include:

- Cluster Network Messages. These describe internode communication, and examples include Bytes Received, Bytes Sent, Messages Received, and Messages Sent.
- Cluster Network Reconnections. These describe attempts made to reestablish connection between cluster nodes, and examples include Normal Message Queue Length, which is a number that should have a value of **0**.
- Global Update Manager. This is a component that establishes a consistent state across cluster nodes. For example, Database Update Messages create changes in the cluster database, and so when you use this component, you can see how many changes were performed on the cluster database.
- Database. This component monitors events when a cluster writes configuration data into the memory and transaction logs, and then into the database. For example, the **Flushes** parameter describes the number of cluster changes that have been flushed from the memory to the database.
- Resource Control Manager. This component allows you to monitor the cluster's resource state and manage resource failures. For example:
    - Groups online. Tells you how many groups are online on the node.
    - Cluster Resources/Resource Failure. Tells you how many times the resource has failed.
    - Resources Online. Tells you how many resources are online on this node.
- APIs. Application programing interfaces (APIs) are triggered by external calls, and examples include Cluster API Calls, Node API Calls, Network API Calls, ClusterAPIHandles, Node API Handles, and Network API Handles.
- Cluster Shared Volumes. Cluster Shared Volumes is a storage architecture that is optimized for Hyper-V Virtual Machines, and examples include IO Read Bytes, IO Reads, IO Write Bytes, and IO Writes.

Using Event Viewer with failover clustering

If you need to troubleshoot failover clustering, you first should analyze the Event Viewer. Another option is to check the Failover Cluster Management snap-in. It has a **Cluster Events** option that allows you to view and filter events across all cluster nodes. Furthermore, by using the Failover Cluster Management snap-in, you can configure a **Recent Cluster Events** option that queries all the errors and warning events from all the cluster nodes in the last 24 hours. Additional logs, such as the debug and analytic logs, are available in the Event Viewer by selecting the **Show Analytic and Debug Logs** options.

Events that are displayed in Event Viewer and require you to troubleshoot clusters include:

- Cluster resource in clustered service or application failed
- Cluster network interface for cluster node on network failed
- File share witness resource failed to arbitrate for the file share
- Cluster node was removed from the active failover cluster membership
- The Cluster service failed to bring clustered service or application completely online or offline.
- Cluster network name resource failed registration of one or more associated DNS name(s)
- Cluster network name resource cannot be brought online

The following table lists common events and solutions for troubleshooting clusters:

Event	Solution
Cluster resources in a clustered service or application failed.	Analyze and repair any issues with the application or service. Adjust cluster properties.
The cluster-network interface for a network cluster node failed.	Run the **Validate a Configuration Wizard**, and select only the network tests.
The file-share witness resource failed to arbitrate for the file share. You should ensure that the file share exists and is accessible by the cluster.	Confirm witness accessibility.
The cluster node was removed from the active failover-cluster membership.	Run the **Validate a Configuration Wizard**, and select only the network and inventory tests. Check network adapter and network devices.
The Cluster service failed to bring the clustered service or application online or offline completely. One or more resources may be in a failed state.	Confirm that resources are installed and configured correctly and that dependencies are correctly configured for all of the cluster's resources.
The cluster network-name resource failed registration of one or more associated DNS name(s).	Ensure that node's network adapter is configured with correct DNS server IP address, and that the DNS is accessible.
The cluster network-name resource cannot be brought online.	Confirm that the cluster nodes are able to connect to one or more domain controllers.

Windows PowerShell troubleshooting cmdlets

In organizations that have clusters with large number of nodes, or that have many different types of clusters, administration becomes more challenging. Therefore, it is more efficient for administrators to use Windows PowerShell to automate the creation, management, and troubleshooting of clusters.

Common cmdlets for troubleshooting failover clustering include:
- **Get-Cluster**
- **Get-ClusterAccess**
- **Get-ClusterDiagnostics**
- **Get-ClusterGroup**
- **Get-ClusterLog**
- **Get-ClusterNetwork**
- **Get-ClusterResourceDependencyReport**
- **Get-ClusterVMMonitoredItem**
- **Test-Cluster**
- **Test-ClusterResourceFailure**

Some of the more common cmdlets for managing and troubleshooting failover clustering, include:

- **Get-Cluster**. Returns information about one or more failover clusters in a given domain.
- **Get-ClusterAccess**. Returns information about permissions that control access to a failover cluster.
- **Get-ClusterDiagnostics**. Returns diagnostics for a cluster that contains virtual machines.
- **Get-ClusterGroup**. Returns information about one or more clustered roles (resource groups) in a failover cluster.
- **Get-ClusterLog**. Creates a log file for all nodes, or a specific a node, in a failover cluster.
- **Get-ClusterNetwork**. Returns information about one or more networks in a failover cluster.
- **Get-ClusterResourceDependencyReport**. Generates a report that lists the dependencies between resources in a failover cluster.
- **Get-ClusterVMMonitoredItem**. Returns the list of services and events being monitored in the virtual machine.
- **Test-Cluster**. Runs validation tests for failover-cluster hardware and settings.
- **Test-ClusterResourceFailure**. Simulates a failure of a cluster resource.

Question: List some of the communication issues that can affect the health of failover clustering.

Question: What is the **Cluster.Log** file, where is it located, and how can you can create it?

Lesson 5

Implementing site high availability with stretch clustering

In some scenarios, you must deploy cluster nodes at different sites. Usually, you do this when you build disaster-recovery solutions or when your users work in different sites or regions, and each site has its own datacenter. In both scenarios, organizations need high availability for their business-critical applications, so if any site failure occurs, the application and data fails over to the cluster nodes in another site. In this lesson, you will learn about deploying stretch clusters.

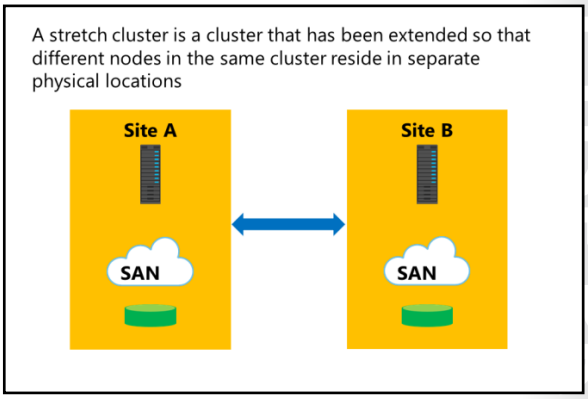
Lesson Objectives

After completing this lesson, you will be able to:

- Describe a stretch cluster.
- Describe the prerequisites for a stretch cluster.
- Describe synchronous and asynchronous replication.
- Describe the Storage Replica feature.
- Describe how to select a quorum mode for a stretch cluster.
- Configure a stretch cluster.
- Describe the challenges for implementing a stretch clusters.
- Describe considerations for multisite cluster failover and failback.

What is a stretch cluster?

A *stretch cluster* provides highly available services in more than one location. Although stretch clusters can solve several specific problems, they also present specific challenges.



In a stretch cluster, each site usually has a separate storage system and replication occurs between the sites. Stretch-cluster storage replication allows each site to be independent, and it provides fast access to the local disk. With separate storage systems, you cannot share a disk between sites.

A stretch cluster has three main advantages in a failover site, when you compare it to a remote server. This advantages include that:

- When a site fails, a stretch cluster can fail over the clustered service or application automatically to another site.
- Because the cluster configuration replicates to each cluster node in a stretch cluster automatically, there is less administrative overhead than if you were to use a standby server, which requires you to replicate changes manually.
- The automated processes in a stretch cluster reduce the possibility of human error, which is inherent in manual processes.

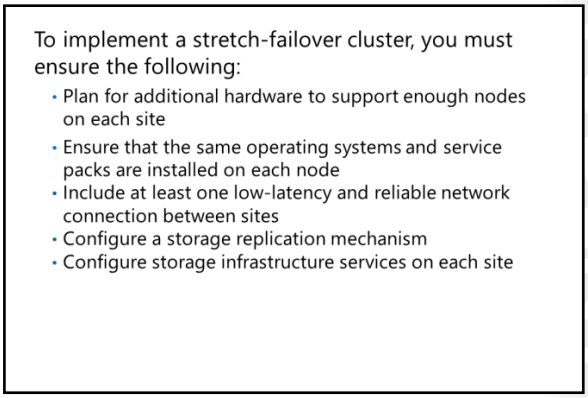
However, because of the increased cost and complexity of a stretch-failover cluster, it might not be an ideal solution for every application or business. When you are considering whether to deploy a stretch cluster, you should evaluate the importance of applications to your business, the type of applications you are using, and any alternative solutions. Some applications can provide stretch redundancy easily by using log shipping or other processes, and you can achieve sufficient availability with only a modest increase in cost and complexity.

The complexity of a stretch cluster requires more-detailed architectural and hardware planning than is required for a single-site cluster. It also requires that you to develop business processes that test cluster functionality regularly.

Note: Many of the new Windows Server 2016 features address the challenges of stretch clusters. Azure Cloud Witness, site-aware failover clusters, and storage replicas all address stretch-clustering challenges that were in many previous Windows Server versions.

Prerequisites for implementing a stretch cluster

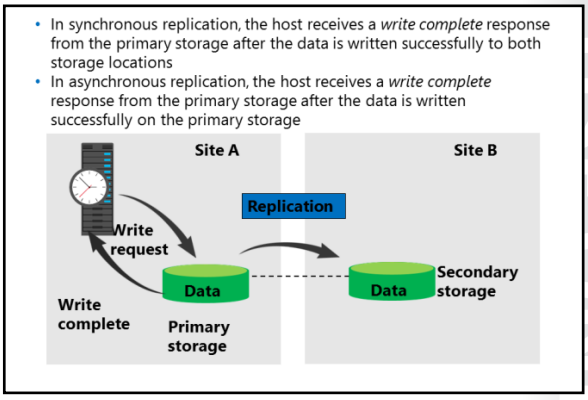
There are different prerequisites for implementing a stretch cluster than for implementing a single-site cluster. It is important that you understand these differences and how to prepare properly for implementing a multisite cluster.



Before you implement a multisite failover cluster, you must ensure that:

- You must have enough nodes and votes on each site so the cluster can be online even if one site is down. This setup requires additional hardware, and can increase costs significantly.
- All nodes must have the same operating-system and service-pack version.
- You must provide at least one low-latency and reliable network connection between sites. This is important for cluster heartbeats. By default, regardless of subnet configuration, heartbeat frequency, or *subnet delay*, is once every second or 1,000 milliseconds. The range for heartbeat frequency is once every 250 to 2,000 milliseconds on a common subnet and 250 to 4,000 milliseconds across subnets. By default, when a node misses a series of five heartbeats, another node initiates failover. This value's range, or *subnet threshold*, is three through 10 heartbeats.
- You must provide a storage-replication mechanism. Failover clustering does not provide a storage-replication mechanism. This also requires that you have multiple storage solutions, including one for each cluster that you create.
- You must ensure that all other necessary services for the cluster, such as AD DS and DNS, are available on a second site. You also must ensure that client connections can be redirected to a new cluster node when failover happens.

Synchronous and asynchronous replication



Until recently, a geographically dispersed Microsoft failover cluster could not use shared storage between physical locations without a vendor-specific storage-replication solution. However, in Windows Server 2016, this specific hardware is not required. The Storage Replica feature utilizes synchronous or asynchronous replication separate from whatever vendor storage might be at the location, and when you:

- Use synchronous replication, after the data writes successfully on both storage systems, the host receives a write complete response from the primary storage. If the data does not write successfully to both storage systems, the application must attempt to write to the disk again. With synchronous replication, data on both storage systems are identical.
- Use asynchronous replication, after the data writes successfully on the primary storage, the node receives a write complete response from the storage. The data writes to the secondary storage on a different schedule, depending on the hardware or software vendor's implementation.

  Asynchronous replication can be storage-based, host-based, or even application-based. However, not all forms of asynchronous replication are sufficient for a stretch cluster. For example, DFS Replication provides file-level asynchronous replication. However, it does not support stretch-failover clustering replication because DFS Replication replicates smaller documents that do not stay open continuously. As a result, it is not for high-speed, open-file replication.

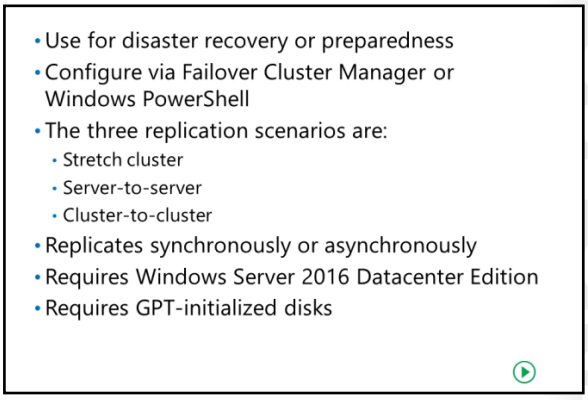
When to use synchronous or asynchronous replication

Synchronous-replication solutions require low-disk write latency, because the application waits for both storage solutions to acknowledge the data writes. The requirement for low-latency disk writes also limits the distance between the storage systems, because increased distance can cause higher latency. If the disk latency is high, this can affect the application's performance and even its stability.

Asynchronous replication overcomes latency and distance limitations by acknowledging local disk writes only, and by reproducing the disk write, in a separate transaction, on the remote storage system. However, because asynchronous replication writes to the remote storage system after it writes to the local storage system, the possibility of data loss during failure increases.

Overview of the Storage Replica feature

The Storage Replica feature is new in Windows Server 2016. In previous Windows Server versions, storage vendors provided the technology to synchronize data on two independent storage units. However, in Windows Server 2016, Storage Replica allows storage-agnostic replication between clusters or servers. Storage Replica offers both synchronous and asynchronous replication. You choose one over the other depending on network latency and distance between servers. All Storage Replica scenarios require GPT-initialized disks.



You can configure Storage Replica to replicate storage among servers and clusters, and clusters in different datacenters. Storage Replica supports three scenarios:

- Stretch cluster
- Server-to-server
- Cluster-to-cluster

Storage Replica can do a one-to-one replication only. Storage Replica cannot create a third replica, such as a Hyper-V replica or Distributed File System (DFS). Storage Replica is not suited for branch-office scenarios because network connections to branch offices tend to be highly latent, and with lower bandwidth, synchronous replication becomes difficult. Storage Replica replicates data on the block level. Other replication engines like Distributed File System Replication (DFSR) cannot replicate open files. Changes in these files will replicate without issues with Storage Replica.

You can use Storage Replica in scenarios of disaster prevention and disaster recovery. Storage Replica is not a replacement for your backup solution. Storage Replica will replicate all changes, regardless of the change type. When a user deletes data from a volume, Storage Replica will replicate the deletion instantly to the other volume.

Storage Replica is not product specific. It is a general purpose, storage-agnostic engine. You cannot configure its functionality as ideally as application-specific replication like DFSR, Hyper-V Replica, or SQL AlwaysOn Availability Groups. The majority of applications most likely will support Storage Replica, but you should confirm support with your software vendor for before you implement Storage Replica on application data. The following table lists where each Microsoft replication solution is applicable.

	Virtual Machine	SYSVOL	File Server	Microsoft Exchange	SQL Server
Hyper-V Replica	Yes	Not applicable	Yes (virtual machines hosting file servers)	No	Yes (virtual machines hosting SQL Server)
Storage Replica	Yes	No	Yes	No	Yes
SQL Server AlwaysOn Failover Clustering Instance (FCI)	No	Not applicable	Not applicable	Not applicable	Yes

	Virtual Machine	SYSVOL	File Server	Microsoft Exchange	SQL Server
SQL Server AlwaysOn Availability Groups	No	Not applicable	Not applicable	Not applicable	Yes
Exchange Database Availability Group (DAG)	No	Not applicable	Not applicable	Yes	Not applicable
DFS Replication	No	Yes	Yes	No	No

Storage Replica synchronous replication

You might have to invest in expensive networking equipment to ensure that your network can perform synchronous replication. Synchronous replication has the following workflow:

1. The application writes data to the storage.
2. Log data is written in the primary site and the data replicates to the remote site.
3. Log data is written at the remote site.
4. The remote site sends an acknowledgement.
5. The primary site acknowledges the application write.

Storage Replica asynchronous replication

Server-to-server is the only scenario that supports asynchronous replication. Asynchronous replication has the following workflow:

1. The application writes data to the storage.
2. Log data is written in primary site.
3. The primary site acknowledges the application write.
4. Data replicates to the remote site.
5. Log data is written at the remote site.
6. The remote site acknowledges the Application write.

Stretch cluster

A stretch cluster is a configuration that has one cluster with nodes in two locations and storage in both locations. Storage Replica synchronously replicates to keep both sets of mirrored storage, which allows the cluster to fail over virtual machines immediately from one location to another. You configure stretch cluster by using Failover Cluster Manager or Windows PowerShell. If you want to configure Storage Replica for a stretched cluster in Failover Cluster Manager, perform the following steps:

1. Add a source data disk to a role or CSV.
2. Enable replication on the source data disk.
3. Select a destination data disk.
4. Select a source log disk.
5. Select a destination log disk.

You can use the following Windows PowerShell cmdlet to test if requirements are met:

```
Test-SRTopology
```

There are several requirements for stretch clusters, including that you have:

- Domain-joined servers.
- Physical servers for the Stretch Cluster Hyper-V scenario. You can use virtual machines for server-to-server and cluster-to-cluster.
- Two sets of shared storage, using serial attached SCSI JBODs, Fibre Channel SAN, or iSCSI Target.

Each storage set must be able to create at least two virtual disks, one for replicated data and one for logs. The sector size must be the same on all data disks on the physical storage. All the log disks must be of the same sector size, but not necessarily the same as the data disks.

- At least 1 Gigabit Ethernet (GbE) connection on each file server, preferably 10 GbE, iWARP, or InfiniBand.
- A minimum of 4 GB of random access memory (RAM) in each server with at least two cores.
- A firewall that is configured to allow Internet Control Message Protocol (ICMP), SMB (port 445, plus 5445 for SMB Direct), and WS-MAN (port 5985) bidirectional traffic between all nodes.
- A network between the two sets of servers with at least 1 Gbps throughput (preferably 8 Gbps or higher) and an average of less than or equal to 5 milliseconds (ms) round-trip latency.
- Local administrator permissions on all server nodes.

Server-to-server replication

Server-to-server replication replicates storage from one server to another server's storage. These servers can be in the same datacenter or in different locations. You can use Windows PowerShell to configure this, as there are no other tools to configure server-to-server replication. To configure server-to-server replication, run the following Windows PowerShell cmdlet at a command line:

```
New-SRPartnership -SourceComputerName LON-SVR1 -SourceRGName RepGroup01 -SourceVolumeName
F: -SourceLogVolumeName G: -DestinationComputerName LON-SVR2 -DestinationRGName RepGroup02
-DestinationVolumeName F: -DestinationLogVolumeName G: -LogSizeInBytes 8GB
```

The requirements for server-to-server replication are that you have:

- Domain-joined servers.
- Two sets of storage, using DAS, serial-attached SCSI JBODs, Fibre Channel SAN, or iSCSI Target.
- Each storage set must have at least two volumes, one for replicated data and one for logs. The sector size must be the same on all data disks on the physical storage. All the log disks also need to be the same sector size, but not necessarily the same as the data disks. The size of the two data volumes must be the same.
- At least 1 GbE connection on each file server, preferably 10 GbE, internet Wide Area RDMA Protocol (iWARP), or InfiniBand.
- A minimum of 4 GB of RAM in each server with at least two cores.
- A firewall that is configured to allow ICMP, SMB (port 445, plus 5445 for SMB Direct) and WS-MAN (port 5985) bi-directional traffic between all nodes.
- A network between the servers that has at least 1 Gbps throughput (preferably 8 Gbps or higher) and an average of less than or equal to 5 ms round trip latency.
- Local administrator permissions on all server nodes.

Cluster-to-cluster replication

Cluster-to-cluster replication occurs when one cluster replicates its storage to another cluster and its storage. These clusters can be next to each other or far apart. You configure and manage cluster-to-cluster replication similar to how you configure and manage server-to-server replication.

The requirements for cluster-to-cluster are that you have:

- Domain-joined servers.
- Two sets of shared storage, using Storage Spaces Direct, serial attached SCSI JBODs, Fibre Channel SAN, or iSCSI Target.
- Each storage set must at least two volumes, one for replicated data and one for logs. The sector size must be the same on all data disks on the physical storage. All the log disks also need to be the same sector size, but not necessarily the same as the data disks. The size of the two data volumes must be the same.
- At least 1 GbE connection on each file server, preferably 10 GbE, iWARP, or InfiniBand.
- A minimum of 4 GB of RAM in each server with at least two cores.
- A firewall that is configured to allow ICMP, SMB (port 445, plus 5445 for SMB Direct), and WS-MAN (port 5985) bi-directional traffic between all nodes.
- A network between the two sets of servers that has at least 1 Gbps throughput (preferably 8 Gbps or higher) and an average of less than or equal to 5 ms round trip latency.
- Local administrator permissions on all server nodes.

Demonstration: Implementing server-to-server storage replica

In this demonstration, you will see how to configure storage replica.

Demonstration Steps

1. On **LON-SVR1**, install the **Storage Replica** feature, and then restart the virtual machine.
2. Repeat step 1 on **LON-SVR4**.
3. In Windows PowerShell, run the following two commands:

```
MD c:\temp
Test-SRTopology -SourceComputerName LON-SVR1 -SourceVolumeName M: -
SourceLogVolumeName N: -DestinationComputerName LON-SVR4 -DestinationVolumeName M: -
DestinationLogVolumeName N: -DurationInMinutes 2 -ResultPath c:\Temp
```

4. Wait for the test to finish (it might take 5 to 7 minutes).
5. Open the report file located in **C:\Temp** folder. The report file is an HTML file which name starts with **TestSrTopologyReport**, and includes the current date. Review the report file data and verify that you meet the Storage Replica requirements.
6. Configure server-to-server replication by running the following command in Windows PowerShell:

```
New-SRPartnership -SourceComputerName LON-SVR1 -SourceRGName RG01 -SourceVolumeName
M: -SourceLogVolumeName N: -DestinationComputerName LON-SVR4 -DestinationRGName RG02
-DestinationVolumeName M: -DestinationLogVolumeName N:
```

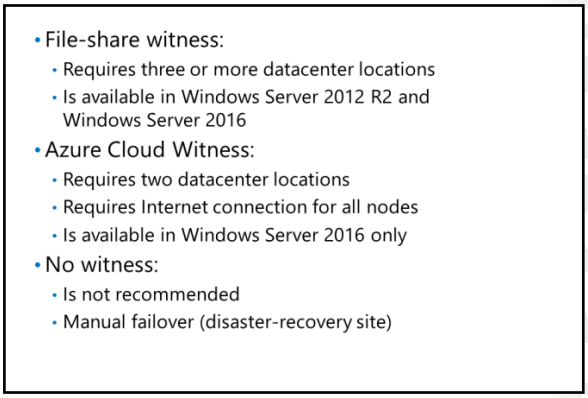
7. Verify the replication source and destination state by running the following three commands in Windows PowerShell:

```
Get-SRGroup
Get-SRPartnership
(Get-SRGroup).replicas
```

8. Run the following command in Windows PowerShell to verify the remaining bytes to be replicated on the destination server:

```
(Get-SRGroup).Replicas | Select-Object numofbytesremaining
```

Selecting a quorum mode for a stretch cluster



When creating a stretch cluster across geographically dispersed nodes in Windows Server 2016, we recommend that you use an Azure Cloud Witness. However, there are cases where organizations choose to utilize a file-share witness. For example, some datacenter where a stretch cluster node is located might not have reliable Internet connection, and some organizations do not use Azure cloud services. Regardless of the witness that you select, you should use the dynamic witness mode, which is the default mode in Windows Server 2016 and Windows Server 2012 R2. A stretch cluster spreads across multiple datacenters, so it is possible that an entire datacenter could go offline. In this situation, the quorum could lose half or more of the cluster nodes at once and might have some servers in maintenance mode. Therefore, it is important that you use dynamic quorum and dynamic witness to avoid a cluster shutdown.

Note: In a stretch cluster, there is no shared storage that is accessible to nodes at different locations. A disk witness is not a suggested witness selection for this scenario.

File-share witness

The primary issue with a file-share witness for most scenarios is that its creation requires a minimum of three datacenters. However, if you are working in an environment where three or more datacenters are in operation, creating a file-share witness on a share at one of the locations might be the quickest and easiest witness option. A file-share witness does require a file share that all nodes in the cluster can access by using the SMB protocol. A file-share witness does not keep a copy of the cluster database. A file-share witness is available on both Windows Server 2016 and Windows Server 2012 R2.

Azure Cloud Witness

Azure Cloud Witness builds on the foundation of a file-share witness. An Azure Cloud Witness utilizes the same basic format as the file-share witness with respect to its arbitration logic, and it does not keep a copy of the cluster database. However, rather than requiring a share and writing over SMB, Azure Cloud Witness utilizes Blob storage and the Microsoft Azure Storage service REST-based API. This configuration does require an Azure subscription and Internet connectivity for all nodes at each site. Azure Cloud Witness is only available in Windows Server 2016.

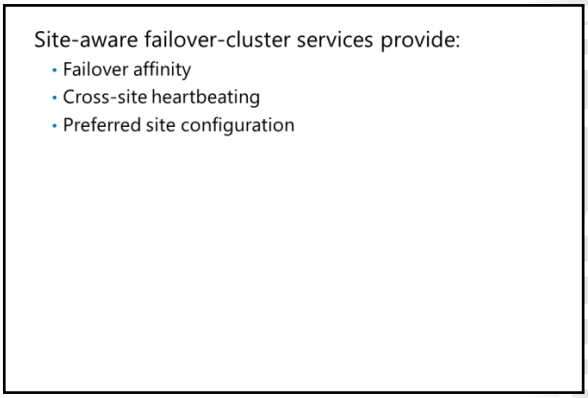
No witness

You also can configure a cluster to not use any witness. We do not recommend this solution, but it is supported to prevent split-brain syndrome in Windows Server 2016 by utilizing site-aware clustering. You also could configure no witness for manual failover, such as for disaster-recovery scenarios. You can accomplish this by removing the votes for the nodes at the disaster-recovery site and then forcing quorum manually for the site that you would like to bring online, while preventing quorum at the site that you want to keep offline.

Configuring a stretch cluster

Site-aware failover clusters are one of the major changes in Windows Server 2016. You can now configure the sites with a value that allows you to differentiate between site locations. For example, if you have a four-node cluster with two nodes at one site and two nodes at another site, you can run the following commands to configure the nodes as site-aware:

```
(Get-ClusterNode Node1).Site=1
(Get-ClusterNode Node2).Site=1
(Get-ClusterNode Node3).Site=2
(Get-ClusterNode Node4).Site=2
```



After you have defined site-aware nodes, there are multiple new and improved failover-cluster services that you can utilize, including:

- Failover affinity. For instance, in the four-node cluster previously mentioned, suppose that you need to take Node2 down for maintenance. If you have site-aware failover clusters, you can ensure that the services running on Node2 fail over to a node on the same site, rather than failing over to a node in the other site.
- Cross-site heartbeating. When you configure the default heartbeat settings based on subnets, it might cause issues, depending on your network configuration. However, if you use site-aware clusters, you can configure this based on location regardless of network configuration. The subnet heartbeat settings become relevant only for site-aware clusters to determine the heartbeat setting for the same site nodes.
- Preferred site configuration. Prior to Windows Server 2016, with a two-site cluster, you could configure one of the sites with **LowerQuorumPriorityNodeID**. This has been deprecated in Windows Server 2016 and replaced with the preferred site configuration based on site-aware clusters. After configuring the nodes in preferred sites, you can identify a preferred site by running the following command in Windows PowerShell:

  ```
  (Get-Cluster).PreferredSite = "Site Number that you would like to be preferred"
  ```

  For example, after you run the preceding configuration on the four-node cluster, you could set site 1 as the preferred site by running the following command:

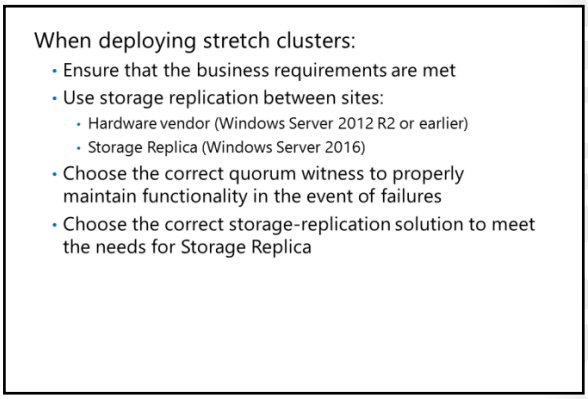
  ```
  (Get-Cluster).PreferredSite = 1
  ```

  This allows you to identify what nodes the roles should attempt to bring online first.

You also can can also take it a step further and configure preferred sites based on cluster groups, so that different groups can have different preferred sites. You can use configure this by using the following Windows PowerShell command:

```
(Get-ClusterGroupGroupName).PreferredSite = "Site number that you would like to be preferred"
```

Challenges for deploying a stretch cluster



Stretch clusters are not appropriate for every application or every organization. When you design a stretch solution with a hardware vendor, clearly identify the business requirements and expectations. Not every scenario that involves more than one location is appropriate for a stretch cluster.

Stretch clustering is a highly available strategy that focuses primarily on hardware-platform availability. However, specific stretch-cluster configurations and deployments might affect availability, such as a user's ability to connect to the application, to the quality of application performance. Stretch clustering can be a powerful solution for managing planned and unplanned downtime, but you must examine its benefits against all dimensions of application availability.

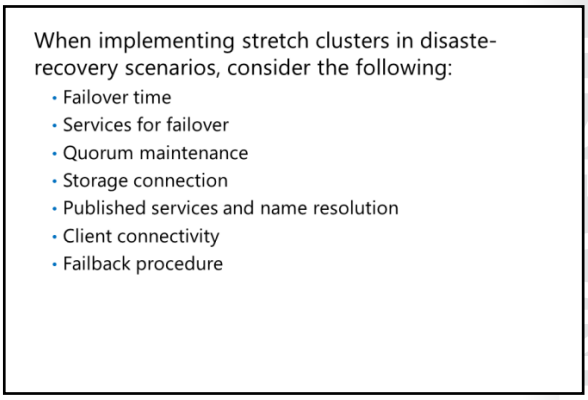
Stretch clusters do require more overhead than local clusters. Instead of a local cluster in which each node of the cluster attaches to the mass storage device, each site of a stretch cluster must have comparable storage. Furthermore, you also must consider setting up replication between the cluster sites. Storage Replicas in Windows Server 2016 provides a storage agnostic replication. When using Storage Replica, you might consider using additional network bandwidth between sites, and develop the management resources within your organization to administer your stretch cluster efficiently.

Note: Applications such as SQL Server, Hyper-V, Exchange Server, and AD DS should use their individual application stretch configurations (Hyper-V Replica, Database Availability Groups, and so on).

Additionally, you should consider the quorum witness that you use carefully, so that you ensure that it maintains functionality if a failure occurs, and the location of the available cluster votes.

Multisite failover and failback considerations

When you establish a stretch-failover clustering structure, it is very important that you define a procedure for tasks that you should perform if a site disaster occurs. Additionally, you also should define a procedure for tasks that you should perform for failback.



In most cases, failover of critical services to another site is not automatic, but rather is a manual or semi-manual procedure. When defining your failover process, you should consider following factors:

- Failover time. You must decide how long you should wait before you pronounce a disaster and start the failover process to another site.
- Services for failover. You should clearly define critical services, such as AD DS, DNS, and DHCP, that should fail over to another site. It is not enough to have a cluster designed to fail over to another site. Failover clustering requires that you have Active Directory services running on a second site. You cannot make all necessary services highly available by using failover clustering, so you must consider other technologies to achieve that result. For example, for AD DS and DNS, you can deploy additional domain controllers and DNS servers or VMs on a second site.
- Quorum maintenance. It is important to design the quorum model so that each site has enough votes for maintaining cluster functionality. If this is not possible, you can use options such as forcing a quorum or dynamic quorum (in Windows Server 2016 and Windows Server 2012 R2) to establish a quorum if a failure occurs.
- Storage connection. A stretch cluster usually requires that you have storage available at each site. However, because of this, you should carefully design storage replication and the procedure for how to fail over to secondary storage if disaster occurs.
- Published services and name resolution. If you have services published to your internal or external users, such as email and webpages, failover to another site requires cluster name or IP address changes in some instances. If that is the case, you should have a procedure for changing DNS records in the internal or the public DNS. To reduce downtime, we recommended that you reduce Time to Live (TTL) on critical DNS records.
- Client connectivity. A failover plan also must include a design for client connectivity in case of disaster. This includes both internal and external clients. If your primary site fails, you should have a way for your clients to connect to a second site.
- Failback procedure. After the primary site comes back online, you should plan and implement a failback process. Failback is as important as a failover, because if you perform it incorrectly, you can cause data loss and services downtime. Therefore, you must clearly define steps for performing failback to a primary site without data loss or corruption. Very rarely is the failback process automated, and it usually happens in a very controlled environment.

Establishing a stretch cluster is much more than just defining the cluster, cluster role, and quorum options. When you design a stretch cluster, you should consider the larger picture of failover as part of a disaster recovery strategy. Windows Server 2016 has several technologies that can help with failover and failback, but you also should consider other technologies that participate in your infrastructure. In addition, each failover and failback procedure greatly depends on the service (or services) implemented in a cluster.

Question: What features does enabling site-aware clustering in a Windows Server 2016 stretch cluster provide?

Check Your Knowledge

Question	
You have only two datacenter locations with a Windows Server 2016 stretch cluster built across both sites. What type of dynamic witness is best for this scenario?	
Select the correct answer.	
	File-share witness
	Azure Cloud Witness
	Disk witness
	No witness

Question: Can a node that runs Windows Server 2016 and Windows Server 2012 R2 run in the same cluster?

Lab B: Managing a failover cluster

Scenario

A. Datum Corporation recently implemented failover clustering for better uptime and availability. The implementation is new and your boss has asked you to go through some failover-cluster management tasks so that you are prepared to manage it moving forward.

Objectives

After completing this lab, you will be able to:

- Evict a node and verify quorum settings.
- Change the quorum from a disk witness to a file-share witness and define node voting.
- Add and remove disks from the cluster.

Lab Setup

Estimated Time: **45 min**

Virtual machines: **20740A-LON-DC1**, **20740A-LON-SVR1**, **20740A-LON-SVR2**, **20740A-LON-SVR3**, **20740A-LON-SVR5**, and **20740A-LON-CL1**

User name: **Adatum\Administrator**

Password: **Pa$$w0rd**

For this lab, you need to use the available VM environment. The required virtual machines should be running.

Exercise 1: Evicting a node and verifying quorum settings

Scenario

You have added a node to the cluster to test your organization's application scalability. Some of your organization employees have moved to another department, and they will not use the clustered application any more. According to your test, you will not need the current number of nodes in the cluster, so you will evict one node from the cluster.

The main tasks for this exercise are as follows:

1. Evict node LON-SVR5.
2. Verify changes in quorum settings and the witness disk.

▶ Task 1: Evict node LON-SVR5

1. On **LON-SVR3**, switch to **Failover Cluster Manager**.
2. Evict **LON-SVR5** from the cluster **Cluster1**.

▶ Task 2: Verify changes in quorum settings and the witness disk

1. On **LON-SVR2**, in the **Windows PowerShell** console, run following cmdlet to check the assigned votes:

```
Get-ClusterNode | select name, nodeweight, ID, state
```

2. Verify that **NodeWeight** property of a cluster node has value **1**, which means that the quorum vote of the node is assigned and is managed by the cluster.

Results: After completing this exercise, you should have evicted a node from the cluster, and verified the changes in quorum settings and witness disk.

Exercise 2: Changing the quorum from disk witness to file-share witness, and defining node voting

Scenario

You have introduced a new application in your organization that works better by using scenarios with the File Share Witness quorum model. Additionally, the new application requires that you configure node voting.

The main tasks for this exercise are as follows:

1. Get the current quorum model.
2. Create a file share on LON-SVR1.
3. Change the current quorum model to a file-share witness.
4. Verify that the current quorum model is a file share witness.

▶ Task 1: Get the current quorum model

- On **LON-SVR2**, in the **Windows PowerShell** console, run the following command:

```
Get-ClusterQuorum | Select Cluster, QuorumResource, QuorumType
```

▶ Task 2: Create a file share on LON-SVR1

- On **LON-SVR1**, in **File Explorer**, create a shared folder called **C:\FSW**. Use **Share with specific people**, and assign **Everyone** Read/Write access.

▶ Task 3: Change the current quorum model to a file-share witness

- On **LON-SVR2**, in the **Windows PowerShell** console, run the following command:

```
Set-ClusterQuorum -NodeAndFileShareMajority "\\LON-SVR1\FSW"
```

▶ Task 4: Verify that the current quorum model is a file share witness

- On **LON-SVR2**, in the **Windows PowerShell** console, type the following command, and then press Enter:

```
Get-ClusterQuorum | Select Cluster, QuorumResource, QuorumType
```

Results: After completing this exercise, you should have changed the quorum from disk witness to file share witness and defined node voting.

Exercise 3: Verifying high availability

Scenario

You want to test your high-availability solution by taking one of your servers offline, and then verify that your application, services, and data are still available to clients. After you verify that high availability works, you will bring the server back online.

The main tasks for this exercise are as follows:

1. Simulate server failure.
2. Verify functionality in Cluster1, and verify file availability.
3. Validate whether the file is still available.
4. Prepare for the next module.

▶ Task 1: Simulate server failure

1. On **LON-SVR2**, verify the current owner of **AdatumFS**.

   Note: The owner will be **LON-SVR2** or **LON-SVR3**.

2. If **LON-SVR3** is not the owner, move the **AdatumFS** clustered role to **LON-SVR3**.
3. Shut down **LON-SVR3**.

▶ Task 2: Verify functionality in Cluster1, and verify file availability

1. On **LON-DC1**, open **File Explorer**, and in the address bar, type **\\AdatumFS**, and then press Enter.
2. Verify that you can access the location and that you can open the **Docs** folder.
3. Create a test text document named **test2.txt** inside this folder.

▶ Task 3: Validate whether the file is still available

1. Start the **LON-SVR3** virtual machine.
2. On **LON-SVR2**, move the **AdatumFS** clustered role to **LON-SVR3**.
3. On **LON-DC1**, open **File Explorer**, and in the address bar, type **\\AdatumFS**, and then press Enter.

4. Verify that you can access the location and that you can open the **Docs** folder.
5. Create a test text document named **test3.txt** inside this folder.

Results: After completing this exercise, you should have tested failover cluster high availability successfully by taking a server offline and then bringing it back online.

▶ 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 **20740A-LON-DC1**, and then click **Revert**.
3. In the **Revert Virtual Machines** dialog box, click **Revert**.
4. Repeat steps 2 and 3 for **20740A-LON-SVR1**, **20740A-LON-SVR2**, **20740A-LON-SVR3**, **20740A-LON-SVR5**, and **20740A-LON-CL1**.

Question: Why would you evict a cluster node from a failover cluster?

Question: Do you perform failure-scenario testing for your high-available applications based on Windows Server failover clustering?

Module Review and Takeaways

Review Questions

Question: What are some of the improvements in Windows Server 2016 failover clustering?

Question: Why is it not a good idea, generally, to use a disk-only quorum configuration?

Question: What is the purpose of CAU?

Question: What is the main difference between synchronous and asynchronous replication in a stretch-cluster scenario?

Question: Identify an enhanced feature in stretch clusters in Windows Server 2016.

Real-world Issues and Scenarios

Your organization is considering the use of a geographically dispersed cluster that includes an alternate datacenter. Your organization has only a single physical location, together with an alternate datacenter. Can you provide an automatic failover in this configuration?

Answer: Yes, you cannot provide an automatic failover in this configuration. To provide an automatic failover, you must configure an Azure Cloud Witness.

Tools

The following is a list of the tools that this module references:

Tool	Use for	Location
Failover Cluster Manager console	Managing Failover Cluster	Server Manager
Cluster-Aware Updating console	Managing Failover Cluster updates	Failover Cluster Manager Console
Windows PowerShell	Managing Failover Cluster	Taskbar, Server Manager, or Start Menu
Server Manager	Managing the operating system	Taskbar or Start Menu
iSCSI initiator	Managing iSCSI storage	Server Manager
Disk Management	Managing Disks	Server Manager

Best Practices

- Try to avoid using a quorum model that depends only on the disk for Hyper-V high availability or Scale-Out File Server.
- Perform regular backups of cluster configuration.
- Ensure that in case of one node failure, other nodes can manage the load.
- Carefully plan stretch clusters.

Common Issues and Troubleshooting Tips

Common Issue	Troubleshooting Tip
Cluster Validation Wizard reports an error	

Common Issue	Troubleshooting Tip
Create Cluster Wizard reports that not all nodes support the desired clustered role	
You cannot create a Print Server cluster	

Module 9

Implementing failover clustering with Windows Server 2016 Hyper-V

Contents:

Module Overview

One benefit of implementing server virtualization is the opportunity to provide high availability, both, for applications or services that have built-in high availability functionality and for applications or services that do not provide high availability in any other way. With the Windows Server 2016 Hyper-V technology, failover clustering, and Microsoft System Center 2012 R2 Virtual Machine Manager (VMM), you can use several different options to configure high availability. In this module, you will learn about how to implement failover clustering in a Hyper-V environment to achieve high availability for a virtual environment.

 **Note:** Many of the features that this module describes are also available in Windows Server 2012 R2 and Windows Server 2012. This module explicitly calls out the features that are new to Windows Server 2016.

Objectives

After completing this module, you will be able to:

- Describe how Hyper-V integrates with failover clustering.
- Implement Hyper-V virtual machines (VMs) on failover clusters.
- Describe the key features for VMs in a clustered environment.

Lesson 1

Overview of the integration of Hyper-V Server 2016 with failover clustering

Failover clustering is a feature that enables you to make applications or services highly available. To make VMs highly available in a Hyper-V environment, you should implement failover clustering on the Hyper-V host computers. This lesson summarizes the high availability options for Hyper-V–based VMs, and then focuses on how failover clustering works, and how to design and implement failover clustering for Hyper-V.

Lesson Objectives

After completing this lesson, you will be able to:

- Describe the options for making applications and services highly available.
- Describe how failover clustering works with Hyper-V nodes.
- Describe failover clustering with Windows Server 2016 Hyper-V features.
- Describe the best practices for implementing high availability in a virtual environment.

Options for making application and services highly available

Most organizations have certain applications that are business critical and must be highly available. To ensure an application or a service is highly available, you must deploy it in an environment that provides redundancy for all components that the application require. You can choose between several options to provide high availability for VMs and the services hosted within VMs, you can:

- Implement VMs as a clustered role (host clustering).
- Implement clustering inside VMs (guest clustering).
- Use Network Load Balancing (NLB) inside VMs.

High availability options	Description
Host clustering	• VMs are highly available • Does not require VM operating system or application to be cluster-aware
Guest clustering	• VM are failover cluster nodes • VM applications must be cluster-aware • Requires iSCSI or virtual Fibre Channel interface for shared storage connections
NLB	• VM are NLB cluster nodes • Use for web-based applications

Host clustering

Host clustering enables you to configure a failover cluster when you use the Hyper-V host servers. When you configure host clustering for Hyper-V, you configure the VM as a highly available resource. You implement failover-clustering protection at the host-server level. This means that the guest operating system and applications that run within the VM do not have to be cluster-aware. However, the VM is still highly available.

Some examples of non-cluster–aware applications are a print server or a proprietary network-based application such as an accounting application. If the host node that controls the VM unexpectedly becomes unavailable, the secondary host node takes control and restarts or resumes the VM as quickly as possible. You also can move the VM from one node in the cluster to another in a controlled manner. For example, you could move the VM from one node to another while updating the host management Windows Server 2016 operating system.

The applications or services that run in the VM do not have to be compatible with failover clustering, and they do not have to be aware that the VM is clustered. Because the failover is at the VM level, there are no dependencies on software that you installed inside the VM.

Guest clustering

You configure guest failover clustering very similar to physical-server failover clustering, except that the cluster nodes are VMs. In this scenario, you create two or more VMs, install, and implement failover clustering within the guest operating systems. The application or service is then able to take advantage of high availability between the VMs. Each VM node's guest operating system implements failover clustering so that you can locate the VMs on a single host. This can be a quick and cost-effective configuration in a test or staging environment.

For production environments, however, you can protect the application or service more robustly if you deploy the VMs on separate failover clustering–enabled Hyper-V host computers. With failover clustering implemented at both the host and VM levels, you can restart the resource regardless of whether the node that fails is a VM or a host. It is considered an optimal high-availability configuration for VMs that run mission-critical applications in a production environment.

You should consider several factors when you implement guest clustering:

- The application or service must be failover cluster-aware. This includes any of the Windows Server 2016 services that are cluster-aware, and any applications, such as clustered Microsoft SQL Server and Microsoft Exchange Server.
- Hyper-V VMs in Windows Server 2016 can use Fibre Channel–based connections to shared storage, or you can implement Internet Small Computer System Interface (iSCSI) connections from the VMs to the shared storage. You can also use the shared virtual hard disk feature to provide shared storage for VMs.

You should deploy multiple network adapters on the host computers and the VMs. Ideally, you should dedicate a network connection to the iSCSI connection (if you use this method to connect to storage), to the private network between the hosts, and to the network connection that the client computers use.

NLB

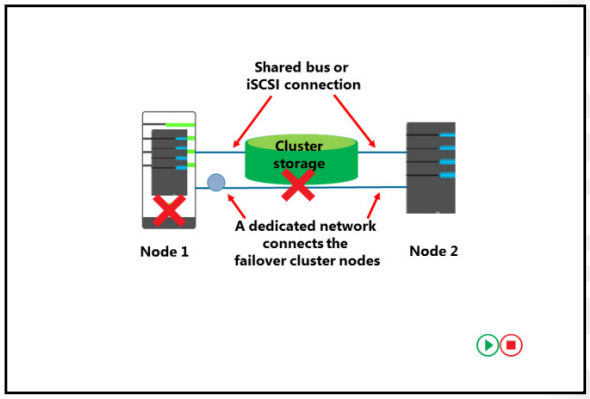
NLB works with VMs in the same way that it works with physical hosts. It distributes IP traffic to multiple instances of a TCP/IP service, such as a web server that runs on a host within the NLB cluster. NLB transparently distributes client requests among the hosts, and it enables the clients to access the cluster by using a virtual host name or a virtual IP address. From the client computer's perspective, the cluster appears to be a single server that answers these client requests. As enterprise traffic increases, you can add another server to the cluster.

Therefore, NLB is an appropriate solution for resources that do not have to accommodate exclusive read or write requests. Examples of NLB-appropriate applications would be web-based front-end VMs to database applications or Exchange Server Client Access servers.

When you configure an NLB cluster, you must install and configure the application on all VMs that will participate in the NLB cluster. After you configure the application, you install the NLB feature in Windows Server 2016 within each VM's guest operating system (not on the Hyper-V hosts), and then configure an NLB cluster for the application. Earlier versions of Windows Server also support NLB, so that the guest operating system is not limited to only Windows Server 2016; however, you should use the same operating system versions within one NLB cluster. Similar to a Guest Cluster Across Hosts, the NLB resource typically benefits from overall increased I/O performance when you locate the VM nodes on different Hyper-V hosts.

Note: As with earlier versions of Windows Server, you should not implement NLB and failover clustering within the same operating system because the two technologies conflict with each other.

How does a failover cluster work with Hyper-V nodes?



When you implement failover clustering and configure VMs as highly available resources, the failover cluster treats the VMs like any other application or service. For example, if there is host failure, failover clustering acts to restore access to the VM as quickly as possible on another host in the cluster. Only one node at a time runs the VM. However, you also can move the VM to any other node in the same cluster as part of a planned migration.

The failover process transfers the responsibility of providing access to resources in a cluster from one node to another. Planned failover (also known as *switchover*) can occur when an administrator intentionally moves resources to another node for maintenance or other reasons, or when unplanned downtime of one node occurs because of hardware failure or other reasons.

The failover process consists of the following steps:

1. The node where the VM is running owns the clustered instance of the VM, controls access to the shared bus or iSCSI connection to the cluster storage, and has ownership of any disks or logical unit numbers (LUNs) that you assign to the VM. All of the nodes in the cluster use a private network to send regular signals, known as *heartbeat signals*, to one another. The heartbeat indicates that a node is functioning and communicating on the network. The default heartbeat configuration specifies that each node sends a heartbeat over TCP/UDP port 3343 each second (or 1,000 milliseconds [ms]).
2. Failover initiates when the node that is hosting the VM does not send regular heartbeat signals over the network to the other nodes. By default, this is five consecutively missed heartbeats (or 5,000 ms elapsed). Failover might occur because of a node failure or network failure. When heartbeat signals stop arriving from the failed node, one of the other nodes in the cluster begins taking over the resources that the VMs use.

   You define the one or more nodes that could take over by configuring the Preferred Owner and the Possible Owners properties. The Preferred Owner property specifies the hierarchy of ownership if there is more than one possible failover node for a resource. By default, all nodes are members of Possible Owners. Therefore, removing a node as a Possible Owner excludes it from taking over the resource in a failure situation.

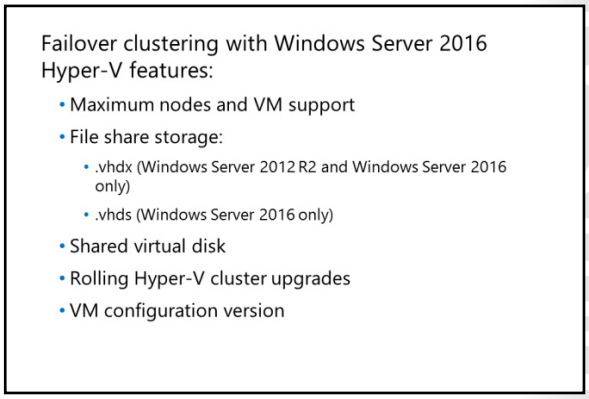
   For example, suppose that you implement a failover cluster by using four nodes. However, you configure only two nodes as Possible Owners. In a failover event, the resource might still be taken over by the third node if neither of the Preferred Owners is online. Although you did not configure the fourth node as a Preferred Owner, as long as it remains a member of Possible Owners, the failover cluster uses it to restore access to the resource, if necessary.

Resources are brought online in order of dependency. For example, if the VM references an iSCSI LUN, it stores access to the appropriate host bus adapters (HBAs), network (or networks), and LUNs in that order. Failover is complete when all the resources are online on the new node. For clients interacting with the resource, there is a short service interruption, which most users might not notice.

3. You also can configure the cluster service to fail back to the offline node after it becomes active again. When the cluster service fails back, it uses the same procedures that it performs during failover. This means that the cluster service takes all of the resources associated with that instance offline, moves the instance, and then brings all of the resources in the instance back online.

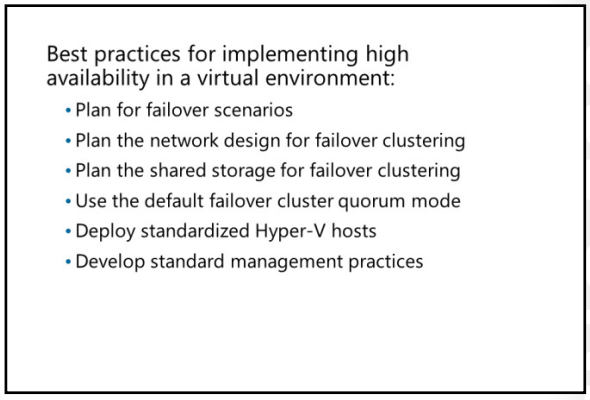
Failover clustering with Windows Server 2016 Hyper-V features

There are many improvements to the functionality of Hyper-V with failover clustering since the introduction of Hyper-V in Windows Server 2008. Windows Server 2016 continues to build on Hyper-V with failover clustering with some updated features and improvements in the following areas:



- Maximum node and VM supported. Failover clustering supports up to 64 nodes and 8,000 VMs per cluster (and 1024 VMs per node).
- File share storage. Windows Server 2012 introduced the possibility to store VMs on Server Message Block (SMB) file shares in a file server cluster. This is a way to provide shared storage that is accessible by multiple clusters by providing the ability to move VMs between clusters without moving the storage. To enable this feature, deploy a file server cluster role and select Scale-Out File Server for application data.
- Shared virtual disk. Windows Server 2012 R2 introduced the ability to use a .vhdx as a shared virtual disk for guest clusters. Windows Server 2016 introduced improved features to the shared disks and introduced a new disk format, .vhds (VHD Set).
- Rolling Hyper-V cluster upgrades. In Windows Server 2016, you can upgrade the nodes one at a time when upgrading from Windows Server 2012 R2. After upgrading all nodes in a Hyper-V cluster, you can upgrade the functional level of the entire cluster.
- VM configuration version. Windows Server 2016 builds on the rolling upgrades by not updating the VM's configuration version automatically. You can now manually update the VM configuration version. This allows a VM to migrate back and forth from both Windows Server 2016 and Windows Server 2012 R2 until you have completed the rolling upgrades, and you are ready to upgrade to the version for Windows Server 2016 and take advantage of the new features for Windows Server 2016 Hyper-V.

Best practices for implementing high availability in a virtual environment



After you determine which applications you will deploy on highly available failover clusters, you need to plan and deploy the failover clustering environment. Apply the following best practices when you implement the failover cluster:

- Plan for failover scenarios. When you design the hardware requirements for the Hyper-V hosts, ensure that you include the hardware capacity that is required when hosts fail. For example, if you deploy a six-node cluster, you must determine the number of host failures that you want to accommodate. If you decide that the cluster must sustain the failure of two nodes, then the four remaining nodes must have the capacity to run all of the VMs in the cluster.
- Plan the network design for failover clustering. To optimize the failover cluster performance and failover, you should dedicate a fast network connection for internode communication. Similar to earlier versions, this network should be logically and physically separate from the network segment (or segments) that clients use to communicate with the cluster. You also can use this network connection to transfer VM memory during a live migration. If you use iSCSI for any VMs, ensure that you also dedicate a network connection to the iSCSI network connection. This also applies if you use SMB 3.0 shares for VMs.
- Plan the shared storage for failover clustering. When you implement failover clustering for Hyper-V, the shared storage must be highly available. If the shared storage fails, the VMs will all fail, even if the physical nodes are functional. To ensure storage availability, you will need to plan for redundant connections to the shared storage, and Redundant Array of Independent Disks (RAID) on the storage device. If you decide to use a shared virtual hard disk, ensure that you locate the shared disk on a highly available resource such as a Scale-Out File Server.
- Use the recommended failover cluster quorum mode. For failover clustering in Windows Server 2016, the default is dynamic quorum mode and dynamic witness. You should not modify the default configuration unless you understand the implications of doing so.
- Deploy standardized Hyper-V hosts. To simplify the deployment and management of the failover cluster and Hyper-V nodes, develop a standard server hardware and software platform for all nodes.
- Develop standard management practices. When you deploy multiple VMs in a failover cluster, you increase the risk that a single mistake might shut down a large part of the server deployment. For example, if an administrator accidentally configures the failover cluster incorrectly and the cluster fails, all VMs in the cluster will be offline. To avoid this, develop and thoroughly test standardized instructions for all administrative tasks.

Question: Why is using shared storage a best practice in Windows Server Hyper-V failover clustering?

Question: You have two clusters; one is a Windows Server 2016 cluster (Cluster1), and the other is a mixed mode cluster of Windows Server 2012 R2 and Windows Server 2016 (Cluster2) that is in the process of upgrading, but it has not finished. In addition, you have two VMs called VM1 and VM2. VM1 and VM2 occasionally need to migrate back and forth between Cluster1 and Cluster2. Should you upgrade the configuration version on VM1?

Lesson 2
Implementing Hyper-V VMs on failover clusters

Implementing highly available VMs is different from implementing other roles in a failover cluster. Failover clustering in Windows Server 2016 provides many features for Hyper-V clustering, in addition to tools for VM high availability management. In this lesson, you will learn about how to implement highly available VMs.

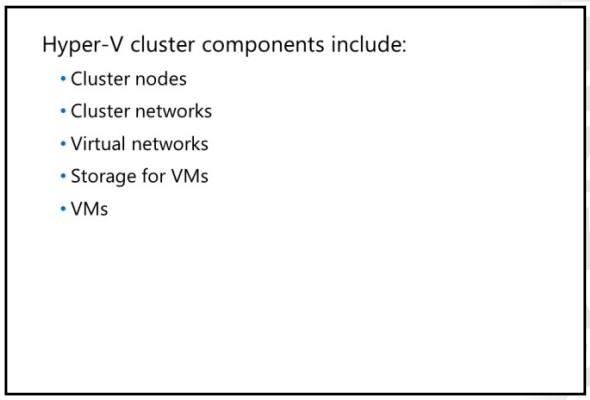
Lesson Objectives

After completing this lesson, you will be able to:

- Describe the components of a Hyper-V cluster.
- Describe the prerequisites for implementing Hyper-V failover clusters.
- Describe how to implement Hyper-V VMs on a failover cluster.
- Describe how to configure Clustered Shared Volumes (CSVs).
- Explain how to configure a shared virtual hard disk.
- Explain how to implement Scale-Out File Servers for VM storage.
- Describe the considerations for implementing Hyper-V VMs in a cluster.
- Explain how to maintain and monitor VMs in clusters.
- Implement failover clustering.

Components of Hyper-V clusters

Hyper-V as a role has some specific requirements for cluster components. To form a Hyper-V cluster, you must have at least two physical nodes. Whereas other clustered roles (such as Dynamic Host Configuration Protocol [DHCP] or file server) allow nodes to be VMs, Hyper-V nodes in most production environments should be physical servers. However, Windows Server 2016 allows you to enable nested virtualization, which enables you to configure Hyper-V host by using a guest VM. Allowing you to simulate clustering scenarios previously needing two physical servers, and by using two guest VMs to create a guest cluster with Hyper-V.



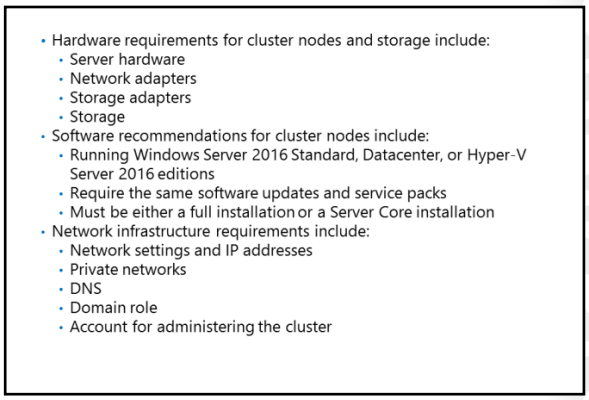
In addition to having nodes, you also must have physical and virtual networks. Failover clustering requires a cluster network interface for internal cluster communication and a network interface for clients. You can also implement a storage network separately, depending on the type of storage you use. As a reminder, specific to the Hyper-V role, you also should consider virtual networks for clustered VMs. It is very important to create the same virtual networks on all physical hosts that participate in one cluster. Failure to do so causes a VM to lose network connectivity when it moves from one host to another.

Storage is an important component of VM clustering. You can use any storage that Windows Server 2016 failover clustering supports. We recommend that you configure storage as a CSV. We will discuss this in a following topic.

When using host clustering, VMs are also components of a Hyper-V cluster. In Failover Cluster Manager, you can create new highly available VMs, or you can make existing VMs highly available. In both cases, the VM storage location must be on shared storage that is accessible to both nodes. You might not want to make all VMs highly available. In Failover Cluster Manager, you can select the VMs that are part of a cluster configuration.

Prerequisites for implementing Hyper-V failover clusters

To deploy a Hyper-V cluster, you must ensure that you meet the hardware, software, account, and network-infrastructure requirements. The following sections detail these requirements.



Hardware requirements

You must have the following hardware for a two-node failover cluster:

- Server hardware. Hyper-V on Windows Server 2016 requires an x64-based processor, hardware-assisted virtualization, and hardware-enforced Data Execution Prevention (DEP). As a best practice, the servers should have very similar hardware.

 **Note:** Microsoft supports a failover cluster solution only if all of the hardware features are marked as Certified for Windows Server. In addition, the complete configuration (servers, network, and storage) must pass all tests in the Validate This Configuration Wizard, which is included in the Failover Cluster Manager snap-in.

- Network adapters. The network adapter hardware, like other features in the failover cluster solution, must be marked as *Certified for Windows Server*. To provide network redundancy, you can connect cluster nodes to multiple networks. Alternatively, to remove single points of failure, you can connect the nodes to one network that uses the following hardware:
  - Redundant switches
  - Teamed network adapters
  - Redundant routers
  - Any similar hardware

  We recommend that you configure multiple physical network adapters on the host computer that you configure as a cluster node. One network adapter should connect to the private network that the inter-host communications use.
- Storage adapters. If you use serial-attached SCSI or Fibre Channel, the mass-storage device controllers in all clustered servers should be identical and should use the same firmware version. If you are using iSCSI, you need to dedicate one or more network adapters to the cluster storage for each clustered server. The network adapters that you use to connect to the iSCSI storage target need to be identical, and you need to use a Gigabit Ethernet or faster network adapter.

- Storage. You must use shared storage that is compatible with Windows Server 2016. If you deploy a failover cluster that uses a witness disk, the storage must contain at least two separate volumes. One volume functions as the witness disk and additional volumes contain the VM files that cluster nodes share. Storage considerations and recommendations include the following:
    - Use basic disks, not dynamic disks. Format the disks with the New Technology File System (NTFS).
    - Use the master boot record (MBR) or GUID partition table (GPT). Remember that there is a two terabyte (TB) limit on the MBR disks. Most production clusters today use GPT volumes for storing virtual disks.
    - If you use a storage area network (SAN), the miniport driver that the storage uses must work with the Microsoft Storport storage driver.
    - Consider using Microsoft Multipath I/O (MPIO) software. If your SAN uses a highly available network design with redundant components, deploy failover clusters with multiple host-bus adapters. To do this, use MPIO. This provides the highest level of redundancy and availability.
    - For environments without direct access to SAN or iSCSI storage, consider using shared virtual hard disks.

Software recommendations

The following are the software recommendations for using Hyper-V and failover clustering:

- All of the servers in a failover cluster need to run Windows Server 2016 Standard, Datacenter, or Microsoft Hyper-V Server 2016 editions. However, different editions are supported during a rolling upgrade failover cluster.
- All of the servers need to have the same software updates and service packs.
- All of the servers need to have the same drivers and firmware.

Network infrastructure requirements

You require the following network infrastructure for a failover cluster and an administrative account with the following domain permissions:

- Network settings and IP addresses. Use identical communication settings on all network adapters, including the speed, duplex mode, flow control, and media-type settings. Ensure that all network hardware supports the same settings.
- Private networks. If you use private networks that you have not routed to your entire network infrastructure for communication between cluster nodes, ensure that each of these private networks uses a unique subnet.
- Domain Name System (DNS). The servers in the cluster must use DNS for name resolution. You need to use the DNS dynamic update protocol.
- Domain role. All servers in the cluster must be in the same Active Directory Domain Services (AD DS) domain. As a best practice, all clustered servers need to have the same domain role (either member server or domain controller). The recommended role is a member server.
- Account for administering the cluster. When you first create a cluster or add servers to it, you must sign in to the domain with an account that has administrator rights and permissions on all of the cluster's servers. In addition, if the account is not a Domain Admins account, the account must have the Create Computer Objects permission in the domain.

Implementing Hyper-V VMs on a failover cluster

To implement failover clustering for Hyper-V, you must complete the following high-level steps:

To implement a Hyper-V VM on a failover cluster:

1. Install and configure Windows Server 2016
2. Configure shared storage
3. Install the Hyper-V and Failover Clustering features
4. Validate the cluster configuration
5. Create the cluster
6. Create a VM on one of the cluster nodes
7. Make the VM highly available (for an existing VM)
8. Test the VM failover

1. Install and configure the required versions of Windows Server 2016. After you complete the installation, configure the network settings, join the computers to an Active Directory domain, and then configure the connection to the shared storage.
2. Configure the shared storage. You must use Disk Manager to create disk partitions on the shared storage.
3. Install the Hyper-V and Failover Clustering features on the host servers. You can use Server Manager in Microsoft Management Console (MMC) or Windows PowerShell to do this.
4. Validate the cluster configuration. The **Validate This Cluster Wizard** checks all of the prerequisite components that are required to create a cluster and provides warnings or errors if any components do not meet the cluster requirements. Before you continue, resolve any issues that the **Validate This Cluster Wizard** identifies.

Note: Although it is possible to create a cluster without running cluster validation, we strongly recommended that you run the **Validate This Cluster Wizard** and resolve all issues before creating a cluster and putting it into production.

5. Create the cluster. When the components pass the validation by the **Validate This Cluster Wizard**, you can create a cluster. When you configure the cluster, assign a cluster name and an IP address. You create a computer object also referred to as the cluster name object (CNO) using the cluster name in AD DS, and register the IP address in DNS. In Windows Server 2012 R2 and later, you can create an Active Directory–detached cluster which allows you create the cluster name object in DNS however does not require you to have the cluster name object in AD DS.

Note: You can enable Clustered Shared Storage for the cluster only after you create the cluster and add eligible storage to it. If you want to use CSV, you should configure CSV before you move to the next step.

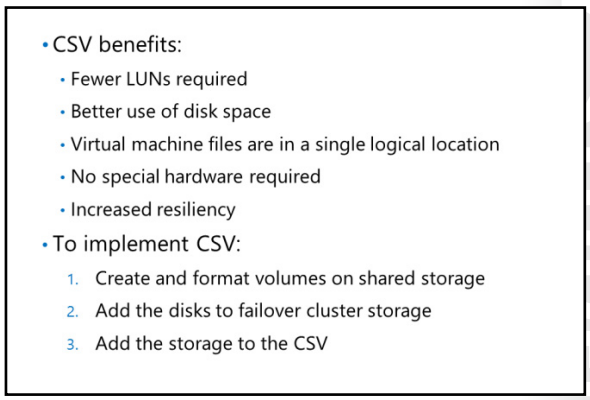
6. Create a VM on one of the cluster nodes. When you create the VM, ensure that all files associated with the VM—including both the virtual hard disk and VM configuration files—are stored on the shared storage. You can create and manage VMs in either Hyper-V Manager or Failover Cluster Manager. We recommended that you use the Failover Cluster Manager console for creating VMs. When you create a VM by using Failover Cluster Manager, the VM automatically highly available.
7. Make the VM highly available only for existing VMs. If you created a VM before implementing failover clustering, you need to make it highly available manually. To make the VM highly available, in the Failover Cluster Manager, select a new service or application to make highly available. Failover Cluster Manager then presents a list of services and applications that can be made highly available. When you select the option to make VMs highly available, you can select the VM that you created on shared storage.

Note: When you make a VM highly available, you see a list of all VMs that are hosted on all cluster nodes, including VMs that are not stored on the shared storage. If you make a VM that is not located on shared storage highly available, you receive a warning, but Hyper-V adds the VM to the services and applications list. However, when you try to migrate the VM to a different host, the migration will fail.

8. Test VM failover. After you make the VM highly available, you can migrate the computer to another node in the cluster. You can select to perform a Quick Migration or a Live Migration. In most cases, you should perform a Live Migration to reduce downtime. We will discuss these differences later in this course.

Configuring CSVs

CSVs in a Windows Server 2016 failover cluster allow multiple nodes in the cluster to have read-write access simultaneously to the same disk that you provision as an NTFS volume, and Windows Server 2016 failover cluster adds them as storage to the cluster. When you use CSVs, clustered roles can fail over from one node to another more quickly, and without requiring a change in drive ownership or dismounting and remounting a volume. CSVs also help in simplifying the management of a potentially large number of LUNs in a failover cluster.



CSVs provide a general-purpose, clustered file system, which you layer on NTFS. Windows Server 2016 does not restrict CSVs to specific clustered workloads, but it only supports them for Hyper-V clusters and Scale-Out File Server clusters.

Although CSVs provide additional flexibility and reduce downtime, you do not need to configure and use CSVs when you implement high availability for VMs in Hyper-V. You also can create clusters on Hyper-V by using the regular approach (with disks that you do not assign as CSVs). However, we recommend that you use CSVs because they provide the following advantages:

- Reduced LUNs for the disks. You can use CSVs to reduce the number of LUNs that your VMs require. When you configure a CSV, you can store multiple VMs on a single LUN, and multiple host computers can access the same LUN concurrently.
- Improved use of disk space. Instead of placing each .vhd file on a separate disk with empty space so that the .vhd file can expand, you can oversubscribe disk space by storing multiple .vhd files on the same LUN.
- Single location for VM files. You can track the paths of .vhd files and other files that VMs use. Instead of using drive letters or GUIDs to identify disks, you can specify the path names.

  When you implement a CSV, all added storage displays in the **\ClusterStorage** folder. The **\ClusterStorage** folder is created on the cluster node's system folder, and you cannot move it. This means that all Hyper-V hosts that are members of the cluster must use the same drive letter as their system drive, or VM failovers fail.

- No specific hardware requirements. There are no specific hardware requirements to implement CSVs. You can implement CSVs on any supported disk configuration, and on either Fibre Channel or iSCSI SANs.
- Increased resiliency. CSVs increases resiliency because the cluster can respond correctly even if connectivity between one node and the SAN is interrupted, or if part of a network is down. The cluster reroutes the CSV traffic through an intact part of the SAN or network.

Implementing CSVs

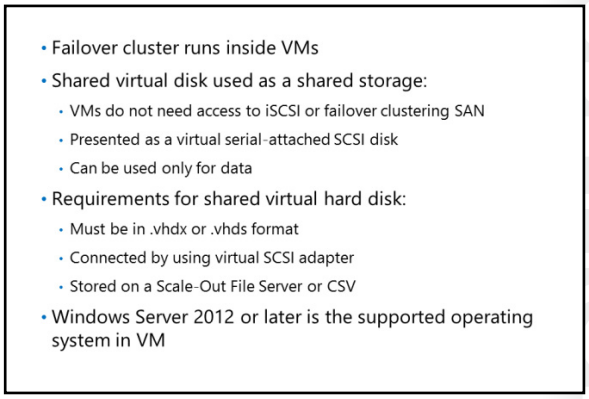
After you create the failover cluster, you can enable a CSV for the cluster, and then add storage to the CSV.

Before you can add storage to the CSV, the LUN must be available as shared storage to the cluster. When you create a failover cluster, all of the shared disks that you configured in Server Manager are added to the cluster, and you can add them to a CSV. Additionally, you have the option to add storage to the cluster, after you create the cluster. If you add more LUNs to the shared storage, you must first create volumes on the LUN, add the storage to the cluster, and then add the storage to the CSV.

We recommend that you configure CSVs before you make any VMs highly available. However, you can convert a VM from regular disk access to CSV after deployment. The following considerations apply for conversion from regular disk access to CSV after deployment:

- The LUN's drive letter (or *mount point*) is removed when you convert from regular disk access to the CSV. This means that you must recreate all VMs that you stored on the shared storage. If you must keep the same VM settings, consider exporting the VMs, switching to a CSV, and then importing the VMs in Hyper-V.
- You cannot add shared storage to a CSV if it is in use. If you have a running VM that uses a cluster disk, you must shut down the VM, and then add the disk to the CSV.

Configuring a shared virtual hard disk



To implement guest clustering in previous versions of Windows Server, you had to expose shared storage to the VM. You could connect to the shared storage by using a virtual Fibre Channel interface or by using iSCSI. In some scenarios, it was a complicated task to perform, if you did not have the support of appropriate drivers for virtual Fibre Channel, or if you did not have iSCSI support on the storage. In addition, in some scenarios, such as when you hosted a VM at a hosting provider, administrators did not want to expose a storage layer to the VM users or tenant administrators. To address these issues, Windows Server 2016 now provides an additional layer of abstraction for VM cluster storage. It is possible to share a virtual hard disk (in .vhdx or .vhds format only) between two or more VMs and use that virtual hard disk as a shared storage when building guest clusters. You can use the shared virtual hard disk as a witness disk or as a data disk in a cluster.

How does a shared virtual hard disk work?

You add shared virtual hard disks as SCSI drives in the VM settings. They appear as virtual serial-attached SCSI disks in the VM. You can add a shared virtual hard disk to any VM with a supported guest operating system running on a Windows Server 2016 Hyper-V platform. When you use this technology, the guest-

clustering configuration is simplified because you have several options for providing shared storage for guest clusters. These options include shared virtual hard disk, Fibre Channel, SMB, Storage Spaces, and iSCSI storage. You can use shared virtual disks to provide storage for solutions such as SQL Server databases and file server clusters.

Shared virtual hard disk limitations

There are limitations to the virtual hard disk while it is shared between two or more VMs compared to a standard .vhd or.vhdx. In Windows Server 2012 R2 this included, dynamic resizing while online, storage live migration, the virtual disk being included in the checkpoints, additionally being included in a Hyper-V Replica of the VM. In Windows Server 2016, online resizing is available and Hyper-V Replica includes the shared virtual hard disk when creating the replica.

How to configure shared virtual hard disks

You can use shared virtual disks in guest cluster scenarios. To configure a guest failover cluster that uses shared virtual hard disks, you must meet the followings requirements:

- At least a two-node Hyper-V failover host cluster.
- All servers must run Windows Server 2012 R2 or later.
- All servers need to belong to the same Active Directory domain.
- Configured shared storage resources must be available—for example, CSVs on block storage (such as clustered storage spaces) or a Scale-Out File Server cluster (running Windows Server 2012 R2 or later) with SMB 3.0 (for file-based storage).
- Sufficient memory, disk, and processor capacity within the failover cluster is necessary to support multiple VMs implemented as guest failover clusters.

For the guest operating systems, you can only use Windows Server 2012 or later. However, if you use Windows Server 2012 in VMs that use shared virtual hard disks, you must install Hyper-V integration services from Windows Server 2012 R2 or later. It supports both Generation 1 and Generation 2 VMs.

When you decide to implement shared virtual hard disks as storage for guest clusters, you must first decide where to store the shared virtual hard disk. You can deploy the shared virtual hard disk at the following locations:

- CSV location. In this scenario, all VM files, including the shared. vhdx or.vhds files are stored on a CSV configured as shared storage for a Hyper-V failover cluster.
- Scale-Out File Server SMB 3.0 share. This scenario uses SMB file-based storage as the location for the shared. vhdx or.vhds files. You must deploy a Scale-Out File Server and create an SMB file share as the storage location. You also need a separate Hyper-V failover cluster.

 **Note:** You should not deploy a shared virtual hard disk on an ordinary file share or a local hard drive on the host machine. You must deploy the shared virtual hard disk on a highly available location.

You can configure a shared virtual hard disk in a Windows Server 2016 Hyper-V cluster when you use the Failover Cluster Manager GUI, or by using Windows PowerShell. If you use a .vhdx, there are extra steps required to create the guest shared virtual disk to enable Hyper-V and failover cluster to know that the .vhdx is a shared disk. However, with the .vhds format introduced in Windows Server 2016, you do not need those steps, and the process is simplified.

Additional Reading: For more information, refer to: "Deploy a Guest Cluster Using a Shared Virtual Hard Disk" at: http://aka.ms/isec0h

When you use Hyper-V Manager, you can create a virtual hard disk using the .vhds. We recommend that you always attach virtual hard disks on a separate virtual SCSI adapter than the virtual disk with the operating system. However, you can connect to the same adapter when running a Generation 2 VM.

Note: Adding virtual SCSI adapters require the VM to be offline. If you already added the SCSI adapters, you can complete all other steps while the VM is online.

To add a shared virtual disk to two VM in Windows Server 2016, go to the Failover Cluster Manager; select the virtual SCSI controller and a Shared Drive. Browse to the created disk and click **Apply**. Then, repeat this procedure on all VMs that will use this shared virtual hard disk.

To add a shared virtual hard disk by using Windows PowerShell, you should use the **Add-VMHardDiskDrive** cmdlet with the **–ShareVirtualDisk** parameter. You must run this command under administrator privileges on the Hyper-V host, for each VM that uses the shared .vhds file.

For example, if you want to create and add a shared virtual hard disk (**Data1.vhds**) that is stored on volume 1 of the CSV to two VMs named **VM1** and **VM2**, you would use the following commands in Windows PowerShell:

```
New-VHD –Path C:\ClusterStorage\Volume1\Data1.vhds –Dynamic –SizeBytes 127GB
Add-VMHardDiskDrive -VMName VM1 -Path C:\ClusterStorage\Volume1\Data1.vhds –
ShareVirtualDisk
Add-VMHardDiskDrive -VMName VM2 -Path C:\ClusterStorage\Volume1\Data1.vhds –
ShareVirtualDisk
```

In addition, if you want to add a shared virtual hard disk (**Witness.vhdx**) that is stored on an SMB file share (**\\Server1\Share1**) to a VM that is named **VM2**, you should use the following command in Windows PowerShell:

```
Add-VMHardDiskDrive -VMName VM2 -Path \\Server1\Share1\Witness.vhds -ShareVirtualDisk
```

The following table lists the different Hyper-V capabilities for each shared storage option when compared to a shared virtual disk.

Capability	Shared .vhdx and .vhds	Virtual Fibre Channel	ISCSI in VM
Supported storage	Storage spaces, serial-attached SCSI, Fibre Channel, iSCSI, SMB	Fibre Channel SAN	iSCSI SAN
Storage presented in the VM as	Virtual serial-attached SCSI	Virtual Fibre Channel LUN	iSCSI LUN
Data flows through the Hyper-V switch	No	No	Yes
Storage is configured at the Hyper-V host level	Yes	Yes	No

Capability	Shared .vhdx and .vhds	Virtual Fibre Channel	ISCSI in VM
Provides low latency and low central processing unit (CPU) use	Yes (remote direct memory access [RDMA] or Fibre Channel)	Yes (Fibre Channel)	No
Requires specific hardware	No	Yes	No
Requires switch to be reconfigured when VM is migrated	No	Yes	No
Exposes storage architecture	No	Yes	Yes

Question: What is the primary benefit of using shared hard virtual disks?

Implementing Scale-Out File Servers for VMs

It is possible to use one more technique to make VMs storage highly available. Instead of using a host or guest clustering, now you can store VM files on a highly available SMB 3.0 file share. When you use this approach, you achieve storage high availability not by clustering Hyper-V nodes, but by clustering file servers that host VM files on their file shares. With this new capability, Hyper-V can store all VM files, including configuration, files, and checkpoints, on highly available SMB file shares.

- In Windows Server 2016, you can store VM files on a SMB 3.0 file share
- File servers need to run Windows Server 2012 or later
- A file server cluster needs to be configured as a Scale-Out File Server for application data
- Use Hyper-V Manager to create or move VM files to a SMB file share

What is a Scale-Out File Server?

A Scale-Out File Server, introduced in Windows Server 2012, provides continuously available storage for file-based server applications. You configure a Scale-Out File Server by creating a File Server role on a failover cluster and selecting the Scale-Out File Server for application data option instead of File Server for general use. This requires the use of a CSV for storage of data.

The Scale-Out File Server is different from the file server clusters that were the only option in previous versions of Windows Server in several ways. An ordinary file server cluster serves the clients only by using one node at a time; however, a Scale-Out File Server can engage all nodes simultaneously. You achieve this with the new Windows Server failover clustering features, and the new capabilities in the new version of Windows file server protocol, SMB 3.0. Therefore, by adding nodes to the failover cluster running the File Server role with the Scale-Out File Server feature, performance of the entire cluster increases. As a result, it is now possible to store resources such as databases or VM hard disks on the folder shares hosted on the Scale-Out File Server.

The key benefits of using a Scale-Out File Server are:

- Active-active clustering. When all other failover clusters work in an active-passive mode, a Scale-Out File Server cluster works in a way that all nodes can accept and serve SMB client requests. In Windows Server 2012 R2, SMB 3.0 is upgraded to SMB 3.0.2. This version improves scalability and manageability for Scale-Out File Servers. Windows Server 2012 R2 tracks SMB client connections per file share (instead of per server), and then redirects clients to the cluster node with the best access to the volume used by the file share.
- Increased bandwidth. In previous versions of Windows Server, the bandwidth of the file server cluster was constrained to the bandwidth of a single cluster node. Because of the active-active mode in the Scale-Out File Server cluster, you can have much higher bandwidth, which you can additionally increase by adding cluster nodes.
- CSV Cache. Because the Scale-Out File Server clusters use CSVs, they also benefit from the use of the CSV Cache. The CSV Cache is a feature that you can use to allocate system memory (RAM) as a write-through cache. The CSV Cache provides caching of read-only unbuffered I/O. This can improve performance for applications such as Hyper-V, which conducts unbuffered I/O when accessing a .vhd file. With Windows Server 2012, you can allocate up to 20 percent of the total physical RAM for CSV write-through cache, and 80 percent with Windows Server 2012 R2 and Windows Server 2016. The total physical RAM that a CSV write-through cache consumes is from nonpaged pool memory.
- Abstraction of the storage layer. When you use a Scale-Out File Server as the storage location for virtual disks, you can migrate live VMs from cluster to cluster, and you do not need to migrate the storage provided the URL location is accessible from the destination cluster.

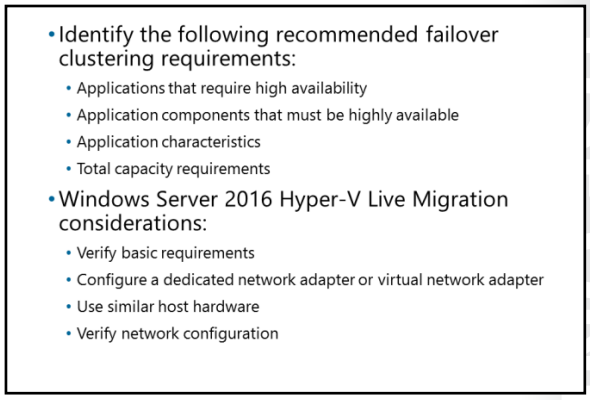
To implement a Scale-Out File Server, you must meet the following requirements:

- One or more computers running Windows Server 2012 or later with the Hyper-V role installed.
- One or more computers running Windows Server 2012 or later with the File and Storage Services role installed.
- A common Active Directory infrastructure. The servers that run AD DS do not need to run Windows Server 2016.

Before you implement VMs on an SMB file share, you need to set up a file server cluster. To do that, you must have at least two cluster nodes with file services and failover clustering installed. In Failover Cluster Manager, you must create a file server and select the Scale-Out File Server for application data configuration. After you configure the cluster, you must deploy the SMB Share – Applications profile. This profile is designed for Hyper-V and other application data. After you create the share, you can use the Hyper-V Manager console to deploy new VMs on the SMB file share, or you can migrate existing VMs to the SMB file share when you use the Storage Migration method.

Question: Have you considered storing VMs on the SMB share? Why or why not?

Considerations for implementing Hyper-V clusters



By implementing failover clustering on servers with the Hyper-V feature installed, you can make VMs highly available. However, this adds significant cost and complexity to a Hyper-V deployment. You must invest in additional server hardware to provide redundancy, and you need to implement or have access to a shared storage infrastructure.

Use the following recommendations to ensure that the failover clustering strategy meets the organization's requirements:

- Identify the applications or services that require high availability. If you were to ask the people who use the organization's applications about their preferences, most of them would probably say that they want all applications to be highly available. However, unless you have the option of making all VMs highly available, you must develop priorities for which applications you will make highly available.
- Identify the application components that must be highly available to make the applications highly available. In some cases, the application might run on a single server. If so, you only need to make that server highly available. Other applications might require that several servers and other components (such as storage or the network) be highly available.
- Identify the application characteristics. You must understand several things about an application:
    - Is virtualizing the server that runs the application an option? A virtual environment is not supported or recommend for certain applications.
    - What options are available for making the application highly available? You can make some applications highly available through options other than host clustering. If other options are available, evaluate the benefits and disadvantages of each option. These options can vary and are based on the application.
    - What are the performance requirements for each application? Collect performance information on the servers currently running the applications to gain an understanding of the hardware requirements that you need to meet when you virtualize the server.
- What capacity is required to make the Hyper-V VMs highly available? As soon as you identify all of the applications that you must make highly available by using host clustering, you can start to design the actual Hyper-V deployment. By identifying the performance requirements and the network and storage requirements for applications, you can define the hardware that you must implement in a highly available environment.

Live Migration is one of the most important aspects of Hyper-V clustering. We will discuss this in more detail in a later lesson. However when implementing Live Migration, consider the following:

- Verify basic requirements. The basic requirements for Live Migration in a cluster requires that all hosts must be part of a Windows Server 2008 R2 or later failover cluster, and that host processors must be from the same manufacturer. In addition, all hosts in the cluster must have access to shared storage.

- Configure a dedicated network adapter or virtual network adapter for live migration communication. When you implement failover clustering, you should configure a separate virtual LAN (VLAN) live migration network. You use this network to transfer the VM memory during a failover. To optimize this configuration, configure a network adapter for this network that has a capacity of one gigabit per second (Gbps) or higher.
- Use similar host hardware. All failover cluster nodes should use the same hardware for connecting to shared storage, and all cluster nodes must have processors from the same manufacturer. Although you can enable failover for VMs on a host with different processor versions by configuring processor compatibility settings, the failover experience and performance is more consistent if all servers have very similar hardware.
- Verify network configuration. As with all failover clusters, the network configurations need to be the same for all nodes in the failover cluster. All trunking and VLAN tagged traffic needs to be the same on all failover cluster nodes. This insurance network connectivity for the guest VM when taking advantage of Hyper-V virtual networking.

Maintaining and monitoring VMs in clusters

Failover clusters provide high availability for the roles configured in the cluster. However, you must monitor the roles and take action when there is an issue with role availability. VM is one of the cluster roles, and when this role does not respond to a heartbeat, the failover cluster can restart or fail over the role to a different cluster node.

In Windows Server 2016 failover clustering, you can implement the following technologies for VM maintenance and monitoring:

- Service and VM health monitoring
- Network health detection (Windows Server 2012 R2 and later only)
- Virtual machine drain on shutdown (Windows Server 2012 R2 and later only)

In Windows Server versions prior to Windows Server 2012, the failover cluster was not able to monitor applications that were running inside a VM. For example, if you used a VM as a print server, the failover cluster was not able to detect if the Print Spooler service in a VM stopped. It would not take any action even though the print server did not work because the VM was still responding to a heartbeat.

Failover clustering in Windows Server 2016 can monitor and detect application health for applications and services that run inside a VM. If a service in a VM stops responding or an event is added to the System, Application, or Security logs, the failover cluster can take actions such as restarting the VM or failing it over to a different node to restore the service. The only requirement is that both the failover cluster node and the VM must run Windows Server 2012 or a later, and have integration services installed.

You can configure VM monitoring by using the Failover Cluster Manager or Windows PowerShell. By default, you configure a failover cluster to monitor VM health. To enable heartbeat monitoring, you must install integration services on the VM. You can verify the monitoring configuration on the **Settings** tab of the VM resource properties. To enable monitoring of any specific services that run on the VM, you must right-click the VM cluster role, click **More actions**, and then click **Configure Monitoring**. In the **Select Services** window, you can select services to monitor inside the VM. The failover cluster will take action only if a service stops responding, and if, in the Services Control Manager, you have configured the service with the **Take No Actions** recovery setting.

Windows Server 2016 also can monitor failure of VM storage and loss of network connectivity with a technology called *network health detection*. Storage failure detection can detect the failure of a VM boot disk or any other virtual hard disk that the VM uses. If a failure happens, the failover cluster moves and restarts the VM on a different node.

You can also configure a virtual network adapter to connect to a protected network. If Windows Server 2016 loses network connectivity to such a network because of reasons such as physical switch failure or disconnected network cable, the failover cluster will move the VM to a different node to restore network connectivity.

Windows Server 2012 R2 also enhances VM availability in scenarios when one Hyper-V node shuts down before you place it in the maintenance mode, and before draining any clustered roles from it. In Windows Server 2012, shutting down the cluster node before draining it results in VMs put into a saved state, and then moved to other nodes and resumed. This causes an interruption to the availability of the VMs. In Windows Server 2016, if such a scenario occurs, the cluster automatically live migrates all running VMs before the Hyper-V node shuts down.

 **Note:** We still recommend that you drain clustered roles (and place the node in maintenance mode) before performing a shutdown operation.

Configuration of this functionality, called *virtual machine drain on shutdown*, is not accessible through Failover Cluster Manager. To configure it, you must use Windows PowerShell, and configure the **DrainOnShutdown** cluster property. It is enabled by default, and the value of this property is set to **1**. If you want to check the value, run Windows PowerShell as Administrator, and then run the following command:

```
(Get-Cluster).DrainOnShutdown
```

Question: What are some alternative Microsoft technologies that you can use for VM monitoring and network monitoring?

Demonstration: Implementing failover clustering with Hyper-V

In this demonstration, you will see how to:

- Configure failover clustering.
- Configure disks for failover cluster.
- Move VM storage to the iSCSI target.
- Configure the VM as highly available.

Demonstration Steps

Configure failover clustering

1. On **LON-HOST1** and **LON-NVHOST2**, install the **Failover Clustering** feature.
2. On **LON-HOST1**, create a failover cluster by using the following settings:
   - Add **LON-HOST1** and **LON-NVHOST2**.
   - Name the cluster **VMCluster**.
   - Assign the address **172.16.0.126**.
   - Clear the **Add all eligible storage to the cluster** option.

Configure disks for failover cluster

1. In **Failover Cluster Manager**, on **LON-HOST1**, add all three iSCSI disks to the cluster.
2. Verify that all three iSCSI disks display as available for cluster storage.
3. Add the **Cluster Disk 1** to **Cluster Shared Volumes**.
4. From the **VMCluster.adatum.com** node, click **More Actions**, and then configure the **Cluster Quorum Settings** to use the default quorum configuration.

Move VM storage to the iSCSI target

1. Ensure that **LON-HOST1** is the owner of the disk that is assigned to Cluster Shared Volume. If it is not, move the disk to **LON-HOST1**.
2. Copy the **20740A-BASE.vhd** from **E:\Program Files\Microsoft Learning\20740\Drives** and **Base16D-WS16-TP5.vhd** from **E:\Program Files\Microsoft Learning\Base** copy virtual hard disk files to the **C:\ClusterStorage\Volume1** location.
3. Launch Windows PowerShell and run the following command:

```
Set-VHD -Path C:\ClusterStorage\Volume1\20740A-BASE.vhd -ParentPath
C:\ClusterStorage\Volume1\Base16D-WS16-TP5.vhd
```

Note: The drive letter might be different depending on the physical machine.

Configure the VM as highly available

1. In **Failover Cluster Manager**, click the **Roles** node, and then start the **New Virtual Machine Wizard**. If an error displays informing you that Microsoft Management has stopped working, restart this step.
2. In the **New Virtual Machine Wizard**, use the following settings:
   - Select **LON-HOST1** as the cluster node.
   - Name the computer as **TestClusterVM**.
   - Store the file in **C:\ClusterStorage\Volume1**.
   - Select **Generation 1**.
   - Assign **1536** megabytes (MB) of **RAM** to **TestClusterVM**.
   - Network: **Not Connected**.
   - Connect the VM to the existing virtual hard disk **20740A-BASE.vhd**, located at **C:\ClusterStorage\Volume1**.
3. Open **Settings** for **TestClusterVM**.
4. Enable the option for migration to computers with a different processor version.
5. On the **Roles** node, start the VM.

Lesson 3
Key features for VMs in a clustered environment

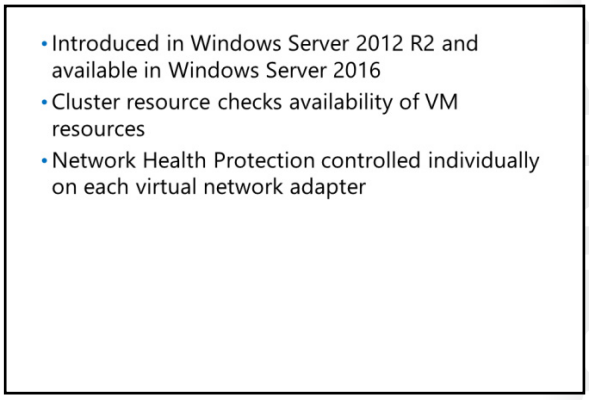
For VMs in a clustered environment, Network Health Protection and drain on shutdown are two key features used by the failover clustering feature that help to increase high availability. This lesson will both demonstrate and explain the configuration of these key features, and how they help to increase virtual high availability during unexpected and expected outages.

Lesson Objectives

After completing this lesson, you will be able to:

- Describe Network Health Protection.
- Configure Network Protection.
- Explain the actions taken on VMs when a host shuts down.
- Explain drain on shutdown.

Overview of Network Health Protection

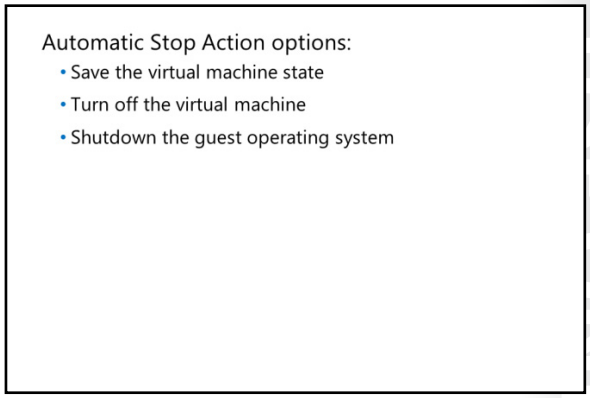


Network Health Protection was introduced in Windows Server 2012 R2 and is available for Windows Server 2016. Though we recommend network teaming as the first level of redundancy for your server to achieve network high availability with Hyper-V, there are many ways that a network can become disconnected and create availability outages. Network Health Protection allows a VM to live migrate from one failover cluster node to another failover cluster node if network connectivity on that specific network adapter becomes disconnected. Increasing the availability of the VM by moving the VM automatically instead of waiting for manual intervention.

Each VM has a cluster resource that continually checks to ensure that resources are available on the failover cluster node that is hosting the VM. This resource checks every 60 seconds so sometimes the network disconnection is quickly discovered other times it takes up 60 seconds. Once it discovers the disconnect, the resource will check the other nodes to see if the resources needed to run the VM are available. If the resources are available, the cluster resource initiates a live migration to move to another failover cluster node. In many cases, a network failure requires the VM to wait in a queued state for movement to another failover cluster node.

Each network adapter per VM can control this feature. By default, the **Protected Network** setting is enabled for all virtual network adapters. You can find this property in the advanced configuration section of the network adapter settings on each VM. This allows you to remove the setting if a network is not important enough to trigger a live migration if communications are lost.

Overview of actions taken on VMs when a host shuts down



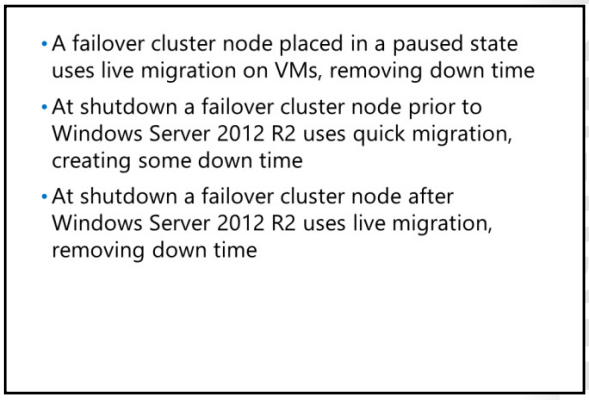
In Windows Server 2012 R2 and later when a shutdown is initiated on a Hyper-V host machine, what action is taken by that VM depends on the settings set for each VM. These options are found in the VM settings by selecting the **Automatic Stop Action** tab.

The options for what a VM does on the shutdown of a host are as follows:

- **Save the virtual machine state**. This option is the first and default option. In Windows Server 2012 R2 and later this option creates a .bin file reserving space for the memory to be saved when placing the VM in a saved state. If the host begins a shutdown, Hyper-V Virtual Machine Management Service (VMMS) will begin saving the VMs' memory to the hard drive and placing the VMs in a saved state.
- **Turn off the virtual machine.** This second option will allow VMMS to turn off the VM in a graceful manner for Hyper-V and entering an off state. However, the VM operating system views this no different from removing power on a physical machine.
- **Shutdown the guest operating system**. Unlike the other two options this third and final option requires that integrated services is working properly on the VM and that specifically, that you have selected and installed **Operating system shutdown** on the guest VM. This option however unlike the **Turn off the virtual machine** option allows a graceful shutdown of the VM from the host's perspective including the guest. By utilizing the integrated services, VMMS will trigger a shut down on the guest machine. Once initiated the VM will shut down the guest operating system and enter an off state.

 **Note:** If the Hyper-V host goes offline unexpectedly, the VMMS process will not have received any information about the shutdown and so none of these actions will occur. This is only useful when a shutdown is initiated on a Hyper-V host.

Overview of drain on shutdown



In Windows 2012 and later when placing a Hyper-V failover cluster node in a paused state, also referred to as maintenance mode, all VMs on that node are live migrated to other nodes in the cluster. This removes down time that would usually be required for shutting down a Hyper-V host. However, if a shutdown was initiated without placing a node in maintenance mode all VMs would be moved to another node via a quick migration. This would mean that the VM would go into a saved state by saving all activates to disk, move the VM role, and then resume the VM.

Windows Server 2012 R2 introduced draining on shutdown to resolve this issue. This feature is also available Windows Server 2016 and enabled by default. A failover cluster configured with drain on shutdown no longer will place a VM in a saved state and then move the VM, but instead will drain the roles first by using live migrations instead of quick migrations. Therefore, removing the previous down time created by a shutdown of failover cluster node.

Drain on shutdown should be enabled by default, however, to verify this setting run the following Windows PowerShell command:

```
(Get-Cluster).DrainOnShutdown
```

After running this Windows PowerShell command, you will see one of two options: "1" means it is enabled, and "0" means it is disabled.

Note: We recommend draining all roles before shutting down a failover cluster node. **Drain on shutdown** provides added protection to user error and circumstances were an application or the operating system initiate a shutdown outside of the user's control. This also does not protect against abrupt shutdowns of the Hyper-V failover cluster node. If the node is shut down before without the operating system initiating a shutdown, the VMs will go to an off state and begin coming online on another node.

Demonstration: Configure drain on shutdown

In this demonstration you see how to:

- Live migrate a VM.
- Configure drain on shutdown.

Demonstration Steps

Live migrate a VM

1. On **LON-NVHOST2**, in **Failover Cluster Manager**, start **Live Migration**.
2. Move **TestClusterVM** from **LON-HOST1** to **LON-NVHOST2**.
3. Connect to **TestClusterVM**, and ensure that you can operate it.

Configure drain on shutdown

1. On **LON-HOST1**, at a **Windows PowerShell** command prompt, type the following command, and then press Enter:

   ```
   (Get-Cluster).DrainOnShutdown
   ```

   Note: Should return a value of **"1"**.

2. Shut Down **LON-NVHOST2**.
3. Observe **TestClusterVM** moving to **LON-HOST1**.

   Question: When is a good time to remove the Network Health Protections settings?

Check Your Knowledge

Question	
What options do you need to enable VMMS to easily shutdown a guest operating system during a host initiated shut down?	
Select the correct answer.	
	Integrated Services, Operating system shutdown
	Automatic Stop Action, Save the virtual machine state
	Automatic Stop Action, Turn off virtual machine
	Automatic Stop Action, Shut down the guest operating system
	Integrated Services, Backup (volume checkpoint)

Lab: Implementing failover clustering with Windows Server 2016 Hyper-V

Scenario

The initial deployment of VMs on Hyper-V has been successful for A. Datum Corporation. As a next step in VM deployment, A. Datum is considering ways to ensure that the services and applications deployed on the VMs are highly available. As part of the implementation of high availability for most network services and applications, A. Datum is also considering options for making the VMs that run on Hyper-V highly available.

As one of the senior network administrators at A. Datum, you are responsible for integrating Hyper-V with failover clustering to ensure that the VMs deployed on Hyper-V are highly available. You are responsible for planning the VM and storage configuration, and for implementing the VMs as highly available services on the failover cluster. You have limited hardware; so to facilitate testing before implementation in your production environment, you will enable nested virtualization to test clustering two Hyper-V Hosts.

Objectives

After completing this lab, you will be able to:

- Configure a failover cluster for Hyper-V.
- Configure a highly available VM.

Lab Setup

Estimated Time: 75 minutes

Virtual machines: **20740A-LON-DC1-B**, **20740A-LON-SVR1-B**

Host machines: **20740A-LON-HOST1**, **20740A-LON-NVHOST2**

User name: **Adatum\Administrator**

Password: **Pa$$w0rd**

For this lab, you need to use the available VM environment.

 **Note:** You must have completed the labs in Modules 2, 5, and 7 to be able to complete this lab. Specifically, you must reconfigure the virtual machines used in the demo to bind to Host Internal Network.

It is also important to disconnect the host from the class network for this module.

Before you begin the lab, you **must** complete the following steps:

1. Restart the classroom computer, and then, in **Windows Boot Manager**, select **20740A-LON-HOST1**.
2. Sign in to **LON-HOST1** with the following credentials:
   - User name: **Adatum\Administrator**
   - Password: **Pa$$w0rd**
3. On **LON-HOST1**, start **Hyper-V Manager**.
4. In **Hyper-V Manager**, if necessary, click **20740A-LON-NVHOST2**, and in the **Actions** pane, click **Shut Down**.
5. In **Hyper-V Manager**, if necessary, click **20740A-LON-DC1-B**, and in the **Actions** pane, click **Start**.

6. In the **Actions** pane, click **Connect**. Wait until the VM starts.
7. Sign in by using the following credentials:
   - User name: **Administrator**
   - Password: **Pa$$w0rd**
   - Domain: **Adatum**
8. Repeat steps 4 through 6 for **20740A-LON-SVR1-B** and **20740A-LON-NVHOST2**.
9. On **LON-NVHOST2**, in **Hyper-V Manager**, in the **Actions** pane, click **Virtual Switch Manager**.
10. In the **Virtual Switch Manager for LON-NVHOST2** window, in the left pane, click **New virtual network switch**.
11. In the **Create virtual switch** pane, click **External**, and then click **Create Virtual Switch**.
12. In the **Virtual Switch Properties** pane, in the **Name** box, type **Host Internal Network**.
13. In the **Connection type** area, verify that **External network** is selected, review the information on the **Apply Networking Changes** dialog box, click **Yes**, and then click **OK**.
14. On **LON-HOST1**, in **Hyper-V Manager**, in the **Actions** pane, click **Virtual Switch Manager**.
15. In the **Virtual Switch Manager for LON-HOST1** window, in the left pane, click **Host Internal Network**.
16. In the details pane, click **External network**.
17. In the left pane, click **Physical Network**, and in the details pane, click **Internal network**.
18. Click **OK**. Click **Yes**.
19. Run the following commands in **Windows PowerShell**:

```
New-NetIPAddress -InterfaceAlias "vEthernet (Host Internal Network)" -IPAddress
172.16.0.160 -PrefixLength 16 -DefaultGateway 172.16.0.1
Set-DnsClientServerAddress -InterfaceAlias "vEthernet (Host Internal Network)" -
ServerAddresses 172.16.0.10
```

20. **Disable** and **Enable** the network adapter **vEthernet (Host internal Network)**.

Exercise 1: Configuring iSCSI storage

Scenario

A. Datum Corporation has important applications and services that they want to make highly available. Some of these services cannot use NLB. Therefore, you have decided to implement failover clustering. You decide to use iSCSI storage for failover clustering. First, you will configure iSCSI storage to support your failover cluster.

The main task for this exercise is as follows:

1. Configure iSCSI targets.

▶ Task 1: Configure iSCSI targets

1. On **LON-SVR1**, sign in as **Adatum\Administrator** with the password **Pa$$w0rd**.
2. Start **Server Manager**.
3. In **Server Manager**, navigate to **File and Storage Services**, and then navigate to **iSCSI**.

4. Create an iSCSI virtual disk with the following values:
   - Storage location: **C:**
   - Disk name: **iSCSIDisk1**
   - Size: **20 GB**
   - Create a new iSCSI target with the following values:
   - Target name: **lon-svr1**
5. Two iSCSI initiators with the following IP addresses:
   - IP Address: **172.16.0.32**
   - IP Address: **172.16.0.160**
6. Repeat step 4 to create two more iSCSI virtual disks with the disk names **iSCSIDisk2** and **iSCSIDisk3**

Results: After completing this exercise, you should have successfully installed an iSCSI Target Server.

Exercise 2: Configuring a failover cluster for Hyper-V

Scenario

The initial deployment of VMs on Hyper-V is very successful for A. Datum. As a next step in the deployment, A. Datum is considering ways to ensure that the services and applications deployed on the VMs are highly available. As part of the implementation of high availability for most network services and applications, A. Datum also is considering options for making the VMs that run on Hyper-V highly available.

You are responsible for planning the VM and storage configuration, and for implementing the VMs as highly available services on the Failover Cluster.

The main tasks for this exercise are as follows:

1. Connect to the iSCSI target from both host machines.
2. Configure failover clustering on both host machines.
3. Configure disks for a failover cluster.

▶ Task 1: Connect to the iSCSI target from both host machines

1. On **LON-HOST1**, in **Server Manager**, start the **iSCSI initiator**.
2. Use the **172.16.0.21** address to discover and connect to iSCSI target.
3. Switch to **LON-NVHOST2**, and use **Server Manager** to start the **iSCSI initiator**.
4. Use the **172.16.0.21** address to discover and connect to the iSCSI target.
5. In **Server Manager**, open **Disk Management**, and initialize and bring all iSCSI drives online.

Note: Note the drive letters used on **LON-HOST1**, while creating new Disks in **LON-NVHOST2** make sure to use an unused letter.

6. Format the first drive, and name it **ClusterDisk**.

7. Format the second drive, and name it **ClusterVMs**.
8. Format the third drive, and name it **Quorum**.
9. Switch back to **LON-HOST1**, open **Disk Management**, and bring all three iSCSI drives online.

Note: Disk numbers might vary based on the number of physical disks in the host computer. Choose the disks that are 20 GB in size.

▶ Task 2: Configure failover clustering on both host machines

1. On **LON-HOST1** and **LON-NVHOST2**, install the **Failover Clustering** feature.
2. On **LON-HOST1**, create a failover cluster by using the following settings:
   - Add **LON-HOST1** and **LON-NVHOST2**.
   - Name the cluster **VMCluster**.
   - Assign the address **172.16.0.126**.
   - Clear the **Add all eligible storage to the cluster** option.

▶ Task 3: Configure disks for a failover cluster

1. In **Failover Cluster Manager**, on **LON-HOST1**, add all three iSCSI disks to the cluster.
2. Verify that all three iSCSI disks display as available for cluster storage.
3. Add the **Cluster Disk 1** to **Cluster Shared Volumes**.
4. From the **VMCluster.adatum.com** node, click **More Actions**, and then configure the **Cluster Quorum Settings** to use the default quorum configuration.

Results: After completing this exercise, you should have successfully configured the failover clustering infrastructure for Hyper-V.

Exercise 3: Configuring a highly available VM

Scenario

After you have configured the Hyper-V failover cluster, you want to add VMs as highly available resources. In addition, you want to evaluate Live Migration and test Storage Migration.

The main tasks for this exercise are as follows:

1. Move VM storage to the iSCSI target.
2. Configure the VM as highly available.
3. Failover VM.
4. Configure drain on shutdown.
5. Prepare for the next module.

▶ Task 1: Move VM storage to the iSCSI target

1. Ensure that **LON-HOST1** is the owner of the disk that is assigned to Cluster Shared Volume. If it is not, move the disk to **LON-HOST1**.
2. Copy the **20740A-BASE.vhd** from **E:\Program Files\Microsoft Learning\20740\Drives** and **Base16D-WS16-TP5.vhd** from **E:\Program Files\Microsoft Learning\Base** copy virtual hard disk files to the **C:\ClusterStorage\Volume1** location.
3. Launch Windows PowerShell and run the following command.

```
Set-VHD -Path C:\ClusterStorage\Volume1\20740A-BASE.vhd -ParentPath
C:\ClusterStorage\Volume1\Base16D-WS16-TP5.vhd
```

Note: The drive letter might be different depending on the physical machine.

▶ Task 2: Configure the VM as highly available

1. In **Failover Cluster Manager**, click the **Roles** node, and then start the **New Virtual Machine Wizard**. If an error displays informing you that Microsoft Management has stopped working, restart this step.
2. In the **New Virtual Machine Wizard**, use the following settings:
   - Select **LON-HOST1** as the cluster node.
   - Name the computer as **TestClusterVM**.
   - Store the file in **C:\ClusterStorage\Volume1**.
   - Select **Generation 1**.
   - Assign **1536** megabytes (MB) of **RAM** to **TestClusterVM**.
   - Network: **Not Connected**.
3. Connect the VM to the existing virtual hard disk **20740A-BASE.vhd**, located at **C:\ClusterStorage\Volume1**.
4. Open **Settings** for **TestClusterVM**.
5. Enable the option for migration to computers with a different processor version.
6. On the **Roles** node, start the VM.

▶ Task 3: Failover VM

1. On **LON-NVHOST2**, in **Failover Cluster Manager**, start **Live Migration**.
1. Move **TestClusterVM** from **LON-HOST1** to **LON-NVHOST2**.
2. Connect to **TestClusterVM**, and ensure that you can operate it.

▶ Task 4: Configure drain on shutdown

1. On **LON-HOST1**, select the **drain on shutdown** option and at a **Windows PowerShell** command prompt, type the following command, and then press Enter:

```
(Get-Cluster).DrainOnShutdown
```

Note: This should return a value of "**1**".

2. Shut down **LON-NVHOST2**.
3. Observe **TestClusterVM** moving to **LON-HOST1**.

▶ Task 5: Prepare for the next module

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

1. On the host computer, start **Hyper-V Manager**.
2. Shutdown all Virtual Machines.
3. Restart your computer, and when prompted, choose **Windows Server 2012 R2**.

Results: After completing this exercise, you should have successfully configured the VM as highly available.

Question: What is an example of when you might not want Protected Network selected for a Virtual Network Adapter?

Question: What is the difference between live migration and storage migration?

Module Review and Takeaways

Review Question

Question: Do you have to implement CSV in order to provide high availability for VMs in VMM in Windows Server 2016?

Tools

Tools for implementing failover clustering with Hyper-V include:

- Failover Cluster Manager
- Hyper-V Manager
- VMM console

Best Practices

- Develop standard configurations before you implement highly available VMs. You should configure the host computers to be as close to identical as possible. To ensure that you have a consistent Hyper-V platform, you should configure standard network names, and use consistent naming standards for CSV volumes.
- Use new features in Hyper-V Replica to extend your replication to more than one server.
- Consider using Scale-Out File Servers clusters as storage for highly available VMs.
- Implement VM Manager. VM Manager provides a management layer on top of Hyper-V and Failover Cluster Manager that can stop you from making mistakes when you manage highly available VMs. For example, it stops you from creating VMs on storage that is inaccessible from all nodes in the cluster.

Common Issues and Troubleshooting Tips

Common Issue	Troubleshooting Tip
VM failover fails after implementing CSV and migrating the shared storage to CSV.	
A VM fails over to another node in the host cluster, but loses all network connectivity.	
Four hours after restarting a Hyper-V host that is a member of a host cluster, there are still no VMs running on the host.	

Module 10

Implementing Network Load Balancing

Contents:

Module Overview

Network Load Balancing (NLB) is a feature available to computers that run the Windows Server operating system. NLB uses a distributed algorithm to balance an IP traffic load across multiple hosts, which in turn helps to improve the scalability and availability of business-critical, IP-based services. NLB also provides high availability, because it detects host failures and automatically redistributes traffic to surviving hosts.

To deploy NLB effectively, you must understand its functionality and the scenarios where its deployment is appropriate. The main update to NLB since Windows Server 2008 R2 is the inclusion of a comprehensive set of Windows PowerShell cmdlets. These cmdlets enhance your ability to automate NLB management in Windows Server 2012 and later clusters.

This module introduces you to NLB and shows you how to deploy this technology. This module also discusses the situations for which NLB is appropriate, how to configure and manage NLB clusters, and how to perform maintenance tasks on NLB clusters.

Objectives

After completing this module, you will be able to:

- Describe NLB.
- Configure an NLB cluster.
- Explain how to plan an NLB implementation.

Lesson 1
Overview of NLB

Before you deploy NLB, you need to have a good understanding of the types of server workloads for which this high availability technology is appropriate. If you do not understand the NLB functionality, you might deploy it in a manner that does not accomplish your overall objectives. For example, you need to understand why NLB is appropriate for web applications, but not for Microsoft SQL Server databases.

This lesson provides an overview of NLB, and its features in Windows Server 2016. It also describes how NLB works under normal circumstances, and how it works during server failure and server recovery.

Lesson Objectives

After completing this lesson, you will be able to:

- Describe the NLB technology.
- Describe how NLB works.
- Explain how NLB accommodates server failures and recovery.
- Describe the NLB features in Windows Server 2016.

What is NLB?

NLB is a scalable, high-availability feature that you can install on all editions of Windows Server 2016. NLB distributes network traffic across a set of servers, balancing the workload each server must handle. It is *scalable* because it enables you to add additional servers (also called *nodes* or *hosts*). A *node* (or *host*) in an NLB cluster in Windows Server 2016 is a computer, either physical or virtual, that is running the Windows Server 2016 operating system. Each node or host runs a copy of the server applications that are also running on the other hosts in the cluster.

- Scalable high-availability technology
- Balances traffic based on node utilization:
  - New traffic is directed to the node that is being utilized the least
  - You can configure NLB to preference some nodes over others
- Use with stateless applications such as:
  - Web tiers of multi-tier applications
- Is failure-aware
- Do not use with stateful applications such as:
  - Traditional file servers
  - Database servers

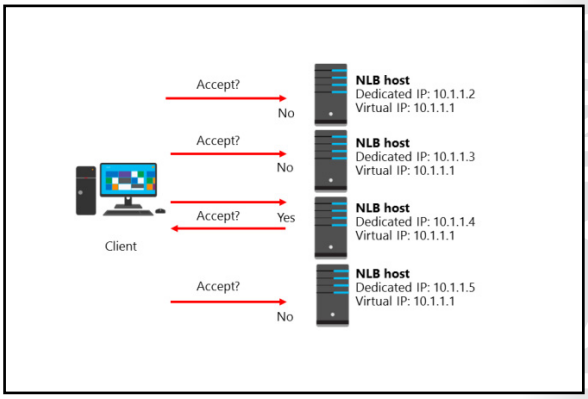
Windows Server 2016 NLB clusters can have between 2 and 32 nodes. When you create an NLB cluster, it creates a virtual network address and virtual network adapter. The virtual network adapter has an IP address and a media access control (MAC) address. Network traffic to this address is distributed evenly across the nodes in the cluster. In a basic NLB configuration, each node in an NLB cluster services requests at a rate that is approximately equal to that of all other nodes in the cluster. When an NLB cluster receives a request, it forwards that request to the node that currently is the least used. You also can configure NLB to direct traffic to a specific host, called a *default host*.

NLB is suitable for stateless applications such as the web tier of multi-tier applications, because it does not matter which web server a client connects to when connecting to a multi-tier application. NLB is not suitable for stateful applications such as traditional file servers and database servers. This is because these applications require a persistent connection to a particular server, rather than having any server handle the connection.

NLB is failure-aware. This means that if one of the nodes in the NLB cluster goes offline, requests will no longer be forwarded to that node, although other nodes in the cluster will continue to accept requests. When the failed node returns to service, incoming requests will be redirected until traffic is balanced across all nodes in the cluster.

How NLB works

When you configure an application to use NLB, clients address the application using the NLB cluster address rather than the address of nodes that participate in the NLB cluster. The *NLB cluster address* is a virtual address that is shared between the hosts in the NLB cluster.



NLB directs traffic in the following manner:

- All hosts in the NLB cluster receive the incoming traffic, but only one node in the cluster—which is determined through the NLB process—accepts that traffic. All other nodes in the NLB cluster drop the traffic.
- The node in the NLB cluster that accepts the traffic depends on the configuration of port rules and affinity settings. Through these settings, you can determine if traffic that uses a particular port and protocol will be accepted by a particular node, or whether any node in the cluster will accept and respond to that traffic.

NLB also sends traffic to nodes based on current node use. New traffic is directed to nodes that are the least used. For example, if you have a four-node cluster where three nodes respond to requests from 10 clients and one node responds to requests from five clients, the node that has fewer clients will receive more incoming traffic until use is more evenly balanced across the nodes.

How NLB works with server failures and recovery

NLB can detect the failure of cluster nodes. When a cluster node is in a failed state, it is removed from the cluster, and the hosts in the cluster do not direct new traffic to the node. Failure is detected by using heartbeats. NLB cluster heartbeats transmit every second between nodes in a cluster. A node is removed automatically from an NLB cluster if it misses five consecutive heartbeats. Heartbeats transmit over a network that is usually different from the network that the client uses to access the cluster.

- NLB cluster heartbeats transmit every second between nodes in a cluster
- Convergence occurs when:
  - A node misses five consecutive heartbeats, at which time it is automatically removed from an NLB cluster
  - A node that was member of a cluster returns to functionality
  - An administrator adds or removes a node manually

When you add or remove a node from a cluster, a process known as *convergence* occurs. Convergence is the process where a new list of cluster members is created and the cluster members record the current configuration of the cluster. Convergence can only occur if you configure each node with the same port rules.

You can configure nodes to rejoin a cluster automatically, by configuring the **Initial host state** setting on the node's properties by using the Network Load Balancing Manager. By default, a host that is a member of a cluster will attempt to rejoin that cluster automatically. For example, after you apply a software update, if you restart a server that is a member of an NLB cluster, the server will rejoin the cluster automatically after the restart process completes.

You can add or remove nodes manually from NLB clusters. When you remove a node, you can choose to perform a Stop or a Drainstop action. The Stop action terminates all existing connections to the cluster node and stops the NLB service. The Drainstop action blocks all new connections without terminating existing sessions. After all current sessions end, the NLB service stops.

NLB can only detect server failure; it cannot detect application failure. This means that if a web application fails but the server remains operational, the NLB cluster will continue to forward traffic to the cluster node that hosts the failed application. One way to manage this problem is to implement a monitoring solution such as Microsoft System Center Operations Manager. With System Center Operations Manager (Operations Manager), you can monitor the functionality of applications. You also can configure Operations Manager to generate an alert in the event that an application on a cluster node fails. An alert, in turn, can configure a remediation action, such as restarting services, restarting the server, or withdrawing the node from the NLB cluster so that the node does not receive further incoming traffic.

NLB features in Windows Server 2016

The most substantial change to NLB features after Windows Server 2008 is the inclusion of Windows PowerShell support. The **NetworkLoadBalancingClusters** module contains 35 NLB–related cmdlets. This module becomes available on a server or workstation once you install the NLB Remote Server Administration Tools (RSATs).

- Use 35 NLB Windows PowerShell cmdlets to manage all aspects of NLB configuration:
  - Use **NlbCluster** noun to manage the cluster
  - Use **NlbClusterNode** noun to manage individual nodes
- Other NLB features:
  - Does not require any hardware changes
  - Does not require any application software changes
  - Hosts can be part of multiple clusters
  - Can add/remove hosts without affecting the rest of the cluster

The Windows PowerShell NLB-related cmdlets have the nouns and verbs listed in the following table.

Windows PowerShell NLB nuns	Description	Windows PowerShell verbs
NlbClusterNode	Use to manage a cluster node	**Add**, **Get**, **Remove**, **Resume**, **Set**, **Start**, **Stop**, and **Suspend**
NlbClusterNodeDip	Use to configure the cluster node's dedicated management IP	**Add**, **Get**, **Remove**, and **Set**
NlbClusterPortRule	Use to manage port rules	**Add**, **Disable**, **Enable**, **Get**, **Remove**, and **Set**
NlbClusterVip	Use to manage the NLB cluster's virtual IP	**Add**, **Get**, **Remove**, and **Set**
NlbCluster	Use to manage the NLB cluster	**Get**, **New**, **Remove**, **Resume**, **Set**, **Start**, **Stop**, and **Suspend**

Windows PowerShell NLB nuns	Description	Windows PowerShell verbs
NlbClusterDriverInfo	Provides information about the NLB cluster driver	**Get**
NlbClusterNodeNetworkInterface	Use to retrieve information about a cluster node's network interface driver	**Get**
NlbClusterIpv6Address	Use to configure the cluster's IPv6 address	**New**
NlbClusterPortRuleNodeHandlingPriority	Use to set priority on a per-port rule basis	**Set**
NlbClusterPortRuleNodeWeight	Use to set node weight on a per-port rule basis	**Set**

Note: To see the list of Windows PowerShell cmdlets for NLB, use the following command:

```
get-command –module NetworkLoadBalancingClusters
```

Other NLB features

NLB on Windows Server 2016 includes other features as well:

- NLB does not require any hardware changes.
- You can manage multiple clusters and hosts from a remote or local computer.
- You can configure each host as part of multiple clusters when using multiple network adapters.
- You do not need to modify server applications for them to work with NLB.
- NLB can automatically re-add hosts to the cluster that have failed and later come online.
- You can take hosts offline without affecting other cluster nodes.

Question: What is the difference between server failure and application failure, and how does that difference affect your high availability solution?

Check Your Knowledge

Question	
How many nodes does NLB support in Windows Server 2016?	
Select the correct answer.	
	2
	8
	16
	32
	64

Lesson 2
Configuring an NLB cluster

To deploy NLB successfully, you must first have a good understanding of its deployment requirements. You must also plan how you are going to use port rules and affinity settings to ensure that traffic to the application that is being hosted on the NLB cluster is managed appropriately.

This lesson provides information about the infrastructure requirements that you must consider before you deploy NLB. It also provides important information on how to configure NLB clusters and nodes to best meet your objectives.

Lesson Objectives

After completing this lesson, you will be able to:

- Describe NLB deployment requirements.
- Describe how to deploy NLB.
- Explain configuration options for NLB.
- Describe how to configure NLB affinity and port rules.
- Describe network considerations for NLB.

Deployment requirements for NLB

There are several requirements that you must meet while designing and deploying an NLB cluster:

- Ensure that all hosts are on the same subnet
- Configure all adapters as either unicast or multicast
- Use only the TCP/IP protocol on adapters
- Configure all adapters that you use in NLB with static IP address

- Ensure that all hosts in the NLB cluster reside on the same TCP/IP subnet. Although you can configure TCP/IP subnets to span multiple geographic locations, NLB clusters are unlikely to achieve convergence successfully if the latency between nodes exceeds 250 milliseconds (ms). When you are designing geographically-dispersed NLB clusters, you should instead choose to deploy an NLB cluster at each site, and then use Domain Name System (DNS) round robin to distribute traffic between sites.

Note: DNS round robin is described in more detail later in this module.

- Configure all network adapters within an NLB cluster as either unicast or multicast. You cannot configure an NLB cluster where there is a mixture of unicast and multicast adapters. When using the unicast mode, the network adapter must support changing its MAC address.
- Use only the TCP/IP protocol with network adapters that participate in NLB clusters. NLB supports IPv4 and IPv6. Do not add any other protocols to the adapter that is part of the NLB cluster.

- Ensure that IP addresses of servers that participate in an NLB cluster are static. When you install NLB, Dynamic Host Configuration Protocol (DHCP) is disabled on each interface that you configure to participate in the cluster.

All editions of Windows Server 2016 support NLB. Microsoft supports NLB clusters with nodes that are running a mixture of Standard edition and Datacenter edition servers. However, as a best practice, ensure that NLB cluster nodes are computers with similar hardware specifications, and are running the same edition of the Windows Server 2016.

Demonstration: Deploying NLB

In this demonstration, you will learn how to create an NLB cluster in Windows Server 2016.

Demonstration Steps

Create an NLB cluster in Windows Server 2016

1. On **LON-SVR1**, open the **Windows PowerShell Integrated Scripting Environment (ISE)**.
2. At the Windows PowerShell command prompt, type the following commands, pressing Enter after each command:

```
Invoke-Command -Computername LON-SVR1,LON-SVR2 -command {Install-WindowsFeature
NLB,RSAT-NLB}
New-NlbCluster -InterfaceName "Ethernet" -OperationMode Multicast -ClusterPrimaryIP
172.16.0.42 -ClusterName LON-NLB
Add-NlbClusterNode -InterfaceName "Ethernet" -NewNodeName "LON-SVR2" -
NewNodeInterface "Ethernet"
```

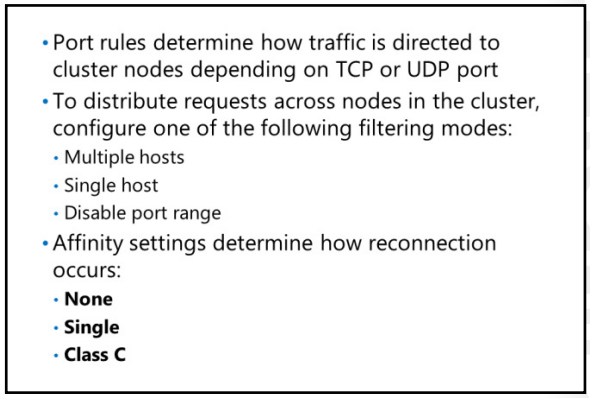
3. From the **Tools** menu, open **Network Load Balancing Manager**, and then view the cluster.

Leave the virtual machines running

- When you finish the demonstration, leave the virtual machines running for the next demonstration.

Configuration options for NLB

Configuring NLB clusters involves specifying how hosts in the cluster will respond to incoming network traffic. How NLB directs traffic depends on the port and protocol that it uses, and whether the client has an existing network session with a host in the cluster. You can configure these settings by using port rules and affinity settings.



Port rules

With port rules, you can configure how the NLB cluster directs requests to specific IP addresses, ports, and protocols. For example, you can load balance traffic on Transmission Control Protocol (TCP) port 80 across all nodes in an NLB cluster, while directing all requests to TCP port 25 to a specific host. Which ports you choose to load balance will depend on the specific server application.

To specify how you want to distribute requests across nodes in the cluster, you configure a filtering mode when creating a port rule. You can do this in the **Add/Edit Port Rule** dialog box, which you use to configure one of the following filtering modes:

- Multiple hosts. When you configure this mode, all NLB nodes respond according to the weight assigned to each node. Node weight is calculated automatically, based on the performance characteristics of the host. If a node fails, other nodes in the cluster continue to respond to incoming requests. Multiple host filtering increases availability and scalability, because you can increase capacity by adding nodes, and the cluster continues to function in the event of node failure.
- Single host. When you configure this mode, the NLB cluster directs traffic to the node that is assigned the highest priority. If the node that is assigned the highest priority is unavailable, the host assigned the next highest priority manages the incoming traffic. Single host rules increase availability but do not increase scalability.

  Note: The highest priority is the lowest number, with a priority of one being a higher priority than a priority of 10.

- Disable this port range. When you configure this mode, all packets for this port range are dropped, automatically without being forwarded to any cluster nodes. If you do not disable a port range, and there is no existing port rule, the traffic is forwarded to the host with the lowest priority number.

You can use the following Windows PowerShell cmdlets to manage port rules:

- **Add-NlbClusterPortRule**. Use this cmdlet to add a new port rule.
- **Disable-NlbClusterPortRule**. Use this cmdlet to disable an existing port rule.
- **Enable-NlbClusterPortRule**. Use this cmdlet to enable a disabled port rule.
- **Set-NlbClusterPortRule**. Use this cmdlet to modify the properties of an existing port rule.
- **Remove-NlbClusterPortRule**. Use this cmdlet to remove an existing port rule.

Note: Each node in a cluster must have identical port rules. The exception to this is the load weight (in multiple-hosts filter mode) and handling priority (in single-host filter mode). Otherwise, if the port rules are not identical, the cluster will not converge.

Affinity

Affinity determines how the NLB cluster distributes requests from a specific client. Affinity settings only apply when you use the multiple hosts filtering mode. You can select from the following affinity modes in the **Add/Edit Port Rule** dialog box:

- **None**. In this mode, any cluster node responds to any client request, even if the client is reconnecting after an interruption. For example, the first webpage on a web application might be retrieved from the third node, the second webpage from the first node, and the third webpage from the second node. This affinity mode is suitable for stateless applications.
- **Single**. When you use this affinity mode, a single cluster node manages all requests from a single client. For example, if the third node in a cluster manages a client's first request, then all subsequent requests are also managed by that node. This affinity mode is useful for stateful applications.

- **Network**. When you set this mode, a single node will respond to all requests from a class C network (one that uses the 255.255.255.0 subnet mask). This mode is useful for stateful applications where the client is accessing the NLB cluster through load-balanced proxy servers. These proxy servers will have different IP addresses, but they will be within the same class C (24-bit) subnet block.

Host parameters

You configure the host parameters for a host by clicking the host in the **Network Load Balancing Manager** console, and then from the **Host** menu, clicking **Properties**. You can configure the following host settings for each NLB node:

- **Priority**. Each NLB node is assigned a unique priority value. If no existing port rule matches the traffic that is addressed to the cluster, traffic is assigned to the NLB node that is assigned the lowest priority value.
- **Dedicated IP address**. You can use this parameter to specify the address that the host uses for remote management tasks. When you configure a dedicated IP address, NLB configures port rules so that they do not affect traffic to that address.
- **Subnet mask**. When you select a subnet mask, ensure that there are enough host bits to support the number of servers in the NLB cluster, and any routers that connect the NLB cluster to the rest of the organizational network. For example, if you plan to have a cluster that has 32 nodes and supports two routes to the NLB cluster, you will need to set a subnet mask that supports 34 host bits or more—such as 255.255.255.192.
- **Initial host state**. You can use this parameter to specify the actions the host will take after a reboot. There are three possible values:
  - **Started**. This value makes the host rejoin the NLB cluster automatically.
  - **Suspended**. This value pauses the host, and allows you to perform operations that require multiple reboots without triggering cluster convergence.
  - **Stopped**. This value stops the node.

Demonstration: Configuring NLB affinity and port rules

In this demonstration, you will learn how to:

- Configure affinity for NLB cluster nodes.
- Configure NLB port rules.

Demonstration Steps

Configure affinity for NLB cluster nodes

1. On **LON-SVR2**, click **Start**, and then click the **Windows PowerShell** tile.
2. In Windows PowerShell, type the following commands, pressing Enter after each command:

```
Mkdir c:\porttest
Xcopy /s c:\inetpub\wwwroot c:\porttest
New-Website –Name PortTest –PhysicalPath “C:\porttest” –Port 5678
New-NetFirewallRule –DisplayName PortTest –Protocol TCP –LocalPort 5678
```

Configure NLB port rules

1. On **LON-SVR1**, open the **Network Load Balancing Manager** console.
2. Remove the **All port** rule.
3. In the **Network Load Balancing Manager** console, edit the properties of the **LON-NLB** cluster.
4. Add a port rule with the following properties:
   - Port range: **80** to **80**
   - Protocols: **Both**
   - Filtering mode: **Multiple Host**
   - Affinity: **None**
5. Create a port rule with the following properties:
   - Port range: **5678** to **5678**
   - Protocols: **Both**
   - Filtering mode: **Single Host**
6. Edit the host properties of **LON-SVR1** (Ethernet).
7. Configure the port rule for port **5678**, and then set handling priority to **10**.

Revert the virtual machines

When you finish the demonstration, revert the virtual machine to its initial state. To do this, complete the following steps:

1. On the host computer, open **Hyper-V Manager**.
2. In **Hyper-V Manager**, in the **Virtual Machines** list, right-click **20740A-LON-DC1**, and then click **Revert**.
3. In the **Revert Virtual Machine** dialog box, click **Revert**.
4. Repeat steps 2 and 3 for **20740A-LON-SVR1** and **20740A-LON-SVR2**.

Network considerations for NLB

When you design a network to support an NLB cluster, you must consider several factors. The primary decision is whether you want to configure the NLB cluster to use the unicast or the multicast cluster operation mode.

- Unicast:
  - Suitable for clusters that have multiple network adapters
- Multicast:
  - Suitable for NLB clusters that have single network adapters
  - Network devices must support multicast MAC addresses
- IGMP multicast:
  - Improves switch performance
  - Requires a network switch that supports this functionality

Unicast

When you configure an NLB cluster to use the unicast mode, all cluster hosts use the same unicast MAC address. Outgoing traffic uses a modified MAC address that is determined by the cluster host's priority setting. This prevents the switch that handles outbound traffic from having problems with all cluster hosts using the same MAC address.

When you use the unicast mode with a single network adapter on each node, only computers that use the same subnet can communicate with the node by using the node's assigned IP address. If you have to perform any node management tasks, (such as connecting with the Remote Desktop feature in the Windows operating system to apply software updates), you will need to perform these tasks from a computer that is on the same TCP/IP subnet as the node.

When you use the unicast mode with two or more network adapters, one adapter is used for dedicated cluster communications, and the other adapter or adapters can be used for management tasks. When you use the unicast mode with multiple network adapters, you can perform cluster management tasks such as connecting to the server by using Windows PowerShell remoting to add or remove roles and features.

The unicast mode also can minimize problems that occur when cluster nodes also host other non-NLB related roles or services. For example, using unicast mode means that a server that participates in a web server cluster on port 80 might also host another service such as DNS or DHCP. Although this is possible, we recommend that all cluster nodes have the same configuration.

Multicast

When you configure an NLB cluster to use the multicast mode, each cluster host keeps its original MAC address, but also is assigned an additional multicast MAC address. Each node in the cluster is assigned the same additional MAC multicast address. You must use multicast mode when each host has only one network adapter installed and the hosts need to communicate directly with each other. The multicast mode requires network switches and routers that support multicast MAC addresses.

If you experience issues in a unicast mode deployment of NLB, such as switch flooding, where NLB traffic routes to all the ports on a switch, then switching to multicast might address the problem. However, depending on your hardware, you might need to add static Address Resolution Protocol (ARP) to your router or switch in order to map the cluster IP address to the MAC address of the NLB cluster. Otherwise, it is possible for multicast mode to result in switch flooding, also.

IGMP multicast

The Internet Group Management Protocol (IGMP) multicast mode is a special form of multicast mode that prevents the network switch from being flooded with traffic. When you deploy the IGMP multicast mode, traffic is forwarded only through switch ports that participate in the NLB cluster. IGMP multicast mode requires switch hardware that supports this functionality.

Network considerations

You can improve NLB cluster performance when you use unicast mode by using separate virtual local area networks (VLANs) for cluster traffic and management traffic. Using VLANs segment traffic, you can prevent management traffic from affecting cluster traffic. When you host NLB nodes on virtual machines using Windows Server 2016, you also can use network virtualization to segment management traffic from cluster traffic.

Question: Describe a situation where the single affinity setting would be appropriate.

Question: When would you want to use port rules other than the default port rule?

Lesson 3
Planning an NLB implementation

When you plan an NLB implementation, you must ensure that the applications that you deploy are appropriate for NLB. Not all applications are suitable for deployment on NLB clusters, and it is important for you identify which applications can benefit from this technology. You also need to know what steps you can take to secure NLB. Additionally, you should be familiar with the options that you have for scaling NLB, in case the application that is hosted on the NLB cluster requires greater capacity.

Lesson Objectives

After completing this lesson, you will be able to:

- Explain how to design application and storage support for NLB.
- Describe the special considerations for deploying NLB clusters on virtual machines.
- Describe the considerations for securing NLB.
- Describe the considerations for scaling NLB.
- Describe the considerations for upgrading an NLB cluster to Windows Server 2016.

Designing applications and storage support for NLB

Because client traffic can be directed to any node in an NLB cluster, each node in the cluster must be able to provide a consistent experience. Therefore, when you are designing applications and storage support for NLB applications, you must ensure that you configure each node in the same way, and that each node has access to the same data.

- Each node in an NLB cluster should have the same configuration
- Each node needs access to the same consistent application data
- Use IIS shared configuration to ensure that web application configuration is consistent across NLB nodes
- Use CSVs to host shared application and configuration data for NLB applications
- NLB hosts do not typically need local storage redundancy

When a highly available application has multiple tiers—such as a web application that includes a SQL Server database tier—the web application tier is hosted on an NLB cluster. SQL Server, as a stateful application, is not made highly available by using NLB. Instead, you use technologies such as failover clustering, mirroring, or AlwaysOn Availability Groups, to make the SQL Server database tier highly available.

You should configure all hosts in an NLB cluster in the same way and they should run the same applications. When you are using web applications, you can use the Internet Information Services (IIS) 8.0 shared configuration functionality to ensure that all nodes in the NLB cluster are configured in the same manner.

You also can use technologies such as file shares that are hosted on Cluster Shared Volumes (CSVs) to host application configuration information. File shares that are hosted on CSVs allow multiple hosts to have access to application data and configuration information. File shares that are hosted on CSVs are a feature of Windows Server 2012 and later.

When configuring NLB hosts, you can avoid the extra expense of configuring redundancy into local storage. If a drive fails and the server fails as a result, other servers in the NLB cluster take on the extra workload. This means there is little advantage in configuring the local drivers to use Redundant Array of Independent Disks (RAID) or provide fault tolerance.

Considerations for deploying an NLB cluster on virtual machines

As organizations transition from physical to virtual deployments, administrators must consider several factors when determining the placement of NLB cluster nodes on Hyper-V hosts. This includes the network configuration of virtual machines, the configuration of the Hyper-V hosts, and the benefits of using the Hyper-V high availability features in conjunction with NLB.

- Configure virtual machines with multiple network adapters
- Configure one network adapter on each node member to use a shared private network switch
- Configure the NLB cluster to use unicast mode and enable MAC address spoofing on the Hyper-V host
- Use the shared private network switch for cluster communication
- Use network virtualization to separate the cluster network when NLB nodes span multiple sites

Virtual machine placement

You should place NLB cluster nodes on separate hard disks on the Hyper-V host. That way, if a disk or disk array fails, and if one node becomes unavailable, other NLB cluster nodes that are hosted on the same Hyper-V host will remain online. We recommend that you configure the Hyper-V host with redundant hardware, including redundant disks, network adapters, and power supplies. This will minimize the chance that hardware failure on the Hyper-V host will lead to all nodes in an NLB cluster becoming unavailable. When you use multiple network adapters, configure network teaming to ensure that virtual machines are able to maintain access to the network even in the event that individual network adapter hardware suffers a failure.

Where possible, deploy NLB cluster nodes running as virtual machines on separate Hyper-V hosts. This protects the NLB cluster from other types of server failure, such as the failure of a motherboard, or any other single point of failure. When you plan this type of configuration, ensure that the virtual machines that participate in the NLB cluster are located on the same TCP/IP subnet.

Virtual machine network configuration

Because adding additional virtual network adapters is a straightforward process, you can configure the NLB cluster to use the unicast mode, and then deploy each virtual machine with multiple network adapters. You should create separate virtual switches for cluster traffic and node management traffic, because segmenting traffic can improve performance. You also can use network virtualization to partition cluster traffic from node management traffic. You can use VLAN tags as a method of partitioning cluster traffic from node management traffic.

When you use the unicast mode, ensure that you enable MAC address spoofing for the virtual network adapter on the Hyper-V host. You can do this by editing the virtual network adapter's settings in the **Virtual Machine Settings** dialog box, which is available through Hyper-V Manager. Enabling MAC address spoofing allows the NLB cluster running in unicast mode to configure MAC address assignment on the virtual network adapter.

NLB cluster vs. virtual machine high availability

Virtual machine high availability is the process of placing virtual machines on failover clusters. When a failover cluster node fails, the virtual machine fails over so that it is hosted on another node. Although failover clustering and NLB are both high availability technologies, they serve different purposes. Failover clustering supports stateful applications such as SQL Server, whereas NLB is suited to stateless applications such as websites.

Highly available virtual machines do not allow an application to scale, because you cannot add nodes to increase capacity. However, it is possible to deploy NLB cluster nodes as highly available virtual machines. In this scenario, the NLB cluster nodes fail over to a new Hyper-V host in the event that the original Hyper-V host fails.

The degree of availability and redundancy required for an application fluctuates, depending on the business requirements of that application. A business-critical application that results in millions of lost dollars in lost revenue when it is down requires an availability that differs from that of an application that causes minimal inconvenience if it is offline.

Considerations for securing NLB

You almost always use NLB clusters to host web applications that are important to the organization. Because of this importance, you should take steps to secure NLB, both by restricting the traffic that can address the cluster, and by ensuring that appropriate permissions apply.

- Use NLB cluster port rules to discard traffic not related to cluster applications
- Use firewall rules to drop traffic not related to cluster applications or node management
- Configure applications to respond only to traffic that is addressed to the cluster
- Use SANs to create certificates that support the application name and node names
- Implement principle of least privilege so only authorized users have permissions on nodes
- Use Privileged Access Management to implement JIT administration

Configure port rules

When you secure NLB clusters, you must first ensure that you create port rules to block traffic to all ports other than those that applications hosted on the NLB cluster use. When you do this, all incoming traffic that is not addressed specifically to applications that are running on the NLB cluster is dropped. If you do not perform this first step, all incoming traffic that is not managed by a port rule is forwarded to the cluster node with the lowest cluster priority value.

Configure firewall rules

You also should ensure that Windows Firewall with Advanced Security is configured on each NLB cluster node. When you enable NLB on a cluster node, the following firewall rules that allow NLB to function and communicate with other nodes in the cluster are created and enabled automatically:

- Network Load Balancing (DCOM-In)
- Network Load Balancing (ICMP4-ERQ-In)
- Network Load Balancing (ICMP6-ERQ-In)
- Network Load Balancing (RPCSS)
- Network Load Balancing (WinMgmt-In)
- Network Load Balancing (ICMP4-DU-In)

- Network Load Balancing (ICMP4-ER-In)
- Network Load Balancing (ICMP6-DU-In)
- Network Load Balancing (ICMP6-EU-In)

When created, these firewall rules do not include scope settings. In high-security environments, you would configure an appropriate local IP address or IP address range, and a remote IP address for each rule. The remote IP address or address range should include the addresses that other hosts in the cluster use.

When you configure additional firewall rules, remember the following guidelines:

- When you use multiple network adapters in the unicast mode, configure different firewall rules for each network interface. For the interface that is used for management tasks, you should configure the firewall rules to allow inbound management traffic only—for example, you would enable the use of remote Windows PowerShell, Windows Remote Management, and Remote Desktop for management tasks. You should configure the firewall rules on the network interface that the cluster node uses, to provide an application to the cluster and to allow access to that application. For example, you should allow incoming traffic on TCP ports 80 and 443 on an application that uses the HTTP and HTTPS protocols.
- When you use multiple network adapters in multicast mode, configure firewall rules that allow access to applications that are hosted on the cluster, but block access to other ports.

 **Note:** Whenever possible, use two or more network adapters in each cluster host. This will allow you to customize firewall and port rules to limit remote access so that it is not possible to connect remotely through the adapter used for NLB traffic, known as the *cluster adapter*.

Configure applications to respond only to traffic that is addressed to the cluster

You should configure applications on each node to respond only to traffic that is addressed to the cluster, and to ignore application traffic that is addressed to the individual node. For example, if you deploy a web application that is designed to respond to traffic addressed to www.adatum.com, there will be a website on each node that will accept traffic on port 80.

Depending on the NLB cluster configuration, it is possible that traffic that is addressed to the node on port 80 will generate a direct response. For example, users might be able to access the A. Datum web application by typing the address **http://nlb-node-3.adatum.com** in a web browser, instead of typing the address **http://www.adatum.com**. You can secure applications from this type of direct traffic by configuring them to respond only to traffic that uses the NLB cluster address. For web applications, you can do this by configuring the website to use a host header. Each application that runs on an NLB cluster will have its own unique method of allowing you to configure the application to respond only to traffic that is directed at the cluster, rather than at the individual cluster node.

Securing traffic with an SSL certificate

All NLB websites must use the same website name. When you secure websites that you make highly available by using NLB, you must ensure that each website has an SSL certificate that matches the website name. You set the host header of each node to point to the IP address of the NLB cluster. In most cases, you will install the same website certificate on each node in the NLB cluster, because this is simpler than procuring separate certificates for each cluster node. In some cases, you will need to procure certificates that support subject alternative names (SANs). Certificates that support SANs allow a server to be identified by multiple names, such as the name that the clustered application uses and the name of the cluster node. For example, a certificate with a SAN might support the names www.adatum.com, node1.adatum.internal, node2.adatum.internal, node3.adatum.internal, and node4.adatum.internal.

Principle of least privilege

Ensure that you delegate permissions to users, only for tasks that they need to perform on the NLB node. Members of the local Administrators group on any single node can add and remove cluster nodes, even if they are not members of the local Administrators group on those nodes. You should configure applications that run on NLB clusters so that they do not require application administrators to have local Administrator privileges on the servers that host the application. Only users whose job role requires them to make remote management connections to NLB cluster nodes should be able to make those connections.

Privileged Access Management

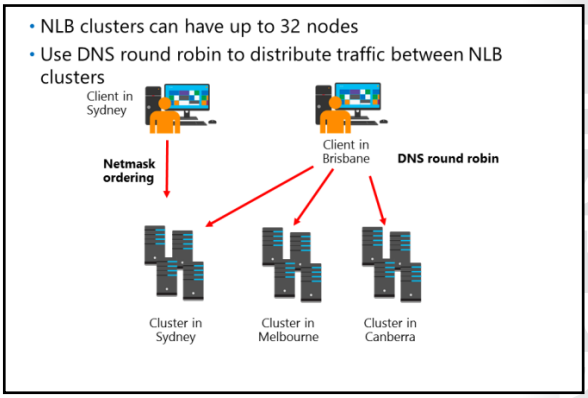
Windows Server 2016 includes the new Privileged Access Management (PAM) feature. PAM is based on the concepts of just-in-time (JIT) administration and just enough administration (JEA). When you implement PAM, users request permissions to perform administrative tasks on a server, and are automatically granted the appropriate privileges for a temporary period, based on rules that might include additional authentication steps. PAM also allows you to require additional authentication steps, such as multi-factor authentication.

Additional Reading: For more information on PAM, refer to: "Privileged Access Management for Active Directory Domain Services (AD DS)" at: http://aka.ms/Rs9mxp

Additional Reading: For more information on JEA, refer to: "Just Enough Administration" at: http://aka.ms/JEA

Considerations for scaling NLB

Scaling is the process of increasing the capacity of an NLB cluster. For example, if you have a four-node NLB cluster, and each cluster node is used to the point where the cluster cannot manage more traffic, you can add additional nodes. Adding nodes will spread the same load across more computers, reducing the load on each current cluster node. As a result, capacity increases because a larger number of similarly configured computers can manage a higher workload than a smaller number of similarly configured computers.



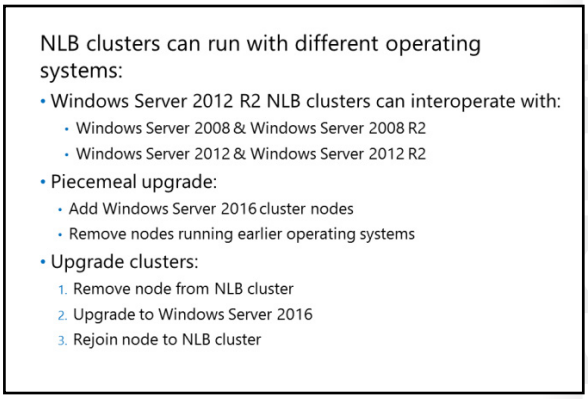
An NLB cluster supports up to 32 nodes. This means that you can scale out a single NLB cluster so that 32 separate nodes participate in that cluster. When you consider scaling an application so that it is hosted on a 32-node NLB cluster, remember that each node in the cluster must be on the same TCP/IP subnet.

An alternative to building single NLB clusters is to build multiple NLB clusters, and use DNS round robin to share traffic between them. DNS *round robin* is a technology that allows a DNS server to provide requesting clients with different IP addresses to the same hostname, in sequential order. For example, if three addresses are associated with a hostname, the first requesting host receives the first address, the second receives the second address, the third receives the third address, and so forth. When you use DNS round robin with NLB, you associate the IP addresses of each cluster with the hostname that the application uses.

Distributing traffic between NLB clusters by using DNS round robin also allows you to deploy NLB clusters across multiple sites. You can use DNS round robin in conjunction with netmask ordering. Using DNS round robin ensures that clients on a subnet are provided with an IP address of a host on the same network, if one is available. For example, you might deploy three four-node NLB clusters in the cities of Sydney, Melbourne, and Canberra, and use DNS round robin to distribute traffic between them. With netmask ordering, a client in Sydney that is accessing the application in Sydney will be directed by DNS to the NLB cluster hosted in Sydney. A client that is not on the same subnet as the NLB cluster nodes, such as a client in the city of Brisbane, would be directed by DNS round robin to either the Sydney, Melbourne, or Canberra NLB cluster.

Considerations for upgrading NLB clusters

Upgrading NLB clusters involves moving cluster nodes from one host operating system—for example, Windows Server 2008 or Windows Server 2012—to Windows Server 2016. Upgrading the cluster might not require you to perform an operating system upgrade on each node, because in some cases the original host operating system might not support a direct upgrade to Windows Server 2016. In cases where the original host operating system does not support a direct upgrade to Windows Server 2016, you can perform a migration.



When you upgrade NLB clusters, remember that NLB supports clusters that run a mixture of operating systems. This means that you can have a cluster that runs a mixture of Windows Server 2008, Windows Server 2012, and Windows Server 2016. Even though NLB supports mixed operating system clusters, we do not recommend them. If you do run NLB clusters with a mixture of operating systems, we recommend that you move all nodes to a single operating system as quickly as possible.

Note: In some situations, it will not be possible to upgrade the operating system of a cluster node. For example, if the server has an x86 version of Windows Server 2008 installed, it will not be possible to upgrade it. In this situation, you should remove the node from the cluster manually, migrate the server to Windows Server 2016, migrate the applications, and then join the migrated server to the NLB cluster.

When you perform an NLB cluster upgrade, you can use one of the following strategies:

- Piecemeal upgrade. During this type of upgrade, you add new Windows Server 2016 nodes to an existing cluster, and then remove the nodes that are running older versions of the Windows Server operating system. This type of upgrade is appropriate when the original hardware and operating system does not support a direct upgrade to Windows Server 2016.
- Rolling upgrade. During this type of upgrade, you upgrade one node in the cluster at a time. You do this by taking the node offline, performing the upgrade, and then rejoining the node back to the cluster.

 **Additional Reading:** For more information, refer to: "Upgrading an Existing Network Load Balancing Cluster" at: http://aka.ms/U4sqyq

Question: Why do you use both port rules and firewall rules when securing NLB?

Question: Why should you use the principle of least privilege when assigning permission to NLB servers?

Lab: Implementing NLB

Scenario

A. Datum Corporation is an engineering and manufacturing company. The organization is based in London, England, and is quickly expanding into Australia. As the company expands, the need for scalable web applications has increased. To address this need, you need to develop a pilot program to test the deployment of NLB on hosts that are running the Windows Server 2016 operating system.

Because you intend to automate the process of deploying Windows NLB clusters, you will use Windows PowerShell to perform many of the cluster setup and configuration tasks. You also will configure port rules and affinity, which will allow you to deploy multiple load-balanced web applications on the same NLB clusters.

Objectives

After completing this lab, you will be able to:

- Implement an NLB cluster.
- Configure and manage an NLB cluster.
- Validate high availability for the NLB cluster.

Lab Setup

Estimated Time: **45 minutes**

Virtual machines: **20740A-LON-DC1**, **20740A-LON-SVR1**, **20740A-LON-SVR2**

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, click start **Hyper-V Manager**.
2. In **Hyper-V Manager**, click **20740A-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: **Administrator**
    - Password: **Pa$$w0rd**
    - Domain: **Adatum**
5. Repeat steps two through four for **20740A-LON-SVR1** and **20740A-LON-SVR2**.

Exercise 1: Implementing a Network Load Balancing (NLB) cluster

Scenario

You want to automate the process of deploying Windows Server 2016 NLB clusters. To accomplish this, you will use Windows PowerShell to perform the majority of the NLB cluster deployment tasks.

The main tasks for this exercise are as follows:

1. Verify website functionality for standalone servers.
2. Install NLB.
3. Create a new Windows Server 2016 NLB cluster.
4. Add a second host to the cluster.
5. Validate the NLB cluster.

▶ Task 1: Verify website functionality for standalone servers

1. On **LON-SVR1**, browse to the **c:\inetpub\wwwroot** folder.
2. Open **iisstart.png** in **Microsoft Paint**, and then use the Paintbrush tool and circle the **IIS** logo.
3. Close **File Explorer**.
4. Switch to **LON-DC1**, and then open **Microsoft Internet Explorer**.
5. Go to **http://LON-SVR1**, and then verify that the web page with the circled IIS logo that you created in the previous step displays.
6. Go to **http://LON-SVR2**, and verify that the IIS logo on the website does not have the circle that you created in step 2.

▶ Task 2: Install NLB

1. On **LON-SVR1**, open **Windows PowerShell ISE**.
2. In the **Windows PowerShell ISE** window, type the following command to install NLB on **LON-SRV1** and **LON-SVR2**, and then press Enter:

```
Invoke-Command -Computername LON-SVR1,LON-SVR2 -command {Install-WindowsFeature
NLB,RSAT-NLB}
```

Note: If you receive warnings about the network connection to each server, ignore these.

▶ Task 3: Create a new Windows Server 2016 NLB cluster

1. On **LON-SVR1**, in the **Windows PowerShell ISE** window, type the following command to create the new NLB cluster, and then press Enter:

```
New-NlbCluster -InterfaceName "Ethernet" -OperationMode Multicast -ClusterPrimaryIP
172.16.0.42 -ClusterName LON-NLB
```

2. In the **Windows PowerShell ISE** window, type the following command to add the NLB cluster to DNS, and then press Enter:

```
Invoke-Command -Computername LON-DC1 -command {Add-DNSServerResourceRecordA      –
zonename adatum.com –name LON-NLB –Ipv4Address 172.16.0.42}
```

▶ Task 4: Add a second host to the cluster

- On **LON-SVR1**, in the **Windows PowerShell ISE** window, type the following command to add a second host to the cluster, and then press Enter:

```
Add-NlbClusterNode -InterfaceName "Ethernet" -NewNodeName "LON-SVR2" -NewNodeInterface
"Ethernet"
```

▶ Task 5: Validate the NLB cluster

1. On **LON-SVR1**, open the **Network Load Balancing Manager** console, and then verify that the nodes **LON-SVR1** and **LON-SVR2** display with the status **Converged**.
2. View the properties of the **LON-NLB** cluster, and then verify the following:
   - The cluster is set to use the **Multicast** operations mode.
   - There is a single port rule with a Cluster IP address of **All** that starts at port **0** and ends at port **65535** for both **TCP** and **UDP** protocols, and that it uses **Single** affinity.

Results: After completing this exercise, you should have successfully implemented an NLB cluster.

Exercise 2: Configuring and managing the NLB cluster

Scenario

As part of the pilot, you want to deploy multiple separate websites to the NLB cluster, and then differentiate these websites based on port address. To do this, you want to ensure that you can configure and validate port rules. You also want to experiment with affinity settings to ensure that requests are distributed evenly across the hosts.

The main tasks for this exercise are as follows:

1. Configure port rules and affinity.
2. Validate port rules.
3. Manage host availability in the NLB cluster.

▶ Task 1: Configure port rules and affinity

Configure affinity for NLB cluster nodes

1. On **LON-SVR2**, open **Windows PowerShell**.
2. In the **Windows PowerShell** window, type the following commands, and then press Enter after each command:

```
Mkdir c:\porttest
Xcopy /s c:\inetpub\wwwroot c:\porttest
New-Website -Name PortTest -PhysicalPath "C:\porttest" -Port 5678
New-NetFirewallRule -DisplayName PortTest -Protocol TCP -LocalPort 5678
```

Configure NLB port rules

1. Open **File Explorer**, browse to **c:\porttest**, and then open **iisstart.png** in **Microsoft Paint**.
2. Use paintbrush to place a line across the IIS logo.
3. Switch to **LON-DC1**.
4. Open **Internet Explorer**, and browse to **http://LON-SVR2:5678**.
5. Verify that the **IIS Start** page displays the IIS logo with a line across it.
6. Switch to **LON-SVR1**.
7. On **LON-SVR1**, open **Network Load Balancing Manager**, and view the cluster properties of **LON-NLB (172.16.0.42)**.
8. Remove the **All port** rule.
9. Add a port rule with the following properties:
   - Port range: **80** to **80**
   - Protocols: **Both**
   - Filtering mode: **Multiple host**
   - Affinity: **None**
10. Create a new port rule with the following properties:
    - Port range: **5678** to **5678**
    - Protocols: **Both**
    - Filtering mode: **Single host**
11. Close the **LON-NLB (172.16.0.42) Properties** dialog box.
12. Edit the host properties of **LON-SVR1 (Ethernet)**.
13. Configure the **Handling Priority** value of the port rule for port **5678** as **10**.
14. Close both the **Add/Edit Port Rule** and **Host Properties** dialog boxes.

▶ Task 2: Validate port rules

1. Switch to **LON-DC1**.
2. In Internet Explorer, browse to **http://lon-nlb**, and refresh the web page 20 times.
3. Verify that you see web pages both with and without the circle you added.
4. In Internet Explorer, browse to **http://LON-NLB:5678**, and refresh the web page 20 times.
5. Verify that now only the web page with the distinctive line displays.

Note: It is possible that you will need to refresh your browser more than 20 times to see the different logos on **http://lon-nlb**.

▶ Task 3: Manage host availability in the NLB cluster

1. Switch to **LON-SVR1**.
2. Use the **Network Load Balancing Manager** console to suspend **LON-SVR1**.
3. Verify that the node **LON-SVR1** displays as **Suspended**, and that the node **LON-SVR2** displays as **Converged**.
4. Resume and then start **LON-SVR1**.
5. Verify that both the nodes **LON-SVR1** and **LON-SVR2** now display as **Converged**.

Results: After completing this exercise, you should have successfully configured and managed an NLB cluster.

Exercise 3: Validating high availability for the NLB cluster

Scenario

As part of preparing to deploy NLB in your organization's environment, you want to ensure that it is possible to perform maintenance tasks such as reboot operations without affecting the availability of the websites that are hosted on the cluster. To accomplish this, you decide to verify availability by rebooting one host while you attempt to access the clustered website. You also will explore the Drainstop functionality.

The main tasks for this exercise are as follows:

1. Validate website availability when the host is unavailable.
2. Configure and validate Drainstop.
3. Prepare for the next module.

▶ Task 1: Validate website availability when the host is unavailable

1. Restart **LON-SVR1**.
2. Switch to **LON-DC1**.
3. On **LON-DC1**, open **Internet Explorer**, and then go to **http://LON-NLB**.
4. Refresh the website 20 times.
5. Verify that the website is available, although it does not display the **IIS** logo with the circle until **LON-SVR1** restarts.

▶ Task 2: Configure and validate Drainstop

1. On **LON-SVR1**, open the **Network Load Balancing Manager** console, and initiate a **Drainstop** on **LON-SVR2**.
2. On **LON-DC1**, go to **http://lon-nlb**, and then verify that only the **Welcome** page with the circled **IIS** logo displays.

Results: After completing this exercise, you should have successfully validated high availability for the NLB cluster.

▶ Task 3: Prepare for the next module

When you finish the lab, revert the virtual machines to their initial state.

1. On the host computer, start **Hyper-V Manager**.
2. In the **Virtual Machines** list, right-click **20740A-LON-DC1**, and then click **Revert**.
3. In the **Revert Virtual Machine** dialog box, click **Revert**.
4. Repeat steps two and three for **20740A-LON-SVR1** and **20740A-LON-SVR2**.

Question: How many additional nodes can you add to the LON-NLB cluster?

Question: What steps would you take to ensure that LON-SVR1 always manages requests for web traffic on port 5678, given the port rules that were established by the end of this set of exercises?

Question: What is the difference between a Stop and a Drainstop command?

Module Review and Takeaways

Review Questions

Question: You have created a four-node Windows Server 2016 NLB cluster. The cluster hosts a website that is hosted on IIS. What happens to the cluster if you shut down the World Wide Web publishing service on one of the nodes?

Question: You want to host the www.contoso.com, www.adatum.com, and www.fabrikam.com websites on a four-node NLB cluster. The cluster IP address will be a public IP address, and each fully qualified domain name (FQDN) is mapped in DNS to the cluster's public IP address. What steps should you take on each node to ensure that traffic is directed to the appropriate site?

Question: You have an eight-node Windows NLB cluster that hosts a web application. You want to ensure that traffic from a client that uses the cluster remains with the same node throughout their session, but that traffic from separate clients distributes equitably across all nodes. Which option do you configure to accomplish this goal?

Real-world Issues and Scenarios

To create a true high-availability solution, use a monitoring solution with NLB that will detect application failure. This is because NLB clusters will continue to direct traffic to nodes with failed applications providing NLB, which is independent of the application, continues to send heartbeat traffic.

Common Issues and Troubleshooting Tips

Common Issue	Troubleshooting Tip
You receive a message about conflicting IP addresses when restarting an NLB host.	
NLB Manager is having trouble connecting to a host.	
Hosts start converging, but do not complete the process.	
A default host is handling all the workload instead of it being balanced across nodes in the cluster.	

Module 11

Creating and managing deployment images

Contents:

Module Overview

With the increase in the number of information technology (IT) solutions in organizations, the number of physical and virtual server images have also increased. Due to this situation, operating system deployments take longer to complete and require valuable organizational resources. As a result, companies are looking for new ways to automate the server deployment process.

The Microsoft Deployment Toolkit (MDT) 2013 Update 2 is a collection of tools, processes, and guidance that you can use to manage and deploy operating system images. You can enhance the deployment process by integrating MDT with Windows Deployment Services (Windows DS) in the Windows Server 2016 operating system.

Virtual machine environments have become ubiquitous in the datacenter, and having the ability to deploy virtual server roles and workloads while deploying operating systems is an important part of the deployment process.

Objectives

After completing this module, you will be able to:

- Describe the Windows Server 2016 image deployment process.
- Create and manage deployment images by using MDT.
- Describe the different workloads in the virtual machine environment.

Lesson 1
Introduction to deployment images

An important part of the deployment process is determining how to handle images. You need to consider the best way to store the images that you create. Additionally, you will need to maintain and service images after building them. In this lesson, you will learn about images and how to deploy them. You also will learn about the different tools you can use in deploying images.

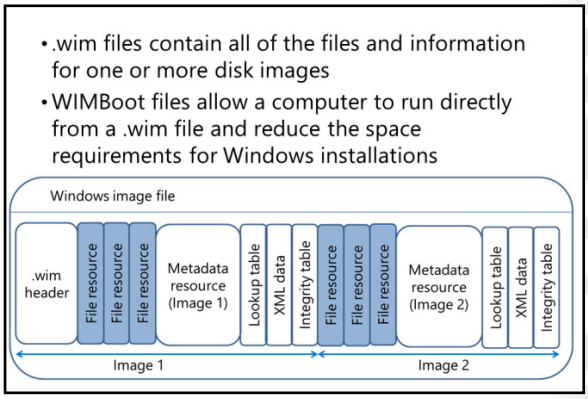
Lesson Objectives

After completing this lesson, you will be able to:

- Describe images.
- Describe image-based installation tools.
- Describe how to create, update, and maintain images.
- Describe the Windows Automated Deployment Kit (ADK) for Windows 10.
- Describe Windows Deployment Services.
- Describe the Microsoft Deployment Toolkit (MDT) 2013 (Update 2).
- Prepare a Windows Server 2016 image using the MDT.

Overview of images

Imaging has been in use for a long time, with early imaging products primarily performing sector-based imaging. Windows operating systems use .wim files that contain file-based images. When you are planning an image management strategy, you must address many considerations. Some of the primary considerations include the type of image and number of images, storage requirements, software and device drivers, and update management.



Type of image

You can choose between sector-based and file-based imaging. File-based imaging has many advantages over sector-based imaging. These include hardware independence, storing multiple images in a single file, single instancing, offline servicing, and nondestructive deployment. However, sector-based images have a few advantages, including:

- They deploy faster than file-based images. File-based images copy files to the destination volume whenever they are applied. File-based images then read answer files and apply configuration options. Sector-based images just copy bits, regardless of what files or configurations you might need.
- They typically include all the necessary drivers, and they work well when all client systems are identical. If your computer includes critical hardware that is not Plug and Play, using file-based imaging requires extra work to ensure that the proper device drivers are available.

Windows Image File format

The Windows image file format enabled administrators to break away from using sector-based imaging tools and methods. Newer file-based formats also can assist in the deployment of Windows operating systems. The following file-based imaging formats are available for Windows 10 and Windows Server 2016:

- Windows image file (.wim). The Windows image file is a file-based disk-image format that has a .wim file extension and that contains one or more individual volume images. The Windows image file structure can contain six types of resources, including:
- Header. Defines the content of the Windows image file, including .wim file attributes.
- File resources. A series of packages that contain captured data.
- Metadata resources. Information about the files that you capture. There is one metadata resource for each image in a .wim file.
- Lookup table. Information about the location of file resources in the .wim file. There is one lookup table for each image.
- XML data. Additional information about the image. There is one XML data field for each image.
- Integrity table. Security hash information that you can use for image verification during operations. There is one integrity table for each image.
- Virtual hard disk (.vhd). Typically, you use .vhd files with virtual machines. Windows 7 and newer operating systems provide the capability to start physical machines by using a .vhd file on the hard drive, instead of installing the operating system files directly on the hard drive. This is the boot from virtual hard disk process. There are multiple ways to create .vhd files, such as the Windows PowerShell **New-VHD** cmdlet, the **DiskPart** command-line tool, the **Disk Management** console, or Microsoft Hyper-V Manager. After you create the .vhd file, you can apply a Windows image file that contains your operating system to it, and boot from it as if it were a physical computer. Additionally, the Windows 8 Enterprise operating system introduced Windows To Go, which enables you to start a physical computer from a removable storage device, such as a USB drive. Windows To Go uses a .vhd file to store an operating system partition on a removable device.

Before capturing an image, you must configure it based on the needs and policies of your organization. Images can be as basic as a simple image with a standard operating system installation, or as complex as an image of the operating system that includes all of the applications that the organization uses. There are three types of images: thin, thick, and hybrid.

Thin images

A thin image is the smallest possible image you can create. It contains only the operating system and the necessary settings for a computer to be used in a network environment. Thin images do not contain any installed applications. A thin image is an appropriate baseline for all computers that will use the same operating system, regardless of the applications and utilities that could be loaded afterwards. However, the downside of thin images is that because they do not contain any installed applications, you must deploy all of the necessary applications to the computer after you deploy the image.

Thick images

A thick image is the opposite of a thin image. It contains the operating system and every application required by the end user. The advantage of a thick image is that after deployed, the user can work on the computer without having to install anything else. The disadvantages are that thick images are larger than thin images, and you might have to service the image more often due to it having multiple applications.

Hybrid images

Most organizations work with images that fall somewhere between thin and thick. Administrators commonly identify the various applications required by most of the users in the organization, and then create an image that contains all of those common applications. Once the image is applied to a computer, the specific applications for an individual user are deployed as well. This type of image is a hybrid image. Large organizations usually have a set of hybrid images for each department, such as one for the accounting department, one for the sales department, and one for the IT department.

Boot images

You can build boot images from Windows Preinstallation Environment (Windows PE) for Windows 10, which is a lightweight version of the Windows operating system. You can use boot images to start a computer in an environment where you can capture or install an operating system image. When you start a computer from a boot image, you load the Windows PE image into random access memory (RAM) and the system creates a RAM disk to which it assigns the drive letter X. The RAM disk provides a virtual file system in memory, which allows you to remove the actual boot media if required. For example, you could remove the boot DVD to put in a DVD that has a .wim file that you want to apply to the hard drive.

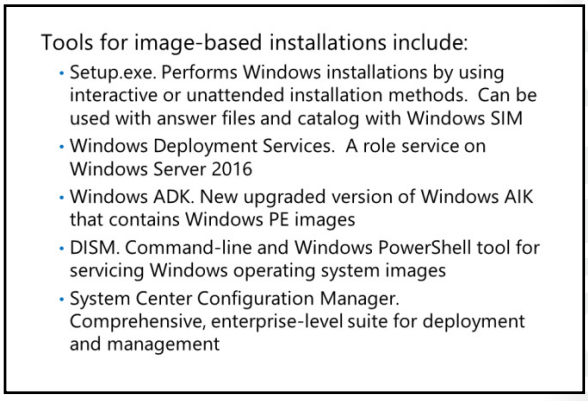
The Windows installation media contains a default boot image named Boot.wim. In many cases, you can use this boot image to start the imaging process, but you can modify the Boot.wim file to meet any special requirements of your organization, such as injecting specific network drivers.

Install images

The install image contains the operating systems that you plan to deploy to client computers. The default install image is Install.wim, and it is in the sources folder in the Windows installation media. Typically, you create your own installation images by building a reference computer based on the Windows installation media for the operating system that you want to install. After the initial installation, you modify it to meet your needs, such as installing apps, and then capture and store it on your deployment server.

Overview of image-based installation tools

You can choose from several tools and technologies to perform an image-based Windows operating system installation. You must be familiar with these tools and know where and when to use them in deployment situations:



- Windows Setup command-line options (Setup.exe). This tool performs Windows installations by using interactive or unattended installation methods.
- Answer file (Unattend.xml). A simple answer file includes basic Windows Setup configuration data, and minimum Windows Welcome customizations, which starts after the Windows Setup program runs.
- Catalog. This tool contains all available components and packages that can be used as a part of the Unattend.xml answer file, and can be modified through Windows System Image Manager (SIM).
- Windows ADK. This is a new upgraded version of Windows Automated Installation Kit (Windows AIK) that contains Windows PE images, which are necessary for customized deployment of Windows Server 2016 and Windows 10.

You might want to modify an existing .wim file by injecting drivers or adding Windows packages to an image. You can use several tools to service .wim files. You can deploy .wim files through the Microsoft Deployment Toolkit (MDT), Windows DS, and Microsoft System Center Configuration Manager (Configuration Manager). You also can use the ImageX and Deployment Image Servicing and Management (DISM) command-line tools or the DISM Windows PowerShell module cmdlets to service and deploy .wim files manually.

ImageX

ImageX.exe is a command-line tool that Microsoft introduced with the .wim file format to manage .wim files. ImageX is installed through the Windows ADK for Windows 10. You can run ImageX from within the Windows operating system when servicing an image, or from the Windows Preinstallation Environment (Windows PE) when deploying an image. ImageX is being deprecated and replaced with DISM.

DISM

DISM.exe is a command-line tool that you can use to service and deploy .wim files. Microsoft developed DISM to replace several image management tools, including ImageX. DISM includes the same functionality that ImageX includes, such as the ability to mount, service, capture, and create .wim files. You also can use DISM to prepare Windows PE images and to deploy .vhd and .vhdx files.

A DISM PowerShell module is available natively in Windows 8 and newer versions, and Windows Server 2012 and newer versions. The DISM PowerShell module also is available through Windows ADK. There are now 43 DISM module cmdlets when using Windows 10 and Windows Server 2016, and it provides the ability to service existing images in .wim files.

Using DISM command-line parameters or Windows PowerShell cmdlets

The command-line parameters and the Windows PowerShell cmdlets provide similar functionality. The following table includes the basic commands for imaging.

Task	DISM command-line parameters	Windows PowerShell cmdlets
Mount a .wim file for servicing	**/mount-image**	**Mount-WindowsImage**
Commit changes made to a mounted .wim file	**/commit-image**	**Save-WindowsImage**
Get information about a Windows image in a .wim file	**/get-imageinfo**	**Get-WindowsImage**
Dismount a .wim file	**/unmounts-image**	**Dismount-WindowsImage**
Add a driver to a mounted image	**/image:PathToImage /add-driver /driver:PathToDriver**	**Add-WindowsDriver –Driver PathToDriverFile –Path PathToRootDirectoryOfImage**
Apply an image to a specified drive	**/apply-image**	**Expand-WindowsImage**
Capture an image of a drive into a new .wim file	**/capture-image**	**New-WindowsImage**

Additional Reading: For more information on Windows PowerShell DISM cmdlets, refer to: "DISM Cmdlets" at: http://aka.ms/dtayll

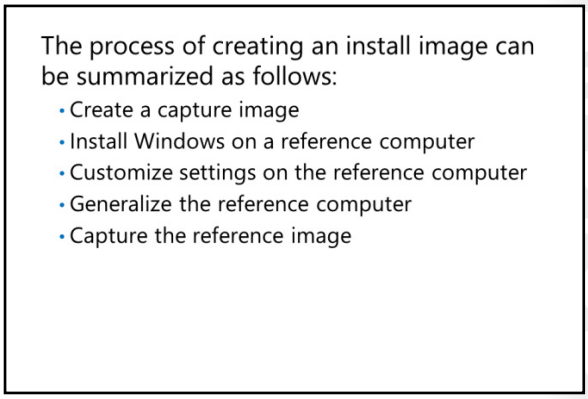
To list all the cmdlets, including those added for this version of DISM in Windows Server 2016, and the Windows PowerShell command prompt, enter the following cmdlets, pressing Enter after each line:

```
Import-Module DISM
Get-Command –Module DISM
```

Creating, updating, and maintaining images

The process for creating an install image can be summarized in the following high-level steps:

1. Start the reference computer from the network and perform a standard Windows operating system installation.
2. Customize the reference computer as required.
3. Generalize the reference computer.
4. Capture the reference computer's Windows operating system image, and upload it back to the Windows Deployment Services server.



Create a capture image

A *capture image* is a boot image that you can use to start a reference computer, capture its system drive, and store it in a .wim file. A *reference computer* is a computer that creates an image that you will later use to deploy an operating system to multiple computers.

Install Windows on a reference computer

You can install a Windows operating system on the reference computer by using any of the following methods:

- Manual install. Start the reference computer by using the Windows install media, or connect a share or USB drive that contains the install media, and then run Setup.exe.
- Windows DS–based install. Start the reference computer by using Pre-boot Execution Environment (PXE), and then start a Windows DS session to apply the standard install.wim for the desired Windows operating system.
- Other methods. You can use any other operating system deployment tool to apply the standard Install.win image to the reference computer. Some of the tools that you can use are:
    - DISM
    - ImageX
    - Configuration Manager

Customize the reference computer

After installing the operating system on a reference computer, configure the reference computer by doing one or more of the following:

- Enable and configure required Windows roles and features.
- Install any required applications.
- Configure all required Windows operating system settings.

Generalize the reference computer

Windows uses a series of GUIDs for different components of the operating system. These unique identifiers must be distinct from identifiers used on other computers on the same local network. When you create a reference image, if you apply that image to multiple computers on the same network, they will all have the same unique identifiers, and therefore will not be able to communicate with one another. To solve this issue, you can use a tool called Sysprep.

To generalize an image using Sysprep, execute the following steps:

1. Open a command prompt with elevated privileges.
2. In the command prompt, type the following command, and then press Enter:

```
sysprep /generalize
```

Capture the reference image

After generalizing the image, you must execute the following steps to capture the image:

1. Restart the reference image by using PXE boot.
2. Connect to a session in the server that is running Windows DS to download the captured image.
3. Follow the **Capture Image** wizard and specify the name of the .wim file that you want to create with the image from the reference computer.

Storage requirements

Depending on what your image includes, the image can take up a large amount of storage space. Typically, the images that sector-based imaging products create include the blank space on a hard drive, because it simply copies everything on the hard drive. This can lead to larger images than what a file-based imaging solution creates, because the file-based image only contains the files installed on the computer. Additionally, if you have several different hardware vendors, you might need to have sector-based images for each different hardware abstraction layer (HAL). This can require substantial disk space for storage.

Number of images

When planning your image management strategy, consider the number of images that you have to create. Besides the space needed to store the images, you will require an appreciable amount of time to maintain them.

When you use sector-based imaging, you might need to create multiple images based on the hardware that your environment is using. Typically, each different storage technology that you use requires an image. Additionally, as you acquire new hardware, you might have to create, store, and maintain additional images. When you use file-based imaging, you can use the same image for deployment to most systems.

Software

Operating system images do not have to include only the operating systems. You can install most software on your reference computer before imaging it. However, the more software that images include, the larger the images become, and the longer they take to deploy.

Deployment of device drivers

You can include device drivers in captured images, provide a custom driver store that supports Plug and Play functionality for your hardware, or you can install them with post-image deployment. You might need to include certain device drivers in the image or make them available during the imaging process when they are critical to the installation. Critical drivers typically are storage and network drivers.

Image updates

When you create an image, you are taking a snapshot of what the computing environment looks like at that time. However, outside of the image, your drivers, operating systems, and applications continue to update. You need to plan for including these ongoing changes in your images. If you are using sector-based images, this typically means deploying the image, making the necessary changes, and then recapturing the image. File-based images that feature offline servicing greatly reduce the time necessary for maintaining images. You need to maintain and update images to keep them current. You can service .wim file images at different stages of the deployment process.

There are three basic strategies for image maintenance, including:

- Using Windows Setup. This strategy involves using an answer file with Windows Setup when deploying the image. You can create or modify answer files by using the Windows SIM tool.
- Online servicing. This strategy involves deploying the image back to a reference computer, making all of the necessary changes, and then reimaging the reference computer. You might need to do this when installing new applications, Windows Installer–based software updates (.msi files), or drivers with .exe installations, and when adding anything that depends on Windows–installed services, such as the Microsoft .NET Framework.
- Offline servicing. This strategy involves using DISM to mount a .wim file and service the image. When servicing images offline, you can add Microsoft Update–based Windows software updates, drivers, and language packs, and add or remove folders, files, and Windows software components. Offline servicing typically does not include installing applications.

Using Windows Setup to customize images

You can use Windows Setup to modify an image during different phases of the deployment process, such as when deploying an image to a reference computer for online servicing or when deploying the image to client machines. By using an unattended Windows Setup answer file, you can perform many different customizations, including the following servicing operations:

- Add or remove a language pack.
- Configure international settings.
- Add and remove drivers.
- Add and remove packages.
- Enable and disable Windows operating system features.

Online servicing

You can perform online servicing with the DISM tool or through manual intervention. After deploying the system to a reference computer, you can add Plug and Play device drivers to the driver store, install applications and system components, install folders and files, and test the changes to the image. After you complete and test the changes, you can recapture the reference system. You can use the following tools to perform various online operations:

- DISM to enumerate drivers, international settings, packages, features, and to apply unattended answer file settings.
- DPInst to add drivers for detected hardware.
- PnPUtil to add, remove, and enumerate drivers.
- Windows Update Standalone Installer to add service packs or other .msu files.
- LPKSetup to add or remove language packs.

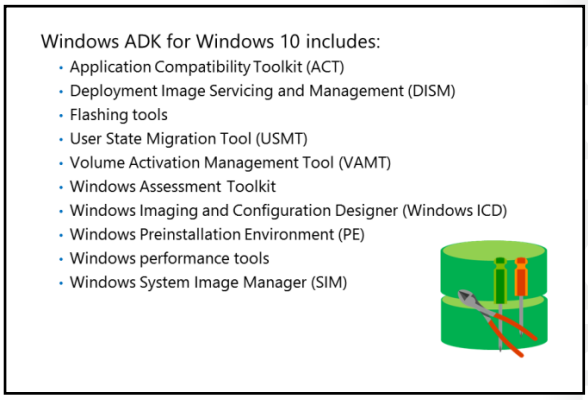
Offline servicing

Offline servicing is available for images that are stored in the .wim file format and use the DISM tool for servicing. The DISM tool can perform one or more of the following:

- Mount, remount, and unmount an image in a .wim file for servicing.
- Query information about a Windows image.
- Add, remove, and enumerate drivers provided as .inf files.
- Add, remove, and enumerate packages, including language packs, provided as .cab files.
- Add .msu files.
- Configure international settings.
- Enable, disable, and enumerate Windows operating system features.
- Upgrade to a newer edition of Windows.
- Check the applicability of a Windows Installer application update (.msp file).
- Enumerate applications and application updates installed in a Windows image.
- Apply the offline servicing section of an unattended answer file.
- Update a Windows PE image.

Windows ADK for Windows 10

You can use Windows ADK to develop deployment processes in your environment. You can create a very basic deployment process, or a complex deployment process that involves application and hardware testing. A few steps that all image-deployment processes have in common are the creation and capture of a reference computer, and the use of that image to build client systems.



A basic deployment process might include the following steps, which you can perform without using Windows ADK. However, by using Windows ADK, you can make this process faster and more consistent across multiple builds by performing the following steps:

1. Create the Windows PE media. You can use a USB device or a bootable CD with Windows PE to capture your image and deploy it after you customize it. You should:
   a. Customize the image with any necessary drivers.
   b. Customize the image with any additional packages, such as the Windows RE.
   c. Use the **makeWinPEMedia /ufd** command to create the bootable USB device.
2. Create and modify answer files. To automate the installation, you need to create answer files with the configuration that you want to use, including:
   a. Using the installation media to create a catalog file that Windows SIM can use.
   b. Modifying a sample answer file to fit your needs, and include any drivers or other packages in the installation.
   c. Creating the answer file for your environment.
   d. Copying the answer file to the root directory of the USB device and name it Autounattend.xml.
   e. Creating a profile that includes the CopyProfile setting, so that you can customize the default user profile. You also can customize the profile manually by making direct changes to the registry, or creating a script that uses the **REG** command.
   f. Copying the answer-file profile to the root directory of the USB device as CopyProfile.xml.
3. Use the answer file that you created to install a Windows operating system on your reference computer:
   a. Plug the USB device into the reference computer.
   b. Use the Windows product installation media to start the reference system. The setup process will use the **Autounattend.xml** file to complete the installation.
   c. Customize the administrator profile.
   d. Ensure that the USB device with the **CopyProfile.xml** is plugged in.

4. Capture the image:
    a. Use **Sysprep** to generalize the system. To use the **CopyProfile.xml** file, use the following **Sysprep** command on a single line with no space after **/unattend**:

       C:\Windows\System32\Sysprep\Sysprep.exe /generalize /oobe /shutdown /unattend:

       D:\CopyProfile.xml

    b. Start the computer from the Windows PE USB device.
5. Use the DISM tool to copy the Windows partition to a network location or external hard drive.
6. Deploy the image to a test computer:
    a. Start the test system with the Windows PE USB device.
    b. Use **diskpart** to configure the hard drive as appropriate.
    c. Use the **applyimage** command to apply the previously captured image.
    d. Verify that the computer image and profile settings are correct.

Windows ADK contains different tools that IT professionals can use to assess, customize, and deploy Windows operating systems to computers. Microsoft released Windows ADK for Windows 10 to incorporate Windows 10 into Windows ADK functionality. You typically use Windows ADK in two key scenarios: Windows assessment and Windows deployment. This topic focuses on Windows deployment.

Windows ADK contains the following deployment tools:

- Application Compatibility Toolkit (ACT). ACT enables software developers, independent software vendors, and IT professionals who work in an enterprise environment to determine whether their applications are compatible with a new version of the Windows operating system. ACT also enables these individuals to determine how updates will affect their applications.
- DISM. DISM is available as part of the Windows operating system, and you can use it to perform offline image servicing. This is a crucial process for maintaining images that an operating system deployment uses.
- Windows SIM. You can use Windows SIM to create unattended Windows Setup answer files.
- Windows PE. Windows PE is the initial operating system that you use during a Windows operating system deployment. Windows PE prepares a computer by running tasks such as partitioning a hard drive, creating and formatting volumes, copying disk image files to a system, and initiating setup.
- User State Migration Tool (USMT). USMT is a collection of executable files that you can use to copy user state data from a computer. You can then restore that data onto a new installation of the Windows operating system.
- Volume Activation Management Tool (VAMT). VAMT provides a centralized tool for managing volume-licensed Microsoft products, including Windows operating systems and Microsoft Office products.
- Additional tools. These are command-line tools, such as **oscdimg**, which creates bootable Windows PE .iso image files, and **makewinpemedia**, which creates Windows PE bootable USB media.
- Technical reference documentation. This includes documentation for Windows Setup, DISM, Sysprep, Windows SIM, Windows Recovery Environment (RE), and additional deployment documentation.

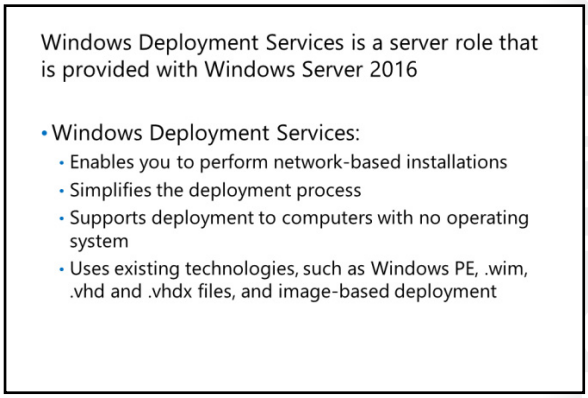
Windows ADK for Windows 10 has the following new deployment tools:

- Flashing tools. These are tools to flash Full Flash Update (FFU) images to Windows mobile devices.
- Windows Imaging and Configuration Designer (Windows ICD). Windows ICD lets you create provisioning packages to customize images without having to reimage them. You can also create customized Windows images for specific markets.
- Windows Assessment Toolkit. The Assessment Toolkit helps you assess a running operating system, determine its status, review results in a report, diagnose problems or issues, and helps you correct the problems or issues. It comes with the Windows Assessment Console and a number of XML and binary files that are loaded with specific computer status checks and measurement components. It also contains an Assessment Toolkit technical reference.
- Windows Performance Toolkit. This contains two tools, the Windows Performance Recorder and the Windows Performance Analyzer. These tools can collect detailed performance profiles of Windows operating systems.

Windows ADK also includes the Microsoft SQL Server Express 2012 SP1 database, which stores objects that are collected by some deployment tools, such as ACT.

Windows Deployment Services

Windows DS is a server role that is intended for deployment specialists responsible for the deployment of Windows operating systems.You can install Windows DS by using the **Add Roles and Features** wizard in Server Manager or by using Windows PowerShell.



It provides the following functions:

- Allows you to perform network-based operating system installations.
- Simplifies the deployment process.
- Supports deployment to computers that have no installed operating system.
- Provides end-to-end deployment solutions for both client and server computers.
- Uses existing technologies, such as Windows PE, Windows image file (.wim) and virtual hard disk (.vhd and .vhdx) image files, and image-based deployment.

Windows DS enables automated deployment of Windows operating systems. You can completely automate deployment of the following operating systems:

- Windows Server 2016
- Windows 10
- Windows 8.1
- Windows Server 2012
- Windows 8
- Windows Server 2008 R2

- Windows 7
- Windows Server 2008
- Windows Vista with Service Pack 1 (SP1)

Windows DS enables you to create, store, and deploy installation images of supported operating systems, and supports .wim, .vhd, and .vhdx image files. Deployment now can be unicast or multicast. With unicast, packets are sent to a particular address one at a time. If more than one device needs those packets, the process is repeated until all devices have the needed packets. With multicasting, the packets are sent once to a multicast group, and all devices in the group get the same packets at the same time. This helps to manage the network traffic that the deployment process in a faster and less bandwidth consuming way. This potentially speeds up deployment without affecting other network services adversely.

Windows DS consists of two role services and three management tools:

- Deployment Server. This role service manages end-to-end Windows operating system deployment solutions, including a PXE component.
- Transport Server. This role service provides basic network services and a PXE listener. This listener forwards the requests to a PXE provider, which the Transport Server does not include, but is part of the Windows DS service. If you install the Transport Server role service as a standalone component, you must use an additional management tool, such as Configuration Manager, Microsoft System Center Virtual Machine Manager (Virtual Machine Manager), or custom deployment services.
- Windows DS snap-in. This is the Windows DS graphical user interface (GUI). You can complete most Windows DS tasks in this snap-in, which you can install only if you install the Deployment Server role service.
- WDSUTIL. The command-line management tool for Windows DS. You also can use WDSUTIL to script Windows DS management.
- Windows PowerShell cmdlets that were introduced in Windows Server 2012 R2.

You can use the Deployment Server and Transport Server roles together, or you can use the Transport Server role alone by using Configuration Manager or Virtual Machine Manager. You cannot run WDSUtil and the Windows PowerShell cmdlets remotely. You must sign in to the Windows DS server to be able to configure Windows DS though the command line.

You can install and integrate Windows DS with Active Directory Domain Services (AD DS), or install it as a standalone service. Installing Windows DS as an AD DS–integrated service provides the following benefits:

- AD DS acts as a data store, and you can prestage a computer in AD DS. During the deployment process, Windows DS will match the physical computer to the AD DS object.
- AD DS allows Windows DS to register as a system services control point. A system services control point identifies the computer account as a Windows DS server and stores configuration settings, such as whether the server is responding to PXE requests.

Components of operating systems

Windows DS utilizes the componentized nature of Windows operating systems. Components allow you to separate the core functionality of the operating system in an image by adding or removing components at any time. For example, you can create an image containing the Windows 10 Enterprise operating system and the applications used by all users in your company. You can use this image as a standard image across your organization. You can save this standard image in a. wim file used for deployment by using Windows DS. As Microsoft releases updates for Windows 10, you can apply these updates to the base .wim file. By using this component approach, you do not need to create new images as updates are released.

Updates are not the only componentized element that you can apply to images. The following elements follow the component infrastructure:

- Updates
- Service packs
- Language packs
- Device drivers

You can reduce the size of images and total number of available images in a server running Windows DS by taking advantage of the componentized nature of the Windows operating system, and the ability to apply components to images managed by Windows DS.

Any organization that wants to reduce administration effort during operating system deployment can do so by using Windows DS. Organizations that use Windows DS require little interaction from users when deploying the operating systems.

To create a Windows DS session, start the target computers by using PXE, and then join the session. After the session starts, the deployment requires no further user interaction. This type of deployment is a *lite-touch installation (LTI)*.

You also can use Windows DS in conjunction with other technologies to provide an even less interactive deployment, called *zero-touch* installation (ZTI). In a zero-touch installation, a designated server can use the Wake On LAN protocol to start computers by using PXE, and then join a session managed by Windows DS. That way, no interaction with the target computers is necessary.

Whether you use lite-touch or zero-touch installations, Windows DS allows you to create a more autonomous and efficient environment for installing Windows. Consider the following scenarios.

Deployment over a small network

In a small network consisting of a single server and around 25 computers running the Windows 7 operating system, you could use Windows DS to expedite the upgrade process of the client computers to Windows 10. After you have installed and configured the Windows DS server role on the single server, you can use Windows DS to perform the following tasks:

1. Add **Boot.wim** from the sources folder of the Windows Server 2016 media as a boot image in Windows DS.
2. Add **Install.wim** from the sources folder of the Windows 10 media as an install image.
3. Create a capture image from the boot image that you added previously.
4. Start your reference computer from the network by using PXE.
5. Perform a standard installation of Windows 10 from the **Install.wim** image.
6. Install Microsoft Office productivity applications and custom applications as required on the reference computer.
7. Generalize the reference computer by using the System Preparation Tool (Sysprep).
8. Restart the reference computer from the network by using PXE.
9. Connect to the capture image that you created, use it to capture the local operating system, and then upload it back to the Windows DS server.
10. Start each of the existing target computers from the network using PXE, and connect to the appropriate boot image.
11. Select the custom install image, and then deployment will start.

The benefits of this deployment method to the organization in this scenario are:

- A standardized desktop computer image.
- Quick deployment of each computer with limited installer interaction.

This solution would not suit larger deployments because you need the installer to start the deployment on the target computer. Additionally, the installer is required to select a disk partition on which to install the selected installation image.

Deployment over a medium to a large organization

In the second scenario, a medium-to-large size organization wants to deploy multiple servers in branch offices that are geographically dispersed. Sending experienced IT staff to each location to deploy the servers would be time-consuming and expensive.

By using Windows DS, IT staff can address this issue remotely:

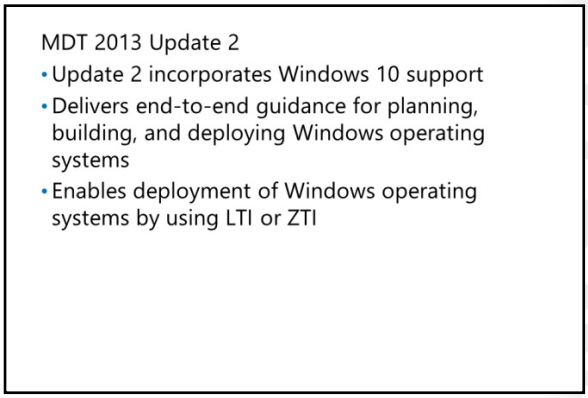
1. Add **Boot.wim** from the Windows Server 2016 media as a boot image in Windows DS.
2. Add **Install.wim** from the Windows Server 2016 media as an install image.
3. Create a capture image.
4. Start the reference computer from the network.
5. Perform a standard installation of Windows Server 2016 from the **Install.wim** image.
6. Customize the reference computer as required.
7. Generalize the reference computer.
8. Restart the reference computer.
9. Capture the reference Windows operating system, and upload it back to the Windows DS server.
10. Configure the necessary Active Directory Domain Services (AD DS) computer accounts. This prestages the computer accounts.
11. Use Windows SIM in the Windows ADK to create an answer file (**Unattend.xml**).
12. Configure the answer file for use with the captured installation image on Windows DS.
13. Configure a custom naming policy in Windows DS so that each server computer receives a suitable computer name during deployment.
14. Configure Windows DS to use a default boot image.
15. Configure Windows DS to respond to PXE requests and start deployment of the install image automatically.
16. Start each of the target computers from the network.

The benefits of this deployment method to the organization in this scenario are:

- Standardized server builds.
- Automatic domain-join following deployment.
- Automatic computer naming.
- Little or no installer interaction.

The solution does not implement multicast transmissions, nor does it use PXE referral. You also could use these technologies to help manage network traffic during the deployment.

Microsoft Deployment Toolkit 2013 (Update 2)



One of the common purposes for using MDT 2013 Update 2 in an LTI or ZTI scenario is to create a reference image. In this case, you separate the reference-image creation process from the production deployment process. MDT creates the reference image by capturing a reference computer operating system into a .wim file. You can configure a particular computer with all of the settings and applications that you want to deploy to other computers, and then capture it to a .wim file. You then can use the .wim file as a basis of deployment through MDT, or alter it by adding drivers, packages, and applications by using task sequences when deployment occurs.

When preparing to use the LTI method, you can divide your preparation into four major tasks:

- Plan the MDT imaging strategy. Your imaging strategy will determine how you build the MDT management computer.
- Install the prerequisites and MDT 2013 Update 2 and the Windows ADK for Windows 10, both of which are no-cost downloadable solution accelerators from Microsoft. The LTI method has fewer prerequisites than other installation strategies.
- Create the deployment share. The deployment share is the repository for all of the deployment files.
- Create and customize the task sequences. You can use task sequences to automate the build and deployment processes.

Installing the MDT is a multistep process that is not complete until after the installer utility has finished running. After choosing or building a system to host the MDT, you can download and run the MDT setup program MicrosoftDeploymentToolkit2013_x64.msi.

Note: Windows ADK for Windows 10 must be installed prior to installing the MDT 2013 Update 2 files. Otherwise, you cannot use the deployment share node. Note that you do not need to install all utilities in Windows ADK for Windows 10. For the MDT, you only need to install the Deployment Tools, Windows Preinstallation Environment (Windows PE), and User State Migration Tool (USMT).

After installing the MDT, the next step is to start the Deployment Workbench and begin configuring the MDT environment. In the Deployment Workbench, you should configure the Components container first. The Components container displays the status of the MDT components. Some components will display as already installed, and some could show as required. Required components will need to be downloaded and installed. If you are connected to the Internet, you can highlight any component, and then click **Download** to download the component for installation.

After the initial installation is complete, you need to create your first deployment share. The deployment share is created as a physical structure on a hard drive, and most of the deployment share folders on the hard drive are directly represented as folders in the Deployment Workbench. In addition to the default folders, you can create subfolders through the Deployment Workbench to keep your objects organized. You can create multiple deployment shares to support multiple deployment configurations, if wanted. You can also create deployment shares on alternate servers across a wide area network (WAN) connection, especially when you have limited bandwidth. To create a new deployment share, right-click

the **Deployment Shares** node, click **Create New Deployment Share**, and then complete the steps in the **New Deployment Share Wizard**.

MDT 2013 Update 2 supports the deployment of the following Microsoft Operating systems:

- Windows 10
- Windows Server 2016
- Windows 8.1
- Windows 8
- Windows Server 2012 R2
- Windows Server 2012
- Windows 7
- Windows Server 2008 R2
- Windows PE version 5.0

Demonstration: Preparing a Windows Server 2016 Image in MDT

In this demonstration, you will see how to:

- Create an MDT deployment share.
- Examine the MDT deployment share properties.
- Import Windows Server 2016 operating system files into an MDT deployment share.

Demonstration Steps

Create an MDT deployment share

1. On **LON-SVR1**, insert the **D:\Program Files\Microsoft Learning\20740\Drives \ WinServer2016_TP5.ISO** into the virtual machine's virtual hard drive.
2. On the Start screen, open the **Deployment Workbench** item.
3. Right-click **Deployment Shares**, and then click **New Deployment Share**.
4. Create a **DeploymentShare** folder on drive **C**.
5. Complete the **New Deployment Share Wizard** with default settings.

Examine the deployment share properties

1. Expand both the **Deployment Share** and the **MDT Deployment Share (C:\DeploymentShare)** nodes.
2. Open the **Properties** window for the MDT Deployment Share.
3. Examine each tab in the **MDT Deployment Share (C:\DeploymentShare) Properties** dialog box.
4. Close the **MDT Deployment Share (C:\DeploymentShare) Properties** dialog box.

Import operating system files into the deployment share

1. From the **Operating System** folder, click **Import an Operating System**.
2. Use the **Import Operating System Wizard** to import source files from the **D:** drive into a **Destination directory name** named **WindowsServer2016**.
3. Complete the **Import Operating System Wizard** using defaults.

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	Uses task sequences to capture and deploy images.
2	Allows you to create provisioning packages to customize images without having to re-image them.
3	Creates the Deployment Share.
4	Needs Windows ADK as a prerequisite before using.
5	Is a Windows Server 2016 server role.
6	Start computers from the network using PXE.
7	Use the makeWinPEMedia /ufd command to create the bootable USB device.
8	Has both a deployment and transport server role service.
9	Contains Windows SIM, which can be used to make answer files.

Category 1		Category 2		Category 3
Windows ADK for Windows 10		Windows DS		MDT 2013 Update 2

Lesson 2

Creating and managing deployment images by using MDT

You can use the MDT to automate the deployment of Windows operating systems, applications, desktops, laptops, tablets, and servers in the enterprise. In essence, the MDT helps you configure the unattended answer files and provides tools for automating additional components and settings. The MDT allows you to automate the creation of a reference computer and then capture that computer to an image, which you then can deploy to target computers.

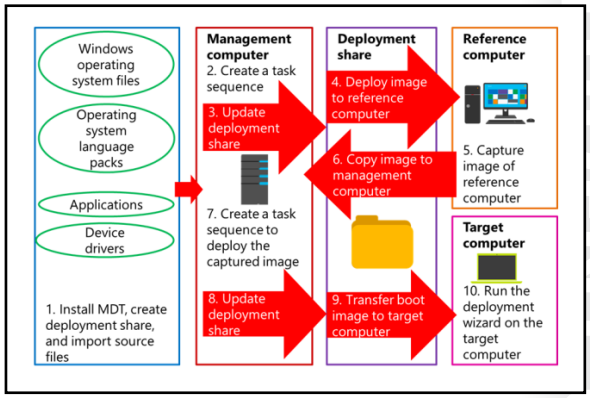
Lesson Objectives

After completing this lesson, you will be able to:

- Create images in MDT.
- Deploy images in MDT.

Creating images in MDT

MDT lets you build and deploy both boot and install images. As previously discussed, both types are available as .wim files found on the installation media for Windows operating systems. Whenever you update a deployment share, the update process checks for changes and creates a new LTI boot image. The boot image is created in both a .wim file and an .iso image file, which you then can use to create bootable media.



While you can use the original Install.wim file found in the sources directory of the installation media to deploy an image, in most cases you would want to customize both the image as it exists as a .wim file in the MDT Deployment Share, and through the deployment of the image. By using MDT, you can deploy a .wim file to a reference computer, configure and add software to the reference computer, and then capture the reference computer in its entirety to a .wim file. You can later deploy this .wim file to many computer devices, and even add software, drivers, and apps to the image as part of customizing it when deploying.

When you follow the LTI process (which uses only the tools available in the MDT), you perform the following high-level steps:

1. Install the MDT, create a deployment share on the management computer, and then import the source files that you want to use.
2. Create a task sequence and boot image for the reference computer.
3. Update the deployment share with any changes.
4. Boot the reference computer with the MDT media. This will provide access to the task sequence files, the task sequence, and the boot image to the reference computer.
5. Run the deployment wizard to install the operating system on the reference computer, and capture an image of the reference computer.
6. Copy the captured image to the management computer.

7. Create the boot image and task sequence to deploy the captured image to target computers.
8. Update the deployment share.
9. Boot the target computer with the MDT media. This will provide the reference computer with access to the task sequence files, the task sequence, and the boot image.
10. Run the deployment wizard to install the operating system on the target computer.

The same captured .wim file from the reference computer can be deployed with different customizations that meet the specific needs of your organization at the time you run the deployment. For example, you might have a hybrid image that includes the Windows 10 Enterprise edition, in addition to Office Professional 2016. You deploy this image out to a group of new computers you purchased for the Sales department. However, you also have a Customer Relationship Manager (CRM) software package you want to deploy to Sales. You can add the CRM software as an application deployment as part of the hybrid image deployment. Later, you might want to deploy the same image to the Accounting department, but this time without the CRM software but with a financial program instead. You can also do this as an application deployment when deploying of the hybrid image.

MDT includes task sequence templates for the most common deployment scenarios. When creating task sequences for your deployments, you start by choosing one of the available templates. Ten predefined task sequence templates and one custom task sequence template are available:

- **Sysprep and Capture**. Use to automate the running of the System Preparation Tool (Sysprep) and the capturing of a reference computer.
- **Standard Client Task Sequence**. Use to create the default task sequence for deploying operating system images to client computers. This template includes several generic tasks, such as creating a reference computer, which you can enable or choose not to perform, as necessary. The next demonstration shows you how to use this functionality.
- **Standard Client Replace Task Sequence**. Use to back up a client system completely, including the user state data, and then wipe the disk before deploying an operating system.
- **Standard Client Upgrade Task Sequence**. Use to automate the process of upgrading a computer currently running Windows 8.1, Windows 8, or Windows 7 to Windows 10.
- **Litetouch OEM Task Sequence**. Use to preload operating system images on computers in a staging environment prior to deploying the target computers in the production environment. Typically, computer original equipment manufacturers (OEMs) use this template.
- **Standard Server Task Sequence**. Use to create the default task sequence for deploying server operating system images to servers.
- **Standard Server Upgrade Task Sequence**. Use to automate the process of upgrading a server currently running Windows Server 2008 or newer Windows Server operating system to Windows Server 2016.
- **Post OS Installation Task Sequence**. Use to perform tasks after you deploy an operating system to a target computer, such as enabling Microsoft Update.
- **Deploy to VHD Client Task Sequence**. Use to deploy an operating system to a target computer's virtual hard disk for Boot from VHD installations on client computers.
- **Deploy to VHD Server Task Sequence**. Use to deploy an operating system to a virtual hard disk on a target computer for Boot from VHD installations on servers.
- **Custom Task Sequence**. Use to create a customized task sequence. A custom task sequence has only one task available after creation—the Install Application task. However, you can add other tasks to the task sequence.

After you create a task sequence, you can further customize each task in the task sequence. You also can add new tasks to the task sequence.

You can use two files to control the behavior of installations that you deploy from a deployment share. The rules shown in the Deployment Shares Properties are stored in the **CustomSettings.ini** file, which is in the deployment share in the Control folder. The **CustomSettings.ini** file is the primary configuration file for the deployment share. All installations from the deployment share process this file's settings.

Alternatively, you can use the **Bootstrap.ini** file on the **Rules** tab, which is stored in the deployment share in the Control folder. The **BootStrap.ini** file processes before the **CustomSettings.ini** file.

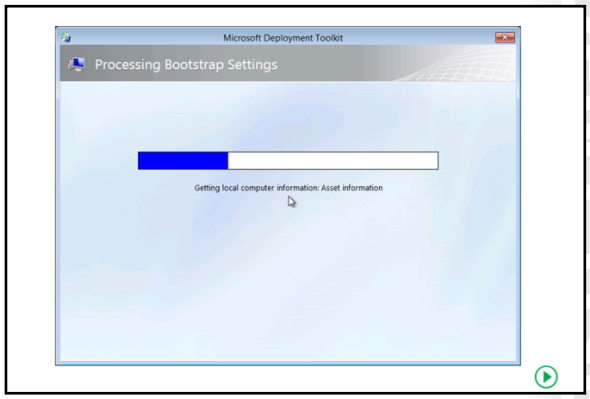
The **Bootstrap.ini** file and the **CustomSettings.ini** file are organized into sections. The first section is the **Settings** section, which defines the file's contents, including:

- Priority. Specifies the sections to process during deployment and the order in which to process them. This property is in both the **Bootstrap.ini** file and the **CustomSettings.ini** file.
- Properties. Specifies the variables that you are defining for use in the file. This property is only in the **CustomSettings.ini** file.

Additionally, each of the files contains the **Default** section, which stores the default properties when you create a deployment share.

Deploying images in MDT

When you update the deployment share, the LTI boot media is either created or modified. The LTI boot media includes the MDT program, which calls the **Windows Deployment Wizard** when performing a deployment. When you boot a system by using the LTI boot media, the MDT program starts automatically and the following actions occur:



1. The **Bootstrap.ini** file is processed. When the computer first starts, the MDT program processes **Bootstrap.ini**, and then uses the information to connect to the deployment share.
2. After you connect to the deployment share, from the **Welcome** page, you can:
   - Run the **Deployment Wizard** to install a new operating system, which starts the **Windows Deployment Wizard**.
   - Run the **Windows Recovery Wizard**, which starts the Windows Recovery Environment.
   - Exit to the command prompt.

Additionally, you can choose the keyboard layout or configure a static IP address. You also can configure the keyboard layout in the **Boostrap.ini** file.

Choosing the **Run the Deployment Wizard** to install a new operating system involves the following steps:

1. The **Credentials** dialog box appears. If you have not configured the **Bootstrap.ini** file with user credentials for accessing the deployment share, you are prompted to enter them.
2. The **CustomSettings.ini** file is processed. The **CustomSettings.ini** file includes settings for preconfiguring and skipping **Windows Deployment Wizard** pages, including skipping the wizard altogether.
3. The **Task Sequence** page appears. After you apply the **CustomSettings.ini** file settings, the **Windows Deployment Wizard** presents the available task sequences.

After you choose a task sequence, the **Windows Deployment Wizard** will proceed to show the pages that are appropriate for the type of deployment and task-sequence template used. Settings in the **CustomSettings.ini** file could prevent certain pages from appearing.

When you perform a new computer deployment by using a task sequence based on the standard client-task sequence and a default **CustomSettings.ini** file, the **Windows Deployment Wizard** will display the following pages:

1. **Computer Details**. This page allows you to specify the **Computer name**, **Join a workgroup**, or **Join a domain**, and if joining a domain, the information required to join the domain.
2. **Move Data and Settings**. If the computer had an existing operating system, you could choose to **Move the user data and settings** to a specified location.
3. **User Data (Restore)**. If you have previously used the **Move the user data and settings** option as part of a computer migration, you can specify the location on this page.
4. **Locale and Time**. This page allows you to specify the language and time settings for your deployment.
5. **Ready**. If you click the **Details** button on this page, you can review all the settings that you have configured. If you need to change anything, use the **Back** button to return to the appropriate page. When the settings are correct, click **Begin** to start the deployment.

Advanced Configuration node

The Deployment Workbench includes an **Advanced Configuration** node that contains several items that you can use to extend LTI deployment features. This includes linking deployment shares, support for standalone media, and configuring an MDT database.

MDT has a monitoring feature that the Deployment Workbench and MDT scripts support. You can use the **Monitoring** node in the Deployment Workbench to view the deployment process.

Selection profiles

Selection profiles allow you to create groups of folders in the Deployment Workbench. You can use any folder that contains at least one item, including Applications, Operating Systems, Out-of-Box Drivers, Packages, and Task Sequences. After you create your selection profiles, you can use them in several different locations, including:

- The **Deployment Share Properties** dialog box, on the **Windows PE** tab, on the **Drivers and Patches** tab. Here you can specify the selection profile to limit the drivers that are added to the Windows PE boot image.
- An Inject Drivers task step. You use the selection profiles in this step to control the drivers that are available for a particular task sequence.

- An Apply Patches task step. You use the selection profiles in this step to control the update packages that are installed.
- The **New Media Wizard**. Here you use the selection profiles to control the Applications, Operating Systems, Out-of-Box Drivers, Packages, and Task Sequences folders that deploy with standalone media.
- The **New Linked Deployment Share Wizard**. Here you use the selection profiles to control the linked content.

The following table details the six selection profiles that are created by default.

Selection profile	Description
Everything	Contains all folders from all nodes
All drivers	Contains all folders from the Out-of-Box Drivers item
All drivers and packages	Contains all folders from the Packages and Out-of-Box Drivers items
All packages	Contains all folders from the Packages item
Nothing	Includes no folders or items
Sample	A sample selection profile that contains folders from the Packages and Task Sequences items

Linked deployment shares

You can use linked deployment shares to connect two deployment shares logically. One deployment share acts as the source and the other deployment share is the target. You use a selection profile to control the content copied to the target deployment share. Using linked deployment shares allows you to use LTI deployments in larger organizations, while keeping the management simple by requiring that you update only the source deployment share.

Media

You can use the Media item to create LTI media for standalone deployment media, which enables you to perform an LTI deployment without contacting the server. You can create media and place it on a DVD, USB drive, or other portable media. You can control the contents of the standalone media by choosing the appropriate selection profile when you start the **New Media Wizard**.

Database

By default, the variables that you use with your task sequences are stored in the **CustomSettings.ini** file. As your deployments grow more complex, the conditions that you define in the **CustomSettings.ini** file might become too numerous to manage effectively. To address this challenge, you can create a SQL Server database to store the conditions that you want to define. After creating the database, you run the **Configure DB Wizard** to configure the **CustomSettings.ini** file to use the MDT database.

Monitoring MDT deployments

Monitoring is not configured by default. The process for enabling monitoring is different for LTI deployments and Configuration Manager–based deployments. To configure monitoring for LTI deployments, you need to enable it in the **Deployment Share Properties** dialog box, on the **Monitoring** tab. Select the **Enable monitoring for this deployment share** option to make changes to your management computer. These changes include:

- Installing the MDT Monitor service (MDT_Monitor). This service receives and stores the events from the computers that are being monitored. It also provides the information to the Deployment Workbench.
- Installing an SQL compact database. Only the MDT Monitor service uses this database.

Updating the CustomSettings.ini file with the **EventService** property, and a value of http://<Management Computer>:9800. This connection does not require Microsoft Internet Information Services (IIS). It uses features from the .NET Framework to provide the HTTP functionality. After you enable the monitoring feature, you can monitor deployments by using the **Monitoring** node in the Deployment Workbench. You will need to refresh the **Monitoring** node periodically.

Check Your Knowledge

Question	
Which one of the following operating systems can MDT 2013 Update 2 deploy? Choose all that apply.	
Select the correct answer.	
	Windows 7
	Windows Server Vista
	Windows 10
	Windows 2008
	Windows Server 2012 R2

Lesson 3
Virtual machine environments for different workloads

Prior to implementing virtualization in your organization, you must first determine key evaluation factors that you can use to assess your organization's virtualization requirements. You will learn about some of the available resources, including solution accelerators such as the Microsoft Assessment and Planning Toolkit (MAP). This lesson also describes some of the principal design factors for implementing a server virtualization solution.

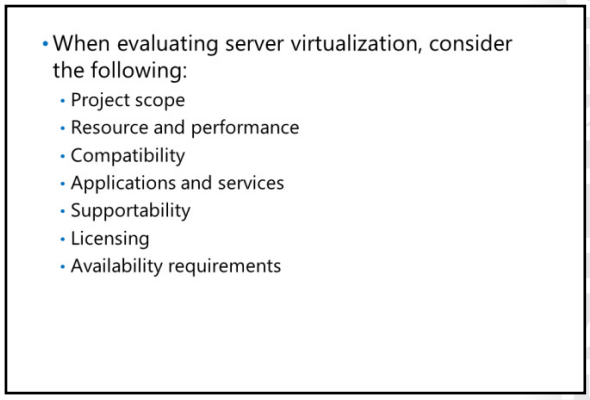
Lesson Objectives

After completing this lesson, you will be able to:

- Evaluate your organization's requirements for server virtualization.
- Describe the virtualization solution accelerators.
- Describe the assessment features of MAP.
- Assess the computing environment by using MAP.
- Design a solution for server virtualization.

Evaluation factors

When you consider the challenges presented by the traditional computer and application environments, server virtualization is an effective way to resolve many of the known issues. Planning your server virtualization project is a very important first step, and evaluating factors that will contribute to a successful virtualization project is the beginning of this process. Some of the important evaluation factors are as follows:



- Project scope. You should define the virtualization project scope as early on as possible. You should determine the business factors driving the project, the staff that is responsible for determining these factors, and their goals.

  You should also determine how you will measure success. For example, if your company is migrating from Microsoft Exchange Server 2007 to Exchange Server 2013, your migration project scope might include server virtualization elements, but the overall success is measured by a transparent upgrade of the organization's email platform. However if your project scope is to implement or upgrade a server virtualization strategy, Exchange Server might just be a milestone goal of the overall consolidation or improvement program. Understanding budgets and documenting the project are also important factors.

- Resource and performance. Assessing the resource and performance of the servers to be virtualized is another evaluation factor. You can use MAP to provide detailed information on the number of hosts and the host hardware requirements.

  Typically, virtual machines require approximately the same resources as a physical server. For example, if a physical server is currently utilizing 1 GB of RAM, you should expect the virtual machine to use the same amount of RAM, assuming that it runs the same operating system and applications as

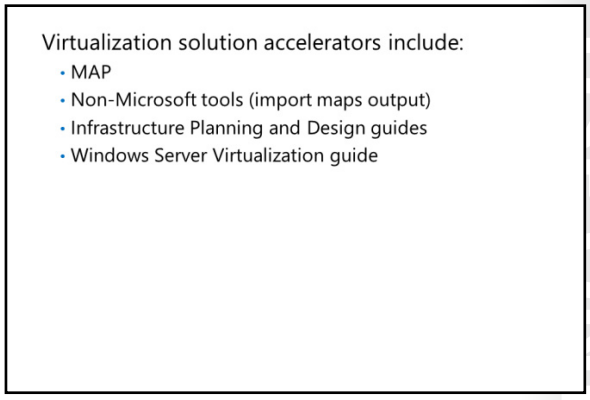
the physical server. If a single virtual machine consumes more than half of your host's workload, you should consider whether virtualization is appropriate or if the host's sizing is adequate.
Hardware is not the only consideration when implementing a server virtualization solution. You also should review all aspects of a service or application's requirements before deciding whether you can host it virtually. Some factors to consider when determining whether to virtualize server workloads are:

- Compatibility. You must determine whether the application can run in a virtualization environment. Business applications range from simple programs to complex, distributed multiple-tier applications. You need to consider requirements for specific components of distributed applications, such as specific needs for communication with other infrastructure components, or requirements for direct access to the system hardware. While you can virtualize some servers easily, other components might need to continue running on dedicated hardware.
- Applications and services. Applications and services that have specific hardware or driver requirements generally are not well suited for virtualization. An application might not be a good candidate for application virtualization if it contains low-level drivers that require direct access to the system hardware. This might not be possible through a virtualization interface, or it could affect performance negatively.
- Supportability. You need to evaluate if a virtualized environment will support your operating system and requisite applications. Verify vendor support policies for operating system and application deployment using the virtualization technologies.
- Licensing. You also need to evaluate whether you can license the application for use in a virtual environment. Reduced licensing costs for multiple applications or operating systems could add up and make a strong financial case for using virtualization.
- Availability requirements. Most organizations have some applications that must always be available in a virtual environment for users. Some applications provide built-in options for enabling high availability, while other applications could be more difficult to make highly available outside of a virtual machine environment. When considering whether to virtualize a server, evaluate whether the application has high availability options, whether a virtual machine environment supports those options, and whether you can use failover clustering to make the virtual machine highly available.

The goal in most organizations is to utilize all servers adequately, whether they are physical or virtual. You can fully utilize some server roles such as SQL Server or Exchange Server Mailbox servers, by deploying additional SQL Server instances or moving more mailboxes to the server. In some cases, you can virtualize server workloads in one scenario, but not in other scenarios. For example, in a very large domain with thousands of users logging on simultaneously, it might not be practical to virtualize a domain controller. However, in a smaller domain or in a branch office deployment, virtualizing domain controllers might be your best option.

Overview of virtualization solution accelerators

You can use MAP to conduct network-wide deployment readiness assessments, and to determine whether you can migrate Microsoft technologies such as servers, desktops, and applications, to a virtual environment. Using MAP, you now can determine which servers you can upgrade to Windows Server 2012, which servers you can migrate to virtual machines on Hyper-V in Windows Server 2008, and which client computers you can upgrade to Windows 10. MAP is the primary tool to help you identify which applications, desktops, and servers would make ideal candidates for virtualization.



Note: As the time of writing this Module, Microsoft last release of MAP is version 9.3, which does not include Windows Server 2016.

The included operating systems are: Windows 10, Windows 8.1, Windows 8, Windows 7 Service Pack 1, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2 SP1

A new version of MAP will be released after the general release of Windows Server 2016.

You can use MAP to perform the following key functions:

- Hardware inventory. MAP uses a secure process, which does not utilize an agent, to collect and organize system resources and device information across your network from a single networked computer. Some of the examples of the information that MAP returns include operating system information, system memory details, installed drivers, and installed applications. MAP saves this information in a local database, and then uses it to provide you with specific reports and recommendations.
- MAP uses technologies that are already available in your IT environment to perform inventory and assessments. These technologies include Windows Management Instrumentation (WMI), the Remote Registry service, Simple Network Management Protocol (SNMP), AD DS, and the Computer Browser service.

You can use MAP to inventory the following operating systems and applications:

- Windows 10
- Windows 8 and 8.1
- Windows 7
- Windows Vista
- Microsoft Office 2010 and newer Office versions
- Windows Server 2012
- Windows Server 2008 or Windows Server 2008 R2
- Windows Internet Explorer 9 and older versions
- Hyper-V

- Microsoft Skype for Business
- System Center Configuration Manager
- System Center Endpoint Protection
- SQL Server
- VMware vSphere
- VMware vCenter
- VMware ESX
- VMware ESXi
- VMware Server
- Select Linux distributions
- LAMP application stack discovery
- MySQL
- Oracle
- Sybase
- Data analysis. MAP performs a detailed analysis of hardware and device compatibility for migration to:
  - Windows 10
  - Windows 8
  - Windows 7
  - Windows Server 2012
  - Windows Server 2008 R2
  - SQL Server 2012
  - SQL Server 2008 R2
  - Microsoft Office 2010
  - Office 365
- Readiness reporting. MAP generates reports containing both summary and detailed assessment results for each migration scenario. MAP provides these results in Microsoft Excel and Microsoft Word documents. Readiness reports are available for many technologies including Windows 10.
- MAP also helps to gather performance metrics and generates server consolidation recommendations. These recommendations identify the candidates for server virtualization, and makes suggestions for how you might place the physical servers in a virtualized environment.

Infrastructure Planning and Design guides

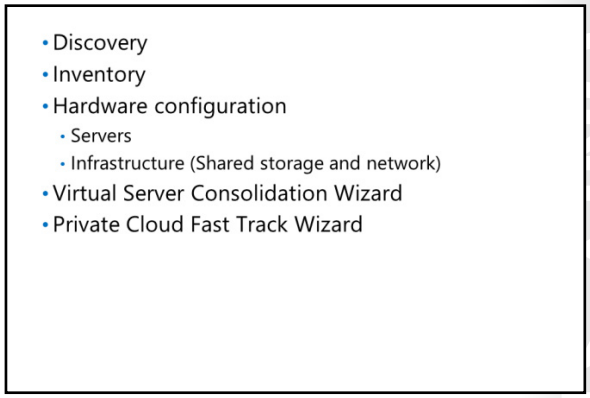
The Infrastructure Planning and Design guides are free guides that describe architectural considerations, and streamline the design processes for planning Microsoft infrastructure technologies. Each guide addresses a unique infrastructure technology or scenario, including server virtualization, application virtualization, and Remote Desktop Services implementations.

Windows Server Virtualization guide

The Windows Server Virtualization guide focuses on an earlier version of Hyper-V. However, it still provides guidance on how to plan and implement server virtualization on Hyper-V.

Assessment features of the MAP toolkit

Microsoft provides MAP as the primary tool for server virtualization planning. It is easy to install and it guides administrators through evaluation by making use of built-in wizards, configurations, and reports.



Gathering information over time is one evaluation factor. You might already have evaluation data suitable for inclusion. For example, if you use Operations Manager to monitor your physical servers and virtual machines, your inventory and performance data might already be collected. You could use these Operations Manager reports to gather useful information. When you want to plan for capacity and growth, you can use Data Protection Manager (DPM) to review data trends by running capacity reports. The following section summarizes MAP features that you can use for server virtualization assessments.

MAP Discovery

MAP can discover Windows, Linux, UNIX, and VMware servers, computers, and virtual machines. It has the following discovery methods and requirements for creating an inventory:

- AD DS. Requires domain credentials. You can use this method to discover all computers in all domains, or in specified domains, containers, and organization units.
- Windows networking protocols, using the WIN32 LAN Manager application programming interface (API). Requires the Computer Browser service to be running on the computer, or the server running MAP. You can use this method to discover Windows workgroups and Windows NT 4.0 domains.
- Configuration Manager. MAP can use either Configuration Manager or Microsoft Systems Management Server (an older version of Configuration Manager), for discovery. For discovery, you require the primary site server name and appropriate credentials for Configuration Manager or Systems Management Server.
- IP Address Range. You can scan for computer and servers using one or more IP address ranges, up to a maximum of 100,000 addresses.
- NetBIOS names. You also can discover computers and servers by entering their NetBIOS names manually, or by importing the names from a text file.

MAP Performance Metrics

After you have an inventory of discovered hardware, you can collect performance metrics for your assessment. To gather performance metrics, you must run the **Performance Metrics Wizard**. You can collect metrics for Windows and Linux-based machines by using WMI or Secure Shell. The minimum collection period is 30 minutes. You are prompted to schedule an end date and time for when the collection should stop.

Note: If required, you can use the **Performance Metrics Wizard** to collect additional metrics. You must choose to either discard previous metrics or append the new ones to existing data.

While the performance metric data collection is running, you might not be able to perform other tasks with MAP.

MAP Hardware Configuration

MAP hardware configuration provides you with details for the proposed hardware that you should use for your virtualization host servers. When you run the **Hardware Library Wizard**, you can enter the resources such as the number and type of processors, amount of RAM, and storage capacity. After configuring these hardware parameters, you can determine the number of host servers required. If required, you also can create a configuration for shared storage and network configurations, which will help ensure that you plan clusters and share components correctly.

MAP Server Consolidation

The **MAP Server Virtualization and Consolidation Wizard** can help provide planning guidance for the following versions of Hyper-V:

- Window Server 2012 Hyper-V
- Window Server 2008 R2 Service Pack 1 (SP1) Hyper-V
- Window Server 2008 R2 Hyper-V
- Window Server 2008 Hyper-V

To use the wizard, you must first complete an inventory, gather performance metrics, and input the hardware configuration. When you run the wizard, you can select a utilization ceiling on the proposed hardware, which allows for periodic spikes in utilization. The utilization settings include processor, memory, storage capacity, storage I/O operations per second, and network throughput. Upon completing this wizard, MAP will provide you with the recommended number of hosts.

MAP Private Cloud Fast Track

The **MAP Private Cloud Fast Track Wizard** provides guidance based upon a program that is a joint effort between Microsoft and its hardware partners. The goal of the program is to help organizations decrease the time, complexity, and risk of implementing private clouds.

Demonstration: Assessing the computing environment by using the MAP toolkit

In this demonstration, you will see how to use MAP for planning server virtualization, including:

- Use MAP to collect inventory data.
- Use MAP to collect performance data.
- Create a hardware configuration.
- Review the collected data.

Demonstration Steps

Use MAP to collect inventory data

1. On **LON-CL1**, open **Microsoft Assessment and Planning and Toolkit**.
2. In **MAP**, on the **Data source** page, in the **Create or select a database** section in the **Name** text box, type **Demo**, and then click **OK**.
3. Click **Server Virtualization**, and then click **Collect inventory data**.
4. In the **Inventory and Assessment Wizard**, on the **Inventory Scenarios** page, select both **Windows computers** and **Use Active Directory Domain Services (AD DS)**.
5. On the **Active Directory Credentials** page, use the following credentials:
   - Domain: **Adatum**
   - Account name: **administrator**
   - Password: **Pa$$w0rd**
6. On the **Active Directory Options** page, ensure that **Find all computers in all domains, containers, and organizational units** is selected, and then click **Next**.
7. On the **All Computer Credentials** page, use the following credentials:
   - Domain: **Adatum**
   - Account name: **administrator**
   - Password: **Pa$$w0rd**
8. Complete the wizard.
9. When the **Inventory and Assessment** page opens, review the results of the data collection, wait for the assessment to show as complete, and then close the page.

Use MAP to collect performance data

1. Run the **Performance Metrics Wizard**.
2. In the wizard, select all computers.
3. On the **All Computer Credential** page, ensure that the **adatum\administrator account** is selected.
4. Review the details on the metrics page, and then close the window.

Create a hardware configuration

Before you can work with MAP features, you must first cancel the running process that was initiated in the previous step.

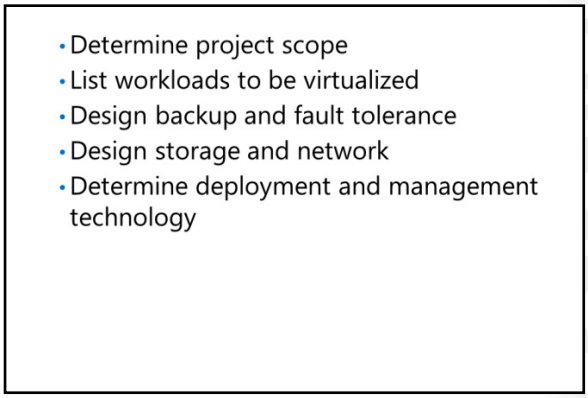
1. At the bottom left of the MAP console screen, in the running task drop-down list box, click **Cancel processing**, and then click **Yes**.
2. Under the **Steps to complete** section, click **Create hardware configuration**.
3. On the **Choose Scenarios** page, click **General Server Consolidation/Desktop Virtualization**, and then click **Next**.
4. On the **Hardware Configuration** page, click **Create New**, and in the **Create New** text box, type **Server-Type1**.
5. Complete the wizard using approximate values based on a server that you might use.

Review the collected data

1. On the **MAP** console, in the console tree, select **Server Virtualization**.
2. In the details pane, select **Hardware Library**.
3. Review the **Configurations** collected. When done, go back to the main **MAP** console.
4. Note that you could also run the **Server Consolidation** and **Private Cloud Fast Track** wizards, which, due to time constraints, will not be done.

Designing a solution for server virtualization

Many organizations that adopt server virtualization develop a server implementation policy to virtualize all new and replaced systems. These organizations opt for deploying physical hardware as an alternative to virtualization only when a valid reason exists, such as when custom server hardware is incompatible with server virtualization, or when a server application vendor does not support their application on virtualized servers.



You now can use Windows Server 2012 R2 to deploy servers with up to 320 logical processors and 4 terabytes (TB) of system memory. This, in turn, allows new capabilities for virtual workloads and is a significant improvement over earlier hypervisors.

Implementing a new virtualization solution can often include assessing physical and virtual servers, or assessing an existing virtualization solution. A new virtualization solution can provide an opportunity to consolidate physical servers, and in an existing server virtualization solution, it can improve virtual machine density per host, possibly by virtualizing some more demanding workloads.

As a general guideline, each virtualization project should include the following steps:

1. Determine the virtualization scope. The first step in planning a virtualization solution is to define the project's scope. You could have one or more projects, each working to address different parts of an overall server virtualization strategy. To ensure that a project is successful, you need to define scope, milestones, and goals.
2. Determine the workloads. Create a list of potential workloads that you want to virtualize, identify the workloads that cannot be virtualized, then use MAP to discover and inventory all the remaining servers. Collect the performance metrics of the required servers for a suitable period of time.
3. Determine the backup and fault-tolerance requirements for each workload. You use these requirements when designing the virtual server deployment. For example, some server workloads might require frequent and consistent backup of data located inside the virtual machine, while other server workloads might require just a virtual machine-level or configuration information backup. You use the fault-tolerance requirements for the server workload when you deploy clustered virtual machines, or to provide another method for ensuring high availability for the virtual machine.

4. Use MAP to aid in the design of the virtualization hosts. Use the hardware configurations and the **MAP Server Virtualization and Consolidation Wizard** to assist in the design of the host server infrastructure. As a best practice, to simplify host server management you should consider creating a standard design for all virtualization hosts. Decide if you will require a maintenance host. As part of the host server design, you also need to consider the number of virtual machines that each host computer will be running.
5. Map workloads to hosts. After designing the host server hardware, you can start mapping the virtual machines to the host servers. There are many factors that you need to consider during this design, including:
    - Host server capacity. How many virtual machines can you place on a host?
    - Reserve capacity. How much of a resource buffer do you want to implement on each host computer?
    - Virtual machine performance characteristics and resource utilization. Can you characterize the network, CPU, disk, and memory utilization for each of the virtual machines on a host? You might choose to deploy virtual machines with different resource requirements on the same host.
6. Design host backup and fault tolerance. Use the information that you collected on the backup and fault tolerance requirements for the virtual machines to design a backup and high availability solution for the host computers.
7. Determine storage requirements. As part of the server workload discovery, you should have documented the storage requirements for each virtual machine. Before moving the server workloads to virtual machines, ensure that you have space for both the operating system virtual hard disks and the data associated with each virtual machine. You also need to include storage availability and performance requirements. You can use the MAP share infrastructure configuration to assist in determining your storage requirements.
8. Determine network requirements. As a final step in the virtual machine design process, you also should plan the network design. When planning your network design, you should consider a number of factors:
    - What type of network access do the virtual machines require? Most virtual machines likely will require access to the physical network, but some virtual machines might only need to communicate with other virtual machines on the same host computer.
    - How much network bandwidth does each virtual machine require?
    - What are the network reliability requirements for each virtual machine?
    - Will network virtualization be used?

 **Note:** A successful virtualization project is a well-documented project. Often, when adopting a new virtualization technology, a proof of concept (POC) can be of great help in determining the final infrastructure. A POC can also help bring staff up to speed on the deployment and management technologies that will be used in the final solution.

Question: You are the IT manager for the Adatum company. Your organization server infrastructure consists of multiple datacenters connected to each other through a Multiprotocol Label Switching (MPLS) network. Over the previous decade, the company has made several different server purchases, and recently added Hyper-V servers with virtual servers running various server roles. The CIO has decided that it is time for a datacenter hardware update. You have been asked to develop a cost-effective plan to upgrade or replace all the older systems to Hyper-V capable servers. As part of the planning phase, you have been gathering comments from the various datacenter administrators about the environment. You are seeing frequent complaints about performance. How could you use the MAP toolkit to assist with the migration planning, and to explore and assess the complaints, and address performance issues, as necessary?

Lab: Using MDT to deploy Windows Server 2016

Scenario

A. Datum Corporation is a global engineering and manufacturing company with a head office based in London, UK. An IT office and datacenter are located in London to support the London location and other locations. A. Datum has recently deployed a Windows Server 2016 server and client infrastructure.

As the datacenter has grown, it has become apparent that there can be significant time savings if server deployment is automated by using customized images rather than manually installing each server. You decided to implement an automation process for deploying servers using MDT.

Objectives

After completing this lab, you will be able to:

- Configure MDT 2013 Update 2.
- Create and deploy server images by using MDT.

Lab Setup

Estimated Time: 45 minutes

Virtual machines: **20740A-LON-DC1**, **20740A-LON-SVR1**, **20740A-LON-SVR6**

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 **20740A-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: **Administrator**
    - Password: **Pa$$w0rd**
    - Domain: **Adatum**
5. Repeat steps 2 through 4 for **20740A-LON-SVR1**. Do not start **20740A-LON-SVR6** until directed to do so in the lab.

Exercise 1: Configuring MDT

Scenario

To make more rapid deployments of custom images in the A. Datum Corporation datacenters, you have been given the task of testing the MDT 2013 Update 2. Your first step for the Windows Server 2016 deployment is to configure MDT before you can begin testing.

The main task for this exercise is as follows:

1. Configure the deployment share.

▶ Task 1: Configure the deployment share

1. On **LON-SVR1**, from the Start screen, open the **Deployment Workbench**.
2. Right-click **Deployment Shares**, and then click **New Deployment Share**.
3. On drive C, create a **DeploymentShare**.
4. Complete the **New Deployment Share Wizard** with default settings.

Results: After completing this exercise, you should have configured MDT 2013 Update 2 and the MDT Deployment Share.

Exercise 2: Creating and deploying an image

Scenario

LON-SVR6 is a new server without an operating system. You decide to test MDT 2013 Update 2 by creating a reference image of Windows Server 2016, and then deploy the image as a deployment to **LON-SVR6**, while also installing the Excel viewer application.

The main tasks for this exercise are as follows:

1. Add a reference image (Windows Server 2016).
2. Add an application to the image.
3. Create the deployment task sequence.
4. Deploy the Image to LON-SVR6.
5. Prepare for the next module.

▶ Task 1: Add a reference image (Windows Server 2016)

1. On **LON-SVR1**, insert the **D:\Program Files\Microsoft Learning\20740\Drives \WinServer2016_TP5.ISO** into the virtual machine's virtual hard drive.
2. From the **Operating System** folder, click **Import an Operating System**.
3. Use the **Import Operating System Wizard** to import source files from the **D:** drive, into a **Destination directory name**, named **WindowsServer2016**.
4. Complete the **Import Operating System Wizard** using default selections.

▶ Task 2: Add an application to the image

1. In the **Deployment Workbench** console on **LON-SVR1**, use **the New Application Wizard** to add the **ExcelViewer** application, with the following settings:
   - **Application with source files**
   - Publisher: **Microsoft**
   - Application name: **ExcelViewer**
   - Source directory: **E:\Labfiles\Mod11**

- Destination directory: **ExcelViewer**
- Command line: **ExcelViewer.exe /quiet /norestart**

2. Complete all other steps in the **New Application Wizard** with the page defaults.

▶ Task 3: Create the deployment task sequence

1. Create a **New Task Sequence** in the **Task Sequence** node of the **Deployment Workbench** with the following properties:
   - Task sequence ID: **11-01**
   - Task sequence name: **Lab 11-01**
   - Task sequence comments: **Windows Server 2016 Deployment to LON-SVR6 task sequence for Module 11 lab**
   - Select Template: **Standard Server Task Sequence**
   - Select OS Operating System: **Windows Server 2016 Technical Preview 5 SERVERDATACENTER in WindowsServer 2016x64 install.wim**
   - **Do not specify a product key at this time**
   - OS Settings Full name: **Administrator**
   - Organization: **A. Datum Corporation**
   - Admin Password: **Pa$$w0rd**
   - All other settings use default values.
2. Open the **Lab 11-01** task sequence properties, and in the **Task Sequence** tab of the properties page, select the **State Restore** node, and in the **Install Application** node, install the **Microsoft ExcelViewer** application as a single application.
3. Update the **Deployment Share** using default settings. The update should take around 20 minutes to complete.
4. In the **MDT Deployment Share (C:\DeploymentShare)** node properties, enable **Monitoring**.

▶ Task 4: Deploy the Image to LON-SVR6

1. Open **20740A-LON-SVR6 on HOST –Virtual Machine Connection**, and in the **Media** menu item, and from the **D:\Program Files\Microsoft Learning\20740\Drives** folder, add the **LiteTouchPE_x64.iso** file as a DVD.
2. Start **20740A-LON-SVR6**.
3. Complete the **Microsoft Deployment Toolkit** wizard with the following values:
   - **Run the Deployment Wizard to install a new Operating system**
   - User Credentials Name: **Administrator**
   - User Credentials Password: **Pa$$w0rd**
   - **Lab 11-01** task sequence
   - Computer name: **LON-SVR6**
   - **Join a domain**

- Domain name: **Adatum.com**
- **Do not enable BitLocker for this computer**
- All other settings use default values.

4. To monitor the progress of the deployment task, on **LON-SVR1**, in the **Deployment Workbench**, select and refresh the **Monitoring** node under the **MDT Deployment Share** main node in the console tree.
5. On **LON-SVR6**, when the **Product Key** page appears, click the **Do this later** hyperlink.
6. After a time, the **Installation Progress** window will appear, and then the **Installing Microsoft Excel Viewer** window will appear under it.
7. When finished, observe the information on the **Deployment Summary** page, and then close it.
8. In **Server Manager** on **LON-SVR6**, observe the values on the **Local server** page, and then confirm they are correct.
9. View the **Start** menu, **All Apps**, and confirm **Microsoft Office Excel Viewer** appears in the list.
10. Close all open windows and sign out of all virtual machines.

Results: After completing this exercise, you should have used MDT 2013 Update 2 to deploy Windows Server 2016 to **LON-SVR6**, and then you should have tested the deployment of an application.

▶ Task 5: Prepare for the next module

After 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 **20740A-LON-DC1**, and then click **Revert**.
3. In the **Revert Virtual Machine** dialog box, click **Revert**.
4. Repeat steps 2 and 3 for **20740A-LON-SVR1** and **20740A-LON-SVR6**.

Question: In the lab, you used the **Monitoring** node to observe the deployment task sequence status. What should you do if there no values in the **Monitoring** node's detail pane?

Question: When you added the Install.win source files, four separate wim files appeared. Why?

Module Review and Takeaways

Review Question

Question: What could you do to bypass having to enter credentials to connect to the deployment share?

Best Practices

- Build your reference system by using a virtual machine. This will avoid having an image with any hardware-specific configurations embedded.
- Create folders in the **Out-of-Box-Drivers** node to organize all your vendor or model-specific drivers.
- Use **Profile Selections** to deploy only the required drivers to a given hardware configuration
- Build thin images and apply applications on demand through the applications node. This will allow you to keep the application current as updates and patches are released, without having to rebuild the image.

Common Issues and Troubleshooting Tips

Common Issue	Troubleshooting Tip
Mismatch between versions of MDT and Windows AIK or Windows ADK.	
Cannot find lite-touch boot media in the Boot folder of the Deployment Share.	
In MAP, when you click on most operations, you receive a warning that states, "The task processor is currently busy. You cannot perform this operation while the task processor is running. Please wait for the task processor to complete or cancel the task process before retrying this operation."	

Real-world Issues and Scenarios

Best Practice

When working with the MAP toolkit, consider backing up your database regularly. If you are running assessments over a long period, the data could become critical to the timeframe of your project.

Module 12

Managing, monitoring, and maintaining virtual machine installations

Contents:

Module Overview

Windows Server Update Services (WSUS) improves security by applying updates to Microsoft products and third-party products in a timely way. It provides the infrastructure to download, test, and approve security updates. Applying security updates quickly helps prevent security incidents resulting from known vulnerabilities. While implementing WSUS, you must keep in mind the WSUS hardware and software requirements, the settings to configure, and the updates to approve or remove according to your organization's needs.

Monitoring and troubleshooting processes are very important because they allow administrators to provide performance-optimized IT infrastructures. Monitoring processes can improve your ability to identify, troubleshoot, and repair issues before end users experience them. By designing a comprehensive monitoring solution for your organization, you can reduce end-user problems and prevent potentially serious issues.

When a system failure or an event that affects system performance occurs, you must be able to repair the problem or resolve the issue quickly and efficiently. With so many variables and components in the modern network environment, the ability to determine the root cause quickly often depends on having an effective performance-monitoring methodology and toolset. You can use performance-monitoring tools to identify components that require additional tuning and troubleshooting. By identifying components that require additional tuning, you can improve the efficiency of your servers.

After you deploy the Windows Server 2016 operating system in your environment, you must make sure that it continues to run efficiently by maintaining a stable environment. This module describes how to monitor and troubleshoot a Windows Server 2016 environment.

Objectives

After completing this module, you will be able to:

- Describe the purpose of Windows Server Update Services (WSUS) and the requirements to implement WSUS.
- Manage the update process with WSUS.
- Describe the purpose and benefits of Windows PowerShell Desired State Configuration (DSC).
- Describe the monitoring tools available in Windows Server 2016.
- Use Performance Monitor.
- Manage event logs.

Lesson 1
WSUS overview and deployment options

The WSUS role provides a central management point for updates to your computers running the Microsoft Windows operating system. By using WSUS, you can create a more efficient update environment in your organization, and stay better informed of the overall update status of the computers on your network. This lesson introduces you to WSUS, and describes the key features of the WSUS server role.

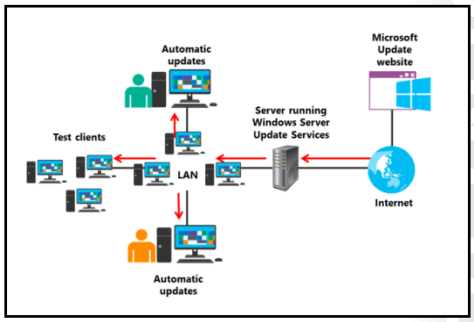
Lesson Objectives

After completing this lesson, you will be able to:

- Describe WSUS.
- Describe the WSUS server deployment options
- Explain the WSUS update management process.
- Identify the server requirements for WSUS.
- Describe how to configure clients to use WSUS.

What is WSUS?

WSUS is a server role included in the Windows Server 2016 operating system that downloads and distributes updates to Windows clients and servers. WSUS can obtain updates that are applicable to the operating system and common Microsoft products such as Microsoft Office Standard 2016 and Microsoft SQL Server.



In the simplest configuration, a small organization can have a single WSUS server that downloads updates from Microsoft Update. The WSUS server then distributes the updates to computers that are configured to obtain automatic updates from the WSUS server. You must approve the updates before clients can download them.

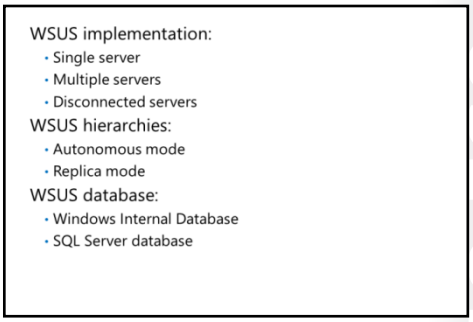
Larger organizations can create a hierarchy of WSUS servers. In this scenario, a single centralized WSUS server obtains updates from Microsoft Update, and other WSUS servers obtain updates from the centralized WSUS server.

You can organize computers into groups to simplify the approval of updates. For example, you can configure a pilot group to be the first set of computers that are used for testing updates.

WSUS can generate reports to help monitor update installation. These reports can identify which computers have not recently applied the approved updates. Based on these reports, you can investigate why updates are not being applied.

WSUS server deployment options

Before installing and configuring WSUS servers, you must consider how to deploy WSUS in your environment. WSUS implementations vary in size and configuration depending on your network environment and how you want to manage updates. You can have a single WSUS server for your entire organization, multiple WSUS servers acting independently, or multiple WSUS servers connected to each other in a hierarchy.



Single WSUS server

The most basic implementation of WSUS uses a single WSUS server, inside your network, connecting to Microsoft Update to download updates through a firewall. In some scenarios there might be a proxy server between the WSUS server and the Internet. In this scenario, the WSUS server uses port 8530 for HTTP communication, and port 8531 for HTTPS. You need to make sure that your firewall has the rules needed to allow the server to connect to Microsoft Update. This basic scenario is commonly used for small networks, with a single physical location.

Multiple WSUS servers

If your environment is composed of several isolated physical locations, you might need to implement a WSUS server in each location. When you implement a WSUS server in each location, you can manage each individual server independently. You can think of this scenario as a single WSUS server per physical location. Although this is a valid option, it requires substantially more administrative effort, especially as the number of physical locations grows. You must download updates to each server separately, approve updates on each server individually, and manage WSUS clients so that they receive updates from the correct WSUS server. In this scenario, each WSUS server has its own connection to the Internet to download updates from Microsoft Update.

You can have individual WSUS servers for organizations that have a small number of physical locations, where each physical location has its own IT management team. You can also use this scenario for a single physical location that has too many clients to for a single WSUS server to manage, and place the WSUS servers in a Network Load Balancing (NLB) cluster.

Additional Reading: For more information about capacity requirements for WSUS servers, refer to: "Determine Capacity Requirements" at: http://aka.ms/qbj2o8

Disconnected WSUS servers

A disconnected WSUS server is a server that does not connect to Microsoft Update over the Internet or receive its updates from any other server in the network. Instead, this server receives its updates from removable media generated on another WSUS server.

A disconnected WSUS server is commonly used in remote environments where Internet connectivity is either limited or extremely expensive. You can use a WSUS server in a different location to synchronize with Microsoft Update, export the updates to portable media, and then ship the portable media to the remote location to be imported into the disconnected WSUS server.

WSUS server hierarchies

All the scenarios mentioned above deal with an independently managed WSUS server that connects directly to Microsoft Update or receives its updates in a disconnected manner. However, in larger organizations with multiple physical locations, you might want to have the ability to synchronize with Microsoft Update on one server. You might also want to push the updates to servers in different locations over your network, and approve updates from a single location.

WSUS server hierarchies allow you to:

- Download updates to servers that are closer to clients, such as servers in branch offices.
- Download updates once, to a single server, and then replicate the updates over your network to other servers.
- Separate WSUS servers based on the language their clients use.
- Scale WSUS for a large organization that has more client computers than a single WSUS server can manage.

In a WSUS server hierarchy, there are two types of servers:

- Upstream servers. Upstream servers connect directly to Microsoft Update to retrieve updates, or are disconnected and receive updates by using portable media.
- Downstream servers. Downstream servers receive updates from a WSUS upstream server.

Downstream servers can be configured in two modes:

- Autonomous mode. Autonomous mode, or distributed administration, allows a downstream server to retrieve updates from an upstream server, but maintain administration of the updates locally. In this scenario, the downstream server maintains its own set of computer groups, and updates can be approved independent of the approval settings in the upstream servers. This allows a different group of administrators to manage updates at their locations, and only use the upstream server as a source of download updates.
- Replica mode. Replica mode, or centralized administration, allows a downstream server to receive updates, computer group membership information, and approvals from an upstream server. In this scenario, a single group of administrators is able to manage updates for the entire organization. In addition, downstream servers can be placed in different physical offices and receive all updates and management data from an upstream server.

You can have multiple layers in your WSUS hierarchy and configure some of your downstream servers to use the autonomous mode, while you use replica mode to configure other servers. For instance, you can have a single upstream server connected to Microsoft Update downloading updates for your entire organization. Then you can have two downstream servers in autonomous mode, one that manages updates for all computers running software in English, and another for all computers running software in Spanish. Finally, you can have another set of downstream servers receiving their updates from the middle-tier WSUS servers, configured in replica mode. These are the actual servers that clients receive updates from, but all the management is done at the middle tier.

 **Note:** You can configure downstream servers to download update information, or metadata, from an upstream server, but to download the actual updates from Microsoft Update. This is a common configuration when the downstream servers have good Internet connectivity and you want to reduce wide area network (WAN) traffic.

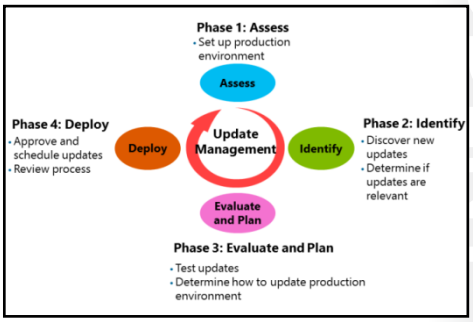
WSUS database

WSUS stores information about updates, computer groups, and approvals in a database. WSUS can use two types of databases:

- Windows Internal Database (WID). This is the default setting for a WSUS database. When you deploy WSUS by using a WID, a file named SUSDB.mdf is created to store the data used by WSUS in the %windir%\wid\data folder. We recommend this scenario for:
  - Environments with a single WSUS server that do not require NLB.
  - Environments with multiple independent WSUS servers in different physical locations.
- SQL Server database. If SQL Server is available in your environment, you can use it to store the data used by WSUS. You can use SQL Server tools to access the WSUS database directly for database management and reports purposes. SQL Server is also necessary for the following scenarios:
  - Environments that require a WSUS NLB cluster.
  - Environments that require database administrators (DBAs) to manage all databases that the organization uses.

The WSUS update management process

The update management process enables you to manage and maintain WSUS and the updates WSUS retrieves. This process is a continuous cycle during which you can reassess and adjust the WSUS deployment to meet the changing needs. The four phases in the update management process are:



- Assess
- Identify
- Evaluate and plan
- Deploy

The assess phase

The goal of the assess phase is to set up a production environment that supports update management for routine and emergency scenarios. The assess phase is an ongoing process that you use to determine the most efficient topology for scaling the WSUS components. As your organization changes, you might need to add more WSUS servers in different locations.

The identify phase

During the identify phase, you identify new updates that are available and determine whether they are relevant to your organization. You have the option to configure WSUS to retrieve all updates automatically, or to retrieve only specific types of updates. WSUS also identifies which updates are relevant to the registered computers.

The evaluate-and-plan phase

After relevant updates have been identified, you need to evaluate whether they work properly in your environment. It is always possible that the specific combination of software in your environment might have problems with an update.

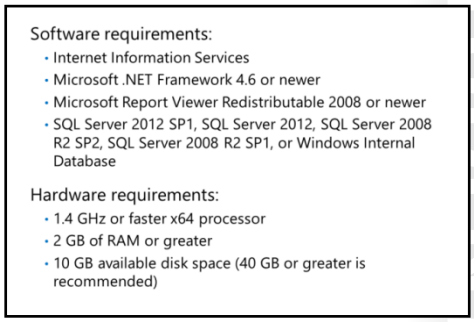
To evaluate updates, you should have a test environment in which you can apply updates to verify proper functionality. During this time, you might identify dependencies that are required for an update to function properly, and you can plan any changes that you need to make. You can achieve this if you use one or more computer groups for testing purposes. For instance, you might have a computer group with client computers that run all the operating systems and applications that are updated by using WSUS. You can use another computer group for servers that run the different applications and operating systems that are updated by WSUS. Before you deploy updates to the entire organization, you can push updates to these computer groups, test them, and, after making sure they work as expected, deploy these updates to the organization.

The deploy phase

After you have thoroughly tested an update and determined any dependencies, you can approve the update for deployment in the production network. Ideally, you should approve the update for a pilot group of computers before approving the update for the entire organization. You can also configure WSUS to use automatic updates. Automatic updates are discussed in the next lesson.

Server requirements for WSUS

You can use Server Manager to install and configure the WSUS server role. However, to be able to implement WSUS, your server must meet some minimum hardware and software requirements.



The following software is required for WSUS on Windows Server 2016:

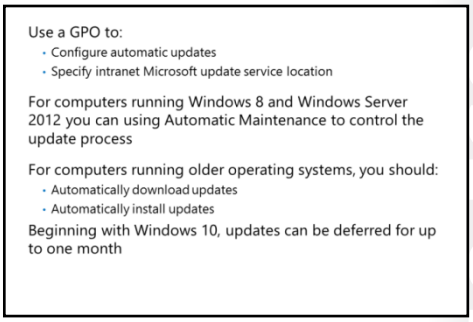
- Internet Information Services (IIS), installed automatically if not previously installed.
- Microsoft .NET Framework 4.6 or newer, installed automatically if not previously installed.
- Microsoft Report Viewer Redistributable 2008 or newer, installed automatically if not previously installed.
- SQL Server 2012 with SP1, SQL Server 2012, SQL Server 2008 R2 SP2, SQL Server 2008 R2 SP1, or Windows Internal Database (WID).

The minimum hardware requirements for WSUS are approximately the same as the minimum hardware requirements for Windows Server operating systems. However, you must consider disk space as part of your deployment. A WSUS server requires approximately 10 gigabytes (GB) of disk space, and you should allocate at least 40 GB of disk space for the downloaded updates. A WSUS server should also have a 1.4-gigahertz (GHz) or faster x64 processor and at least 2 GB of random access memory (RAM).

A single WSUS server can support thousands of clients. For example, a single WSUS server with 4 GB of RAM and dual quad-core CPUs can support up to 100,000 clients. However, in most cases, an organization with that many clients likely will have multiple WSUS servers to reduce the load on WAN links.

Configuring clients to use WSUS

You can configure computers to use a WSUS server instead of defaulting to Microsoft Update if you use a Group Policy Object (GPO) or if you manually change the settings of each individual computer. We recommend using a GPO because it is the easiest way to configure clients. To create a GPO that configures computers to use a WSUS server, follow these steps:



1. Open **Server Manager** on a domain controller, and from the **Tools** menu, click **Group Policy Manager**.
2. In the **Group Policy Manager** window, in the navigation pane, expand your forest, then right-click your domain, and then click **Create a GPO in this domain, and Link it here...**.

   Note: Depending on your WSUS environment, you might need to create different GPOs for different sites, instead of a single GPO for the entire domain.

3. In the **New GPO** dialog box, in the **Name** text box, type a name for your GPO, and then click **OK**.
4. Right-click the GPO you just created, and then click **Edit**.
5. In **Group Policy Management Editor**, expand **Computer Configuration / Policies / Administrative Templates / Windows Components / Windows Update**.
6. In the details pane, double-click **Configure Automatic Updates**.
7. In the **Configure Automatic Updates** dialog box, select **Enabled**.
8. Select one of the following options:
   - **2 – Notify for download and notify for install.**
   - **3 - Auto download and notify for install.**
   - **4 – Auto download and schedule the install.**
   - **5 – Allow local admin to choose setting.**
9. If you choose option 4, you can select a simple schedule by specifying the installation day and scheduled install time. The default is every day at 3:00 AM. After specifying the **Automatic Updates** settings click **OK**.
10. In the details pane, double-click **Specify intranet Microsoft update service location**.
11. In the **Specify intranet Microsoft update service location** dialog box, select **Enabled**.
12. In the **Set the intranet update service for detecting updates** text box, type the URL for the WSUS server, followed by the port you want to use. For instance, if the server is named **LON-SVR1** and you are using HTTP, the URL would be **http://LON-SVR1:8530**.
13. In the **Set the Intranet statistics server** text box, type the URL of the WSUS server as specified in step 9 above, and then click **OK**.
14. Close the Group Policy Editor.

After Windows Update is configured on the WSUS clients, the Windows update agent service will run continuously on the clients. The agent is responsible for retrieving updates from WSUS and deploying those updates.

Scheduling Windows updates

Microsoft introduced a feature in Windows 8 and Windows Server 2012 named Automatic Maintenance. Automatic Maintenance reduces the usage of system resources because it eliminates the need for the Windows Update Agent to run constantly in the background. Instead, Automatic Maintenance uses a scheduled task that runs nightly by default. Automatic Maintenance performs several maintenance activities, such as performing hard drive defragmentation, running antivirus scans, and installing updates.

Note: To take advantage of the Automatic Maintenance feature in Windows 8 and Windows Server 2012 and newer operating systems, configure your GPO using the **4 – Auto download and schedule the install** and then select the **Install during automatic maintenance** check box in the **Configure Automatic Updates** setting.

When you use Automatic Maintenance, the scheduled task runs nightly and downloads all updates available to the client, along with any deadlines set for the computer. All updates are then offered to the end user. If a deadline is set, and the automatic maintenance task is not scheduled to run, the Windows Update Agent will be scheduled to run at the time of the deadline to ensure the update is installed.

Deferring Windows updates

Beginning with Windows 10 and Windows Server 2016 you can choose to delay updates for up to one month. Use the **Computer Configuration / Policies / Administrative Templates / Windows Components / Windows Update / Defer Upgrades and Updates** setting to configure update deferment.

Question: What are some benefits of using WSUS to manage Windows updates?

Lesson 2
Update management process with WSUS

This lesson explains the specifics of deploying updates with WSUS to client computers. Deploying updates to Windows Update clients through WSUS can provide numerous benefits. You can configure updates to be downloaded, approved, and installed automatically, without an administrator's input. Alternatively, you can exercise more control over the update process and provide a controlled environment in which to deploy updates. You can perform testing on an isolated test computer group before approving an update for deployment in your entire organization.

Lesson Objectives

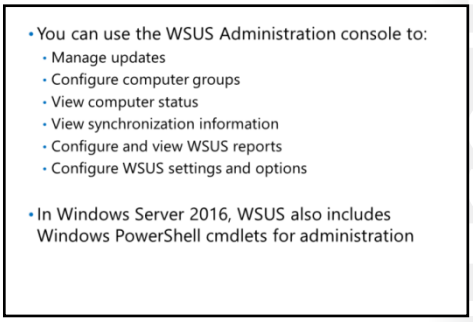
After completing this lesson, you will be able to:

- Explain how to administer WSUS.
- Identify computer groups in WSUS.
- Describe the options for approving WSUS updates.
- Describe how to configure the Automatic Updates feature to use WSUS.
- Deploy updates by using WSUS.
- View WSUS reports.
- Troubleshoot WSUS.

WSUS administration

The WSUS administration console is a Microsoft Management Console (MMC) snap-in that you can use to administer WSUS. You can use this tool to:

- Identify and download updates.
- Approve updates for deployment.
- Organize computers into groups.
- Review the update status of computers.
- Generate reports.



Monitoring is an essential part of maintaining a service. WSUS logs health information in great detail to the event log. In addition, you can download a management pack to facilitate monitoring in Microsoft System Center 2012 - Operations Manager (Operations Manager) and newer.

Controlling updates on client computers

Client computers perform updates according to either manual configuration or, in most Active Directory Domain Services (AD DS) environments, Group Policy. In some cases, you might want to initiate the update process outside of the normal update schedule. You can use the wuauclt.exe tool to control the auto-update behavior on Windows Update client computers. The following command initiates the detection of Microsoft Updates from the Windows Update source:

```
Wuauclt.exe /detectnow
```

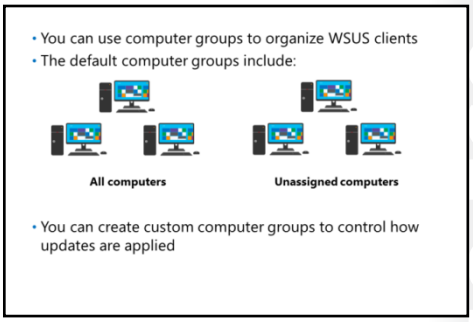
Administration with Windows PowerShell

In Windows Server 2016, WSUS includes Windows PowerShell cmdlets that you can use to manage your WSUS server. The following table lists these cmdlets.

Cmdlet	Description
Add-WsusComputer	Adds a specified client computer to a specified target group.
Add-WsusDynamicCategory	Adds a dynamic category to a WSUS server.
Approve-WsusUpdate	Approves an update to be applied to clients.
Deny-WsusUpdate	Declines the update for deployment.
Get-WsusClassification	Gets the list of all WSUS classifications currently available in the system.
Get-WsusComputer	Gets the WSUS computer object that represents the client computer.
Get-WsusDynamicCategory	Gets dynamic categories on a WSUS server.
Get-WsusProduct	Gets the list of all products currently available on WSUS by category.
Get-WsusServer	Gets the value of the WSUS update server object.
Get-WsusUpdate	Gets the WSUS update object with details about the update.
Invoke-WsusServerCleanup	Performs the process of cleanup on a specified WSUS server.
Remove-WsusDynamicCategory	Removes a dynamic category from a WSUS server.
Set-WsusClassification	Sets whether the classifications of updates that WSUS synchronizes are enabled or disabled.
Set-WsusDynamicCategory	Sets the synchronization status of a dynamic category.
Set-WsusProduct	Sets whether the product representing the category of updates that needs to be synchronized is enabled or disabled.
Set-WsusServerSynchronization	Sets whether the WSUS server synchronizes from Microsoft Update or from an upstream server, and if it uses the upstream server's properties.

What are computer groups?

Computer groups are a way to organize the computers to which a WSUS server deploys any updates. The two computer groups that exist by default are All Computers and Unassigned Computers. New computers that contact the WSUS server are assigned automatically to both of these groups.



Note: WSUS computer groups are separate from AD DS groups.

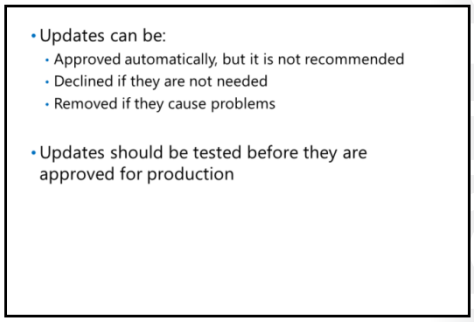
You can create custom computer groups for controlling how updates are applied. Typically, custom computer groups contain computers with similar characteristics. For example, you might create a custom computer group for each department in your organization. You can also create a custom computer group for a test lab where you first deploy updates for testing. You would also typically group servers separately from client computers.

When you manually assign new computers to a custom computer group, it is called server-side targeting. You can also use client-side targeting to assign computers to a custom computer group. To use client-side targeting, you need to configure a registry key or GPO for the computer that specifies the custom computer group to be joined, during initial registration with the WSUS server.

Server-side targeting enables administrators to manage WSUS computer group membership manually. This is useful when the AD DS structure does not support the logical client-side for computer groups, or when computers need to be moved between groups for testing or other purposes. Client-side targeting is used most commonly in large organizations where automated assignment is required and computers must be assigned to specific groups.

Approving updates

The default configuration for WSUS does not automatically approve updates for application to computers. Although it is possible to approve updates automatically, it is not recommended. The best practice for approving updates is to first test the updates in a lab environment, then test the updates in a pilot group, and only then update the production environment. This process reduces the risk of an update causing an unexpected problem in your production environment. You would perform this process by approving updates for specific groups of computers before approving the update for the All Computers group.

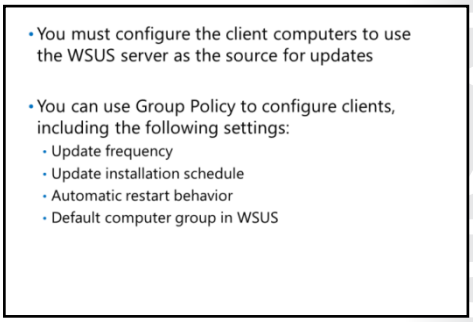


Some updates are not considered critical and do not have any security implications. You might decide not to implement some of these updates. For any updates that you decide not to implement, you can decline the update. After an update is declined, it is removed from the list of updates on the WSUS server, in the default view.

If you apply an update and find that it is causing problems, you can use WSUS to remove that update. However, the update can be removed only if that specific update supports removal. Most updates support removal.

When you look at the update's details, those details will indicate if the update is superseded by another update. Superseded updates are typically no longer required, because a newer update also includes the changes in this update. Superseded updates are not declined by default because, in some cases, they are still required. For example, the older update might be required if some servers are not running the latest service pack.

Configuring automatic updates



When you enable the Automatic Updates feature on a server, the default configuration automatically downloads updates from Microsoft Update and installs them. After you have implemented WSUS, your clients should be configured to obtain updates automatically from the WSUS server instead.

The location from which Automatic Updates obtains updates is controlled by a registry key. Although it is possible to configure the registry key manually by using the Microsoft Registry Editor (Regedit) tool, this method is not recommended except when the computer is not in a domain. If a computer is in a domain, it is much more efficient to create a GPO that configures the registry key.

For AD DS environments, Automatic Updates are typically configured in a GPO as discussed in the previous topic, "Configuring clients to use WSUS".

In addition to configuring the source for updates, you can also use a GPO to configure the following settings:

- Update frequency. This setting determines how often the updates are detected.
- Update installation schedule. This setting determines when updates are installed. When updates cannot be installed at the scheduled time, this setting also determines when updates are rescheduled.
- Automatic restart behavior. This setting determines whether the computer will restart automatically if required to do so by an update.
- Default computer group in WSUS. This setting determines the computer group in which the computer will be registered during initial registration with WSUS.

Demonstration: Deploying updates by using WSUS

In this demonstration, you will see how to:

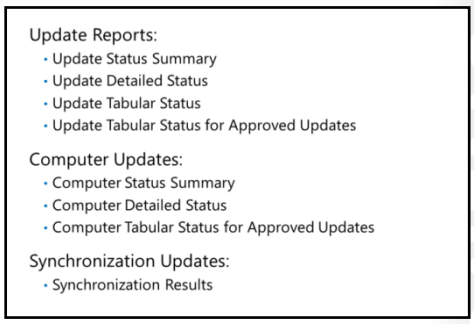
- Approve an update.
- Deploy an update.

Demonstration Steps

1. On **LON-SVR2**, open the **Windows Server Update Services** console.
2. Approve the **Update for Windows 10 Version 1511 for x64-based Systems (KB3140741)** update.

WSUS reporting

WSUS provides a series of reports that you can use to manage your WSUS environment. Reports are divided into three categories:



- Update Reports. Shows reports related to the updates available in WSUS.
  - Update Status Summary. Shows a summary of the update status.
  - Update Detailed Status. Shows details of each update status. Each page shows a single update, with a list of computers for that update.
  - Update Tabular Status. Shows a summary of update status in a tabular view.
  - Update Tabular Status for Approved Updates. Shows a summary of update status for approved updates in a tabular view.
- Computer Updates. Shows reports related to computers and computer groups managed by WSUS.
  - Computer Status Summary. Shows a summary of computer status.
  - Computer Detailed Status. Shows details of each computer status. Each page shows the updates for a single computer.
  - Computer Tabular Status. Shows a summary of computer status in a tabular view.
  - Computer Tabular Status for Approved Updates. Shows a summary of computer status for approved updates in a tabular view.
- Synchronization Updates. Shows reports related to synchronization of update data.
  - Synchronization Results. Shows the results of the last synchronization.

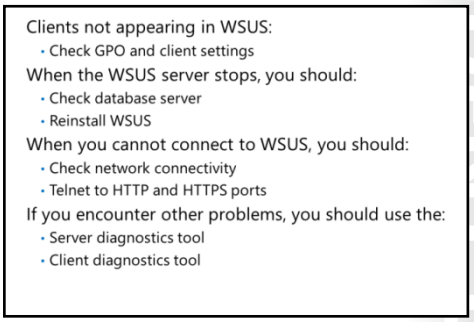
Although you will be able to see these reports in the WSUS console right after installing WSUS, the reports will not be available until you configure your server to support viewing reports. To configure your server for reporting, execute the following steps:

1. Sign in to the WSUS server by using an account that has administrative rights.
2. From **Server Manager**, click **Add roles and features**.
3. In the **Add Roles and Features Wizard** window, in the **Before you begin** page, click **Next**.
4. On the **Installation type** page, click **Next**.
5. On the **Select destination server** page, click **Next**.
6. On the **Server roles** page, click **Next**.
7. On the **Features** page, select **.NET Framework 3.5 features**, and then click **Next**.

8. On the **Confirmation** page, click **Specify alternate source path**.
9. On the **Specify Alternate Source Path** page, in the **Path** text box, type the path to the location containing the SxS files, and then click **OK**.
10. On the **Confirmation** page, click **Install**.
11. After the installation is complete, in the **Confirmation** page, click **Close**.
12. From **Server Manager**, from the **Tools** menu, click **Windows Server Update Services**.
13. In the **Update Services** window, under the navigation pane, click **Reports**.
14. In the details pane, click any report.
15. In the **Feature Unavailable** dialog box, click **Microsoft Report Viewer 2008 Redistributable**.
16. In **Internet Explorer**, click **Download**.
17. In the pop-up dialog box in Internet Explorer, click **Run**.
18. In the **Microsoft Report Viewer Redistributable 2008 SP1 Setup** dialog box, click **Next**, and then click **Finish**.

WSUS troubleshooting

After your WSUS environment is configured and in use, you might find problems that must be addressed. Some problems might be simple to handle, while others might require you to use special debugging tools. Here is a list of common problems that you might encounter when managing a WSUS environment:



- Computers do not appear in WSUS. This results from misconfiguration of the client computer, or a GPO that is not applied to the client computer.
- WSUS server stops with full database. When this happens, you will notice a SQL Server dump file (**SQLDump*nnnn*.txt**) in the Logs folder for SQL Server. This usually occurs because of index corruption in the database. You might need help from a SQL Server DBA to recreate indexes, or you might need to reinstall WSUS to fix the problem.
- You cannot connect to WSUS. Verify network connectivity. Ensure that the client can connect to the ports used by WSUS by using the Telnet client utility.
- Other problems. Consider using the server diagnostics tool and the client diagnostics tool available from Microsoft.

Additional Reading: For more information on the downloadable tools and utilities for WSUS and its components, refer to: "Windows Server Update Services Tools and Utilities" at: http://aka.ms/vz5zxz

Note: The WSUS server and WSUS client diagnostics tools are available from Microsoft as is, and are not supported tools. Make sure that you view the readme.txt file for each tool before you use them.

Note: You can use the **Get-** Windows PowerShell cmdlets to retrieve server settings and product settings, and to update settings during troubleshooting.

Question: Why would you use Group Policy to configure Windows systems to use WSUS?

Lab A: Implementing WSUS and deploying updates

Scenario

A. Datum Corporation is a global engineering and manufacturing company with its head office in London, United Kingdom. An IT office and a datacenter are located in London to support the London location and other branch office locations. A. Datum has recently deployed a Windows Server 2016 server and client infrastructure.

A. Datum has been applying updates manually to servers in a remote location. This has made it difficult to identify which servers have the updates applied and which do not. This is a potential security issue. You have been asked to automate the update process by extending A. Datum's WSUS deployment to include the branch office.

Objectives

After completing this lab, you will be able to:

- Implement the WSUS server role.
- Configure update settings.
- Approve and deploy an update by using WSUS.

Lab Setup

Estimated Time: **60 minutes**

Virtual machines: **20740A-LON-DC1**, **20740A-LON-SVR2**, **20740A-LON-SVR4**, and **20740A-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, on the Start screen, click **Hyper-V Manager**.
2. In **Microsoft Hyper-V Manager**, click **20740A-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. Perform steps 2 through 4 for **20740A-LON-SVR2**, **20740A-LON-SVR4**, and **20740A-LON-CL1**.

Exercise 1: Implementing WSUS

Scenario

Your organization has a WSUS server called LON-SVR2, which is located in the head office. You need to install the WSUS server role on LON-SVR4 at a branch location. LON-SVR4 will use LON-SVR1 as the source for Windows Update downloads. The installation on LON-SRV4 will use the Windows Internal Database for the deployment.

The main tasks for this exercise are as follows:

1. Install the WSUS server role.
2. Configure WSUS to synchronize with an upstream WSUS server.

▶ Task 1: Install the WSUS server role

1. Sign in to **LON-SVR4** as **Adatum\Administrator** with the password **Pa$$w0rd**.
2. From **Server Manager**, install the **Windows Server Update Services** role with the WID connectivity and WSUS Services Role Services. Also, configure the location where the updates need to be stored as **C:\WSUSUpdates**.
3. Open the **Windows Server Update Services** console, and complete the installation when prompted.

▶ Task 2: Configure WSUS to synchronize with an upstream WSUS server

1. On **LON-SVR4**, complete the **Windows Server Update Services Configuration Wizard**, specifying the following settings:
   - Upstream Server: **LON-SVR2.Adatum.com**
   - No proxy server
   - Default languages
   - Manual sync schedule
   - Begin initial synchronization
2. In the **Windows Server Update Services** console, under **Options**, set **Computers** to **Use Group Policy or registry settings on computers**. You might need to wait until synchronization is complete before confirming this option.

Results: After completing this exercise, you should have implemented the WSUS server role.

Exercise 2: Configuring update settings

Scenario

You need to configure the Group Policy settings to deploy automatic WSUS settings to client computers. With the WSUS role configured on LON-SVR4, you must ensure that the Research Department has its own computer group in WSUS on LON-SVR4. You must also configure client computers in the Research organizational unit (OU) to use LON-SVR4 as their source for updates.

The main tasks for this exercise are as follows:

1. Configure WSUS groups.
2. Configure Group Policy to deploy WSUS settings.
3. Verify the application of Group Policy settings.
4. Initialize Windows Update.

▶ Task 1: Configure WSUS groups

- On **LON-SVR4**, in the **Windows Server Update Services** console, create a new computer group named **Research**.

▶ Task 2: Configure Group Policy to deploy WSUS settings

1. Switch to **LON-DC1**.
2. Open **Group Policy Management**.
3. Create and link a new GPO to the **Research** OU named **WSUS Research**.
4. Configure the following policy settings under the **Windows Update** node:
   - Configure Automatic Updates: **Auto download and schedule the install**
   - Microsoft Update service location: **http://LON-SVR4.Adatum.com:8530**
   - Intranet statistics server: **http://LON-SVR4.Adatum.com:8530**
   - Client-side targeting group: **Research**
5. Move **LON-CL1** to the **Research** OU.

▶ Task 3: Verify the application of Group Policy settings

1. Switch to **LON-CL1**.
2. Restart **LON-CL1**.
3. On **LON-CL1**, sign in as **Adatum\Administrator** with the password **Pa$$w0rd**.
4. Open the command prompt by using the **Run as Administrator** option.
5. At the command prompt, run the following command:

```
Gpresult /r
```

6. In the output of the command, confirm that, under **Computer Settings**, **WSUS Research** is listed under **Applied Group Policy Objects**.

▶ Task 4: Initialize Windows Update

1. On **LON-CL1**, at the command prompt, run the following command:

```
Wuauclt.exe /detectnow /reportnow
```

2. Switch to **LON-SVR4**.
3. In the **Update Services** console, expand **Computers**, expand **All Computers**, and then click **Research**.
4. Verify that **LON-CL1** appears in the **Research** Group. If it does not, then repeat steps 1 through 3. It might take several minutes for **LON-CL1** to display.
5. Verify that updates are reported as needed. If updates are not reported, repeat steps 1 through 3. It might take 10 to 15 minutes for updates to register.

Results: After completing this exercise, you should have configured update settings for client computers.

Exercise 3: Approving and deploying an update by using WSUS

Scenario

After you have configured the Windows Update settings, you can view, approve, and then deploy required updates. You have been asked to use LON-CL1 as a test case for the Research Department. You will approve, deploy, and verify an update on LON-CL1 to confirm the proper configuration of the WSUS environment.

The main tasks for this exercise are as follows:

1. Approve WSUS updates for the Research computer group.
2. Deploy updates to **LON-CL1**.
3. Verify update deployment to **LON-CL1**.
4. Prepare for the next lab.

▶ Task 1: Approve WSUS updates for the Research computer group

- On **LON-SVR4**, in the **WSUS** console, approve the **Update for Windows 10 Version 1511 for x64-based Systems (KB3140741)** update for the **Research** group.

▶ Task 2: Deploy updates to LON-CL1

1. On **LON-CL1**, at the command prompt, run the following command:

```
Wuauclt.exe /detectnow
```

2. Open **Windows Update** and then check for updates.
3. Notice the update you approved begins to download.

▶ Task 3: Verify update deployment to LON-CL1

1. On **LON-CL1**, open **Event Viewer**.
2. Go to **Applications and Services Logs\ Microsoft\Windows**, and view the events under **WindowsUpdateClient / Operational**.
3. Confirm that events are logged in relation to the update.

Results: After completing this exercise, you should have approved and deployed an update by using WSUS.

▶ Task 4: Prepare for the next lab

When you finish the lab, revert all virtual machines back to their initial state. To do this, perform the following steps:

1. On the host computer, start **Microsoft Hyper-V Manager**.
2. In the **Virtual Machines** list, right-click **20740A-LON-DC1**, and then click **Revert**.
3. In the **Revert Virtual Machines** dialog box, click **Revert**.
4. Repeat steps 2 to 3 for **20740A-LON-SVR2**, **20740A-LON-SVR4**, and **20740A-LON-CL1**.

Lesson 3
Overview of Windows PowerShell DSC

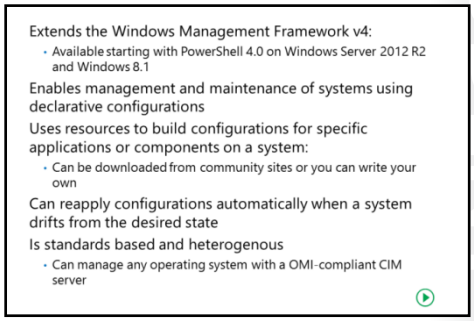
Windows PowerShell DSC (Desired State Configuration) is a new component of the Windows Management Framework that Windows PowerShell 4.0 first introduced. Windows PowerShell DSC enables you to manage and maintain systems in a scalable and standardized manner by pushing or pulling declarative configurations.

Lesson Objectives

After completing this lesson, you will be able to:

- Describe the benefits of Windows PowerShell DSC.
- Describe the requirements for using Windows PowerShell DSC.
- Describe how to implement Windows PowerShell DSC.
- Describe how to troubleshoot Windows PowerShell DSC.

Benefits of Windows PowerShell DSC



Windows PowerShell DSC (Desired State Configuration) is an extension of Windows PowerShell and the Windows Management Framework. Windows PowerShell 4.0 first introduced Windows PowerShell DSC in Windows Server 2012 R2 and Windows 8.1. You can use Windows PowerShell DSC to manage and maintain systems using declarative configurations. The unique feature of this approach is that instead of creating a Windows PowerShell script to execute a sequence of commands (imperative approach), you deploy a configuration that tells Windows PowerShell what you want to do. In a declarative approach such as DSC, you do not need to worry about including error handling or other logic, because the underlying automation framework handles that automatically.

Imperative Approach (Windows PowerShell)	Declarative Approach (Windows PowerShell DSC)
Script defines how a task should be performed.	Configurations define what should be done.
Scripts can be hard to read.	Configurations are easier to understand.
Scripts will not rerun themselves and must be rerun through an administrative action to re-apply settings, if needed.	Configurations reapply as necessary; at whatever interval you choose.
Scripts require custom logic to detect and correct configuration drift.	Configurations use the logic built into DSC resources to detect and correct configuration drift.

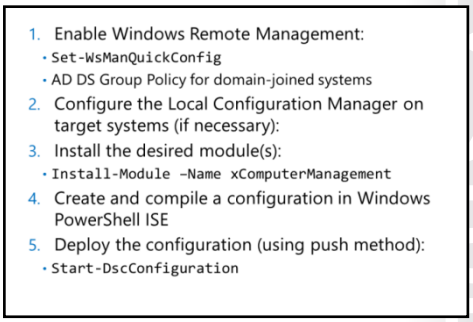
DSC relies on resources, which are the imperative building blocks used to author configurations. DSC, by default, includes resources that you can use to manage basic components of the Windows operating system, such as services, files, and registry settings. However, the real power of DSC lies in the fact that

anyone can create resources. In addition, there are growing communities where you can share and download DSC resources to configure a variety of applications and components within your organization.

Because configurations can change unintentionally over time, DSC can automatically reapply any deployed configurations whenever it detects that the system has deviated from the desired state. DSC is also very scalable, and you can utilize it in a variety of environments, large or small, and centralized or decentralized. DSC does not require that systems belong to an AD DS domain. In addition, DSC is standards-based and is built around the Open Management Infrastructure (OMI) model. Therefore, you can also use it to manage any operating system with an OMI-compliant Common Information Model (CIM) server, such as CentOS, or other varieties of Linux.

Requirements for Windows PowerShell DSC

Authoring and deploying DSC configurations for your organization is a multistep process. The steps include:



1. Enable Windows Remote Management. Because DSC relies on Windows Remote Management (WinRM), you have to ensure that WinRM listeners are configured on the systems that you want to manage by using DSC. By default, WinRM is enabled on Windows Server 2012 R2 and newer systems, but not on Windows 8.1 or Windows 10 clients. You can enable WinRM on individual systems by using the **Set-WSManQuickConfig** cmdlet, or you can additionally leverage Group Policy to enable the listener on systems joined to the domain.
2. Configure the Local Configuration Manager. The Local Configuration Manager (LCM) agent processes DSC configurations on the systems that you are managing. Before you begin deploying DSC configurations, you should configure the LCM agent according to your needs. You can configure the LCM by using a special Managed Object Format (MOF) file that sets the LCM-specific parameters, and you can then apply the configuration by using the **Set-DscLocalConfiguration** cmdlet. For most configurations, the default push mode LCM configuration is sufficient. The following list describes some of the LCM-specific parameters.
    - **RefreshMode**. The LCM agent receives configurations through this mode. By default, **RefreshMode** is set to Push, which means that you apply configurations by running the **Start-DscConfiguration** cmdlet on the local system or on a remote system. A **RefreshMode** of Pull means that the LCM agent regularly checks a remote HTTP server or server message block (SMB) share for configurations. You can also set **RefreshMode** to Disabled, which prevents the LCM agent from applying any configurations. Configuring a Pull server is not required to use DSC. However, pull servers can be beneficial in large, distributed environments.
    - **RefreshFrequencyMins**. This is the time interval, in minutes, at which the LCM polls the remote HTTP server or SMB share for configurations. When configured in Push mode, this value is ignored. The default value is 30.

- **ConfigurationMode**. This mode indicates the action that the LCM agent takes when applying configurations. By default, the LCM agent is configured to ApplyAndMonitor, meaning that the initial configuration is applied, but future deviations are only logged and are not corrected automatically. A **ConfigurationMode** of ApplyAndAutoCorrect means that the initial configuration is applied, and that any future deviations are corrected automatically.
- **ConfigurationModeFreqencyMins**. This is the time interval, in minutes, at which the LCM checks and (if necessary) reapplies configurations. By default, this value is 15.

3. Install desired Modules. The modules developed for DSC are available in the Windows PowerShell Gallery located at https://www.powershellgallery.com. To install modules from the Windows PowerShell Gallery, you need the **PowerShellGet** module, which is included with Windows PowerShell 5.0. Optionally, you can install the **PowerShellGet** module for Windows PowerShell 4.0 by downloading an MSI installer. The **PowerShellGet** module includes the **Find-Module** and **Install-Module** cmdlets needed to install a module from the Windows PowerShell Gallery. To install the latest version of the xComputerManagement module, you can run the following Windows PowerShell command:

```
Install-Module -Name xComputerManagement
```

Running this command will create a new folder named xComputerManagement under the **C:\Program Files\WIndowsPowerShell\Modules** folder. If necessary, you can copy the xExchange folder manually to any target system that does not have **PowerShellGet**. This might be necessary on systems where you cannot install **PowerShellGet** or do not have Internet connectivity. When you use a pull configuration, you can also stage modules on the pull server, and they will be downloaded automatically, as required, to the target system.

4. Create and compile a basic DSC configuration. After you have met all prerequisites and installed the desired module(s) on the target servers that you want to configure, you can begin authoring configuration scripts by using DSC resources. Configuration scripts do not actually modify target systems. Configuration scripts are only a template that you use to compile a MOF file that the LCM agent pushes to or pulls from the target system. You can author configuration scripts in any Windows PowerShell or text editor. Lastly, the configuration is called, much like a function, to compile the configuration data into MOF files for each defined node.

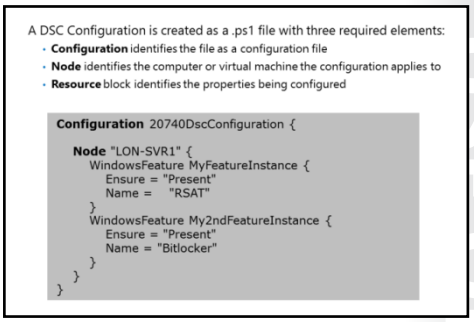
5. Deploy the configurations to the desired servers. After you have compiled the configuration into a .mof file, you push the configuration to the Local Configuration Manager (LCM) on the target node by using the **Start-DscConfiguration** cmdlet. Running this command invokes the LCM agent to process the configuration, and if necessary, make changes on the target node. To deploy a configuration named LON-SRV1.mof file, you run the following command:

```
Start-DscConfiguration –Wait –Verbose –Path C:\DSC –ComputerName LON-SRV1
```

You can run this command with the **–Wait** and **–Verbose** parameters to see the detailed steps that the LCM agent on the target node is going through. Using these parameters is essential when you troubleshoot configuration deployment. After you have deployed a configuration, or anytime afterward, you can run the **Test-DscConfiguration** cmdlet to verify if the target node is in the desired state. **Test-DscConfiguration** will return True if the system is in desired state, and will return False if it is not.

Implementing Windows PowerShell DSC

DSC configurations are Windows PowerShell scripts that define a function. To create a configuration, you use the Windows PowerShell keyword **Configuration** in a .ps1 file.




```
Configuration 20740DscConfiguration {
    Node "LON-SVR1" {
        WindowsFeature MyFeatureInstance {
            Ensure = "Present"
            Name =    "RSAT"
        }
        WindowsFeature My2ndFeatureInstance
{
            Ensure = "Present"
            Name = "Bitlocker"
        }
    }
}
```

Configuration syntax

The above example shows a simple configuration script. A configuration script consists of at least three parts:

- The Configuration block. This is the outermost script block. You define it by using the Configuration keyword and providing a name. In example above, the name of the configuration is 2740DscConfiguration.
- One or more Node blocks. These define the nodes (computers or virtual machines) that you are configuring. In the example configuration above, there is one Node block that targets a computer named **LON-SVR1**.
- One or more Resource blocks. This is where the configuration sets the properties for the resources that it is configuring. In the example above, there are two resource blocks, each of which call the WindowsFeature resource.

Within a Configuration block, you can do anything that you normally could do in a Windows PowerShell function. In the example above, you could replace the name of the target computer with a parameter.

```
Configuration 20740DscConfiguration {
   param(
        [string[]]$NodeName="localhost"
    )
    Node $NodeName {
        WindowsFeature MyFeatureInstance {
            Ensure = "Present"
            Name =    "RSAT"
        }
        WindowsFeature My2ndFeatureInstance {
            Ensure = "Present"
            Name = "Bitlocker"
        }
    }
}
```

When you compile the configuration you specify the name of the node by passing the $NodeName parameter. The default value for the parameter is localhost.

Compiling the configuration

Before you can use a configuration, you have to compile it into a MOF file. You do this by calling the configuration the same was that you would call a Windows PowerShell function.

Note: To call a configuration, the function must be in global scope (as with any other PowerShell function). You can make this happen either by using ".\" when calling the configuration file, or by running the configuration file by pressing F5 or clicking the **Run Script** button in PowerShell ISE. For example, to compile the first example above, run the following command: **.\20740DscConfiguration.ps1**.

When you call the configuration, it creates:

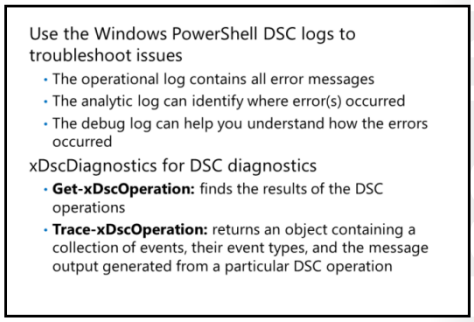
- A folder in the current directory with the same name as the configuration.
- A file named NodeName.mof in the ConfigurationName directory, where *NodeName* is the name of the target node of the configuration. If more than one node is targeted, a MOF file will be created for each node.

If the configuration takes a parameter, the parameter has to be provided at compile time. For the second example above, the command would be:

```
20740DscConfiguration -NodeName 'LON-SVR1'
```

Troubleshooting Windows PowerShell DSC

There are two steps for troubleshooting Windows PowerShell DSC. First you should review the available logs. Then, you should recycle the DSC cache to clear any scripts stored in memory.



Using Windows PowerShell DSC logs to diagnose script errors

Windows PowerShell DSC records errors and events in logs accessible through the Event Viewer. Examining these logs can help you understand why a particular script or operation failed, and how to fix and prevent the failure in the future. Writing configuration scripts can be complex, so to make tracking errors easier as you author, use the DSC Log resource to track the progress of your configuration in the DSC Analytic event log.

In Event Viewer, DSC events are in: **Applications and Services Logs/Microsoft/Windows/Desired State Configuration**. You can also use the PowerShell cmdlet **Get-WinEvent** to view the event logs. To view the operational log, run the following command:

```
Get-WinEvent -LogName "Microsoft-Windows-Dsc/Operational"
```

As shown in the example above, the Windows PowerShell DSC's primary log name is **Microsoft-Windows-DSC**. The primary name is appended to the channel name to create the complete log name. The DSC engine writes mainly into three logs: Operational, Analytic, and Debug. The analytic and debug logs are turned off by default and are not shown by default in the Event Viewer. To view them in the

Event Viewer, perform the following steps, click the **Start** button, click **Windows Administrative Tools**, and then click **Event Viewer**. Optionally, you can start the event viewer by typing **Show-EventLog** in a Windows PowerShell window. On the **View** menu in Event Viewer, click **Show Analytic and Debug Logs**. The log name for the analytic channel is **Microsoft-Windows-Dsc/Analytic**, and the debug channel is **Microsoft-Windows-Dsc/Debug**. You could also use the **wevtutil** utility to enable the logs, as shown in the following example.

```
wevtutil.exe set-log "Microsoft-Windows-Dsc/Analytic" /q:true /e:true
```

Windows PowerShell DSC logs are split over the three log channels based on the importance of the message. The operational log contains all error messages, and can be used to identify a problem. The analytic log has a higher volume of events, and can identify where error(s) occurred. This channel also contains verbose messages (if any). The debug log contains logs that can help you understand how the errors occurred. Windows PowerShell DSC event messages are structured so that every event message begins with a job ID that uniquely represents a Windows PowerShell DSC operation.

Tools to analyze DSC logs

xDscDiagnostics is a PowerShell module that consists of two functions that can help analyze DSC failures on a system: **Get-xDscOperation** and **Trace-xDscOperation**. These functions can help you identify all events from past DSC operations from either local or remote computers, provided you have valid credentials. Here, the term DSC operation is used to define a single unique DSC execution from its start to its end. For example, **Test-DscConfiguration** would be a separate DSC operation. Similarly, every other cmdlet in DSC (such as **Get-DscConfiguration** and **Start-DscConfiguration**.) could each be identified as separate DSC operations. The two functions are explained in xDscDiagnostics PowerShell Module (DSC Resource Kit).

- **Get-xDscOperation**. This function lets you find the results of the DSC operations that run on one or multiple computers, and returns an object that contains the collection of events produced by each DSC operation.
- **Trace-xDscOperation**. This cmdlet returns an object containing a collection of events, their event types, and the message output generated from a particular DSC operation. Typically, when you find a failure in any of the operations by using **Get-xDscOperation**, you would trace that operation to find out which of the events caused a failure.

How to reset the cache

The DSC engine caches resources implemented as a Windows PowerShell module for efficiency purposes. However, this can cause problems when you are authoring a resource and testing it simultaneously because Windows PowerShell DSC will load the cached version until the process is restarted. The only way to make Windows PowerShell DSC load the newer version is to explicitly end the process hosting the Windows PowerShell DSC engine.

When you run **Start-DscConfiguration**, after adding and modifying a custom resource, the modification might not execute unless the computer is rebooted. This is because DSC runs in the WMI Provider Host Process (WmiPrvSE), and usually, there are many instances of WmiPrvSE running at once. When you reboot, the host process is restarted and the cache is cleared.

To successfully recycle the configuration and clear the cache without rebooting, you must stop and then restart the host process. This can be done on a per-instance basis, whereby you identify the process, stop it, and restart it.

To identify which process is hosting the DSC engine and stop it on a per-instance basis, you can list the process ID of the WmiPrvSE which is hosting the DSC engine. Then, to update the provider, stop the WmiPrvSE process, and finally run **Start-DscConfiguration** again.

You can use the following commands to identify the process ID of the WmiPrvSE and stop the host WmiPrvSE process.

```
###
### find the process that is hosting the DSC engine
###
$dscProcessID = Get-WmiObject msft_providers |
Where-Object {$_.provider -like 'dsccore'} |
Select-Object -ExpandProperty HostProcessIdentifier
###
### Stop the process
###
Get-Process -Id $dscProcessID | Stop-Process
```

Question: How can PowerShell DSC help you manage your environment?

Lesson 4
Overview of Windows Server 2016 monitoring tools

Windows Server 2016 provides a range of tools to monitor an operating system and the applications on a computer. You can use these tools to configure your system for efficiency and troubleshoot problems. Small and medium-sized organizations can use the monitoring tools in Windows Server 2016 to monitor their server infrastructure. However, enterprise organizations that deploy more a complex IT infrastructure will need a more complex monitoring and management solution, such as Microsoft System Center 2016.

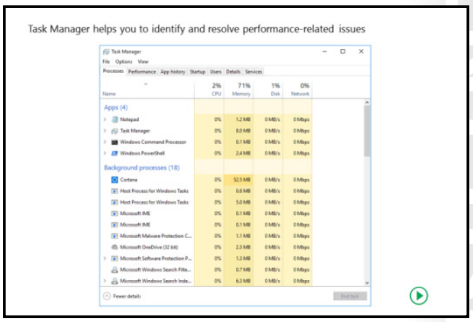
Lesson Objectives

After completing this lesson, you will be able to:

- Describe how the Task Manager tool works.
- Describe the features of Performance Monitor.
- Describe the role of the Resource Monitor tool.
- Describe Reliability Monitor.
- Describe the Event Viewer tool.
- Describe how to monitor other servers with the Server Manager tool.

Overview of Task Manager

Enhancements to Task Manager in Windows Server 2016 provide more information to help you identify and resolve performance-related issues. Task Manager includes the following tabs:



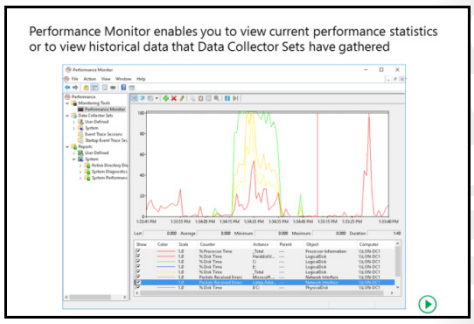
- **Processes**. The **Processes** tab displays a list of running programs, subdivided into applications and internal processes of the Windows operating system. For each running process, this tab displays a summary of processor and memory usage.
- **Performance**. The **Performance** tab displays a summary of central processing unit (CPU) usage, memory usage and network statistics.
- **App history**. The **App history** tab displays how much CPU time, network activity, metered network activity, and network usage for tile updates and notifications have been used by each running app in the current profile.
- **Startup**. Shows the applications that automatically start with the computer. This also provides the ability to manage the startup applications.
- **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 processes on the server, providing statistics about the CPU, memory, and consumption of other resources. You can use this tab to manage the running processes. For example, you can stop a process, stop a process and all related processes, and change the processes' priority values. By changing a process's priority, you determine how much of the CPU's resources the process can consume. By increasing the priority of a process, you allow the process to request more of the CPU's resource.
- **Services**. The **Services** tab provides a list of the running Windows services and related information. This includes information about whether the service is running and information about the process identifier (PID) of the running service. You can start and stop services by using the list on the **Services** tab.

You might consider using Task Manager when a performance-related problem arises. For example, you might examine the running processes to determine if a particular program is using excessive CPU resources. Always remember that Task Manager shows a snapshot of current resource consumption, and that you might need to examine historical data to determine a true picture of a server's performance and response under load.

Overview of Performance Monitor

Performance Monitor enables you to view either current performance statistics or historical data that was gathered during a selected timeframe. With Windows Server 2016, you can monitor operating system performance through performance objects and counters in the objects. Windows Server 2016 collects the following types of data from counters in various ways:



- A real-time snapshot value.
- The total since the last computer startup.
- An average over a specific time interval.
- An average of last values.
- The number per second.
- A maximum value.
- A minimum value.

Performance Monitor provides you a collection of objects and counters that record data about computer resource usage. There are many counters that you can research and consider monitoring to meet your specific requirements.

The three components of Performance Monitor you can use to view performance data are:

- Monitoring tools. Allows you to configure performance objects and counters to monitor performance data in real time, or to store monitoring data in a log file or a database.
- Data collector sets. Represents a custom set of performance counters for monitoring specific technologies, such as AD DS diagnostics, and system diagnostics and performance.
- Reports. Each data collector set automatically creates performance reports. The reports include performance data that was collected during the time data collector set was running.

Processor counters

CPU counters are a feature of the computer's CPU that stores the count of hardware-related events. The most commonly used processor counters include:

- **Processor > % Processor Time**. This counter measures the percentage of elapsed time the processor spends executing a nonidle thread. If the percentage is greater than 85 percent, the processor is overwhelmed and the server might require a faster processor. In other words, this counter displays the percentage of elapsed processor time used by a given thread to run instructions. An instruction is the basic unit of execution in a processor, and a thread is the object that executes instructions. This count includes 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.
- **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 for an extended period, then it means that 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 is representative only of a current snapshot of the processor. Therefore, you must observe this counter over an extended period to notice data trends. Additionally, the **System > Processor Queue Length** counter reports a total queue length for all processors, not a length for each processor.

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 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 for resolving hard-page faults. If excessive paging results in a value that is greater than 1,000, there might be a memory leak. In other words, the **Memory > Pages/sec** counter displays the number of hard page faults per second. A hard page fault occurs when the requested memory page cannot be located in RAM because it exists currently in the paging file. An increase in this counter indicates that more paging is occurring, which in turn suggests a lack of physical memory.

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 items are written to disks to record 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 most commonly used 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 might be 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 I/O manager 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.

 **Note:** *Throughput* is the total amount of traffic that passes a given network-connection point for each unit of time. *Workload* is the amount of processing that the computer performs at a given time.

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:

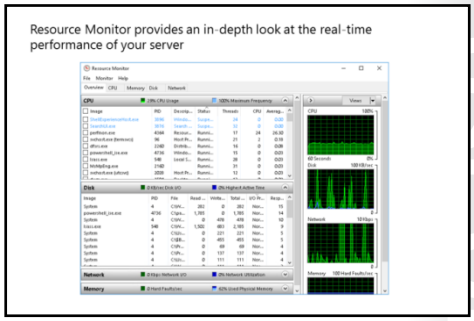
- Public network access.
- Networks for performing backups and other maintenance tasks.
- Dedicated remote-management connections.
- Network-adapter teaming for performance and failover.
- Connections to the physical host computer.
- Connections to network-based storage arrays.

By monitoring the 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 value given 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.

Overview of Resource Monitor

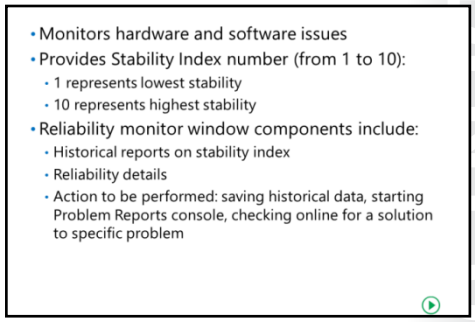
The Resource Monitor interface in Windows Server 2016 provides detailed information about your server's real-time performance. You can use Resource Monitor to monitor the use and performance of CPU, disk, network, and memory resources in real time. The resource monitor is similar to the Task Manager. However, the Task Manager only shows the current value, the resource monitor shows recent historical data as well. This enables you to identify and resolve resource conflicts and bottlenecks.



By expanding the monitored elements, system administrators can identify which processes are using which 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 in every pane of Resource Monitor, which provides the information that you require regarding that process at the top of the screen, no matter where you are in the interface.

Overview of Reliability Monitor

The Windows Server 2016 operating system installs the Reliability Monitor tool by default. It monitors hardware and software issues that occur during the selected time interval. Based on the number and type of issues, it assigns a number called the stability index that indicates the server's reliability. The stability index ranges from 1 to 10, where 1 represents the least stable server state and 10 represents the most stable state. By using the stability index, administrators can evaluate the server's reliability quickly. Any issue that affects the server potentially can change the value of the stability index.

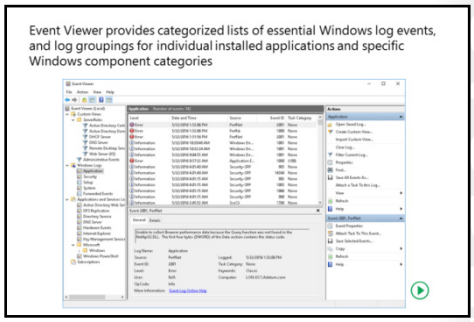


There are two ways to open the **Reliability Monitor** window: by searching in the Control Panel and clicking **View reliability history**, or from within Performance Monitor, by right-clicking **Monitoring Tools** and selecting **View system reliability**. The **Reliability Monitor** window includes:

- A reporting history on the stability index values shown during previous days or weeks. The following stability index information is available about Application failures, Windows failures, Miscellaneous failures, Warnings, and Information.
- A reliability details table that contains the source of the issue, summary information, date, and action taken.

- A group of actions that you can elect to perform, represented as links in the console, and which include:
  - Saving the reliability history to an xml file. You can use this option if you want to keep track of older reliability history information.
  - Starting the **Problem Reports** console. You can use this to view issues related to specific applications. For each problem that the Reliability Monitor detects, options in the console allow you to view more details about the problem, check online for a solution, or delete the reported problem information.
  - Checking for a solution for all reported problems. You can use this option if you want Reliability Monitor to connect to the Internet to locate online information about resolving the all reported problems.

Overview of Event Viewer



Windows Event Viewer provides access to the Windows Server 2016 event logs. Event logs provide information about system events that occur within the Windows operating system. These events include information, warning, and error messages about Windows components and installed applications.

Event Viewer provides categorized lists of essential Windows log events, including application, security, setup, and system events. Event Viewer also provides log groupings for individual installed applications and specific Windows component categories. Individual events provide detailed information about the type of event that occurred. When an event occurs, Event Viewer provides details about the source of the event, and detailed technical information to assist you in troubleshooting the event.

Additionally, Event Viewer allows you to consolidate logs from multiple computers onto a centralized server by using subscriptions. Finally, you can configure event viewer to run a specific action when a specified type of event occurs. This might include sending an email message, launching an application, running a script, or other types of maintenance actions.

Event Viewer in Windows Server 2016 contains the following important features:

- The ability to view multiple logs. You can filter for specific events across multiple logs. This makes it easier to investigate issues and troubleshoot the problems that might appear in several logs.
- Customized views. You can use filtering to narrow searches down to only the 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 is integrated with Task Scheduler.
- The ability to create and manage event log 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 such as:

- 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 event.
- 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 type of event.

Windows Server Logs

The following table lists several of the Event Viewer built-in logs.

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, the Simple Mail Transfer Protocol (SMTP) service, and other applications.
Security log	This log reports the results of auditing, if you enable it. Audit events report success or failure, depending on the event. For example, the log would report success or failure depending on whether a user was able to access a file or not.
Setup log	This log contains events related to application setup.
System log	Windows components and services log general events, and classify them as error, warning, or information. The Windows operating system predetermines the events that system components log.
Forwarded events	This log stores events that Windows components collect from remote computers. To collect events from remote computers, you must create an event subscription.

Application and Services Logs

Applications and Services logs store events from a single application or component rather than events that might have system-wide impact. This category of logs includes four subtypes:

- Admin
- Operational
- Analytic
- Debug

Admin logs are of interest to end users, administrators, and support personnel who use Event Viewer to troubleshoot problems. These logs provide guidance about how to respond to issues. The events found in the Admin logs indicate a problem and a well-defined solution upon which an administrator can act.

Events in the Operational log are also useful for IT professionals, but they are likely to require more interpretation. You can use operational events to analyze and diagnose a problem or occurrence, and to trigger tools or tasks based on the problem or occurrence.

Analytic and Debug logs are not very user friendly. Analytic logs store events that trace an issue, and they often log a high volume of events. Developers use debug logs when they are debugging applications. By default, both Analytic and Debug logs are hidden and disabled.

Windows log files are 1,028 kilobytes (KB) in size by default, and the operating system overwrites events in the log files, as necessary. If you want to clear a log manually, you must log in to the server as a local administrator.

If you want to configure event log settings centrally, you can do so by using Group Policy. Open the Group Policy Management Editor for your selected Group Policy Object (GPO), and then go to **Computer Configuration\Policies\Administrative Templates\Windows Components\Event Log Service**.

For each log, you can define the following properties:

- The location of the log file.
- The maximum size of the log file.
- Automatic backup options.
- Permissions on the logs.
- Behavior that occurs when the log is full.

Monitoring a Server with Server Manager

Organizations typically have multiple servers, both physical and virtual, that they must monitor. The number of servers in an organization depends on the organization's size and the complexity of its IT infrastructure. The most efficient way to monitor multiple servers is to deploy management and monitoring software that provides a centralized dashboard where administrators will be able to monitor all components of the IT infrastructure.

Server Manager console:
- Installed by default on Windows Server 2016, and can be installed on Windows 10
- Supports monitoring of Windows Server operating systems
- Provides a centralized monitoring dashboard
- Analyzes or troubleshoots different types of issues
- Identifies critical events
- Monitors the status of Best Practices Analyzer tool

Depending on the size of the organization and the complexity of its IT infrastructure, monitoring software can be classified in two ways:

- Enterprise management and monitoring solutions, such as the System Center suite of tools.
- Small and medium-sized organization monitoring solutions, such as Server Manager.

Windows Server 2016 installs the Server Manager software by default, and additionally, you can install the Windows Server 2016 Remote Server Administration Tools, which includes Server Manager, a Windows 10 client computer. It provides monitoring of both local and remote servers, and collects monitoring data from specific servers and presents it in a centralized dashboard. By using Server Manager, administrators can monitor up to 100 servers. For monitoring more than 100 servers, you should consider an enterprise monitoring solution such as System Center or Operations Management Suite.

Server Manager can monitor Windows Server 2008 and newer Windows Server operating systems. Additionally, it can monitor Server Core editions of Windows Server 2008 R2 and newer Windows Server Core operating systems. You must configure remote servers to allow remote management if you want your administrators to monitor remote servers with Server Manager. Configuration for remote management and monitoring is enabled by default, and you can change it by using Server Manager and Windows PowerShell on the monitored server. Server Manager does not support monitoring of the Windows client operating system.

When using Server Manager, you can perform following monitoring tasks on remote servers, such as:

- Adding remote servers to a pool of servers that Server Manager will monitor. Administrators can choose which servers to monitor.
- Creating custom groups of monitored servers. Administrators can group monitored servers in Server Manager by different criteria, such as department, city, or country/region. Grouping servers helps organizations assign different administrators to monitor different groups of servers.
- Starting different tools on remote servers. Administrators can start different tools remotely, such as MMC consoles for monitoring different types of data or starting Windows PowerShell on remote servers. This ensures that administrators do not have to sign in locally to a server to perform different management tasks, such as starting a service.
- Determining server status and identifying critical events. Server Manager displays servers with critical issues on the centralized dashboard in the color red. This alerts administrators to start troubleshooting the issue immediately.
- Analyzing or troubleshooting different types of issues. You can configure centralized console monitoring information to display by type, such as AD DS, Domain Name System (DNS), IIS or Remote Access. This enables administrators to locate the type of issue and begin troubleshooting it. The centralized console also provides general monitoring information that displays on the console as All Servers.
- Monitoring the status of Best Practices Analyzer tool. The Best Practices Analyzer tool runs on every server, and compares current server role configuration with recommended settings from Microsoft, based on best practices. Server Manager displays results of the Best Practices Analyzer tool from all monitored servers in the centralized dashboard.
- Customizing how monitoring data displays. Administrators can customize how monitoring data displays, so that they can focus on the type of monitoring data that is relevant for troubleshooting particular issues.

Question: Which of the tools discussed in this lesson would you use if you want to check which resources an application is using?

Lesson 5
Using Performance Monitor

You can use Performance Monitor to collect, analyze, and interpret performance-related data about your organization's servers. This enables you to make informed capacity planning decisions. However, to make informed decisions, it is important to know how to establish a performance baseline, how to use data collector sets, and how to use reports to help you compare performance data to your baseline.

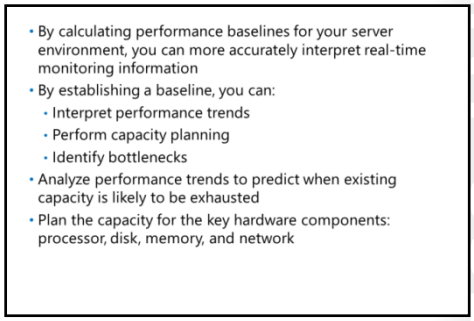
Lesson Objectives

After completing this lesson, you will be able to:

- Explain what a baseline is.
- Describe data collector sets.
- Describe how to capture counter data with a data collector set.
- Describe how to configure an alert.
- Describe how to view Performance Monitor reports.
- Identify the key parameters that you should track when monitoring network infrastructure services.
- Identify considerations for monitoring virtual machines.

Overview of baseline, trends, and capacity planning

By calculating performance baselines for your server environment, you can interpret real-time monitoring information more accurately. A baseline for your server's performance indicates what your performance-monitoring statistics look like during normal use. You can establish a baseline by monitoring performance statistics over a specific period. When an issue or symptom occurs in real time, you can compare your baseline statistics to your real-time statistics, and then identify anomalies.



Trends analysis

You should consider the value of performance data carefully to ensure that it reflects your server environment. Additionally, you should gather performance data that you can use to plan for business or technological growth, and create upgrade plans. You might be able to reduce the number of servers that are in operation after you measure performance and assess the required environment.

By analyzing performance trends, you can predict when existing capacity is likely to be exhausted. Review historical analysis along with your business requirements, and use this data to determine when additional capacity is required. Some peaks are associated with one-time activities, such as extremely large orders. Other peaks occur on a regular basis, such as a monthly payroll processing. These peaks could make a capacity increase necessary to meet the demands of an increased number of employees.

Capacity planning

Planning for future server capacity is a best practice for all organizations. Planning for business changes often requires additional server capacity to meet targets. By aligning your IT strategy with your business strategy, you can support business objectives. Furthermore, you should consider virtualizing your environment to reduce the number of physical servers that you require. You can consolidate servers by implementing the Hyper-V role in the Windows Server 2016 environment.

Capacity planning focuses on assessing server workload, the number of users that a server can support, and the ways to scale systems to support additional workload and users in the future. New server applications and services affect the performance of your IT infrastructure. These services could receive dedicated hardware, although they often use the same LAN and WAN infrastructure. Planning for future capacity should include all hardware components and the way that new servers, services, and applications affect the existing infrastructure. Factors such as power, cooling, and rack space are often overlooked during initial exercises to plan capacity expansion. You should consider how your servers can scale up and out to support an increased workload.

Tasks such as upgrading to Windows Server 2016 might affect the performance of your servers and network. An update can sometimes cause problem with an application that might be incompatible with Windows Server 2016. Careful performance monitoring before and after you apply updates can identify these problems and help you rectify them.

An expanding business can require your infrastructure to support a growing number of users. You should consider your organization's current and anticipated business requirements when purchasing hardware. This will help you to meet future business requirements by increasing the number of servers or by adding capacity to existing hardware when needed.

Additional capacity requirements can include:

- More servers.
- Additional hardware.
- Reducing application loads.
- Reducing the number of users that connect to a server. You can do this by distributing the users to multiple servers.

Understanding bottlenecks

A performance bottleneck occurs when a computer is unable to service requests for a specific resource. The resource might be a key component, such as a disk, memory, processor, or network. Alternatively, the shortage of a component within an application package might cause the bottleneck. By using performance-monitoring tools on a regular basis, and comparing the results to your baseline and to historical data, you can often identify performance bottlenecks before they affect users.

After you identify a bottleneck, you must decide how to remove it. Your options for removing a bottleneck include:

- Running fewer applications.
- Adding resources to the computer.

A computer suffering from a severe resource shortage might stop processing user requests. This requires immediate attention. However, if your computer experiences a bottleneck but still operates within acceptable limits, you might decide to defer any changes until you resolve the situation or have an opportunity to take corrective action.

Analyzing key hardware components

There are four key hardware components: processor, disk, memory, and network. By understanding how your operating system uses these components, and how they interact with one another, you will have a better understanding of how to optimize server performance.

Processor

Processor speed is an important factor in determining your server's overall computing capacity. Processor speed is the number of operations that are performed in a measured period, such as a billion processor cycles per second is one gigahertz (GHz). Servers with multiple processors and processors with multiple cores generally perform processor-intensive tasks with greater efficiency and speed than single processor or single-core processor computers.

Processor architecture also is important. A 64-bit processor can access more memory than 32-bit processors and has a significant effect on performance. However, it is important to note that Windows Server 2016 is only available in a 64-bit edition.

Disk

Server hard disks store programs and data. Consequently, the throughput of hard disks affects the speed of the workstation or server, especially when the workstation or server is performing disk-intensive tasks. Most hard disks have moving parts, and it takes time to position the read/write heads over the appropriate disk sector to retrieve the requested information. Furthermore, disk controller performance and configuration also affects the overall disk performance. By selecting faster disks, and by using array of disks such as Redundant Array of Independent Disks (RAID), to optimize access times, you can alleviate the potential for the disk subsystem to create a performance bottleneck.

You also should remember that information on the disk moves into memory before it is used. 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. Installing additional memory in a server can often improve the disk subsystem performance, because accessing the cache is faster than moving the information into memory.

Memory

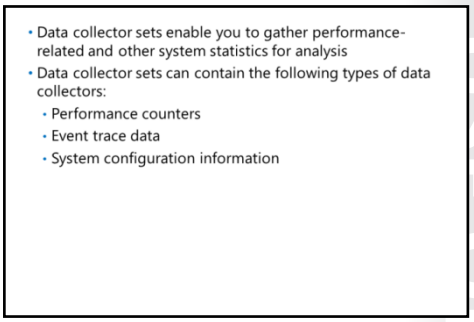
Programs and data load from the disk into memory before the program manipulates the data. In servers that run multiple programs, or where datasets are extremely large, increasing the amount of memory installed can help improve server performance.

Windows Server uses a memory model in which it does not reject memory requests by applications that exceed the computer's total available memory. Rather, it performs paging for these requests. During paging, Windows Server moves data and programs in memory that processors are not using currently. It moves them into an area on the hard disk, known as the paging file, and this frees up physical memory to satisfy the excessive requests. However, if a hard disk is comparatively slow, it has a negative effect on workstation performance. You can reduce the need for paging by adding more memory and using a 64-bit processor architecture that supports larger memory.

Network

The network is a critical component for performance monitoring, because many network applications are dependent on network communications performance. Poor network performance can cause slow or unresponsive applications and server functionality. Therefore, network capacity planning is very important. While planning for network capacity, you must consider bandwidth capacity and the capacity of any network devices, such as router and switch capacity. In many cases, optimized configuration of network devices such as switches or routers, improves the performance of the network and network applications.

What are data collector sets?



Data collector sets are a custom set of performance counters, event traces, and system configuration data.

A data collector set organizes multiple data-collection points into a single, portable component. You can use a data collector set on its own, or group it with other data collector sets. You can also incorporate a data collector set into logs, or view it in the Performance Monitor. You can configure a data collector set to generate alerts when it reaches thresholds in performance counters.

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 comparison to determine resource usage to plan for growth and to identify potential performance problems.

You also can configure a data collector set to run at a scheduled time, for a specific length of time, or until it reaches a predefined size. For example, you can run the data collector set for 10 minutes every hour during your working hours, to create a performance baseline. You also can set the data collector to restart when it reaches set limits, so that it creates a separate file for each interval. You can configure a schedule for performance monitoring when configuring a data collector set. Scheduling options are located in the **Schedule** tab of the data collector set properties window. The schedule monitoring options that you can select include beginning date, expiration date, and start time. You can also choose which day of the week you want performance monitoring to run.

After you have created a combination of data collectors that describe useful system information, you can save them as a data collector set. Data collector sets can be run at any time to view the results.

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, and is often useful for troubleshooting.
- 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: Capturing counter data with a data collector set

In this demonstration, you will see how to:

- Create a data collector set.
- Create a disk load on the server.
- Analyze the resulting data in a report.

Demonstration Steps

Create a data collector set

1. Switch to **LON-SVR1**, and open **Performance Monitor**.
2. Create a new **User Defined** data collector set with the following key counters:
   - **Processor > % Processor Time**
   - **Memory > Pages/sec**
   - **PhysicalDisk > % Disk Time**
   - **PhysicalDisk > Avg. Disk Queue Length**
   - **System > Processor Queue Length**
   - **Network Interface > Bytes Total/sec**
3. Start the data collector set.

Create a disk load on the server

1. Open a **Windows PowerShell** prompt, and then use the **fsutil** command to create a large file with a size of 104,857,600 bytes.
2. Copy the file to the **LON-DC1** server to generate network load.
3. Create a new copy of the large file on the local hard disk by copying it from **LON-DC1**.
4. Delete all the newly created files.

Analyze the resulting data in a report

1. Switch to **Performance Monitor**, and then stop the data collector set.
2. Select the **Performance Monitor** tool, and then select **View Log Data**.
3. Add the data that you collected in the data collector set to the chart.
4. Change the view to **Report**.

Demonstration: Configuring an alert

By using alert counters, you can create a custom data collector set that contains performance counters. You then can configure actions that occur based on the measured counters exceeding the maximum or dropping below the minimum limits that you define. After you create the data collector set, you must configure the actions that the system will take when the alert criteria are met. Alert counters are especially useful in situations where a performance issue arises periodically. You can configure the actions to run programs, generate events, or a combination of these.

In this demonstration, you will see how to:

- Create a data collector set with an alert counter.
- Generate a server load that exceeds the configured threshold.
- Examine the event log for the resulting event.

Demonstration Steps

Create a data collector set with an alert counter

1. Create a new **User Defined** data collector set.
2. Use the **Performance Counter Alert** option, and then add only the **Processor > % Processor Time** counter.
3. Set the threshold to be above **10** percent and to generate an entry in the event log when this condition is met.
4. Start the data collector set.

Generate a server load that exceeds the configured threshold

1. Open the **Windows PowerShell ISE** prompt, and then run the following script to generate a load on the server:

```
E:\Labfiles\Mod12\StressTest.ps1
```

2. When the script has finished running, close Windows PowerShell ISE.

Examine the event log for the resulting event

- Open **Event Viewer**, and then examine the **Diagnosis-PLA** log for performance alerts.

Demonstration: Viewing reports in Performance Monitor

In this demonstration, you will see how to view a performance report.

Demonstration Steps

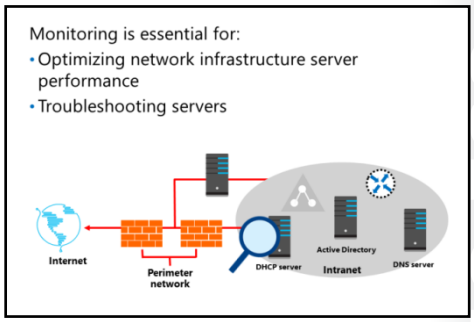
View a performance report

1. In the navigation pane, expand **Reports/User Defined/LON-SVR1 Performance**.
2. Expand the folder beneath **LON-SVR1 Performance**. The data collector set's previous collection process generated this report. You can change from the chart view to any other supported view.
3. If the report is not displayed, click the **Refresh** button on the toolbar, and then repeat **Step 2**.
4. Close all open windows.

Monitoring network infrastructure services

Because network infrastructure services are an essential foundation of many other server-based services, it is important that you configure them correctly and that they run optimally.

Your organization can benefit in several ways by gathering performance-related data on your network infrastructure services.



- Optimizing network-infrastructure server performance. Providing performance baseline and trend data enables you to help your organization optimize the performance of your network infrastructure server.
- Troubleshooting servers. When server performance degrades, either over time or during periods of peak activity, you can help identify possible causes and take corrective action. This can help you quickly bring a service back within the limits of your service level agreement (SLA).

Monitoring DNS

DNS provides name-resolution services on your network. You can monitor the Windows Server 2016 DNS Server role to determine the following aspects of your DNS infrastructure, including the following:

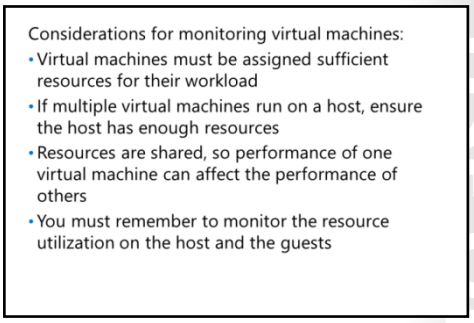
- General DNS server statistics, including the number of overall queries and responses that the DNS server is processing.
- User Datagram Protocol (UDP) or Transmission Control Protocol (TCP) counters, which measure DNS queries and responses that the DNS server processes by using either of these transport protocols.
- Dynamic update and secure dynamic-update counters for measuring registration and update activity that dynamic clients generate.
- Memory-usage counter for measuring the system's memory usage and memory-allocation patterns that are created by operating the server computer as a DNS server.
- Recursive lookup counters for measuring queries and responses when the DNS Server service uses recursion to look up and fully resolve DNS names on behalf of requesting clients.
- Zone transfer counters, including specific counters for measuring all zone transfer (AXFR), incremental zone transfer (IXFR), and DNS zone-update notification activity.

Monitoring DHCP

The Dynamic Host Configuration Protocol (DHCP) service provides dynamic IP configuration services for your network, and provides data on your DHCP server, including the following:

- The **Average Queue Length**, which indicates the current length of the DHCP server's internal message queue. This number represents the number of unprocessed messages that the server receives. A large number might indicate heavy server traffic.
- The **Milliseconds per packet** counter is the average time in milliseconds that the DHCP server uses to process each packet that it receives. This number varies depending on the server hardware and its I/O subsystem. A spike could indicate a problem, either with the I/O subsystem becoming slower or because of an intrinsic processing overhead on the server.

Considerations for monitoring virtual machines



Server virtualization has only been a part of the Windows Server operating system since the release of Windows Server 2008 and the introduction of the Hyper-V role. Many organizations have migrated some or all of their server workloads to virtual machines that are running virtualization servers. From a monitoring perspective, it is important to remember that servers running as guest virtual machines consume resources in the same way as physical host-server computers.

Hyper-V server virtualization enables you to create separate virtual machines, and run them concurrently by using the resources of the operating system that is running on a single physical server. The operating systems running within each virtual machine are guests, while the computer that is running Hyper-V is the host.

Virtual machine guests function as physical computers. Virtual machine guests that are hosted on the same hypervisor remain independent of one another. You can run multiple virtual machines that are using different operating systems on a host server simultaneously, as long as the host server has enough resources.

When you create a virtual machine, you configure characteristics that define the available resources for that guest. These resources include memory, processors, disk-configuration and storage technology, and network-adapter configuration. These virtual machines operate within the boundaries of the resources that you allocate to them, and can suffer from the same performance bottlenecks as host servers. As a result, it is important that you monitor virtual machines in the same way that you monitor your host servers.

Note: It addition to monitoring the virtual machine guests, always remember that you must monitor the host that runs them.

Microsoft provides a tool, Hyper-V Resource Metering, which enables you to monitor resource consumption on your virtual machines. Resource metering allows you to track the resource utilization of virtual machines hosted on Windows Server 2016 computers that have the Hyper-V role installed.

With resource metering, you can measure the following parameters on individual Hyper-V virtual machines:

- Average graphics processing unit (GPU) use.
- Average physical memory use, including:
  - Minimum memory use.
  - Maximum memory use.
- Maximum disk-space allocation.
- Incoming network traffic for a network adapter.
- Outgoing network traffic for a network adapter.

Measuring how much of these resources each virtual machine uses enables an organization to bill departments or customers based on their hosted virtual-machine use, rather than charging a flat fee per virtual machine. An organization with only internal customers also can use these measurements to see use patterns and plan future expansions.

You perform resource-metering tasks by using Windows PowerShell cmdlets in the Hyper-V Windows PowerShell module. There is no graphical user interface (GUI) tool that enables you to perform this task. You can use the following cmdlets to perform resource metering tasks:

- **Enable-VMResourceMetering**. Starts collecting data on a per-virtual-machine basis.
- **Disable-VMResourceMetering**. Disables resource metering on a per-virtual-machine basis.
- **Reset-VMResourceMetering**. Resets virtual machine resource-metering counters.
- **Measure-VM**. Displays resource-metering statistics for a specific virtual machine.

Question: Why is it important to determine the baseline performance of a server?

Lesson 6
Monitoring event logs

Event Viewer provides a convenient and accessible location for you to view events that occur and that Windows Server records into one of several log files based on the type of event that occurs. To support your users, you should know how to access event information quickly and conveniently, and know how to interpret the data in the event log.

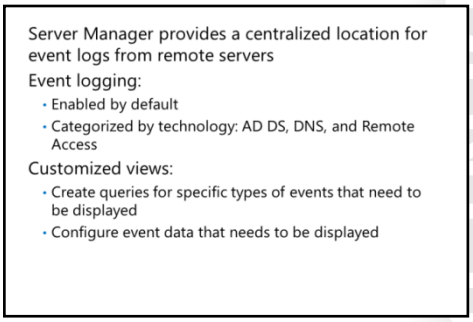
Lesson Objectives

After completing this lesson, you will be able to:

- Describe how to use Server Manager to view event logs.
- Explain what a custom view is.
- Describe how to create a custom view.
- Explain event log subscriptions.
- Describe how to configure an event subscription.

Using Server Manager to view event logs

Server Manager provides a centralized location in which you can store and access event logs for multiple remote servers that you are monitoring. Server Manager provides a monitoring and troubleshooting solution where administrators can view, in one console, information regarding specific events from different servers and applications. This is more efficient than viewing event logs by connecting to a specific server from a remote location.



You can view Server Manager event logs for all servers, a specific server, or a per-server role, such as AD DS, DNS, or Remote Access. You can choose different event log views from the navigation pane in Server Manager:

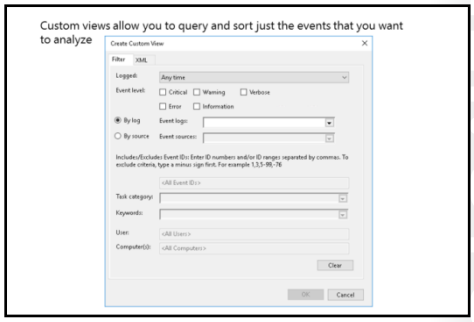
- Local Server. Displays event logs that are generated on the local server where Server Manager is running. By default, Application, Security, and System event logs are displayed.
- All Servers. Displays event logs from all servers that server manager is monitoring.
- AD DS, DNS, and Remote Access. Displays event logs from all servers that Server Manager is monitoring and have specific server roles installed, such as AD DS, DNS, or the Remote Access role. These logs display specific information that the AD DS, DNS, or the Remote Access server role generate.
- Roles and Server Groups tiles in Server Manager Dashboard. You also can choose an Events link in a specific Server Group tile in the Server Manager Dashboard, such as AD DS tile, DNS tile, or Remote Access tile, to display the events for the specific server role.

You can further customize the event log views by:

- Creating queries for specific types of events that need to be displayed. You can save these queries, and use them later when you are searching for events that are defined in the query criteria.
- Configuring event data that needs to be displayed. You can choose what type of events to display, such as Critical, Error, Warning, and Informational. Additionally, you can choose the event-log files from where the events will be displayed, such as Application, Directory Service, DNS Server, Security, System, and Setup.

What is a custom view?

Event logs contain vast amounts of data, and it could be a challenge to narrow the set of events to just those events that interest you. Custom views allow you to query and sort just the events that you want to analyze. You also can save, export, import, and share these custom views.



Event Viewer allows you to filter for specific events across multiple logs, and display all events that might relate to an issue that you are investigating. To specify a filter that spans multiple logs, you need to create a custom view. You create custom views in the **Action** pane in Event Viewer.

You can filter custom views based on multiple criteria, including the:

- Time that the event was logged.
- Event level, including such as errors or warnings.
- Logs from which to include events.
- Specific Event IDs to include or exclude.
- User context of the event.
- Computer on which the event occurred.

Demonstration: Creating a custom view

In this demonstration, you will see how to:

- View Server Roles custom views.
- Create a custom view.

Demonstration Steps

View Server Roles custom views

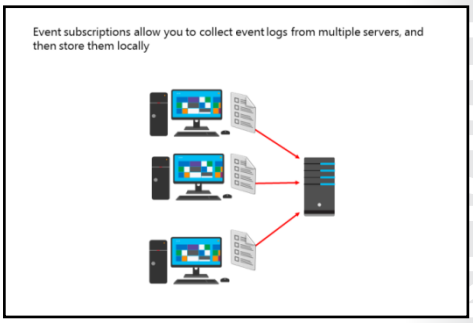
- In **Event Viewer**, examine the predefined **Server Roles** custom views.

Create a custom view

1. Create a new custom view to select the following event types:
   - Critical
   - Warning
   - Error
2. Select the following logs:
   - System
   - Application
3. Name the custom view as **Adatum Custom View**.
4. View the resulting filtered events in the details pane.

What are event log subscriptions?

Event log subscriptions is a feature that, when configured, enables a single server to collect copies of events from multiple systems. Using the Windows Remote Management (WinRM) service and the Windows Event Collector service (Wecsvc), you can collect events in the event logs of a centralized server, where you can analyze them together with other computers' event logs that are being collected on the same central server.



Subscriptions can be either collector-initiated or source computer-initiated:

- Collector-initiated. A collector-initiated subscription, or a pull subscription, identifies all of the computers from which the collector will receive events, and will typically pull events from these computers. In a collector-initiated subscription, the subscription definition is stored and maintained on the collector computer. You use pull subscriptions when you need to configure many of the computers to forward the same types of events to a central location. In this manner, you have to define and specify only one subscription definition to apply to all computers in the group.
- Source computer-initiated. In a source computer-initiated subscription, or push subscription, source computers push events to the collector. In a source computer-initiated subscription, you create and manage the subscription definition on the source computer, which is the computer that is sending events to a central source. You can define these subscriptions manually or by using Group Policy. You create push subscriptions when each server is forwarding a different set of events than other servers are, or when you must maintain control over the event-forwarding process at the source computer. This might be the case when you must make frequent changes to the subscription.

To use the event subscription, you must configure the forwarding and the collecting computers. The event-collecting functionality depends on the WinRM service and Wecsvc. Both of these services must be running on computers that are participating in the forwarding and collecting process.

Enabling Subscriptions

To enable subscriptions, perform the following set of tasks:

1. On each source computer, run the following command at an elevated command prompt to enable WinRM:

```
winrm quickconfig
```

2. On the collector computer, type the following command at an elevated command prompt to enable the Wecsvc:

```
wecutil qc
```

3. Add the computer account of the collector computer to the local Administrators group on each of the source computers.

Demonstration: Configuring an event subscription

In this demonstration, you will see how to:

- Configure the source computer.
- Configure the collector computer.
- Create and view the subscribed log.

Demonstration Steps

Configure the source computer

1. Switch to **LON-DC1** and, if necessary, sign in as **Adatum\Administrator** with the password **Pa$$w0rd**.
2. Run the **winrm quickconfig** command at a command prompt.

   Note that the service is already running.
3. Open **Active Directory Users and Computers**, and then add the **LON-SVR1** computer as a member of the domain local **Administrators** group.

Configure the collector computer

1. Switch to **LON-SVR1**, and then open a command prompt.
2. Run the **wecutil qc** command.

Create and view the subscribed log

1. Switch to **Event Viewer.**
2. Create a new subscription to collect events from **LON-DC1**:
   - Collector initiated
   - Source computer **LON-DC1**
   - All events types
   - Last 30 days

Question: In your environment, how often do you check the event logs on your servers?

Lab B: Monitoring and troubleshooting Windows Server 2016

Scenario

A. Datum is a global engineering and manufacturing company with its head office in London, England. An IT office and datacenter are in London to support the London office and other locations. A. Datum recently deployed a Windows Server 2016 server and client infrastructure.

Because the organization has deployed new servers, it is important to establish a performance baseline with a typical load for these new servers. You have been asked to work on this project. Additionally, to make the process of monitoring and troubleshooting easier, you decide to perform centralized monitoring of event logs.

Objectives

After completing this lab, you will be able to:

- Establish a performance baseline.
- Identify the source of a performance problem.
- View and configure centralized event logs.

Lab Setup

Estimated Time: **60 minutes**

Virtual machines: **20740A-LON-DC1** and **20740A-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, click **Start**, point to **Administrative Tools**, and then click **Hyper-V Manager**.
2. In **Microsoft Hyper-V Manager**, click **20740A-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 using the following credentials:
    - User name: **Administrator**
    - Password: **Pa$$w0rd**
    - Domain: **Adatum**
5. Repeat steps 2 through 4 for **20740A-LON-SVR1**.

Exercise 1: Establishing a performance baseline

Scenario

In this exercise, you will use Performance Monitor on the server, and create a baseline by using typical performance counters.

The main tasks for this exercise are as follows:

1. Create and start a data collector set.
2. Create a typical workload on the server.
3. Analyze the collected data.

▶ Task 1: Create and start a data collector set

1. Switch to the **LON-SVR1** computer.
2. Open **Performance Monitor**.
3. Create a new **User Defined** data collector set by using the following information to complete the process:
   - Name: **LON-SVR1 Performance**
   - Create: **Create manually (Advanced)**
   - Type of data: **Performance counter**
   - Select the following counters:
     - **Memory, Pages/sec**
     - **Network Interface, Bytes Total/sec**
     - **PhysicalDisk, %Disk Time**
     - **PhysicalDisk, Avg. Disk Queue Length**
     - **Processor, %Processor Time**
     - **System, Processor Queue Length**
   - Sample interval: **1 second**
   - Where to store data: **Default value**
4. Save and close the data collector set.
5. In **Performance Monitor**, in the **Results** pane, right-click **LON-SVR1 Performance**, and then click **Start**.

▶ Task 2: Create a typical workload on the server

1. Open a command prompt, and then run the following commands by pressing Enter after each command:

```
Fsutil file createnew bigfile 104857600
Copy bigfile \\LON-dc1\c$
Copy \\LON-dc1\c$\bigfile bigfile2
Del bigfile*.*
Del \\LON-dc1\c$\bigfile*.*
```

2. Do not close the **Windows PowerShell** window.

▶ Task 3: Analyze the collected data

1. Switch to **Performance Monitor**.
2. Stop the **LON-SVR1 Performance** data collector set.
3. In **Performance Monitor**, in the navigation pane, go to **Reports**, **User Defined**, **LON-SVR1**, **LON-SVR1_DateTime-000001**, and then review the report data.
4. Record the values that are listed in the report for later analysis. Recorded values include:
   - **Memory, Pages/sec**
   - **Network Interface, Bytes Total/sec**
   - **PhysicalDisk, %Disk Time**
   - **PhysicalDisk, Avg. Disk Queue Length**
   - **Processor, %Processor Time**
   - **System, Processor Queue Length**

Results: After this exercise, you should have established a baseline for performance-comparison purposes.

Exercise 2: Identifying the source of a performance problem

Scenario

In this exercise, you will simulate a load to represent the system in live usage, gather performance data by using your data collector set, and then determine the potential cause of the performance problem.

The main tasks for this exercise are as follows:

1. Capture performance data by using a data collector set.
2. Create additional workload on the server.
3. Remove the workload, and then review the performance data.

▶ Task 1: Capture performance data by using a data collector set

1. Switch to **Performance Monitor**.
2. In **Performance Monitor**, go to **Data Collector Sets**, **User Defined**, and in the results pane start the **LON-SVR1 Performance** data collector set.

▶ Task 2: Create additional workload on the server

1. On **LON-SVR1**, open the **Windows PowerShell ISE** window, and then run the following script to generate a load on the server:

```
E:\Labfiles\Mod12\StressTest.ps1
```

2. When the script is complete, close **Windows PowerShell ISE**.

▶ Task 3: Remove the workload, and then review the performance data

1. Switch to **Performance Monitor**.
2. Stop the **LON-SVR1 Performance** data collector set.

3. In **Performance Monitor**, in the navigation pane, go to **Reports**, **User Defined**, **LON-SVR1**, **LON-SVR1_DateTime-000002**, and then review the report data.

   Record the following values:

   - **Memory, Pages/sec**
   - **Network Interface, Bytes Total/sec**
   - **PhysicalDisk, %Disk Time**
   - **PhysicalDisk, Avg. Disk Queue Length**
   - **Processor, %Processor Time**
   - **System, Processor Queue Length**

   Question: Compared with your previous report, which values have changed?

   Question: What would you recommend?

Results: After this exercise, you should have used performance tools to identify a potential performance bottleneck.

Exercise 3: Viewing and configuring centralized event logs

Scenario

In this exercise, you will use **LON-DC1** to collect event logs from **LON-SVR1**. Specifically, you will use this process to gather performance-related alerts from your network servers.

The main tasks for this exercise are as follows:

1. Configure subscription prerequisites.
2. Create a subscription.
3. Configure a performance counter alert.
4. Introduce additional workload on the server.
5. Verify the results.
6. Prepare for course completion.

▶ Task 1: Configure subscription prerequisites

1. Switch to **LON-DC1**.
2. Open a command prompt and run **winrm quickconfig** to enable the administrative changes that are necessary on a source computer.
3. Add the **LON-SVR1** computer to the built-in **Administrators** group.
4. Switch to **LON-SVR1**.
5. At the command prompt, run **wecutil qc** to enable the administrative changes that are necessary on a collector computer.

▶ Task 2: Create a subscription

1. On **LON-SVR1**, open **Event Viewer**.
2. Create a new subscription with the following properties:
   - Computers: **LON-DC1**
   - Name: **LON-SVR1 Events**
   - **Collector initiated**
   - Logged: **Last 7 days**
   - Events: **Critical**, **Warning**, **Information**, **Verbose**, and **Error**
   - Logs: **Applications and Services Logs> Microsoft > Windows > Diagnosis-PLA > Operational**

▶ Task 3: Configure a performance counter alert

1. Switch to **LON-DC1**.
2. Open **Performance Monitor**.
3. Create a new **User Defined** data collector set by using the following information to complete the process:
   - Name: **LON-DC1 Alert**
   - Create: **Create manually (Advanced)**
   - Type of data: **Performance counter Alert**
   - Select the following counters: **Processor, %Processor Time** above **10** percent
   - Sample interval: **1** second
   - Where to store data: default value
   - Alert Action: **Log an entry in the application event log**
4. Start the **LON-SVR1 Alert** data collector set.

▶ Task 4: Introduce additional workload on the server

1. On **LON-DC1**, open the **Windows PowerShell ISE** window, and then run the following script to generate a load on the server:

```
E:\Labfiles\Mod12\StressTest.ps1
```

2. When the script is complete, close **Windows PowerShell ISE**.

▶ Task 5: Verify the results

- Switch to **LON-SVR1**, and then open **Forwarded Events**.

Question: In Performance Monitor, are there any performance-related alerts in the subscribed application log? Hint: They have an ID of 2031. If you do not receive any events, proceed with the rest of the lab.

Results: At the end of this exercise, you should have successfully centralized event logs and examined these logs for performance-related events.

▶ Task 6: Prepare for course completion

When you are finished with the lab, revert all virtual machines to their initial state. To do this, perform the following steps:

1. On the host computer, start **Microsoft Hyper-V Manager**.
2. In the **Virtual Machines** list, right-click **20740A-LON-DC1**, and then click **Revert**.
3. In the **Revert Virtual Machines** dialog box, click **Revert**.
4. Repeat steps 2 and 3 for **20740A-LON-SVR1**.

Question: During the lab, you collected data in a data collector set. What is the advantage of collecting data this way?

Module Review and Takeaways

Review Questions

Question: Your manager has asked if all updates to the Windows operating system should be applied automatically when they are released. Do you recommend an alternative process?

Question: Your organization implements several applications that are not Microsoft applications. A colleague has proposed using WSUS to deploy application and operating system updates. Are there any potential issues with using WSUS?

Question: Why is WSUS easier to manage in an Active Directory Domain Services (AD DS) domain?

Question: What significant counters should you monitor in Performance Monitor?

Question: Why is it important to monitor server performance periodically?

Question: Why should you use performance alerts?

Tools

The following table lists the tools that this module references.

Tool	Use	Where to find it
WSUS Administration console	Administer WSUS	Server Manager - Tools
Windows PowerShell WSUS cmdlets	Administer WSUS from the command-line interface	Windows PowerShell
Server Manager Dashboard	Monitoring multiple servers	Server Manager
Performance Monitor	Monitoring and analyzing real-time and logged performance data	Server Manager/Tools
Reliability Monitor	Monitoring hardware and software issues	Control Panel
Resource Monitor	Monitoring the use and performance of CPUs, disks, networks, and memory in real time	Server Manager/Tools
Event Viewer	Viewing and managing event logs	Server Manager/Tools
Task Manager	Identifying and resolving performance-related problems	Server Manager/Tools

Best Practices

- Create an end-to-end monitoring strategy for your IT infrastructure. Monitoring should focus on proactively detecting potential failures or performance issues.
- When monitoring, estimate the baseline system utilizations for each server. This will help you determine whether the system is performing well or is overused.

Common Issues and Troubleshooting Tips

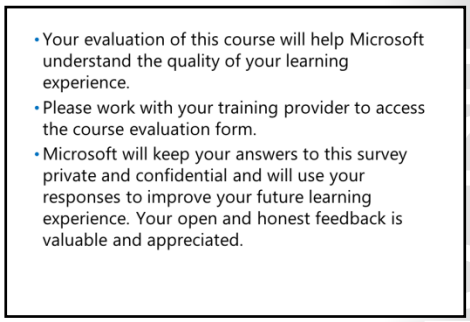
Common Issue	Troubleshooting Tip
During monitoring, multiple sources are concurrently reporting different problems.	

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.



Module 1: Installing, upgrading, and migrating servers and workloads

Lab: Installing and configuring Nano Server

Exercise 1: Installing Nano Server

▶ Task 1: Copy the required Windows PowerShell scripts

1. Switch to **LON-DC1**.
2. Right-click **Start**, and then click **Windows PowerShell (Admin)**.
3. In the **Windows PowerShell** window, type **cd**, and then press Enter.
4. In the **Windows PowerShell** window, type **md Nano**, and then press Enter.
5. In the **Windows PowerShell** window, type the following command, and then press Enter:

```
copy d:\NanoServer\NanoServerImageGenerator\*.ps* c:\nano
```

▶ Task 2: Import Windows PowerShell modules

- In the **Windows PowerShell** window, type the following command, and then press Enter:

```
Import-Module c:\nano\NanoServerImageGenerator.psm1
```

▶ Task 3: Create a virtual hard drive

1. In the **Windows PowerShell** window, type the following command, and then press Enter:

```
new-NanoServerImage -Edition Standard -mediapath D:\ -Basepath c:\nano -targetpath
c:\nano\nano-svr1.vhdx -DeploymentType Guest -computername NANO-SVR1 -storage -
packages Microsoft-NanoServer-IIS-Package
```

2. At the **AdministratorPassword** prompt, type **Pa$$w0rd**, and then press Enter.
3. When the process is completed, on the taskbar, click **File Explorer**, navigate to **C:\Nano**, and then examine the files listed. Verify that **nano-svr1.vhdx** exists.

Note: Normally, you would now create a virtual machine to use the **nano-svr1.vhdx** file. However, to expedite the process, you will start a virtual machine that has already been created.

▶ Task 4: Sign in to the NANO-SVR1 virtual machine

1. On **NANO-SVR1**, in the **User name** box, type **Administrator**, and then press the Tab key.
2. In the **Password** box, type **Pa$$w0rd**, and then press Enter.

Results: After completing this exercise, you will have successfully created the required virtual hard drive for Nano Server.

Exercise 2: Completing post-installation tasks on Nano Server

▶ Task 1: Use the Nano Server Recovery Console to view basic settings

1. On **NANO-SVR1**, in the **Nano Server Recovery Console**, observe that the computer name is **NANO-SVR1** and that the computer is in a workgroup. Press the Tab key until **Networking** is selected, and then press Enter.
2. Press Enter on the **Ethernet** adapter. In **Network Adapter Settings**, notice that DHCP is providing the IP configuration.
3. Make a note of the IP address.
4. Press Esc twice.

▶ Task 2: Add Nano Server to the domain

1. Switch to **LON-DC1**.
2. Switch to the **Administrator: Windows PowerShell** window.
3. At the command prompt, type the following cmdlet, and then press Enter:

```
djoin.exe /provision /domain adatum /machine nano-svr1 /savefile .\odjblob
```

Note: Replace the IP address 172.16.0.X in the following commands with the IP address you recorded earlier from your Nano Server installation.

4. At the command prompt, type the following cmdlet, and then press Enter. Your IP address will be different.

```
Set-Item WSMan:\localhost\Client\TrustedHosts "172.16.0.X"
```

5. Type **Y**, and when prompted, press Enter.
6. At the command prompt, type the following cmdlet, and then press Enter. Your IP address will be different.

```
$ip = "172.16.0.X"
```

7. At the command prompt, type the following cmdlet, and then press Enter:

```
Enter-PSSession -ComputerName $ip -Credential $ip\Administrator
```

8. In the **Windows PowerShell credential request** dialog box, in the **Password** box, type **Pa$$w0rd**, and then click **OK**.
9. At the command prompt, type the following cmdlet, and then press Enter:

```
netsh advfirewall firewall set rule group="File and Printer Sharing" new enable=yes
```

10. At the command prompt, type the following cmdlet, and then press Enter:

```
Exit-PSSession
```

11. At the command prompt, type the following command, and then press Enter. Your IP address will be different.

```
net use z: \\172.16.0.X\c$
```

12. At the command prompt, type **Z:**, and then press Enter.
13. At the command prompt, type the following command, and then press Enter:

```
copy c:\odjblob
```

14. At the command prompt, type the following cmdlet, and then press Enter:

```
Enter-PSSession -ComputerName $ip -Credential $ip\Administrator
```

15. In the **Windows PowerShell credential request** dialog box, in the **Password** box, type **Pa$$w0rd**, and then click **OK**.
16. At the command prompt, type **cd**, and then press Enter.
17. At the command prompt, type the following cmdlet, and then press Enter:

```
djoin /requestodj /loadfile c:\odjblob /windowspath c:\windows /localos
```

18. At the command prompt, type the following cmdlet, and then press Enter. Nano Server restarts.

```
shutdown /r /t 5
```

19. Switch to **NANO-SVR1**.
20. In the **User name** box, type **Administrator**, and then press the Tab key.
21. In the **Password** box, type **Pa$$w0rd** and then press Tab.
22. In the **Domain** box, type **Adatum**, and then press Enter.
23. In the **Nano Server Recovery Console**, observe that the computer is in the adatum.com domain.

▶ Task 3: Use Windows PowerShell to configure the settings of Nano Server

1. Switch to **LON-DC1**, and then close Windows PowerShell.
2. Right-click **Start**, and then click **Windows PowerShell (Admin)**.
3. At the command prompt, type the following cmdlet, and then press Enter:

```
get-windowsfeature –comp Nano-svr1
```

4. At the command prompt, type the following cmdlet, and then press Enter:

```
install-windowsfeature Fs-fileserver –comp Nano-svr1
```

5. Do not worry if you receive a yellow warning message. At the command prompt, type the following cmdlet, and then press Enter:

```
get-windowsfeature –comp Nano-svr1
```

6. At the command prompt, type the following cmdlet, and then press Enter. Substitute the X for the last octet of the IP address on the Nano server.

```
$ip = "172.16.0.X"
```

7. At the command prompt, type the following cmdlet, and then press Enter:

```
Enter-PSSession -ComputerName $ip -Credential $ip\Administrator
```

8. In the **Windows PowerShell credential request** dialog box, in the **Password** box, type **Pa$$w0rd**, and then click **OK**.
9. At the command prompt, type the following cmdlet, and then press Enter:

```
get-netipaddress
```

10. At the command prompt, type the following cmdlet, and then press Enter:

```
bcdedit /enum
```

11. At the command prompt, type the following cmdlet, and then press Enter:

```
net share
```

12. At the command prompt, type the following cmdlet, and then press Enter:

```
Exit-PSSession
```

Results: After completing this exercise, you will have successfully configured the domain and network settings of Nano Server and installed an additional role.

Exercise 3: Performing remote management

▶ Task 1: Enable remote management with Server Manager

1. On **LON-DC1**, if necessary, open **Server Manager**.
2. In **Server Manager**, in the navigation pane, right-click **All Servers**, and then click **Add Servers**.
3. In the **Add Servers** dialog box, in the **Name (CN):** box, type **Nano-SVR1**, and then click **Find Now**.
4. In the **Name** list, click **Nano-svr1**, and then to add the computer to the **Computer** list, press the Right Arrow key and then click **OK**.
5. In **Server Manager**, expand **File and Storage Services**.
6. Click **Shares**, and then in the **TASKS** list, click **New Share**.
7. In the **New Share Wizard**, click **SMB Share – Quick**, and then click **Next**.
8. On the **Select the server and path for this share** page, in the **Server** list, click **nano-svr1**, and then click **Next**.
9. On the **Specify share name** page, in the **Share name** box, type **Data**, and then click **Next**.
10. To complete the wizard, click **Next** twice, and then click **Create**.
11. Click **Close**.

▶ Task 2: Test the file server and web server on Nano Server

1. On **LON-DC1**, switch to the **Administrator: Windows PowerShell** window.
2. At the command prompt, type the following command, and then press Enter:

```
net use z: /d
```

3. At the command prompt, type the following command, and then press Enter:

```
net use z: \\Nano-svr1\c$
```

4. Click **Start**, type **Notepad**, and then press Enter.
5. In Notepad, type **<H1> Nano Server Website </H1>**.
6. Click **File**, and then click **Save As**.
7. In the **Save As** dialog box, in the **File name** box, type **z:\Inetpub\wwwroot**, and then press Enter.
8. In the **Save as type** list, click **All Files**.
9. In the **File name** box, type **Default.htm**, and then click **Save**.
10. Close Notepad.
11. Click **Start**, click **All apps**, click **Windows Accessories**, and then click **Internet Explorer**.
12. Navigate to **http://nano-svr1**. Does your web page display?
13. Close Windows Internet Explorer.
14. On **LON-DC1**, at the command prompt, type the following command, and then press Enter:

```
net use y: \\nano-svr1\data
```

15. Type **cmd** and press Enter.
16. Type **write**, and then press Enter.
17. In WordPad, type **This is my document**, click **File**, and then click **Save**.
18. In the **Save As** dialog box, in the **File name** box, type **Y:**, and then press Enter.
19. In the **File name** box, type **My document**, and then click **Save**.
20. In File Explorer, navigate to **data (\\nano-svr1) (Y:)**. Is your file listed?

▶ Task 3: Prepare for the next module

After you finish the lab, revert the virtual machines to their initial state by completing the following steps:

1. On the host computer, switch to the **Hyper-V Manager** console.
2. In the **Virtual Machines** list, right-click **20740A-LON-DC1**, and then click **Revert**.
3. In the **Revert Virtual Machine** dialog box, click **Revert**.
4. Repeat steps 2 and 3 for **20740A-NANO-SVR1**.

Module 2: Configuring local storage

Lab: Configuring local storage

Exercise 1: Creating and managing volumes

▶ Task 1: Create a hard disk volume and format for Resilient File System (ReFS)

1. Switch to **LON-SVR1**.
2. Right-click **Start**, and then click **Windows PowerShell (Admin)**.
3. To list all the available disks that have yet to be initialized, at the Windows PowerShell command prompt, type the following command, and then press Enter:

```
Get-Disk | Where-Object PartitionStyle –Eq "RAW"
```

4. To initialize disk 2, at the Windows PowerShell command prompt, type the following command, and then press Enter:

```
Initialize-disk 2
```

5. To review the partition table type, at the Windows PowerShell command prompt, type the following command, and then press Enter:

```
Get-disk
```

6. To create an ReFS volume by using all available space on disk 1, at the Windows PowerShell command prompt, type the following command, and then press Enter:

```
New-Partition -DiskNumber 2 -UseMaximumSize -AssignDriveLetter | Format-Volume -
NewFileSystemLabel "Simple" -FileSystem ReFS
```

7. On the taskbar, click **File Explorer**.
8. If you are prompted "Do you want to format it," click **Cancel**.
9. On the taskbar, click **File Explorer**.

Question: What drive letter has been assigned to the newly created volume?

Answer: Answers might vary, but it is assumed to be drive F.

▶ Task 2: Create a mirrored volume

1. Right-click **Start**, and then click **Disk Management**.
2. In the lower half of the display, scroll down and right-click **Disk 3** and then click **Online**.
3. Repeat for Disk 4.
4. Close and reopen **Disk Management**.
5. In the **Initialize Disk** dialog box, click **OK** to initialize disks 3 and 4.
6. On Disk 3, right-click **Unallocated**, and then click **New Mirrored Volume**.
7. In the **New Mirrored Volume Wizard**, click **Next**.
8. On the **Select Disks** page, in the available list, click **Disk 4**, and then click **Add >**.
9. In the **Select the amount of space in MB** box, accept the default value, and then click **Next**.

10. On the **Assign Drive Letter or Path** page, in the **Assign the following drive letter** box, click **M**, and then click **Next**.
11. On the **Format Volume** page, in the **Volume label** text box, type **MIRROR**.
12. Select the **Perform a quick format** check box, and then click **Next**.
13. Click **Finish** to create your mirrored volume.
14. In the **Disk Management** dialog box, click **Yes** to convert both disks to dynamic disks.

Results: After completing this exercise, you should have successfully created several volumes.

Exercise 2: Resizing volumes

▶ Task 1: Create a simple volume and resize it

1. Switch to **Windows PowerShell (Admin)**.
2. At the Windows PowerShell command prompt, type the following command, and then press Enter:

```
Initialize-disk 5
```

3. At the Windows PowerShell command prompt, type the following command, and then press Enter:

```
Diskpart
```

4. At the command prompt, type the following command, and then press Enter:

```
List disk
```

5. At the command prompt, type the following command, and then press Enter:

```
Select disk 5
```

6. At the command prompt, type the following command, and then press Enter:

```
Convert dynamic
```

7. At the command prompt, type the following command, and then press Enter:

```
Create volume simple size=10000 disk=5
```

8. At the command prompt, type the following command, and then press Enter:

```
Assign letter=z
```

9. At the command prompt, type the following command, and then press Enter:

```
Format
```

10. Switch to Disk Management. Verify the presence of an NTFS volume on **Disk 5** of size approximately **10** gigabytes (GB).
11. At the Windows PowerShell command prompt, type the following command, and then press Enter:

```
Extend size 10000
```

12. Switch to **Disk Management**.
13. Verify the presence of an NTFS volume on **Disk 5** of size approximately **20** GB.

▶ Task 2: Shrink a volume

1. At the Windows PowerShell command prompt, type the following command, and then press Enter:

```
Shrink desired=15000
```

2. Switch to **Disk Management**.
3. Verify the presence of an NTFS volume on **Disk 5** of size approximately **5** GB.
4. Close the **Windows PowerShell (Admin)** window.

Results: After completing this exercise, you should have successfully resized a volume.

▶ Task 3: Prepare for the next exercise

1. On the host computer, start **Microsoft Hyper-V Manager**.
2. In the **Virtual Machines** list, right-click **20740A-LON-DC1**, and then click **Revert**.
3. In the **Revert Virtual Machine** dialog box, click **Revert**.
4. Repeat steps 2 and 3 for **20740A-LON-SVR1**.
5. Restart your computer and select **20740A-LON-HOST1** when prompted.
6. Sign in as **Administrator** with the password **Pa$$w0rd**.

Exercise 3: Managing virtual hard disks

▶ Task 1: Install the Windows PowerShell Hyper-V module

1. On your host computer, click **Start** and then click **Server Manager**.
2. In **Server Manager**, 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, select the **Hyper-V** check box, click **Add Features**, and then click **Next**.
7. On the **Select features** page, click **Next**.
8. On the **Hyper-V** page, click **Next**.
9. On the **Create Virtual Switches** page, click **Next**.
10. On the **Virtual Machine Migration** page, click **Next**.
11. On the **Default Stores** page, click **Next**.

12. On the **Confirm installation selections** page, select **Restart the destination server automatically if required**, click **Yes**, and then click **Install**.

Note: Your computer might restart several times following installation of the Hyper-V components.

13. Sign in as **Administrator** with the password **Pa$$w0rd**.

▶ Task 2: Create a virtual hard disk

1. On your host computer, right-click **Start**, and then click **Windows PowerShell (Admin)**.
2. At the Windows PowerShell command prompt, type the following command, and then press Enter:

```
New-VHD -Path c:\sales.vhd -Dynamic -SizeBytes 10Gb | Mount-VHD -Passthru |Initialize-Disk -Passthru |New-Partition -AssignDriveLetter -UseMaximumSize |Format-Volume -FileSystem NTFS -Confirm:$false -Force
```

Note: If you get a Microsoft Windows pop-up dialog box prompting you to format the disk, you can close it and continue.

▶ Task 3: Reconfigure the virtual hard disk

Note: These steps are a duplicate of the high-level steps.

3. To dismount the virtual hard disk, at the Windows PowerShell command prompt, type the following command, and then press Enter:

```
Dismount-vhd C:\Sales.vhd
```

4. To check the properties of the virtual hard disk, at the Windows PowerShell command prompt, type the following command, and then press Enter:

```
Get-vhd C:\Sales.vhd
```

Question: What is the physical sector size?

Answer: Answers will vary, but is likely to be 512.

5. To convert to a .vhdx file, at the Windows PowerShell command prompt, type the following command, and then press Enter:

```
Convert-VHD –Path C:\Sales.vhd –DestinationPath c:\Sales.vhdx
```

6. To change the sector size, at the Windows PowerShell command prompt, type the following command, and then press Enter:

```
Set-VHD –Path c:\Sales.vhdx –PhysicalSectorSizeBytes 4096
```

7. To check the properties of the .vhdx file, at the Windows PowerShell command prompt, type the following command, and then press Enter:

```
Get-vhd C:\Sales.vhdx
```

Question: What is the physical sector size?

Answer: Answers will vary, but is likely to be 4096.

8. To optimize the .vhdx file, at the Windows PowerShell command prompt, type the following command, and then press Enter:

```
Optimize-VHD –Path c:\Sales.vhdx –Mode Full
```

Results: After completing this exercise, you should have successfully created and managed virtual hard disks by using Windows PowerShell.

▶ Task 4: Prepare for the next module

- Restart your computer and when prompted, choose Windows Server 2012.

Module 3: Implementing enterprise storage solutions

Lab: Planning and configuring storage technologies and components

Exercise 1: Planning storage requirements

▶ Task 1: Read the supporting documentation

- Read the supporting documentation in the lab exercise scenario.

▶ Task 2: Record your planned course of action

1. You plan to evaluate iSCSI, Fibre Channel, and InfiniBand solutions to meet the requirements. Which solution do you expect to select?

   You would not use InfiniBand because the requirements call for reasonable performance and low cost. InfiniBand is for high-performance solutions, and it is expensive. Meanwhile, of the two remaining choices, iSCSI most closely matches the low cost and reasonable performance requirements that you expect. You should deploy an iSCSI solution to each of the geographic locations that has an Information Technology (IT) infrastructure and that requires storage.

2. Which storage type do you plan to implement for the SQL databases, block-level storage or file-level storage?

   Based on the requirements alone, you could use either type, because each has advantages and disadvantages. SQL databases can run SMB file shares since the release of SMB 3.0, and the overall performance is similar to that of block-level storage. The answer might depend on whether you have an existing highly available SMB file server infrastructure and whether the server team or the storage team will manage the storage.

3. How will your solution minimize administrative overhead for the storage administrators?

   By selecting iSCSI, you avoid the complexities of Fibre Channel and InfiniBand solutions. In addition, an iSCSI solution requires less hardware and less software. All of these choices reduce the administrative overhead for the storage administrators.

4. Which server role(s) do you plan to use for the provisioning of VMWare ESX/ESXi virtual machines?

   You can use the Server for NFS role to create NFS file shares that VMWare ESX/ESXi virtual machines support.

5. Will you run the Hyper-V in Windows Server 2012 virtual machines on NFS or SMB?

   The Hyper-V virtual machines can run on SMB, but NFS does not support them. As a result, you will need to run the virtual machines on SMB.

6. Which file sharing protocol will you use for UNIX clients that require access?

   Historically, NFS was the protocol of choice for UNIX clients to access file shares. However, today most UNIX clients equally support NFS and SMB natively. Therefore, you can use either of the technologies. If you have an existing NFS file sharing deployment, you would likely choose NFS. If you have an existing SMB file sharing deployment, you would likely choose SMB.

7. How do you plan to disable legacy SMB access for existing SMB file shares?

   a. First, you need to locate all the existing file servers that have legacy SMB shares. You can check for legacy shares on the current host by using the following command at a Windows PowerShell prompt:

   ```
   Get-SmbServerConfiguration | Select EnableSMB1Protocol
   ```

   You also can create a Windows PowerShell script to check for legacy shares on all the file servers.

   b. After you have located all of the existing file servers that have legacy SMB shares, you need to disable the SMB access. You can disable the SMB 1 protocol on each server, by using the following command:

   ```
   Set-SmbServerConfiguration -EnableSMB1Protocol $false
   ```

   You also can create a Windows PowerShell script to disable legacy SMB access across all of your servers.

Results: After completing this exercise, you should have successfully planned a storage solution that will meet your organization's requirements.

Exercise 2: Configuring iSCSI storage

▶ Task 1: Enable network adapters

1. On **LON-DC1**, right-click the **Start** button and click **Windows PowerShell (Admin)**.
2. At the Windows PowerShell prompt, type **Get-NetAdapter | Enable-NetAdapter** and press Enter.
3. Close the Window PowerShell prompt.
4. On **LON-SVR1**, right-click the **Start** button and click **Windows PowerShell (Admin)**.
5. At the Windows PowerShell prompt, type **Get-NetAdapter | Enable-NetAdapter** and press Enter.
6. Close the Window PowerShell prompt.

▶ Task 2: Install the iSCSI target feature

1. On **LON-DC1**, in **Server Manager**, click the **Manage** menu and 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, click **Next**.
4. On the **Select destination server** page, ensure that **Select a server from the server pool** is selected, and then click **Next**.
5. On the **Select server roles** page, expand **File and Storage Services (2 of 12 Installed)**, expand **File and iSCSI Services (1 of 11 Installed)**, select the **iSCSI Target Server** check box, and then click **Next**.
6. On the **Select features** page, click **Next**.
7. On the **Confirm installation selections** page, click **Install**.
8. When the installation completes, click **Close**.

▶ Task 3: Create and configure an iSCSI target

1. On **LON-DC1**, in **Server Manager**, in the navigation pane, click **File and Storage Services**.
2. In the **File and Storage Services** pane, click **iSCSI**.
3. In the **iSCSI VIRTUAL DISKS** pane, click **TASKS**, and then click **New iSCSI Virtual Disk**.
4. In the **New iSCSI Virtual Disk Wizard**, on the **Select iSCSI virtual disk location** page, under **Storage location**, click volume **C**, and then click **Next**.
5. On the **Specify iSCSI virtual disk name** page, in the **Name** text box, type **iSCSIDisk1**, and then click **Next**.
6. On the **Specify iSCSI virtual disk size** page, in the **Size** text box, type **5**, ensure that **GB** is selected, and then click **Next**.
7. On the **Assign iSCSI target** page, ensure that the **New iSCSI target** option is selected, and then click **Next**.
8. On the **Specify target name** page, in the **Name** box, type **LON-DC1**, and then click **Next**.
9. On the **Specify access servers** page, click **Add**.
10. In the **Select a method to identify the initiator** dialog box, click **Enter a value for the selected type**, in the **Type** list, click **IP Address**, in the **Value** text box, type **10.100.100.3**, and then click **OK**.
11. On the **Specify access servers** page, click **Add**.
12. In the **Select a method to identify the initiator** dialog box, click **Enter a value for the selected type**, in the **Type** list, click **IP Address**, in the **Value** text box, type **10.200.100.3**, and then click **OK**.
13. On the **Specify access servers** page, click **Next**.
14. On the **Enable Authentication** page, click **Next**.
15. On the **Confirm selections** page, click **Create**.
16. On the **View results** page, wait until the virtual disk is created, and then click **Close**.
17. In the **iSCSI VIRTUAL DISKS** pane, click **TASKS**, and then click **New iSCSI Virtual Disk**.
18. In the **New iSCSI Virtual Disk Wizard**, on the **Select iSCSI virtual disk location** page, under **Storage location**, click volume **C**, and then click **Next**.
19. On the **Specify iSCSI virtual disk name** page, in the **Name** box, type **iSCSIDisk2**, and then click **Next**.
20. On the **Specify iSCSI virtual disk size** page, in the **Size** box, type **5**, ensure that **GB** is selected, and then click **Next**.
21. On the **Assign iSCSI target** page, click **lon-dc1**, and then click **Next**.
22. On the **Confirm selection** page, click **Create**.
23. On the **View results** page, wait until the virtual disk is created, and then click **Close**.

▶ Task 4: Configure MPIO

1. On **LON-SVR1**, click **Start**, and then click **Server Manager**.
2. In **Server Manager**, click the **Manage** menu and 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, ensure that **Select a server from the server pool** is selected, and then click **Next**.
6. On the **Select server roles** page, click **Next**.
7. On the **Select features** page, click **Multipath I/O**, and then click **Next**.
8. On the **Confirm installation selections** page, click **Install**.
9. When installation is complete, click **Close**.
10. Restart **LON-SVR1**, and then sign in as **Adatum\Administrator** with the password **Pa$$w0rd**.
11. Click **Start**, and then click **Server Manager**.
12. In **Server Manager**, on the menu bar, click **Tools**, and then click **iSCSI Initiator**.
13. In the **Microsoft iSCSI** dialog box, click **Yes**.
14. In the **iSCSI Initiator Properties** dialog box, on the **Targets** tab, in the **Target** box, type **10.100.100.2**, and then click **Quick Connect**.
15. In the **Quick Connect** box, click **Done**.
16. In the **iSCSI Initiator Properties** dialog box, click **OK** to close the dialog box.
17. In **Server Manager**, on the menu bar, click **Tools**, and then click **MPIO**.
18. In the **MPIO Properties** dialog box, on the **Discover Multi-Paths** tab, select **Add support for iSCSI devices**, and then click **Add**.
19. When you are prompted to restart the computer, click **Yes**.
20. After the computer restarts, sign in to **LON-SVR1** as **Adatum\Administrator** with the password **Pa$$w0rd**.
21. Click **Start**, and then click **Server Manager**.
22. In **Server Manager**, on the menu bar, click **Tools**, and then click **MPIO**.
23. In the **MPIO Properties** dialog box, on the **MPIO Devices** tab, notice that **Device Hardware Id MSFT2005iSCSIBusType_0x9** has been added to the list.
24. In the **MPIO Properties** dialog box, click **OK** to close the dialog box.

▶ Task 5: Connect to the iSCSI target

1. On **LON-SVR1**, in **Server Manager**, on the menu bar, click **Tools**, and then click **iSCSI Initiator**.
2. In the **iSCSI Initiator Properties** dialog box, on the **Targets** tab, click **Disconnect**.
3. In the **Disconnect From All Sessions** dialog box, click **Yes**.
4. In the **iSCSI Initiator Properties** dialog box, on the **Targets** tab, click **Connect**.
5. In the **Connect To Target** dialog box, select the **Enable multi-path** check box, verify that the **Add this connection to the list of Favorite Targets** check box is selected, and then click **Advanced**.
6. In the **Advanced Settings** dialog box, on the **General** tab, change the **Local adapter** from **Default** to **Microsoft iSCSI Initiator**.
7. In the **Initiator IP** list, select **10.100.100.3**.
8. In the **Target portal IP** list, click **10.100.100.2 / 3260**.
9. In the **Advanced Settings** dialog box, click **OK**.
10. In the **Connect To Target** dialog box, click **OK**.

11. In the **iSCSI Initiator Properties** dialog box, on the **Targets** tab, click **Connect**.
12. In the **Connect To Target** dialog box, click **Enable multi-path**, verify that the **Add this connection to the list of Favorite Targets** check box is selected, and then click **Advanced**.
13. In the **Advanced Settings** dialog box, on the **General** tab, change the **Local adapter** from **Default** to **Microsoft iSCSI Initiator**.
14. In the **Initiator IP** list, select **10.200.100.3**.
15. In the **Target portal IP** list, select **10.200.100.2 / 3260**.
16. In the **Advanced Settings** dialog box, click **OK**.
17. In the **Connect To Target** dialog box, click **OK**.
18. In the **iSCSI Initiator Properties** dialog box, on the **Volumes and Devices** tab, click **Auto Configure**.
19. In the **iSCSI Initiator Properties** dialog box, on the **Targets** tab, in the **Targets** list, select **iqn.1991-05.com.microsoft:lon-dc1-lon-dc1-target**, and then click **Devices**.
20. In the **Devices** dialog box, click **MPIO**.
21. Verify that, in **Load balance policy**, **Round Robin** is selected.
22. Under **This device has the following paths**, notice that two paths are listed. Select the first path, and then click **Details**.
23. Note the IP address of the source and target portals, and then click **OK**.
24. Select the second path, and then click **Details**.
25. Verify that this path is using another network, and then click **OK**.
26. In the **Device Details** dialog box, click **OK**.
27. In the **Devices** dialog box, click **OK**.
28. In the **iSCSI Initiator Properties** dialog box, click **OK**.

▶ Task 6: Initialize the iSCSI disks

1. On **LON-SVR1**, in **Server Manager**, click **File and Storage Services**, and then in the left pane, click **Disks**.
2. In the right pane, right-click an offline disk with a bus type of **iSCSI**, and then click **Bring Online**.
3. In the **Bring Disk Online** dialog box, click **Yes** to bring the disk online.
4. Right-click the iSCSI disk that you brought online, and then click **New Volume**.
5. In the **New Volume Wizard**, on the **Before you begin** page, click **Next**.
6. On the **Select the server and disk** page, ensure that your iSCSI disk is selected, and then click **Next**.
7. In the **Offline or Uninitialized Disk** dialog box, click **OK** to initialize the disk as a GPT disk.
8. On the **Specify the size of the volume** page, click **Next** to accept the default of using the entire disk size for the volume.
9. On the **Assign to a drive letter or folder** page, in the **Drive letter** list, select **J**, and then click **Next**.
10. On the **Select file system settings** page, in the **Volume label** text box, type **SMBShares**, and then click **Next**.
11. On the **Confirm selections** page, to finish creating the volume, click **Create**.

12. After the volume is created, on the **Completion** page, click **Close**.
13. In **Server Manager**, in the right pane, right-click the remaining offline disk with a bus type of iSCSI, and then click **Bring Online**.
14. In the **Bring Disk Online** dialog box, click **Yes** to bring the disk online.
15. Right-click the iSCSI disk that you brought online, and then click **New Volume**.
16. In the **New Volume Wizard**, on the **Before you begin** page, click **Next**.
17. On the **Select the server and disk** page, ensure that your iSCSI disk is selected, and then click **Next**.
18. In the **Offline or Uninitialized Disk** dialog box, click **OK** to initialize the disk as a GPT disk.
19. On the **Specify the size of the volume** page, click **Next** to accept the default of using the entire disk size for the volume.
20. On the **Assign to a drive letter or folder** page, in the **Drive letter** list, select **K**, and then click **Next**.
21. On the **Select file system settings** page, in the **File system** box, select **NTFS**.
22. In the **Volume label** text box, type **NFSShares**, and then click **Next**.
23. On the **Confirm selections** page, to finish creating the volume, click **Create**.
24. After the volume is created, on the **Completion** page, click **Close**.
25. On the taskbar, click **File Explorer**, browse to **This PC**, and then verify that the **SMBShares** and **NFSShares** volumes are displayed.

Results: After completing this exercise, you should have successfully configured an iSCSI target that uses MPIO for redundancy.

Exercise 3: Configuring and managing the share infrastructure

▶ Task 1: Create an SMB share on iSCSI storage

1. On **LON-SVR1**, in **Server Manager**, in the navigation pane, click **File and Storage Services**, and then click **Shares**.
2. In the **Shares** area, click **TASKS**, and then click **New Share**.
3. In the **New Share Wizard**, on the **Select the profile for this share** page, in the **File share profile** box, click **SMB Share – Quick**, and then click **Next**.
4. On the **Select the server and path for this share** page, select **LON-SVR1**, click **Select by volume**, click **J:**, and then click **Next**.
5. On the **Specify share name** page, in the **Share name** box, type **Data**, and then click **Next**.
6. On the **Configure share settings** page, select the **Enable access-based enumeration** check box, and then click **Next**.
7. On the **Specify permissions to control access** page, click **Customize permissions**.
8. In the **Advanced Security Settings for Data** window, on the **Permissions** tab, click **Add**.
9. In the **Permission Entry for Data** window, click **Select a principal**, type **Domain Users**, and then click **OK**.
10. In the **Basic permissions** area, select the **Modify** check box, and then click **OK**.

11. In the **Advanced Security Settings for Data** window, click **OK**.
12. On the **Specify permissions to control access** page, click **Next**.
13. On the **Confirm selections** page, click **Create**.
14. When the creation of the share is complete, click **Close**.

▶ Task 2: Create an NFS share on iSCSI storage

1. On **LON-SVR1**, in the **Shares** area, click **TASKS**, and then click **New Share**.
2. In the **New Share Wizard**, on the **Select the profile for this share** page, in the **File share profile** box, click **NFS Share – Quick**, and then click **Next**.
3. On the **Select the server and path for this share** page, click **LON-SVR1**, click **Select by volume**, click **K:**, and then click **Next**.
4. On the **Specify share name** page, in the **Share name** box, type **LinuxData**, and then click **Next**.
5. On the **Specify authentication methods** page, select **Kerberos v5 authentication(Krb5)**, and then click **Next**.
6. On the **Specify the share permissions** page, click **Add**.
7. In the **Add Permissions** window, click **All Machines.**
8. In the **Share permissions** box, select **Read / Write**, and then click **Add**.
9. On the **Specify the share permissions** page, click **Next**.
10. On the **Specify permissions to control access** page, click **Next**.
11. On the **Confirm selections** page, click **Create**.
12. On the **View results** page, click **Close**.

▶ Task 3: Use Windows PowerShell to view share information

1. On **LON-DC1**, on the taskbar, click **File Explorer**.
2. In **File Explorer**, in the address bar, type **\\LON-SVR1\Data**, and then press Enter.
3. Click the **Home** tab, click **New item**, and then click **Text Document**.
4. Type **NewFile**, and then press Enter to rename the document.
5. Double-click **NewFile.txt** to open it in Notepad.
6. Leave Notepad open for later in the task.
7. On **LON-SVR1**, right-click **Start**, and then click **Windows PowerShell (Admin)**.
8. At the Windows PowerShell prompt, type the following command, and then press Enter:

```
Get-NfsShare
```

9. Type the following command, and then press Enter:

```
Get-NfsShare LinuxData | FL *
```

10. Type the following command, and then press Enter:

```
Get-SmbShare
```

11. Type the following command, and then press Enter:

```
Get-SmbShare Data | FL *
```

12. Type the following command, and then press Enter:

```
Get-SmbSession
```

13. Type the following command, and then press Enter:

```
Get-SMBSession -ClientUserName Adatum\Administrator | FL *
```

14. Type the following command, and then press Enter:

```
Get-SmbOpenFile
```

Note: There are two entries for **Adatum\Administrator**. File Explorer creates one, and Notepad creates the other. **NewFile.txt** is not included because the file connection is maintained only for brief periods when you open the file initially or save it. If you do not see two entries, switch to **LON-DC1**, close Notepad and then double-click **NewFile.txt**. Then, on **LON-SVR1**, repeat step 14.

15. Leave the Windows PowerShell prompt open for the next task.

▶ Task 4: Disable the legacy SMB1 protocol

1. On **LON-SVR1**, at the Windows PowerShell prompt, Type the following command, and then press Enter:

```
Set-SmbServerConfiguration -AuditSmb1Access $true
```

2. Type **Y** to confirm and press Enter.
3. Type the following command, and then press Enter:

```
Get-SmbServerConfiguration | FL enable*
```

4. Type the following command, and then press Enter:

```
Set-SmbServerConfiguration -EnableSMB1Protocol $false
```

5. Type **Y** to confirm, and then press Enter.
6. Type the following command, and then press Enter:

```
Get-WindowsFeature *SMB*
```

7. Type the following command, and then press Enter:

```
Remove-WindowsFeature FS-SMB1
```

8. Close the Windows PowerShell prompt.

Results: After completing this exercise, you should have successfully created SMB and NFS shares.

▶ Task 5: Prepare for the next module

After you finish the lab, revert the virtual machines to their initial state by completing the following steps:

1. On the host computer, switch to the **Hyper-V Manager** console.
2. In the **Virtual Machines** list, right-click **20740A-LON-DC1**, and then click **Revert**.
3. In the **Revert Virtual Machines** dialog box, click **Revert**.
4. Repeat steps 2 and 3 for **20740A-LON-SVR1**.

Module 4: Implementing Storage Spaces and Data Deduplication

Lab A: Implementing Storage Spaces

Exercise 1: Creating a Storage Space

▶ Task 1: Create a storage pool from six disks that are attached to the server

1. On **LON-SVR1**, click **Start**, and then click **Server Manager**.
2. In **Server Manager**, in the left pane, click **File and Storage Services**, and then in the **Servers** pane, click **Storage Pools**.
3. In the **STORAGE POOLS** pane, click **TASKS**, and then, in the **TASKS** drop-down list, click **New Storage Pool**.
4. In the **New Storage Pool Wizard**, on the **Before you begin** page, click **Next**.
5. On the **Specify a storage pool name and subsystem** page, in the **Name** text box, type **StoragePool1**, and then click **Next**.
6. On the **Select physical disks for the storage pool** page, select the first six disks in the **Physical disks** list and then click **Next**.
7. On the **Confirm selections** page, click **Create**.
8. On the **View results** page, wait until the task completes, and then click **Close**.

▶ Task 2: Create a three-way mirrored virtual disk (need at least five physical disks)

1. On **LON-SVR1**, in **Server Manager**, in the **Storage Pools** pane, click **StoragePool1**.
2. In the **VIRTUAL DISKS** pane, click **TASKS**, and then, from the **TASKS** drop-down list, click **New Virtual Disk**.
3. In the **New Virtual Disk Wizard**, on the **Before you begin** page, click **Next**.
4. On the **Select the storage pool** page, click **StoragePool1**, and then click **Next**.
5. On the **Specify the virtual disk name** page, in the **Name** text box, type **Mirrored Disk**, and then click **Next**.
6. On the **Specify enclosure resiliency** page, click **Next**.
7. On the **Select the storage layout** page, in the **Layout** list, click **Mirror**, and then click **Next**.
8. On the **Configure the resiliency settings** page, click **Three-way mirror**, and then click **Next**.

   Note: If the three-way resiliency setting is unavailable, proceed to the next step in the lab.

9. On the **Specify the provisioning type** page, click **Thin**, and then click **Next**.
10. On the **Specify the size of the virtual disk** page, in the **Specify size** text box, type **10**, and then click **Next**.
11. On the **Confirm selections** page, click **Create**.
12. On the **View results** page, wait until the task completes.

13. Ensure that the **Create a volume when this wizard closes** check box is selected, and then click **Close**.
14. In the **New Volume Wizard** window, on the **Before you begin** page, click **Next**.
15. On the **Select the server and disk** page, in the **Disk** pane, click the **Mirrored Disk** virtual disk, and then click **Next**.
16. On the **Specify the size of the volume** page, click **Next** to confirm the default selection.
17. On the **Assign to a drive letter or folder** page, in the **Drive letter** drop-down list, ensure that **H** is selected, and then click **Next**.
18. On the **Select file system settings** page, in the **File system** drop-down list, click **ReFS**, in the **Volume label** text box, type **Mirrored Volume**, and then click **Next**.
19. On the **Confirm selections** page, click **Create**.
20. On the **Completion** page, wait until the creation completes, and then click **Close**.

▶ Task 3: Copy a file to the volume, and verify it is visible in File Explorer

1. On **LON-SVR1**, click **Start**, on the **Start** screen, type **command prompt**, and then press Enter.
2. When you receive the command prompt, type the following command, and then press Enter:

```
Copy C:\windows\system32\write.exe H:\
```

3. Close **Command Prompt**.
4. On the taskbar, click the **File Explorer** icon.
5. In the **File Explorer** window, in the navigation pane, click **Mirrored Volume (H:)**.
6. Verify that **write.exe** is visible in the file list.
7. Close **File Explorer**.

▶ Task 4: Remove a physical drive to simulate drive failure

1. On the host computer, open **Hyper-V Manager**.
2. In the **Virtual Machines** pane, right-click **20740A-LON-SVR1**, and then click **Settings**.
3. In **Settings** for **20740A-LON-SVR1**, in the **Hardware** pane, click the hard drive that begins with **20740A-LON-SVR1-Disk1**.
4. In the **Hard Drive** pane, click **Remove**, click **OK**, and then click **Continue**.

▶ Task 5: Verify that the file is still available

1. Switch to **LON-SVR1**.
2. On the taskbar, click the **File Explorer** icon.
3. In the **File Explorer** window, in the navigation pane, click **Mirrored Volume (H:)**.
4. In the **file list** pane, verify that **write.exe** is still available.
5. Close **File Explorer**.
6. In **Server Manager**, in the **STORAGE POOLS** pane, on the menu bar, click **Refresh "Storage Pools"**.

Note: Notice the warning that is visible next to Mirrored Disk.

7. In the **VIRTUAL DISK** pane, right-click **Mirrored Disk**, and then click **Properties**.
8. In the **Mirrored Disk Properties** dialog box, in the left pane, click **Health**.

   Note: Notice that the Health Status indicates a warning. The Operational Status should indicate one or more of the following: Incomplete, Unknown, or Degraded.

9. In the **Mirrored Disk Properties** dialog box, click **OK**.

▶ Task 6: Add a new disk to the storage pool and remove the broken disk

1. On **LON-SVR1**, in **Server Manager**, in the **STORAGE POOLS** pane, on the menu bar, click **Refresh "Storage Pools"**.
2. In the **STORAGE POOLS** pane, right-click **StoragePool1**, and then click **Add Physical Disk**.
3. In the **Add Physical Disk** window, click the first disk in the list, and then click **OK**.
4. Right-click **Start**, and then click **Windows PowerShell (Admin)**.
5. In **Windows PowerShell**, type the following command, and then press Enter:

```
Get-PhysicalDisk
```

6. Note the FriendlyName for the disk that shows an OperationalStatus of Lost Communication.
7. In **Windows PowerShell**, type the following command, and then press Enter:

```
$Disk = Get-PhysicalDisk -FriendlyName 'diskname'
```

   Replace *diskname* with the name of the disk that you noted in Step 6.

8. In **Windows PowerShell**, type the following command, and then press Enter:

```
Remove-PhysicalDisk -PhysicalDisks $disk -StoragePoolFriendlyName StoragePool1
```

9. In **Windows PowerShell**, type **Y**, and then press Enter.
10. In **Server Manager**, in the **STORAGE POOLS** pane, on the menu bar, click the **Refresh "Storage Pools"** button to see the warnings disappear.

Results: After completing this exercise, you will have successfully created a storage pool and added five disks to it. Additionally, you should have created a three-way mirrored, thinly-provisioned virtual disk from the storage pool. You also should have copied a file to the new volume and then verified that it is accessible. Next, after removing a physical drive, you should have verified that the virtual disk was still available and that you could access it. Finally, you should have added another physical disk to the storage pool.

Lab B: Implementing Data Deduplication

Exercise 1: Installing Data Deduplication

▶ Task 1: Install the Data Deduplication role service

1. On **LON-SVR1**, in **Server Manager**, in the navigation pane, click **Dashboard**.
2. In the details pane, 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, in the **Roles** list, expand **File and Storage Services (4 of 12 installed)**.
7. Expand **File and iSCSI Services (3 of 11 installed)**.
8. Select the **Data Deduplication** check box, and then click **Next**.
9. On the **Select features** page, click **Next**.
10. On the **Confirm installation selections** page, click **Install**.
11. When installation is complete, on the **Installation progress** page, click **Close**.

▶ Task 2: Check the status of Data Deduplication

1. On **LON-SVR1**, switch to **Windows PowerShell**.
2. In the **Windows PowerShell command prompt** window, type the following command, and then press Enter:

```
Get-DedupVolume
```

3. In the **Windows PowerShell command prompt** window, type the following command, and then press Enter:

```
Get-DedupStatus
```

4. These commands return no results. This is because you need to enable it on the volume after installing it.

▶ Task 3: Verify the virtual machine performance

- On **LON-SRV1**, in the **Windows PowerShell** window, type the following, and then press Enter:

```
Measure-Command -Expression {Get-ChildItem –Path E:\ -Recurse}
```

Note: You will use the values returned from the previous command later in the lab.

Results: After completing this exercise, you should have successfully installed the Data Deduplication role service and enabled it on one of your file servers.

Exercise 2: Configuring Data Deduplication

▶ Task 1: Configure Data Deduplication

1. On **LON-SVR1**, on the taskbar, click the **File Explorer** icon.
2. In **Server Manager**, in the navigation pane, click **File and Storage Services**, and then click **Disks**.
3. In the **Disks** pane, click **1**.
4. Beneath **VOLUMES**, click **E**.
5. Right-click **E**, and then click **Configure Data Deduplication**.
6. In the **Allfiles (E:\) Deduplication Settings** dialog box, in the **Data deduplication** list, click **General purpose file server**.
7. In the **Deduplicate files older than (in days)** text box, type **0**.
8. Click **Set Deduplication Schedule**.
9. In the **LON-SVR1 Deduplication Schedule** dialog box, select the **Enable throughput optimization** check box, and then click **OK**.
10. In the **Allfiles (E:\) Deduplication Settings** dialog box, click **Add**.
11. In the **Select Folder** dialog box, expand **Allfiles (E:)**, click **shares**.
12. Click **Select Folder**, and then click **OK**.

▶ Task 2: Configure optimization to run now and view the status

1. On **LON-SRV1**, in the **Windows PowerShell** window, type the following command, and then press Enter:

```
Start-DedupJob E: -Type Optimization –Memory 50
```

2. In the **Windows PowerShell** window, type the following command, and then press Enter:

```
Get-DedupJob –Volume E:
```

Note: Verify the status of the optimization job from the previous command. Repeat the previous command until the Progress shows as 100%.

▶ Task 3: Verify if the file has been optimized

1. On **LON-SVR1**, in **File Explorer**, navigate to **e:\Labfiles\Mod04**.
2. Right-click **ContosoP1AnnualReport.docx**, and then select **Properties**.
3. In the **Properties** window, observe the values of **Size** and **Size on disk** and note any differences.
4. Repeat steps 2 and 3 for a few more files to verify deduplication.
5. Switch to **Windows PowerShell**.
6. In the **Windows PowerShell command prompt** window, type the following command, and then press Enter:

```
Get-DedupStatus –Volume E: |fl
```

7. In the **Windows PowerShell command prompt** window, type the following command, and then press Enter:

```
Get-DedupVolume –Volume E: |fl
```

Note: Observe the number of optimized files.

8. In **Server Manager**, in the navigation pane, click **File and Storage Services**, and then click **Disks**.
9. In the **DISKS** pane, click **1**.
10. Beneath **VOLUMES**, click **E**.
11. Click **Refresh** and observe the values for **Deduplication Rate** and **Deduplication Savings**.

Note: Because most of the files on drive E are small, you may not notice a significant amount of saved space.

▶ Task 4: Verify VM performance again

- In the **Windows PowerShell** window, type the following command, and then press Enter:

```
Measure-Command -Expression {Get-ChildItem –Path E:\ -Recurse}
```

Note: Compare the values returned from the previous command with the value of the same command earlier in the lab to assess if system performance has changed.

Results: After completing this exercise, you should have successfully configured Data Deduplication for the appropriate data volume on **LON-SVR1**.

▶ Task 5: Prepare for the next module

When you complete the lab, revert the virtual machines to their initial state.

1. On the host computer, start **Hyper-V Manager**.
2. In the **Virtual Machines** list, right-click **20740A-LON-SVR1**, and then click **Revert**.
3. In the **Revert Virtual Machine** dialog box, click **Revert**.
4. Repeat steps 2 and 3 for **20740A-LON-DC1**.

Module 5: Installing and configuring Hyper-V and virtual machines

Lab: Installing and configuring Hyper-V

Exercise 1: Verifying installation of the Hyper-V server role

▶ Task 1: Verify the presence of the Hyper-V server role

1. On **LON-HOST1**, sign in as **Administrator** by using **Pa$$w0rd** as the password.
2. Click **Start**, and then click **Server Manager**.
3. Click **Tools**, and then click **Hyper-V Manager**.
4. In **Hyper-V Manager**, click **LON-HOST1**, and then click **Hyper-V Settings**.
5. In the **Hyper-V Settings** for **LON-HOST1** window, click each of the available options in the left pane and read the description.
6. Click **Cancel**.

Results: After completing this exercise, you should have successfully verified the presence and configuration of the Hyper-V server role on a physical server.

Exercise 2: Configuring Hyper-V networks

▶ Task 1: Create an external network

Note: To perform this task, your computer must have physical network card (wired or wireless) and be connected to a network.

1. In **Hyper-V Manager**, click **LON-HOST1**, and then, in the **Actions** pane, click **Virtual Switch Manager**.
2. In the **Virtual Switch Manager for LON-HOST1** window, in the left pane, click **New virtual network switch**.
3. In the **Create virtual switch** pane, click **External**, and then click **Create Virtual Switch**.
4. In the **Virtual switch properties** pane, in the **Name** box, type **Physical Network**.
5. In the **Connection type** area, click **External network**, select the **Allow management operating system to share this network adapter** check box, and then click **OK**.
6. In the **Apply Networking Changes** dialog box, read the warning that is displayed, and then click **Yes**.
7. In **Server Manager**, click **Local Server**, and then verify that the name of the network adapter has changed to **vEthernet (Physical Network)**.

▶ Task 2: Create a private network

1. On **LON-HOST1**, in **Hyper-V Manager**, in the **Actions** pane, click **Virtual Switch Manager**.
2. In the **Virtual Switch Manager for LON-HOST1** window, in the left pane, click **New virtual network switch**.
3. In the **Create virtual switch** pane, click **Private**, and then click **Create Virtual Switch**.
4. In the **Virtual Switch Properties** pane, in the **Name** box, type **Isolated Network**.
5. In the **Connection type** area, verify that **Private network** is selected, and then click **OK**.
6. In **Server Manager**, verify that no new network adapters are visible.

▶ Task 3: Create an internal network

1. On **LON-HOST1**, in **Hyper-V Manager**, in the **Actions** pane, click **Virtual Switch Manager**.
2. In the **Virtual Switch Manager for LON-HOST1** window, in the left pane, click **New virtual network switch**.
3. In the **Create virtual switch** pane, click **Internal**, and then click **Create Virtual Switch**.
4. In the **Virtual Switch Properties** pane, in the **Name** box, type **Host Internal Network**.
5. In the **Connection type** area, verify that **Internal network** is selected, and then click **OK**.
6. In **Server Manager**, verify that a new network adapter named **vEthernet (Host Internal Network)** has been created.

Results: After completing this exercise, you should have successfully configured an external, internal, and private network.

Exercise 3: Creating and configuring virtual machines

▶ Task 1: Create a Generation 2 virtual machine

1. On **LON-HOST1**, on the taskbar, click **File Explorer**.
2. In **File Explorer**, go to **E:\Program Files\Microsoft Learning\20740\Drives**.

   Note: The drive letter for this path might vary depending on the configuration of the physical host.

3. Verify that the **20740A-BASE.vhd** hard disk image file is present.
4. Click the **Home** tab, and then click the **New Folder** icon twice to create two new folders. Right-click each folder and rename them:
   - **LON-GUEST1**
   - **LON-GUEST2**
5. Close **File Explorer**.
6. In **Hyper-V Manager**, in the **Actions** pane, click **New**, and then click **Virtual Machine**.
7. On the **Before You Begin** page of the **New Virtual Machine Wizard**, click **Next**.

8. On the **Specify Name and Location** page of the **New Virtual Machine Wizard**, select **Store the virtual machine in a different location**, enter the following values, and then click **Next**:
   - Name: **LON-GUEST2**
   - Location: **E:\Program Files\Microsoft Learning\20740\Drives\LON-GUEST2**
9. On the **Specify Generation** page, click **Generation 2**, and click **Next**.
10. On the **Assign Memory** page of the **New Virtual Machine Wizard**, enter a value of **1024 MB**, and then click **Next**.
11. On the **Configure Networking** page of the **New Virtual Machine Wizard**, select **Isolated Network**, and then click **Next**.
12. On the **Connect Virtual Hard Disk** page, choose **Create a virtual hard disk**.
13. In the **Name** box, type **LON-GUEST2.vhdx**.
14. In the **Location** box, type **E:\Program Files\Microsoft Learning\20740\Drives\LON-GUEST2**.
15. In the **Size** box, type **127**, and then click **Finish**.
16. Right-click **LON-GUEST2**, and then click **Settings**.
17. In the **Settings for LON-GUEST2 on LON-HOST1** window, in the **Hardware** area, click **SCSI Controller**.
18. In the right pane, click **DVD Drive**, and then click **Add**.
19. In the **DVD Drive** area, click **Image file**.
20. In the **Image file** box, type **E:\Program Files\Microsoft Learning\20740\Drives \WinServer2016_TP5.iso**, and then click **Apply**.
21. In the **Hardware** area, click **Firmware**.
22. In the **Boot order** area, click **Network Adapter**, click **Move Down** twice, and then click **OK**.
23. Right-click **LON-GUEST2**, and then click **Connect**.
24. In the **LON-GUEST2 on LON-HOST1 – Virtual Machine Connection** window, click **Start**.
25. Press a key to boot from DVD.
26. In the **Windows Setup** window, click **Next**, and then click **Install now**.
27. On the **Activate Windows** page, click **I don't have a product key**.
28. On the **Select the operating system you want to install** page, click **Windows Server 2016 Datacenter Technical Preview 5 (Desktop Experience)**, and then click **Next**.
29. On the **License terms** page, select the **I accept the license terms** check box, and then click **Next**.
30. On the **Which type of installation do you want** page, click **Custom: Install Windows only (advanced)**.
31. On the **Where do you want to install Windows** page, click **Drive 0 Unallocated Space**, and then click **Next**.

Note: The installation of Windows requires an extended period of time. You can work on the next task while waiting for the installation to complete.

32. On the **Customize settings** page, in the **Password** and **Reenter password** text boxes, type **Pa$$w0rd**, and then click **Finish**.
33. After the installation is complete, in the **LON-GUEST2 on LON-HOST1 – Virtual Machine Connection** window, click **Shut Down**, and then click **Shut Down** again to confirm.

▶ Task 2: Create a Generation 1 virtual machine

1. Click **Start**, and then click the **Windows PowerShell** icon.
2. At the Windows PowerShell prompt, type the following command to link **20740A-BASE.vhd** to the correct parent disk and press Enter:

```
Set-VHD "E:\Program Files\Microsoft Learning\20740\Drives\20740A-BASE.vhd" -
ParentPath "E:\Program Files\Microsoft Learning\Base\Base16D-WS16-TP5.vhd"
```

3. In **Hyper-V Manager**, in the **Actions** pane, click **New**, and then click **Hard Disk**.
4. On the **Before You Begin** page of the **New Virtual Hard Disk Wizard**, click **Next**.
5. On the **Choose Disk Format** page, select **VHD**, and then click **Next**.
6. On the **Choose Disk Type** page, select **Differencing**, and then click **Next**.
7. On the **Specify Name and Location** page, specify the following details, and then click **Next**:
   - Name: **LON-GUEST1.vhd**
   - Location: **E:\Program Files\Microsoft Learning\20740\Drives\LON-GUEST1**
8. On the **Configure Disk** page, type **E:\Program Files\Microsoft Learning\20740\Drives \20740A-BASE.vhd** as the location, and then click **Finish**.
9. Click **Start**, and then click the **Windows PowerShell** icon.
10. At the **Windows PowerShell** prompt, enter the following command to create a new virtual machine named **LON-GUEST1**:

```
New-VM –Name LON-GUEST1 –MemoryStartupBytes 1024MB –VHDPath "E:\Program
Files\Microsoft Learning\20740\Drives\LON-GUEST1\LON-GUEST1.vhd" –SwitchName
"Isolated Network"
```

11. Close the **Windows PowerShell** window.

▶ Task 3: Configure virtual machines

1. On **LON-HOST1**, in **Hyper-V Manager**, right-click **LON-GUEST1**, and then click **Settings**.
2. In the **Settings for LON-GUEST1 on LON-HOST1** window, note the list of hardware for **LON-GUEST1**.
3. In the **Hardware** area, click **Memory**.
4. Select the **Enable Dynamic Memory** check box.
5. In the **Maximum RAM** box, type **4096**.
6. In the **Hardware** area, click **Processor**.
7. In the **Number of virtual processors** box, type **2**.
8. In the **Hardware** area, click **Network Adapter**.
9. In the **Bandwidth Management** area, select the **Enable bandwidth management** check box.
10. In the **Minimum bandwidth** text box, type **10**.

11. In the **Maximum bandwidth** text box, type **100**.
12. In the **Management** area, click **Integration Services**.
13. Select the **Guest services** check box, and then click **OK**.

> **Note:** You must have completed the previous tasks in this exercise before you can continue. This includes shutting down LON-GUEST2.

14. In **Hyper-V Manager**, right-click **LON-GUEST2**, and then click **Settings**.
15. In the **Settings for LON-GUEST2 on LON-HOST1** window, note the list of hardware for **LON-GUEST2**. Note the differences from **LON-GUEST1**.
16. In the **Hardware** area, click **Security**, and then read the settings that are available.
17. In the **Hardware** area, click **Memory**.
18. Verify that the **Enable dynamic memory** check box is not selected.
19. In the **Hardware** area, click **Processor**.
20. In the **Number of virtual processors** text box, type **2**.
21. In the **Hardware** area, expand **Hard Drive**, and then click **Quality of Service**.
22. Select the **Enable Quality of Service management** check box.
23. In the **Minimum** text box, type **10**.
24. In the **Management** area, click **Integration Services**.
25. Select the **Guest services** check box, and then click **OK**.

▶ Task 4: Create checkpoints

1. On **LON-HOST1**, in **Hyper-V Manager**, right-click **LON-GUEST2**, and then click **Checkpoint**.
2. Right-click **LON-GUEST2**, and then click **Start**.
3. Right-click **LON-GUEST2**, and then click **Connect**.
4. On **LON-GUEST2**, sign in as **Administrator** by using **Pa$$w0rd** as the password.
5. In **Server Manager**, click **Local Server** and notice that there is only one network adapter.
6. On **LON-HOST1**, in **Hyper-V Manager**, right-click **LON-GUEST2**, and then click **Settings**.
7. In the **Settings for LON-GUEST2 on LON-HOST1** window, in the **Hardware** area, click **Add Hardware**.
8. In the **Add Hardware** area, click **Network Adapter**, and then click **Add**.
9. In the **Network adapter** area, in the **Virtual switch** box, select **Host Internal Network**, and then click **OK**.
10. On **LON-GUEST2**, in **Server Manager**, refresh the view and verify that a second network adapter has been added.
11. On **LON-HOST1**, in **Hyper-V Manager**, right-click **LON-GUEST2**, and then click **Checkpoint**.
12. Read the information in the **Virtual Machine Checkpoint** window, and then click **OK**.
13. Right-click the most recent checkpoint, and then click **Apply**.

14. In the **Apply Checkpoint** dialog box, click **Apply**.
15. Verify that the **Status for LON-GUEST2** is stopped because it was a production checkpoint.

▶ Task 5: Enable host resource protection

1. On **LON-HOST1**, click the **Start** button, and then click **Windows PowerShell**.
2. At the **Windows PowerShell** prompt, type the following command, and then press Enter.

```
Set-VMProcessor LON-GUEST2 -EnableHostResourceProtection $true
```

3. Close the **Windows PowerShell** window.

▶ Task 6: Export a virtual machine

1. On **LON-HOST1**, in **Hyper-V Manager**, right-click **LON-GUEST2**, and then click **Export**.
2. In the **Export Virtual Machine** dialog box, in the **Location** text box, type **E:\Program Files \Microsoft Learning\20740\Drives\Guest2-Bak**, and then click **Export**.

Results: After completing this exercise, you should have successfully created and configured both a Generation 1 virtual machine and a Generation 2 virtual machine.

Exercise 4: Enabling nested virtualization for a virtual machine

▶ Task 1: Import LON-NVHOST2

Note: Before beginning this task, verify the location of the base drives and 20740 course drives. You need the drive letter for both locations in this exercise. The exercise assumes that the drive letter **E:** is used for both, but substitute the correct drive letter as necessary.

1. On **LON-HOST1**, click **Start**, and then click **Windows PowerShell**.
2. At the **Windows PowerShell** prompt, type the following, and then press Enter:

```
& 'E:\Program Files\Microsoft Learning\20740\Drives\CreateVirtualSwitches.ps1'
```

3. At the **Windows PowerShell** prompt, type the following, and then press Enter:

```
& 'E:\Program Files\Microsoft Learning\20740\Drives\LON-HOST1_VM-Pre-Import-
20740A.ps1'
```

4. Type the drive letter for the base images, and then press Enter.
5. Type the drive letter for the course images, and then press Enter.
6. Press Enter to continue.

▶ Task 2: Enable nested virtualization

1. At the **Windows PowerShell** prompt, type the following command, and then press Enter:

```
C:\Labfiles\Mod05\Enable-NestedVm.ps1 -vmName "20740A-LON-NVHOST2"
```

2. To accept the changes that will be made to the virtual machine, type **Y**, and then press Enter.
3. To enable MAC address spoofing, type **Y**, and then press Enter.
4. To set the memory at 4 GB, type **Y**, and then press Enter.

▶ Task 3: Enable Hyper-V

1. On **LON-HOST1**, at the **Windows PowerShell** prompt, type the following, and then press Enter:

```
Get-VM | FT Name,Version
```

2. Type the following, and then press Enter:

```
Update-VMVersion 20740A-LON-NVHOST2
```

3. To confirm the change, type **Y**, and then press Enter:
4. Type the following, and then press Enter:

```
Start-VM 20740A-LON-NVHOST2
```

5. To view the activity on **LON-NVHOST2**, in **Hyper-V Manager**, right-click **20740A-LON-NVHOST2** and click **Connect**.
6. Wait until **LON-NVHOST2** has started, and then type the following at the Windows PowerShell prompt, and then press Enter:

```
Enter-PSSession -VMName 20740A-LON-NVHOST2
```

7. When you receive a prompt, sign in as **Adatum\Administrator** by using **Pa$$w0rd** as the password.
8. Type the following, and then press Enter:

```
Install-WindowsFeature -Name Hyper-V -IncludeAllSubFeature -IncludeManagementTools -
Restart
```

9. Wait for **LON-NVHOST2** to restart. The virtual machine might restart several times.
10. Sign in to **LON-NVHOST2** as **Adatum\Administrator** by using **Pa$$w0rd** as the password.
11. Click **Start**, and then click **Server Manager**.
12. In **Server Manager**, click **Tools**, and then click **Hyper-V Manager**.
13. Verify that **LON-NVHOST2** is listed in **Hyper-V Manager**, and then close **Hyper-V Manager**.

Results: After completing this exercise, you should have successfully configured a virtual machine for nested virtualization.

▶ Task 4: Prepare for the next module

- Leave your host computer started as **LON-HOST1**.

Module 7: Overview of high availability and disaster recovery

Lab: Planning and implementing a high availability and disaster recovery solution

Exercise 1: Determining the appropriate high availability and disaster recovery solution

▶ Task 1: Design the appropriate high availability and disaster recovery solution

Question:

What actions should you take and which technologies should you consider using?

Answer:

Create a Business Recovery Plan to outline and prioritize the divisional and service requirements, with the customer facing financial requirements having the most critical requirements

Consider using Live Migration for monthly planned downtime to allow for patching of your virtual machines.

Consider using Storage Migration to migrate the virtual machine storage off the existing server, to upgrade the existing servers' storage, and to migrate back the virtual machine storage to the server without any virtual machine downtime.

Consider using Hyper-V Recovery Manager solution, integrated with Hyper-V Replica, to provide disaster recovery for critical VMs in the event of a disaster in any of offices.

Exercise 2: Implementing storage migration

▶ Task 1: Configure and perform storage migration

1. On **LON-HOST1**, in **Hyper-V Manager**, right-click **LON-SVR1-B**, and then click **Settings**.
2. In **Settings** for **LON-SVR1**, under **IDE Controller 0**, click **Hard Drive**. Confirm that it is using the **LON-SVR1-B.vhd** that is stored locally, and then click **OK**.
3. In **Hyper-V Manager**, right-click **20740A-LON-SVR1-B**, and then click **Move**.
4. In the **Move "20740A-LON-SVR1-B" Wizard**, on the **Before You Begin** page, click **Next**.
5. On the **Choose Move Type** page, select the **Move the virtual machine's storage** option, and then click **Next**.
6. On the **Choose Options for Moving Storage** page, select the **Move only the virtual machine's virtual hard disks** option, and then click **Next**.
7. On the **Select Items to Move** page, confirm that only **20740A-LON-SVR1-B-Allfiles.vhd** is selected, and then click **Next**.
8. On the **Choose a new location for attached virtual hard disk** page, in the **Folder** text box, type **C:\VMs\LON-SVR1-B**, and then click **Next**.
9. On the **Completing Move Wizard** page, click **Finish**.

Note: Because the VHD is dynamically expanding and is small, the move occurs quickly.

10. In **Hyper-V Manager**, right-click **LON-SVR1-B**, and then click **Settings**.
11. In **Settings** for **LON-SVR1-B**, under **IDE Controller 0**, click **Hard Drive**. Confirm that **20740A-LON-SVR1-B-Allfiles.vhd** is stored on **C:\VMs** folder structure.

Note: This confirms that the VHD was moved while the virtual machine was running.

Results: After completing this exercise, you should have moved Hyper-V storage and virtual machines.

Exercise 3: Configuring Hyper-V Replicas

▶ Task 1: Configure a replica on both host machines

1. On **LON-NVHOST2**, open the **Hyper-V Manager** console.
2. In **Hyper-V Manager**, right-click **LON-NVHOST2**, and then select **Hyper-V Settings**.
3. In **Hyper-V Settings** for **LON-NVHOST2**, click **Replication Configuration**.
4. In the **Replication Configuration** pane, click **Enable this computer as a Replica server**.
5. In the **Authentication and ports** section, select **Use Kerberos (HTTP)**.
6. In the **Authorization and storage** section, click **Allow replication from any authenticated server**, and then click **Browse**.
7. Expand **This PC**, double-click **Local Disk (C)**, and then click **New folder**. For the folder name, type **VMReplica**, and press Enter. Select the **C:\VMReplica** folder, and then click **Select Folder**.
8. In **Hyper-V Settings** for **LON-NVHOST2**, click **OK**.
9. In the **Settings** dialog box, read the notice, and then click **OK**.
10. Click **Start**, and then click **Control Panel**.
11. In **Control Panel**, click **System and Security**, and then click **Windows Firewall**.
12. Click **Advanced settings**.
13. Click **Inbound Rules**.
14. In the right pane, in the rule list, find and right-click the **Hyper-V Replica HTTP Listener (TCP-In)** rule, and then click **Enable Rule**.
15. Close the **Windows Firewall with Advanced Security** console, and then close the **Windows Firewall**.
16. Repeat steps 1 through 15 on **LON-HOST1**.

▶ Task 2: Configure replication for LON-SVR1-B virtual machine

1. On **LON-HOST1**, open **the Hyper-V Manager** console. Click **20740A-LON-NVHOST2**, and then right-click **20740A-LON-SVR1-B**.
2. Click **Enable Replication**.
3. On the **Before You Begin** page, click **Next**.
4. In the **Replica Server** box, type **LON-NVHOST2** and then click **Next**.

5. On the **Specify Connection Parameters** page, click **Use Kerberos authentication (HTTP)**, and then click **Next**.
6. On the **Choose Replication VHDs** page, click **Next**.
7. On the **Configure Replication Frequency** page, from drop-down list box, select **30 seconds**, and then click **Next**.
8. On the **Configure Additional Recovery Points** page, select **Maintain only the latest recovery point**, and then click **Next**.
9. On the **Choose Initial Replication Method** page, click **Send initial copy over the network**, select **Start replication immediately**, and then click **Next**.
10. On the **Completing the Enable Replication Wizard** page, click **Finish**.
11. At the **Replication enabled successfully** prompt, click **Close**.
12. Wait five to seven minutes. You can monitor the progress of the initial replication in the **Status** column in the **Hyper-V Manager** console. When it completes (progress reaches 100 percent), ensure that **20740A-LON-SVR1-B** has appeared on **LON-NVHOST2** in **Hyper-V Manager**.

▶ Task 3: Validate a planned failover to the replica site

1. On **LON-HOST1**, in **Hyper-V Manager**, right-click **20740A-LON-SVR1-B**.
2. Select **Replication**, and then click **View Replication Health**.
3. Review content of the window that appears, and ensure that there are no errors.
4. Click **Close**.
5. On **LON-NVHOST2**, open **Hyper-V Manager**, and then verify that **20740A-LON-SVR1-B** is turned off.
6. From **LON-HOST1**, connect to the **20740A-LON-SVR1-B** virtual machine.
7. On **LON-SVR1-B**, click **Start**, click **Power**, click **Shut down**, and then click **OK**.
8. On **LON-HOST1**, in **Hyper-V Manager**, right-click **20740A-LON-SVR1-B**, point to **Replication,** and then click **Planned Failover**.
9. In the **Planned Failover** window, ensure that the option **Start the Replica virtual machine after failover** is selected, and then click **Fail Over**.
10. On **LON-NVHOST2**, in **Hyper-V Manager**, ensure that **20740A-LON-SVR1-B** is running.

▶ Task 4: Prepare for the next module

1. Right-click **20740A-LON-SVR1-B** on **LON-NVHOST2**.
2. Click **Replication** and then click **Cancel Failover**. Click **Yes**.
3. Right-click **20740A-LON-SVR1-B**, point to **Replication**, and then click **Remove Replication**.
4. Click **Remove Replication**.
5. Repeat step 3 and 4 on **LON-HOST1**.
6. On **LON-HOST1**, in **Hyper-V Manager**, right-click **LON-HOST1** and then click **Hyper-V Settings**.
7. In **Replication Configuration**, clear the **Enable this computer as a Replica server** check box and click **OK**.
8. Repeat step 6 and 7 on **LON-NVHOST2**.
9. On **LON-HOST1**, in **Hyper-V Manager**, right-click **20740A-LON-SVR1-B**, and then click **Move**.

10. In the **Move "20740A-LON-SVR1-B" Wizard**, on the **Before You Begin** page, click **Next**.
11. On the **Choose Move Type** page, select the **Move the virtual machine's storage** option, and then click **Next**.
12. On the **Choose Options for Moving Storage** page, select the **Move only the virtual machine's virtual hard disks** option, and then click **Next**.
13. On the **Select Items to Move** page, confirm that only **20740A-LON-SVR1-B-Allfiles.vhd** is selected, and then click **Next**.
14. On the **Choose a new location for attached virtual hard disk** page, in the **Folder** text box, type **E:\Program Files\Microsoft Learning\20740\Drives\20740A-LON-SVR1-B\Virtual Hard Disks**, and then click **Next**.
15. On the **Completing Move Wizard** page, click **Finish**.
16. Restart the host computer.
17. When you are prompted with the boot menu, select **Windows Server 2012**, and then press Enter.
18. Sign in to the host machine as directed by your instructor.

Results: After completing this exercise, you will have configured Hyper-V Replica.

Module 8: Implementing failover clustering

Lab A: Implementing failover clustering

Exercise 1: Creating a failover cluster

▶ Task 1: Connect cluster nodes to iSCSI shared storage

Configure the iSCSI targets

1. On **LON-SVR1**, on the taskbar, click **Start**, and then click **Server Manager**
2. In **Server Manager**, in the navigation pane, click **File and Storage Services**.
3. In the **File and Storage Services** pane, click **iSCSI**.
4. In the **iSCSI VIRTUAL DISKS** pane, click **TASKS**, and then in the **TASKS** drop-down list, select **New iSCSI Virtual Disk**.
5. In the **New iSCSI Virtual Disk Wizard**, on the **Select iSCSI virtual disk location** page, under **Storage location**, click **C:**, and then click **Next**.
6. On the **Specify iSCSI virtual disk name** page, in the **Name** text box, type **iSCSIDisk1**, and then click **Next**.
7. On the **Specify iSCSI virtual disk size** page, in the **Size** text box, type **5**, ensure **GB** is selected in the drop-down list, and then click **Next**.
8. On the **Assign iSCSI target** page, click **New iSCSI target**, and then click **Next**.
9. On the **Specify target name** page, in the **Name** text box, type **lon-svr1**, and then click **Next**.
10. On the **Specify access servers** page, click **Add**.
11. In the **Select a method to identify the initiator** dialog box, click **Enter a value for the selected type**, and in the **Type** drop-down list, select **IP Address**. In the **Value** text box, type **172.16.0.22**, and then click **OK**.
12. On the **Specify access servers** page, click **Add**.
13. In the **Select a method to identify the initiator** dialog box, click **Enter a value for the selected type**, and in the **Type** drop-down list, select **IP Address**. In the **Value** box, type **172.16.0.23**, and then click **OK**.
14. On the **Specify access servers** page, click **Next**.
15. On the **Enable Authentication** page, click **Next**.
16. On the **Confirm selections page**, click **Create**.
17. On the **View results** page, wait until creation is complete, and then click **Close**.
18. In the **iSCSI VIRTUAL DISKS** pane, click **TASKS**, and then in the **TASKS** drop-down list, select **New iSCSI Virtual Disk**.
19. In the **New iSCSI Virtual Disk Wizard**, on the **Select iSCSI virtual disk location** page, under **Storage location**, click **C:**, and then click **Next**.
20. On the **Specify iSCSI virtual disk name** page, in the **Name** text box, type **iSCSIDisk2**, and then click **Next**.
21. On the **Specify iSCSI virtual disk size** page, in the **Size** text box, type **5**, ensure **GB** is selected in the drop-down list box, and then click **Next**.

22. On the **Assign iSCSI target** page, click **lon-svr1**, and then click **Next**.
23. On the **Confirm selections** page, click **Create**.
24. On the **View results** page, wait until the creation is completed, and then click **Close**.
25. In the **iSCSI VIRTUAL DISKS** pane, click **TASKS**, and then in the **TASKS** drop-down list, select **New iSCSI Virtual Disk**.
26. In the **New iSCSI Virtual Disk Wizard**, on the **Select iSCSI virtual disk location** page, under **Storage location**, click **C:**, and then click **Next**.
27. On the **Specify iSCSI virtual disk name** page, in the **Name** text box, type **iSCSIDisk3**, and then click **Next**.
28. On the **Specify iSCSI virtual disk size** page, in the **Size** text box, type **5**, ensure **GB** is selected in the drop-down list, and then click **Next**.
29. On the **Assign iSCSI target** page, click **lon-svr1**, and then click **Next**.
30. On the **Confirm selections** page, click **Create**.
31. On the **View results** page, wait until the creation is complete, and then click **Close**.

Connect nodes to the iSCSI targets

1. On **LON-SVR2**, open **Server Manager**, click **Tools**, and then click **iSCSI Initiator**.
2. In the **Microsoft iSCSI** dialog box, click **Yes**.
3. In the **iSCSI Initiator** window, click the **Discovery** tab, and then click **Discover Portal**.
4. In the **IP address or DNS name** text box, type **172.16.0.21**, and then click **OK**.
5. Click the **Targets** tab, and then click **Refresh**.
6. In the **Targets** list, click **iqn.1991-05.com.microsoft:lon-svr1-lon-svr1-target**, and then click **Connect**.
7. Ensure that **Add this connection to the list of Favorite Targets** is selected, and then click **OK** two times.
8. On **LON-SVR3**, open **Server Manager**, click **Tools**, and then click **iSCSI Initiator**.
9. In the **Microsoft iSCSI** dialog box, click **Yes**.
10. In the **iSCSI Initiator** window, click the **Discovery** tab, and then click **Discover Portal**.
11. In the **IP address or DNS name** text box, type **172.16.0.21**, and then click **OK**.
12. Click the **Targets** tab, and then click **Refresh**.
13. In the **Targets** list, click **iqn.1991-05.com.microsoft:lon-svr1-lon-svr1-target**, and then click **Connect**.
14. Ensure that the **Add this connection to the list of Favorite Targets** check box is selected, and then click **OK** two times.
15. On **LON-SVR2**, in **Server Manager**, click **Tools**, and then click **Computer Management**.
16. Expand **Storage**, and then click **Disk Management**.
17. Right-click **Disk 4**, and then click **Online**.
18. Right-click **Disk 4**, and then click **Initialize Disk**.
19. In the **Initialize Disk** dialog box, click **OK**.

20. Right-click the unallocated space next to **Disk 4**, and then click **New Simple Volume**.
21. On the **Welcome** page, click **Next**.
22. On the **Specify Volume Size** page, click **Next**.
23. On the **Assign Drive Letter or Path** page, click **Next**.
24. On the **Format Partition** page, in the **Volume Label** text box, type **Data1**. Select the **Perform a quick format** check box, and then click **Next**.
25. Click **Finish**.

> **Note:** If a dialog box appears with a prompt to format the disk, click **Cancel**.

26. Repeat steps 17 through 25 for **Disk 5** and **Disk 6**, using **Data2** and **Data3** respectively for volume labels.
27. Close the **Computer Management** window.
28. On **LON-SVR3**, in **Server Manager**, click **Tools**, and then click **Computer Management**.
29. Expand **Storage**, and click **Disk Management**.
30. Select and right-click **Disk Management**, and then click **Refresh**.
31. Right-click **Disk 3**, and then click **Online**.
32. Right-click **Disk 4**, and then click **Online**.
33. Right-click **Disk 5**, and then click **Online**.
34. Close the **Computer Management** window.

▶ Task 2: Install the Failover Cluster feature

1. On **LON-SVR2**, if Server Manager is not open, click the **Server Manager** icon.
2. 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, ensure that **Select a server from the server pool** is selected, and then click **Next**.
6. On the **Select server roles** page, click **Next**.
7. On the **Select features** page, in the **Features** list, select **Failover Clustering**.
8. In the **Add features that are required for Failover Clustering** window, click **Add Features**, and then click **Next**.
9. On the **Confirm installation selections** page, click **Install**.
10. When installation completes and you receive the **Installation succeeded on LON-SVR2.Adatum.com** message, click **Close**.
11. On **LON-SVR3**, repeat steps 1 through 10.
12. When installation completes and you receive the **Installation succeeded on LON-SVR3.Adatum.com** message, click **Close**.

▶ Task 3: Validate the servers for failover clustering

1. On **LON-SVR2**, in **Server Manager**, click **Tools**, and then click **Failover Cluster Manager**.
2. In **Failover Cluster Manager**, in the **Actions** pane, click **Validate Configuration**.
3. In the **Validate a Configuration Wizard**, click **Next**.
4. In the **Enter Name** text box, type **LON-SVR2**, and then click **Add**.
5. In the **Enter Name** text box, type **LON-SVR3**.
6. Click **Add**, and then click **Next**.
7. Verify that **Run all tests (recommended)** is selected, and click **Next**.
8. On the **Confirmation** page, click **Next**.
9. Wait for the validation tests to finish, which might take between 5 and 7 minutes, and then on the **Summary** page, scroll through the report. Verify that all tests completed without errors. Some warnings are expected.
10. On the **Summary** page, click **Finish**.

▶ Task 4: Create the failover cluster

1. On **LON-SVR2**, in the **Failover Cluster Manager**, in the **Actions** pane, click **Create Cluster**.
2. On the **Before you begin** page, click **Next**.
3. On the **Select Servers** page, in the **Enter server name** box, type **LON-SVR2**, and then click **Add**.
4. In the **Enter server name** box, type **LON-SVR3**, click **Add**, and then click **Next**.
5. On the **Access Point for Administering the Cluster** page, in the **Cluster Name** text box, type **Cluster1**.
6. In the **Address** text box, type **172.16.0.125**, and then click **Next**.
7. On the **Confirmation** page, click **Next**.
8. On the **Summary** page, click **Finish**.

▶ Task 5: Add the file-server application to the failover cluster

1. On **LON-SVR2**, in the **Failover Cluster Manager** console, expand **Cluster1.Adatum.com**, expand **Storage**, and then click **Disks**.
2. Ensure that three disks named **Cluster Disk 1**, **Cluster Disk 2**, and **Cluster Disk 3** are present and online.
3. Right-click **Roles**, and then click **Configure Role**.
4. On the **Before You Begin** page, click **Next**.
5. On the **Select Role** page, click **File Server**, and then click **Next**.
6. On the **File Server Type** page, click **File Server for general use**, and then click **Next**.
7. On the **Client Access Point** page, in the **Name** text box, type **AdatumFS**, in the **Address** text box, type **172.16.0.130**, and then click **Next**.
8. On the **Select Storage** page, select the **Cluster Disk 2** check box, and then click **Next**.
9. On the **Confirmation** page, click **Next**.
10. On the **Summary** page, click **Finish**.

▶ Task 6: Add a shared folder to a highly-available file server

1. On **LON-SVR3**, in the **Server Manager** console, click **Tools**, and then click **Failover Cluster Manager**.
2. Expand **Cluster1.Adatum.com**, click **Roles**, right-click **AdatumFS**, and then click **Add File Share**.
3. In the **New Share Wizard**, on the **Select the profile for this share** page, click **SMB Share – Quick**, and then click **Next**.
4. On the **Select the server and the path for this share** page, click **Next**.
5. On the **Specify share name** page, in the **Share name** text box, type **Docs**, and then click **Next**.
6. On the **Configure share settings** page, review the available options but do not make any changes, and then click **Next**.
7. On the **Specify permissions to control access** page, click **Next**.
8. On the **Confirm selections** page, click **Create**.
9. On the **View results** page, click **Close**.

▶ Task 7: Configure failover and failback settings

1. On **LON-SVR3**, in the **Failover Cluster Manager** console, click **Roles**, right-click **AdatumFS**, and then click **Properties**.
2. In the **AdatumFS Properties** dialog box, click the **Failover** tab, and then click **Allow failback**.
3. Click **Failback between**, and set the values to **4** and **5** hours.
4. Click the **General** tab.
5. Select both **LON-SVR2** and **LON-SVR3** as preferred owners.
6. Select **LON-SVR3**, and click **Up** so that it is first in the preferred owners list.
7. To close the **AdatumFS Properties** dialog box, click **OK**.

▶ Task 8: Validate the highly available file-server deployment

1. On **LON-DC1**, open **File Explorer**, and in the address bar, type **\\AdatumFS**, and then press Enter.
2. Verify that you can access the location and that you can open the **Docs** folder.
3. Create a text document inside this folder named **test.txt**.
4. On **LON-SVR2**, switch to **Failover Cluster Manager**.
5. In the **Failover Cluster Manager** console, expand **Cluster1.Adatum.com**, and then click **Roles**.
6. In the **Owner Node** column, note the current owner of **AdatumFS**.

   Note: The owner will be **LON-SVR2** or **LON-SVR3**.

7. Right-click **AdatumFS**, click **Move**, and then click **Select Node**.
8. In the **Move Clustered Role** dialog box, select the cluster node (it will be either **LON-SVR2** or **LON-SVR3**), and then click **OK**.
9. Verify that **AdatumFS** has moved to a new owner.

10. Switch to **LON-DC1**.
11. To verify that you can still access the **\\AdatumFS** location, open **File Explorer**, and in the address bar, type **\\AdatumFS**, and then press Enter.

▶ Task 9: Validate the failover and quorum configuration for the File Server role

1. On **LON-SVR2**, in the **Failover Cluster Manager** console, click **Roles**.
2. In the **Owner Node** column, verify the current owner for the AdatumFS role.

   Note: The owner will be **LON-SVR2** or **LON-SVR3**.

3. Click **Nodes**, and then select the node that is the current owner of the AdatumFS role.
4. Right-click the node, click **More Actions**, and then click **Stop Cluster Service**.
5. In the **Failover Cluster Manager** console, click **Roles**, and verify that AdatumFS is running.

   Note: This confirms that AdatumFS has moved to another node.

6. Switch to **LON-DC1**.
7. On **LON-DC1**, to verify that you can still access the **\\AdatumFS** location, open **File Explorer**, and in the address bar, type **\\AdatumFS**, and then press Enter.
8. Switch to **LON-SVR2**.
9. In the **Failover Cluster Manager** console, click **Nodes**, right-click the stopped node, click **More Actions**, and then click **Start Cluster Service**.
10. Expand **Storage**, and then click **Disks**.
11. In the center pane, find the disk that is assigned to **Disk Witness in Quorum**.

    Note: You can view this in the **Assigned To** column.

12. Right-click the disk, click **Take Offline**, and then click **Yes**.
13. Switch to **LON-DC1**.
14. On **LON-DC1**, to verify that you can still access the **\\AdatumFS** location, open **File Explorer**, and in the address bar, type **\\AdatumFS**, and then press Enter.

    Note: This verifies that the cluster is running even if the witness disk is offline.

15. Switch to **LON-SVR2**.
16. In the **Failover Cluster Manager** console, expand **Storage**, click **Disks**, right-click the disk that is in **Offline** status, and then click **Bring Online**.
17. Right-click **Cluster1.Adatum.com**, click **More Actions**, and then click **Configure Cluster Quorum Settings**.
18. On the **Before You Begin** page, click **Next**.

19. On the **Select Quorum Configuration Option** page, click **Advanced quorum configuration**, and then click **Next**.
20. On the **Select Voting Configuration** page, review the available settings.

    Note: Notice that you can select a node or nodes that will, or will not, have a vote in the cluster.

21. Do not make any changes, and then click **Next**.
22. On the **Select Quorum Witness** page, ensure that **Configure a disk witness** is selected, and then click **Next**.
23. On the **Configure Storage Witness** page, click **Cluster Disk 3**, and then click **Next**.
24. On the **Confirmation** page, click **Next**.
25. On the **Summary** page, click **Finish**.

Results: After completing this exercise, you should have created a failover cluster successfully, configured a highly available file server, and tested the failover scenarios.

Exercise 2: Verifying quorum settings and adding a node

▶ Task 1: Remotely connect to a cluster

1. If necessary, sign in to **LON-CL1** with username **Administrator** and password **Pa$$w0rd**.
2. Click **Start**, click **All apps**, and then click **Windows Administrative Tools**.
3. Click **Failover Cluster Manager**.
4. In **Failover Cluster Manager**, right-click **Failover Cluster Manager**, and then click **Connect to Cluster**.
5. In the **Select Cluster** dialog box, in the **Cluster name** box, type **Cluster1.Adatum.com**, and click **OK**.
6. Expand **Cluster1.Adatum.com**, and then click **Roles**.

▶ Task 2: Check the assigned votes in the Nodes section

1. On **LON-SVR2**, right-click **Start**, and then click **Windows PowerShell (Admin)**.
2. In **Windows PowerShell** console, run following cmdlet to check the assigned votes:

```
Get-ClusterNode | select name, nodeweight, ID, state
```

3. Verify that **NodeWeight** property of a cluster node has value **1**, which means that the quorum vote of the node is assigned and that the cluster is managing it.

▶ Task 3: Verify the status of the disk witness

- On **LON-SVR2**, in the **Windows PowerShell** console, type the following command, and then press Enter:

```
Get-ClusterQuorum | Select Cluster, QuorumResource, QuorumType
```

▶ Task 4: Add a node in the cluster

1. On **LON-SVR2**, in the **Failover Cluster Manager**, click **Nodes**.
2. In the **Actions** pane, click **Add Node**.
3. On the **Before You Begin** page, click **Next**.
4. On the **Select Servers** page, in the **Enter server name** box, type **LON-SVR5**, click **Add**, and then click **Next**.
5. On the **Validation Warning** page, click **Next**.
6. Complete the validation by using the defaults.
7. On the **Summary** page of the **Validate a Configuration Wizard**, click **Finish**.
8. In the **Add Node Wizard**, on the **Confirmation** page, click **Next**.
9. On the **Summary** page, click **Finish**.

▶ Task 5: Verify the assigned votes

1. On **LON-SVR2**, in **Windows PowerShell** console, type following cmdlet, and then press Enter:

```
Get-ClusterNode | select name, nodeweight, ID, state
```

2. Verify that **NodeWeight** property of a cluster node has value **1**, which means that the quorum vote of the node is assigned and that the cluster is managing it.

Results: After completing this exercise, you should have added another node in the cluster successfully, and changed the quorum to the witness disk.

▶ Task 6: Prepare for the next lab

- When you finish the lab, leave the virtual machines running for the subsequent lab.

Lab B: Managing a failover cluster

Exercise 1: Evicting a node and verifying quorum settings

▶ Task 1: Evict node LON-SVR5

1. On **LON-SVR3**, if necessary, open **Failover Cluster Manager**.
2. Expand the **Cluster 1.Adatum.com** cluster, and then click **Nodes**.
3. Right-click the **LON-SVR5** node, click **More Actions**, and then click **Evict**.
4. In the **Evict node LON-SVR5** dialog box, click **Yes** to evict the node.

▶ Task 2: Verify changes in quorum settings and the witness disk

1. On **LON-SVR2**, in the **Windows PowerShell** console, type following cmdlet, and then press Enter:

```
Get-ClusterNode | select name, nodeweight, ID, state
```

2. Verify that **NodeWeight** property of a cluster node has value **1**, which means that the quorum vote of the node is assigned and is managed by the cluster.

Results: After completing this exercise, you should have evicted a node from the cluster, and verified the changes in quorum settings and witness disk.

Exercise 2: Changing the quorum from disk witness to file-share witness, and defining node voting

▶ Task 1: Get the current quorum model

- On **LON-SVR2**, in the **Windows PowerShell** console, type the following command, and then press Enter:

```
Get-ClusterQuorum | Select Cluster, QuorumResource, QuorumType
```

▶ Task 2: Create a file share on LON-SVR1

1. On **LON-SVR1**, on the **Taskbar**, click **File Explorer**, right-click the disk **Local Disk (C:)**, click **New**, and then click **Folder**.
2. Type **FSW**, and press Enter.
3. Right-click **FSW**, click **Share with**, and then click **Specific people**.
4. In the **File Sharing** dialog box, type **Everyone**, and then click **Add**.
5. In the **Read** list, click **Read/Write**.
6. Click **Share**, and then click **Done**.

▶ Task 3: Change the current quorum model to a file-share witness

- On **LON-SVR2**, in the **Windows PowerShell** console, type the following command, and then press Enter:

```
Set-ClusterQuorum -NodeAndFileShareMajority "\\LON-SVR1\FSW"
```

▶ Task 4: Verify that the current quorum model is a file share witness

- On **LON-SVR2**, in the **Windows PowerShell** console, type the following command, and then press Enter:

```
Get-ClusterQuorum | Select Cluster, QuorumResource, QuorumType
```

Results: After completing this exercise, you should have changed the quorum from disk witness to file share witness and defined node voting.

Exercise 3: Verifying high availability

▶ Task 1: Simulate server failure

1. On **LON-SVR2**, in the **Failover Cluster Manager** console, expand **Cluster1.Adatum.com**, and then click **Roles**.
2. In the **Owner Node** column, note the current owner of AdatumFS.

Note: The owner will be **LON-SVR2** or **LON-SVR3**.

3. If **LON-SVR3** is not the owner, right click **AdatumFS**, click **Move**, click **Select Node**, click **LON-SVR3**, and then click **OK**.
4. Shut down **LON-SVR3**.

▶ Task 2: Verify functionality in Cluster1, and verify file availability

1. On **LON-DC1**, open **File Explorer**, and in the address bar, type **\\AdatumFS**, and then press Enter.
2. Verify that you can access the location and that you can open the **Docs** folder.
3. Create a test text document named **test2.txt** inside this folder.

▶ Task 3: Validate whether the file is still available

1. Start **LON-SVR3** virtual machine.
2. On **LON-SVR2**, In the **Failover Cluster Manager** console, expand **Cluster1.Adatum.com**, and then click **Roles**.
3. Right-click **AdatumFS**, click **Move**, click **Select Node**, click **LON-SVR3**, and then click **OK**.
4. On **LON-DC1**, open **File Explorer**, and in the address bar, type **\\AdatumFS**, and then press Enter.
5. Verify that you can access the location and that you can open the **Docs** folder.
6. Create a test text document named **test3.txt** inside this folder.

Results: After completing this exercise, you should have tested failover cluster high availability successfully by taking a server offline and then bringing it back online.

▶ Task 4: Prepare for the next module

When you finish the lab, revert the VMs 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 **20740A-LON-DC1**, and then click **Revert**.
3. In the **Revert Virtual Machines** dialog box, click **Revert**.
4. Repeat steps 2 and 3 for **20740A-LON-SVR1**, **20740A-LON-SVR2**, **20740A-LON-SVR3**, **20740A-LON-SVR5**, and **20740A-LON-CL1**.

Module 9: Implementing failover clustering with Windows Server 2016 Hyper-V

Lab: Implementing failover clustering with Windows Server 2016 Hyper-V

Exercise 1: Configuring iSCSI storage

▶ Task 1: Configure iSCSI targets

1. On **LON-SVR1**, sign in as **Adatum\Administrator** with the password **Pa$$w0rd**.
2. On the taskbar, click the **Windows** button, and then click **Server Manager**.
3. In **Server Manager**, in the navigation pane, click **File and Storage Services**.
4. In the **File and Storage Services** pane, click **iSCSI**.
5. In the **iSCSI VIRTUAL DISKS** pane, click **TASKS**, and then in the **TASKS** drop-down list box, click **New iSCSI Virtual Disk**.
6. In the **New iSCSI Virtual Disk Wizard**, on the **Select iSCSI virtual disk location** page, under **Storage location**, click **C:**, and then click **Next**.
7. On the **Specify iSCSI virtual disk name** page, in the **Name** box, type **iSCSIDisk1**, and then click **Next**.
8. On the **Specify iSCSI virtual disk size** page, in the **Size** box, type **20**, ensure that **GB** is selected in the drop-down list box, and then click **Next**.
9. On the **Assign iSCSI target** page, click **New iSCSI target**, and then click **Next**.
10. On the **Specify target name** page, in the **Name** box, type **lon-svr1**, and then click **Next**.
11. On the **Specify access servers** page, click **Add**.
12. In the **Select a method to identify the initiator** dialog box, click **Enter a value for the selected type**, and then in the **Type** drop-down list box, click **IP Address**. In the **Value** box, type **172.16.0.32**, and then click **OK**.
13. On the **Specify access servers** page, click **Add**.
14. In the **Select a method to identify the initiator** dialog box, click **Enter a value for the selected type**, and then in the **Type** drop-down list box, select **IP Address**. In the **Value** box, type **172.16.0.160**, and then click **OK**.
15. On the **Specify access servers** page, click **Next**.
16. On the **Enable Authentication** page, click **Next**.
17. On the **Confirm selections page**, click **Create**.
18. On the **View results** page, wait until the creation completes, and then click **Close**.
19. In the **iSCSI VIRTUAL DISKS** pane, click **TASKS**, and then in the **TASKS** drop-down list box, select **New iSCSI Virtual Disk**.
20. In the **New iSCSI Virtual Disk Wizard**, on the **Select iSCSI virtual disk location** page, under **Storage location**, click **C:**, and then click **Next**.
21. On the **Specify iSCSI virtual disk name** page, in the **Name** box, type **iSCSIDisk2**, and then click **Next**.

22. On the **Specify iSCSI virtual disk size** page, in the **Size** box, type **20**, ensure that **GB** is selected in the drop-down list box, and then click **Next**.
23. On the **Assign iSCSI target** page, click **lon-svr1**, and then click **Next**.
24. On the **Confirm selections** page, click **Create**.
25. On the **View results** page, wait until the creation completes, and then click **Close**.
26. In the **iSCSI VIRTUAL DISKS** pane, click **TASKS**, and then in the **TASKS** drop-down list box, select **New iSCSI Virtual Disk**.
27. In the **New iSCSI Virtual Disk Wizard**, on the **Select iSCSI virtual disk location** page, under **Storage location**, click **C:**, and then click **Next**.
28. On the **Specify iSCSI virtual disk name** page, in the **Name** box, type **iSCSIDisk3**, and then click **Next**.
29. On the **Specify iSCSI virtual disk size** page, in the **Size** box, type **20**, ensure that **GB** is selected in the drop-down list box, and then click **Next**.
30. On the **Assign iSCSI target** page, click **lon-svr1**, and then click **Next**.
31. On the **Confirm selections** page, click **Create**.
32. On the **View results** page, wait until the creation completes, and then click **Close**.

Results: After completing this exercise, you should have successfully installed an iSCSI Target Server.

Exercise 2: Configuring a failover cluster for Hyper-V

▶ Task 1: Connect to the iSCSI target from both host machines

1. On **LON-HOST1**, click **Start**, click the **Server Manager** icon, click **Tools**, and then click **iSCSI Initiator**.
2. In the **Microsoft iSCSI** dialog box, click **Yes**.
3. Click the **Discovery** tab.
4. On the **Discovery** tab, click **Discover Portal**.
5. In the **IP address or DNS name** text box, type **172.16.0.21**, and then click **OK**.
6. Click the **Targets** tab, and then click **Refresh**.
7. In the **Discovered targets** list, click **iqn.1991-05.com.microsoft:lon-svr1-lon-svr1-target**, and then click **Connect**.
8. Ensure **Add this connection to the list of Favorite Targets** is selected and click **OK**.
9. To close the **iSCSI Initiator Properties** dialog box, click **OK**.
10. Switch to **LON-NVHOST2**.
11. On **LON-NVHOST2**, open **Server Manager**, click **Tools**, and then click **iSCSI Initiator**.
12. In the **Microsoft iSCSI** dialog box, click **Yes**.
13. In the **iSCSI Initiator** dialog box, click the **Discovery** tab.
14. On the **Discovery** tab, click **Discover Portal**.

15. In the **IP address or DNS name** text box, type **172.16.0.21**, and then click **OK**.
16. Click the **Targets** tab, and then click **Refresh**.
17. In the **Discovered targets** list, click **iqn.1991-05.com.microsoft:lon-svr1-lon-svr1-target**, and then click **Connect**.
18. Ensure **Add this connection to the list of Favorite Targets** is selected and then click **OK**. To close the **iSCSI Initiator Properties** dialog box, click **OK**.
19. On **LON-NVHOST2**, in **Server Manager**, click **Tools**, and then click **Computer Management**.
20. Expand **Storage**, and click **Disk Management**.
21. Right-click **Disk 1**, and then click **Online**. (This is the first disk that is 20 GB in size. Your disk number might be different.)
22. Right-click **Disk 1**, and click **Initialize Disk**.
23. In the **Initialize Disk** dialog box, click **OK**.
24. Right-click the unallocated space next to **Disk 1**, and click **New Simple Volume**.
25. On the **Welcome** page, click **Next**.
26. On the **Specify Volume Size** page, click **Next**.
27. On the **Assign Drive Letter or Path** page, click **Next**.

 **Note:** Note the drive letters used on **LON-HOST1**, while creating new Disks in **LON-NVHOST2** make sure to use an unused letter.

28. On the **Format Partition** page, in the **Volume label** text box, type **ClusterDisk**. Select the **Perform a quick format** check box, and then click **Next**.
29. Click **Finish**.
30. Close the dialog box asking to again format the disk.
31. Repeat steps 21 through 30 for Disk 2 and Disk 3. In step 28, use the following settings:
    - Disk 2 name: **ClusterVMs**
    - Disk 3 name: **Quorum**
32. Switch back to **LON-HOST1**.
33. On **LON-HOST1** in **Server Manager**, click **Tools**, and then click **Computer Management**.
34. Expand **Storage**, and click **Disk Management**.
35. Right-click **Disk Management**, and then click **Refresh**.
36. Right-click **Disk 2**, and then click **Online**.
37. Right-click **Disk 3**, and then click **Online**.
38. Right-click **Disk 4**, and then click **Online**.

 **Note:** Disk numbers might vary based on the number of physical disks in the host computer. Choose the disks that are 20 GB in size.

▶ Task 2: Configure failover clustering on both host machines

1. On **LON-HOST1**, in **Server Manager**, on the **Dashboard**, 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, ensure that **Select server from the server pool** is selected, and then click **Next**.
5. On the **Select server roles** page, click **Next**.
6. On the **Select features** page, in the **Features** list, click **Failover Clustering**. At the **Add features that are required for failover clustering** prompt, click **Add Features**, and then click **Next**.
7. On the **Confirm installation selections** page, click **Install**.
8. When installation is complete, click **Close**.
9. Switch to **LON-NVHOST2**.
10. Repeat steps 1 through 8 on **LON-NVHOST2**.
11. Switch back to **LON-HOST1**.
12. On **LON-HOST1**, in **Server Manager**, click **Tools**, and then click **Failover Cluster Manager**.
13. In **Failover Cluster Manager**, in the center pane, under **Management**, click **Create Cluster**.
14. On the **Before You Begin** page of the **Create Cluster Wizard**, read the information, and then click **Next**.
15. On the **Select Servers** page, in the **Enter server name** text box, type **LON-HOST1**, and then click **Add**. Again in the **Enter server name** text box, type **LON-NVHOST2**, and then click **Add**.
16. Verify the entries, and then click **Next**.
17. On the **Validation Warning** page, click **No. I do not require support from Microsoft for this cluster**, and then click **Next**.
18. On the **Access Point for Administering the Cluster** page, in the **Cluster Name** text box, type **VMCluster**.
19. In the **Address** text box, type **172.16.0.126**, and then click **Next**.
20. In the **Confirmation** dialog box, verify the information, clear the **Add all eligible storage to the cluster** option check box, and then click **Next**.
21. On the **Summary** page, click **Finish**.

▶ Task 3: Configure disks for a failover cluster

1. On **LON-HOST1**, in the **Failover Cluster Manager** console, expand **VMCluster.Adatum.com**, expand **Storage**, right-click **Disks**, and then click **Add Disk**.
2. In the **Add Disks to Cluster** dialog box, verify that all disks are selected, and then click **OK**.
3. Click **Disks**, and then verify that all disks display as available for cluster storage in **Failover Cluster Manager**.
4. Click **Cluster Disk 1**. Right-click that disk, and then click **Add to Cluster Shared Volumes**.
5. Right-click **VMCluster.Adatum.com**, click **More Actions**, click **Configure Cluster Quorum Settings**, and then click **Next**.

6. On the **Select Quorum Configuration Option** page, click **Use default quorum configuration**, and then click **Next**.
7. On the **Confirmation** page, click **Next**.
8. On the **Summary** page, click **Finish**.

Results: After completing this exercise, you should have successfully configured the failover clustering infrastructure for Hyper-V.

Exercise 3: Configuring a highly available VM

▶ Task 1: Move VM storage to the iSCSI target

1. Ensure that **LON-HOST1** is the owner of the disk that you just assigned to Cluster Shared Volume. You can read owner value in the **Owner node** column. If that is not the case, then move the disk to **LON-HOST1** before proceeding to step two.

Note: To move the disk:

- Right-click the disk and then click **Move**.
- Click **Select Node**, click **LON-HOST1**, and then click **OK**.

2. On **LON-HOST1**, on the desktop, on the taskbar, click the **File Explorer** icon.
3. In **File Explorer**, expand drive **E:**, expand **Program Files**, expand **Microsoft Learning**, expand **20740**, expand **Drives**.

Note: The drive letter might be different depending on the physical machine.

4. Copy the **20740A-BASE.vhd** virtual hard disk file to the **C:\ClusterStorage\Volume1** location.
5. In **File Explorer**, expand drive **E:** expand **Program Files**, expand **Microsoft Learning**, expand **Base**.
6. Copy the **Base16D-WS16-TP5**.vhd virtual hard disk file to the **C:\ClusterStorage\Volume1** location.
7. Click **Start,** select **Windows PowerShell**.
8. Run the following command:

```
Set-VHD -Path C:\ClusterStorage\Volume1\20740A-BASE.vhd -ParentPath
C:\ClusterStorage\Volume1\Base16D-WS16-TP5.vhd
```

▶ Task 2: Configure the VM as highly available

1. On **LON-HOST1**, in **Failover Cluster Manager**, click **Roles**, and then in the **Actions** pane, click **Virtual Machines**.
2. Click **New Virtual Machine**.
3. Select **LON-HOST1** as the cluster node, and then click **OK**.
4. In the **New Virtual Machine Wizard**, on the **Before You Begin** page, click **Next**.

5. On the **Specify Name and Location** page, in the **Name** text box, type **TestClusterVM**, click **Store the virtual machine in a different location**, and then click **Browse**.
6. Browse to and select **C:\ClusterStorage\Volume1**, click **Select Folder**, and then click **Next**.
7. On the **Specify Generation** page, click **Generation 1**, and then click **Next**.
8. On the **Assign Memory** page, type **1536**, and then click **Next**.
9. On the **Configure Networking** page, click **Next**.
10. On the **Connect Virtual Hard Disk** page, click **Use an existing virtual hard disk**, and then click **Browse**.
11. Browse to **C:\ClusterStorage\Volume1**, click **20740A-BASE.vhd**, and then click **Open**.
12. Click **Next**, and then click **Finish**. If an error occurs informing you that the Microsoft Management has stopped working, restart this task from step 1.
13. On the **Summary** page of the **High Availability Wizard**, click **Finish**.
14. Right-click the **TestClusterVM**, and then click **Settings**.
15. On **LON-HOST1**, in the **Settings for TestClusterVM**, in the left navigation pane, expand **Processor**, and then click **Compatibility**.
16. In the right pane, select the **Migrate to a physical computer with a different processor version** check box, and then click **OK**.
17. Right-click **TestClusterVM**, and then click **Start**.
18. Ensure that the VM starts successfully.

▶ Task 3: Failover VM

1. On **LON-NVHOST2**, open **Failover Cluster Manager**.
2. Expand **VMCluster.Adatum.com**, and then click **Roles**.
3. Right-click **TestClusterVM**, click **Move**, click **Live Migration**, and then click **Select Node**.
4. Click **LON-NVHOST2**, and then click **OK**. Wait until the VM is migrated. You will see that the **Owner Node** column will change the value when migration completes.
5. Right-click **TestClusterVM**, and then click **Connect**.
6. Ensure that you can access and operate the VM when it migrated to another host.

▶ Task 4: Configure drain on shutdown

1. On **LON-HOST1,** select **Windows Start**, and then launch **Windows PowerShell**.
2. At the **Windows PowerShell** command prompt, type the following command, and then press Enter:

```
(Get-Cluster).DrainOnShutdown
```

Note: This should return a value of "**1**".

3. On **LON-HOST1** launch **Server Manager**.
4. Select **Tools**, and then **Failover Cluster Manager**.
5. Select **Roles** in **Failover Cluster Manager**.
6. On **LON-NVHOST2** click on **Windows Start**, select **Power,** and then select **Shut down**.

7. On the popup dialog select **Continue**.
8. On **LON-HOST1** observe **TestClusterVM** live migrate to **LON-HOST1** from **LON-NVHOST2** before shutting down.

▶ Task 5: Prepare for the next module

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

1. On the host computer, start **Hyper-V Manager**.
2. Shut down all Virtual Machines.
3. Restart your computer, and when prompted, choose **Windows Server 2012 R2**.

Results: After completing this exercise, you should have successfully configured the VM as highly available.

Module 10: Implementing Network Load Balancing

Lab: Implementing NLB

Exercise 1: Implementing a Network Load Balancing (NLB) cluster

▶ Task 1: Verify website functionality for standalone servers

1. On **LON-SVR1**, on the taskbar, click the **File Explorer** icon.
2. In the File Explorer address bar, browse to **c:\inetpub\wwwroot**.
3. Double-click the file **iisstart.png** to open it in Microsoft Paint.
4. Ensure that the **Paintbrush** tool is selected.
5. Create a circle around the **IIS** logo.
6. Save the changes that you made to **iisstart.png**, and then close **Microsoft Paint**.
7. Close **File Explorer**.
8. Switch to **LON-DC1**.
9. Click **Start**, click **All Apps**, click **Windows Accessories**, and then click **Internet Explorer**.
10. In the **Microsoft Internet Explorer** Address Bar, type the address **http://LON-SVR1**, and then press Enter.
11. Verify that the webpage displays the IIS logo with the circle that you just added.
12. In the Internet Explorer Address Bar, type the address **http://LON-SVR2**, and then press Enter.
13. Verify that the webpage does not display the IIS logo with the circle.

▶ Task 2: Install NLB

1. Switch to **LON-SVR1**.
2. Click **Start**, and then click **Server Manager**.
3. In the **Server Manager** console, click **Tools**, and then click **Windows PowerShell ISE**.
4. In the **Windows PowerShell ISE** window, type the following command to install NLB on **LON-SRV1** and **LON-SVR2**, and then press Enter:

```
Invoke-Command -Computername LON-SVR1,LON-SVR2 -command {Install-WindowsFeature
NLB,RSAT-NLB}
```

Note: If you receive warnings about the network connection to each server, ignore these.

▶ Task 3: Create a new Windows Server 2016 NLB cluster

1. On **LON-SVR1**, in the **Windows PowerShell ISE** window, type the following command to create the new NLB cluster, and then press Enter:

```
New-NlbCluster -InterfaceName "Ethernet" -OperationMode Multicast -ClusterPrimaryIP
172.16.0.42 -ClusterName LON-NLB
```

2. In the **Windows PowerShell ISE** window, type the following command to add the NLB cluster to Domain Name System (DNS), and then press Enter:

```
Invoke-Command -Computername LON-DC1 -command {Add-DNSServerResourceRecordA –zonename
adatum.com –name LON-NLB –Ipv4Address 172.16.0.42}
```

▶ Task 4: Add a second host to the cluster

- On **LON-SVR1**, in the **Windows PowerShell ISE** window, type the following command to add a second host to the cluster, and then press Enter:

```
Add-NlbClusterNode -InterfaceName "Ethernet" -NewNodeName "LON-SVR2" -
NewNodeInterface "Ethernet"
```

▶ Task 5: Validate the NLB cluster

1. On **LON-SVR1**, in **Server Manager**, click **Tools**, and then click **Network Load Balancing Manager**.
2. Click **OK** to dismiss the **Warning** message box.
3. In the **Network Load Balancing Manager** window, click **LON-NLB (172.16.0.42)**.
4. In the **Host configuration information for hosts in cluster LON-NLB (172.16.0.42)** pane, verify that the nodes **LON-SVR1** and **LON-SVR2** display with the status **Converged**.
5. Right-click the **LON-NLB (172.16.0.42)** cluster, and then click **Cluster properties**.
6. In the **LON-NLB(172.16.0.42) Properties** dialog box, on the **Cluster Parameters** tab, verify that the cluster is set to use the **Multicast** operations mode.
7. On the **Port Rules** tab, verify that there is a single port rule with a Cluster IP address of **All** that starts at port **0** and ends at port **65535** for both **TCP** and **UDP** protocols, and that it uses **Single** affinity.
8. Click **OK** to close the **LON-NLB(172.16.0.42) Properties** dialog box.

Results: After completing this exercise, you should have successfully implemented an NLB cluster.

Exercise 2: Configuring and managing the NLB cluster

▶ Task 1: Configure port rules and affinity

Configure affinity for NLB cluster nodes

1. On **LON-SVR2**, click **Start**, and then click **Windows PowerShell**.
2. In the **Windows PowerShell** window, type the following commands and then press Enter:

```
Mkdir c:\porttest
```

3. In the **Windows PowerShell** window, type the following commands and then press Enter:

```
Xcopy /s c:\inetpub\wwwroot c:\porttest
```

4. In the **Windows PowerShell** window, type the following commands and then press Enter:

```
New-Website –Name PortTest –PhysicalPath “C:\porttest” –Port 5678
```

5. In the **Windows PowerShell** window, type the following commands and then press Enter:

```
New-NetFirewallRule –DisplayName PortTest –Protocol TCP –LocalPort 5678
```

Configure NLB port rules

1. On the **Taskbar**, click the **File Explorer** icon.
2. In File Explorer, click drive **C**, double-click the **porttest** folder, and then double-click **iisstart.png** to open the file in **Microsoft Paint**.
3. Use the paintbrush to place a line across the **IIS** logo.
4. Save the changes to **iisstart.png**, and then close **Microsoft Paint**.
5. Switch to **LON-DC1**.
6. In the Internet Explorer Address Bar, type **http://LON-SVR2:5678**, and then press Enter.
7. Verify that the **IIS Start** page displays the IIS logo with a line across it.
8. Switch to **LON-SVR1**.
9. On **LON-SVR1**, switch to **Network Load Balancing Manager**.
10. In the **Network Load Balancing Manager** console, right-click **LON-NLB(172.16.0.42)**, and then click **Cluster Properties**.
11. In the **LON-NLB (172.16.0.42) Properties** dialog box, on the **Port Rules** tab, select the **All** port rule, and then click **Remove**.
12. On the **Port Rules** tab, click **Add**.
13. In the **Add/Edit Port Rule** dialog box, type the following information, and then click **OK**:
    - Port range: **80** to **80**
    - Protocols: **Both**
    - Filtering mode: **Multiple host**
    - Affinity: **None**
14. On the **Port Rules** tab, click **Add**.
15. In the **Add/Edit Port Rule** dialog box, type the following information, and then click **OK**:
    - Port range: **5678** to **5678**
    - Protocols: **Both**
    - Filtering mode: **Single host**
16. Click **OK** to close the **LON-NLB(172.16.0.42) Properties** dialog box.
17. In the **Network Load Balancing Manager** console, right-click **LON-SVR1 (Ethernet)**, and then click **Host Properties**.

18. On the **Port Rules** tab, click the port rule that has **5678** as the **Start** and **End** value, and then click **Edit**.
19. In the **Handling priority** list, click **10**.
20. Click **OK** twice to close both the **Add/Edit Port Rule** dialog box and the **LON-SVR1 (Ethernet) Properties** dialog box.

▶ Task 2: Validate port rules

1. Switch to **LON-DC1**.
2. In the Internet Explorer Address Bar, type **http://lon-nlb**, and then press Enter.
3. Click the **Refresh** icon 20 times.
4. Verify that you see web pages both with and without the circle you added.
5. In the Internet Explorer Address Bar, type the address **http://LON-NLB:5678**, and then press Enter.
6. Click the **Refresh** icon 20 times.
7. Verify that now only the web page with the distinctive line displays.

Note: It is possible that you will need to refresh your browser more than 20 times to see the different logos on **http://lon-nlb**.

▶ Task 3: Manage host availability in the NLB cluster

1. Switch to **LON-SVR1**.
2. In the **Network Load Balancing Manager** console, right-click **LON-SVR1 (Ethernet)**, click **Control Host**, and then click **Suspend**.
3. Click the **LON-NLB (172.16.0.42)** node. Verify that the node **LON-SVR1** displays as **Suspended**, and that the node **LON-SVR2** displays as **Converged**.
4. Right-click **LON-SVR1(Ethernet)**, click **Control Host**, and then click **Resume**.
5. Right-click **LON-SVR1(Ethernet)**, click **Control Host**, and then click **Start**.
6. Click the **LON-NLB (172.16.0.42)** node. Verify that both the nodes **LON-SVR1** and **LON-SVR2** now display as **Converged**.

Note: You might have to refresh the view.

Results: After completing this exercise, you should have successfully configured and managed an NLB cluster.

Exercise 3: Validating high availability for the NLB cluster

▶ Task 1: Validate website availability when the host is unavailable

1. On **LON-SVR1**, click **Start**, and then click **Windows PowerShell**.
2. In the **Windows PowerShell** window, type the following command, and then press Enter:

```
restart-computer
```

3. Switch to **LON-DC1**.
4. In the Internet Explorer Address Bar, type **http://LON-NLB**, and then press Enter.
5. Refresh the website 20 times.
6. Verify that the website is available while **LON-SVR1** reboots, and verify that it does not display the **IIS** logo with the circle until **LON-SVR1** restarts.

▶ Task 2: Configure and validate Drainstop

1. Sign in to **LON-SVR1** with the username **Adatum\Administrator** and the password **Pa$$word**.
2. Click **Start**, and then click the **Server Manager** tile.
3. In **Server Manager**, click **Tools**, and then click **Network Load Balancing Manager**.
4. Click **OK** to dismiss the **Warning** message box.
5. In the **Network Load Balancing Manager** console, right-click **LON-SVR2(Ethernet)**, click **Control Host**, and then click **Drainstop**.
6. Switch to **LON-DC1**.
7. In the Internet Explorer Address Bar, type **http://lon-nlb**, and then press Enter.
8. Refresh the site 20 times, and then verify that only the **Welcome** page with the circled IIS logo displays.

Results: After completing this exercise, you should have successfully validated high availability for the NLB cluster.

▶ Task 3: Prepare for the next module

When you finish the lab, revert the virtual machines to their initial state.

1. On the host computer, start **Hyper-V Manager**.
2. In the **Virtual Machines** list, right-click **20740A-LON-DC1**, and then click **Revert**.
3. In the **Revert Virtual Machine** dialog box, click **Revert**.
4. Repeat steps two and three for **20740A-LON-SVR1** and **20740A-LON-SVR2**.

Module 11: Creating and managing deployment images

Lab: Using MDT to deploy Windows Server 2016

Exercise 1: Configuring MDT

▶ Task 1: Configure the deployment share

1. On **LON-SVR1**, click the **Start** button, click **All Apps**, scroll down the list of apps, expand **Microsoft Deployment Toolkit**, and then click the **Deployment Workbench** item.
2. In the **Deployment Workbench** console, click the **Deployment Shares** node.
3. Right-click the **Deployment Shares** node, and then click **New Deployment Share**.
4. In the **New Deployment Share Wizard**, on the **Path** page, in the **Deployment share path** field, ensure that **C:\DeploymentShare** is listed in the **Deployment share path** text box. If it is not, enter it into the text box, and then click **Next**.
5. On the **Share** page, notice the name of the deployment share (it is a hidden share), and then click **Next**.
6. On the **Descriptive Name** page, note that this name, and not the path, will appear in the Deployment Workbench, and then click **Next**.
7. Review the **Options** page, ensure that the **Ask for a product key** and **Ask to set the local Administrator password** check boxes are cleared, and then click **Next**.
8. On the **Summary** page, click **Next**.
9. On the **Confirmation** page, click **Finish**.

Results: After completing this exercise, you should have configured MDT 2013 Update 2 and the MDT Deployment Share.

Exercise 2: Creating and deploying an image

▶ Task 1: Add a reference image (Windows Server 2016)

1. On **LON-SVR1**, in the **20740A-LON-SVR1 on localhost Virtual Machine Connection** window, click **Media**, point to **DVD Drive**, and then click **Insert Disk**.
2. In the **Open** dialog box, browse to **D:\Program files\Microsoft Learning\20740\Drives**.
3. Click the **WinServer2016_TP5.ISO** file, and then click **Open**.
4. Return to the **Deployment Workbench**, and expand **Deployment Shares**, and then expand **MDT Deployment Share (C:\DeploymentShare)**.
5. Under the **MDT Deployment Share (C:\DeploymentShare)** node, right-click the **Operating Systems** folder, and then click **Import Operating System**.
6. In the **Import Operating System Wizard**, on the **OS Type** page, select the **Full set of source files** option, and then click **Next**.
7. On the **Source** page, in the **Source directory** text box, type **D:**, and then click **Next**.

8. On the **Destination** page, in the **Destination directory name** text box, type **WindowsServer2016x64**, and then click **Next**.
9. On the **Summary** page, click **Next**.
10. The operating system import will take about 5 minutes. On the **Confirmation** page, click **Finish**.

▶ Task 2: Add an application to the image

1. Return to the **Deployment Workbench** console.
2. Right-click **Applications**, and then select **New Application**.
3. In the **New Application Wizard**, on the **Application Type** page, ensure the **Application with source files** option is selected, and then click **Next**.
4. On the **Details** page, in the **Publisher** text box, type **Microsoft** and in the **Application Name** text box, type **ExcelViewer**, and then click **Next**.
5. On the **Source** page, in the **Source directory** text box, type **E:\Labfiles\Mod11**, and then click **Next**.
6. On the **Destination** page, in the **Specify the name of the directory that should be created** text box, type **ExcelViewer**, and then click **Next**.
7. On the **Command Details** page, in the **Command line** text box, type **excelviewer.exe /quiet /norestart**, and then click **Next**.
8. On the **Summary** page, click **Next**.
9. On the **Confirmation** page, click **Finish**.

▶ Task 3: Create the deployment task sequence

1. Click **Task Sequences**.
2. Right-click **Task Sequences**, and then select **New Task Sequence**.
3. The **New Task Sequence Wizard** opens to the **General Settings** page. In the **General Settings** page, in the **Task sequence ID** text box, type **11-01**, and in the **Task sequence name** text box, type **Lab 11-01**, and in the **Task sequence comments**, type **Windows Server 2016 Deployment to LON-SVR6 task sequence for Module 11 lab**, and then click **Next**.
4. On the **Select Template** page, in the drop-down list, select the **Standard Server Task Sequence**, and then click **Next**.
5. On the **Select OS** page, in the **Operating Systems** list, click **Windows Server 2016 Technical Preview 5 SERVERDATACENTER in WindowsServer 2016x64 install.wim**, and then click **Next**.
6. On the **Specify a Product Key** page, ensure the **Do not specify a product key at this time** option is selected, and then click **Next**.
7. On the **OS Settings** page, in the **Full Name** text box, type **Administrator**, and in the **Organization** text box, type **A. Datum Corporation**, and then click **Next**.
8. On the **Admin Password** page, select the **Use the specified Administrator password** option, and in the **Administrator Password** and **Please confirm Administrator Password** text boxes, type **Pa$$w0rd**, and then click **Next**.
9. On the **Summary** page, review the selected options, and then click **Next**.
10. On the **Confirmation** page, click **Finish**.
11. In the details pane of the **Task Sequences** node in **the Deployment Workbench**, double-click the **Lab11-01** task sequence.

12. In the **Lab 11-01 Properties** window, select the **Task Sequence** tab.
13. In the console tree, expand the **State Restore** node, and below it, select the **Install Applications** node.
14. In the details pane of **Install Applications**, select the **Install a single application** option, and then click **Browse**.
15. In the **Select an item** window, select the **Microsoft ExcelViewer** item, and then click **OK**.
16. To close the **Lab 11-01 Properties** window, click **OK**.
17. In the console tree of the **Deployment Workbench**, select and then right-click the **MDT Deployment Share (C:\DeploymentShare)** node, and then select **Update Deployment Share**.
18. The **Update Deployment Share Wizard** will start. On the **Options** page, click **Next**.
19. On the **Summary** page, click **Next**.
20. The boot image will be made, and the deployment will be completed. This could take several minutes.
21. On the **Confirmation** page, click **Finish**.
22. Right-click the **MDT Deployment Share (C:\DeploymentShare)** node, and select **Properties**, and then select the **Monitoring** tab.
23. Check the box that says **Enable Monitoring for this Deployment Share**, and then click **OK**.

▶ Task 4: Deploy the Image to LON-SVR6

1. In **Hyper-V Manager** on the **HOST** computer, double-click **20740A-LON-SVR6**.
2. In the **20740A-LON-SVR6 on HOST-Virtual Machine Connection**, select **Media**, and in the context menu, select **DVD Drive**, and then select **Insert Disk**.
3. In the **Open** window, expand **This PC**, navigate to **D:\Program Files\Microsoft Learning\20740 \Drives**, select **LiteTouchPE_x64.iso**, and then click **Open**.
4. Start the **20740A-LON-SVR6** virtual machine.
5. The **Microsoft Deployment Toolkit** splash screen will appear as it loads the deployment task.
6. The **Microsoft Deployment Toolkit** wizard will start. On the **Welcome** page, select the **Run the Deployment Wizard to install a new Operating system** item.
7. On the **User Credentials** page, in the **User Name** text box, type **Administrator**, in the **Password** text box, type **Pa$$w0rd**, and in the **Domain** text box, type **Adatum.com**, and then click **OK**.
8. On the **Task Sequence** page, select the **Lab 11-01** task sequence item, and then click **Next**.
9. On the **Computer Details** page, in the **Computer name** text box, type **LON-SVR6**, and then click the **Join a domain** option.
10. In the **Domain to join** text box, type **Adatum.com**, and then click **Next**.
11. On the **Locale and Time** page, click **Next**.
12. On the **BitLocker** page, ensure the **Do not enable BitLocker for this computer** option is selected, and then click **Next**.
13. On the **Ready** page, click **Begin**.
14. An **Installation Progress** window appears that allows you to monitor the progress of the deployment.

15. Switch to **LON-SVR1**. In the **Deployment Workbench**, expand the **MDT Deployment Share (C:\DeploymentShare)** node, and then select the **Monitoring** node. Right-click it, and then select **Refresh**. You will see updating information for the Lab 11-01 task sequence in the details pane.
16. After approximately 5–10 minutes, **LON-SVR6** will reboot and stop at **Product Key** page. Click the **Do this later** hyperlink.
17. After a few moments, **LON-SVR6** will restart and finalize the settings.
18. The Windows Server 2016 desktop will appear. Wait until the **Installation Progress** window appears, and you should see the installation take place within this window.
19. You will see the **Installing Microsoft Excel Viewer** progress bar appear under the **Running Action: Install Applications** progress bar. The **Installation Progress** window will then close after a few minutes.
20. A **Deployment Summary** page appears, stating **Operating system deployment completed successfully**. Click **Finish**.
21. In the **Server Manager** console tree, select **Local server**. In the details pane of local server, examine the **Computer Name** and **Domain** status. If the **Domain** status shows as **Unknown**, click the **Refresh** icon. It should be named **LON-SVR6** and be in the **Adatum.com** domain.
22. Click the **Start menu** icon and then click **All Apps**.
23. In the returned list, observe the **Microsoft Office Excel Viewer** app is listed.
24. Close all open windows and sign out of all virtual machines.

Results: After completing this exercise, you should have used MDT 2013 Update 2 to deploy Windows Server 2016 to **LON-SVR6**, and then you should have tested the deployment of an application.

▶ Task 5: Prepare for the next module

After 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 **20740A-LON-DC1**, and then click **Revert**.
3. In the **Revert Virtual Machine** dialog box, click **Revert**.
4. Repeat steps 2 and 3 for **20740A-LON-SVR1** and **20740A-LON-SVR6**.

Module 12: Managing, monitoring, and maintaining virtual machine installations

Lab A: Implementing WSUS and deploying updates

Exercise 1: Implementing WSUS

▶ Task 1: Install the WSUS server role

1. Sign in to **LON-SVR4** as **Adatum\Administrator** with the password **Pa$$w0rd**.
2. On **LON-SVR4**, if necessary, open **Server Manager**, click **Manage**, and then click **Add Roles and Features**.
3. In the **Add Roles and Features Wizard**, click **Next**.
4. On the **Select installation type** page, ensure that **Role-based or feature-based installation** is selected, and then click **Next**.
5. On the **Select destination server** page, click **Next**.
6. On the **Select server roles** page, select the **Windows Server Update Services** check box.
7. In the pop-up window, click **Add Features**.
8. On the **Select server roles** page, click **Next**.
9. On the **Select features** page, click **Next**.
10. On the **Web Server Role (IIS)** page, click **Next**.
11. On the **Select role services** page, click **Next**.
12. On the **Windows Server Update Services** page, click **Next**.
13. On the **Select role services** page, confirm that both **WID Connectivity** and **WSUS Services** are selected, and then click **Next**.
14. On the **Content location selection** page, in the text box, type **C:\WSUSUpdates**, and then click **Next**.
15. On the **Confirm installation selections** page, click **Install**.
16. When the installation completes, click **Close**.
17. In **Server Manager**, click **Tools**, and then click **Windows Server Update Services**.
18. In the **Complete WSUS Installation** dialog box, click **Run**, and wait for the task to complete. Click **Close**.
19. Do not close **the Windows Server Update Services (WSUS) Configuration Wizard:LON-SVR4** window.

▶ Task 2: Configure WSUS to synchronize with an upstream WSUS server

1. In the **Windows Server Update Services Configuration Wizard:LON-SVR4** window, click **Next** twice.
2. On the **Choose Upstream Server** page, click **Synchronize from another Windows Server Update Services server**, in the **Server name** text box, type **LON-SVR2.Adatum.com**, and then click **Next**.
3. On the **Specify Proxy Server** page, click **Next**.

4. On the **Connect to Upstream Server** page, click **Start Connecting**. Wait for the upstream server settings to be applied, and then click **Next**.
5. On the **Choose Languages** page, click **Next**.
6. On the **Set Sync Schedule** page, click **Next**.
7. On the **Finished** page, select the **Begin initial synchronization** check box, and then click **Finish**.
8. In the **Windows Server Update Services** console, in the navigation pane, double-click **LON-SVR4**, and then click **Options**.
9. In the **Options** pane, click **Computers**.
10. In the **Computers** dialog box, select **Use Group Policy or registry settings on computers**. Click **OK**.

Note: You might need to wait until synchronization is complete before you can click **OK**.

Results: After completing this exercise, you should have implemented the WSUS server role.

Exercise 2: Configuring update settings

▶ Task 1: Configure WSUS groups

1. On **LON-SVR4**, in the **WSUS** console, in the navigation pane, double-click **Computers**.
2. Click **All Computers**, and then, in the **Actions** pane, click **Add Computer Group**.
3. In the **Add Computer Group** dialog box, in the **Name** text box, type **Research**, and then click **Add**.

▶ Task 2: Configure Group Policy to deploy WSUS settings

1. Switch to **LON-DC1**.
2. In **Server Manager**, click **Tools**, and then click **Group Policy Management**.
3. In the **Group Policy Management** console, double-click **Forest: Adatum.com**, double-click **Domains**, and then double-click **Adatum.com**.
4. Right-click the **Research** organizational unit (OU), and then click **Create a GPO in this domain, and Link it here**.
5. In the **New GPO** dialog box, in the **Name** text box, type **WSUS Research**, and then click **OK**.
6. Double-click the **Research** OU, right-click **WSUS Research**, and then click **Edit**.

Note: If the **Group Policy Management Console** dialog box appears, click **OK** to continue.

7. In the **Group Policy Management Editor**, under **Computer Configuration**, double-click **Policies**, double-click **Administrative Templates**, double-click **Windows Components**, and then click **Windows Update**.
8. In the **Settings** pane, double-click **Configure Automatic Updates**, and then click the **Enabled** option.

9. In the **Configure automatic updating** field, click and select **4 – Auto download and schedule the install**, and then click **OK**.
10. In the **Settings** pane, double-click **Specify intranet Microsoft update service location**, and then click the **Enabled** option.
11. In the **Set the intranet update service for detecting updates** and the **Set the intranet statistics server** text boxes, type **http://LON-SVR4.Adatum.com:8530**, and then click **OK**.
12. In the **Settings** pane, double-click **Enable client-side targeting**.
13. In the **Enable client-side targeting** dialog box, click the **Enabled** option, in the **Target group name for this computer** text box, type **Research**, and then click **OK**.
14. Close the **Group Policy Management Editor** and the **Group Policy Management** console.
15. In **Server Manager**, click **Tools**, and then click **Active Directory Users and Computers**.
16. In **Active Directory Users and Computers**, double-click **Adatum.com**, click **Computers**, right-click **LON-CL1**, and then click **Move**.
17. In the **Move** dialog box, click the **Research** OU, and then click **OK**.
18. Close **Active Directory Users and Computers**.

▶ Task 3: Verify the application of Group Policy settings

1. Switch to **LON-CL1**.
2. On **LON-CL1**, click the **Start** button, click **Power**, and then click **Restart**.
3. After **LON-CL1** restarts, sign in as **Adatum\Administrator** with the password **Pa$$w0rd**.
4. In Cortana's search box, type **cmd**, right-click the **Command Prompt** tile, and then click **Run as administrator**.
5. At the command prompt, type the following command, and then press Enter:

```
Gpresult /r
```

6. In the output of the command, confirm that, under **Computer Settings**, **WSUS Research** is listed under **Applied Group Policy Objects**.

▶ Task 4: Initialize Windows Update

1. On **LON-CL1**, at the command prompt, type the following command, and then press Enter:

```
Wuauclt.exe /detectnow /reportnow
```

2. Switch to **LON-SVR4**.
3. In the **Update Services** console, expand **Computers**, expand **All Computers**, and then click **Research**.
4. Verify that **LON-CL1** appears in the **Research** group. If it does not, then repeat steps 1 through 3. It might take several minutes for **LON-CL1** to display.
5. Verify that updates are reported as needed. If updates are not reported, repeat steps 1-3. It might take 10 to 15 minutes for updates to register.

Results: After completing this exercise, you should have configured update settings for client computers.

Exercise 3: Approving and deploying an update by using WSUS

▶ Task 1: Approve WSUS updates for the Research computer group

1. On **LON-SVR4**, in **Windows Server Update Services**, under **Updates**, click **All Updates**, right-click **Update for Windows 10 Version 1511 for x64-based Systems (KB3140741)**, and then click **Approve**.
2. In the **Approve Updates** window, in the **Research** drop-down list box, select **Approved for Install**.
3. Click **OK**, and then click **Close**.

▶ Task 2: Deploy updates to LON-CL1

1. On **LON-CL1**, at the command prompt, type the following command, and then press Enter:

```
Wuauclt.exe /detectnow
```

2. In the **I'm Cortana. Ask me anything** box of the Start screen, type **Windows Update**.
3. In the **Best match** list, click **Check for updates**.
4. Click **Check for updates**.
5. The update begins to download.
6. Close the **Windows Update** window when the installation is complete.

▶ Task 3: Verify update deployment to LON-CL1

1. On **LON-CL1**, in Cortana's search box, type **Event Viewer**, and then click **View event logs**.
2. In **Event Viewer**, expand **Applications and Services Logs**, expand **Microsoft**, expand **Windows**, expand **WindowsUpdateClient** and then click **Operational** to view events.
3. Confirm that events are logged in relation to the update.

Results: After completing this exercise, you should have approved and deployed an update by using WSUS.

▶ Task 4: Prepare for the next lab

When you finish the lab, revert all virtual machines back to their initial state. To do this, perform the following steps:

1. On the host computer, start **Microsoft Hyper-V Manager**.
2. In the **Virtual Machines** list, right-click **20740A-LON-DC1**, and then click **Revert**.
3. In the **Revert Virtual Machines** dialog box, click **Revert**.
4. Repeat steps 2 to 3 for **20740A-LON-SVR2**, **20740A-LON-SVR4**, and **20740A-LON-CL1**.

Lab B: Monitoring and troubleshooting Windows Server 2016

Exercise 1: Establishing a performance baseline

▶ Task 1: Create and start a data collector set

1. Switch to the **LON-SVR1** computer.
2. Click the **Search** button, type **Perfmon** in the **Search the web and Windows** text box, and, then in the **Best match** list, click **Perfmon**.
3. In **Performance Monitor**, in the navigation pane, expand **Data Collector Sets**, and then click **User Defined**.
4. Right-click **User Defined**, point to **New**, and then click **Data Collector Set**.
5. In the **Create new Data Collector Set** wizard, in the **Name** box, type **LON-SVR1 Performance**.
6. Click **Create manually (Advanced)**, and then click **Next**.
7. On the **What type of data do you want to include?** page, select the **Performance counter** check box, and then click **Next**.
8. On the **Which performance counters would you like to log?** page, click **Add**.
9. In the **Available counters** list, expand **Processor**, click **%Processor Time**, and then click **Add >>**.
10. In the **Available counters** list, expand **Memory**, click **Pages/sec**, and then click **Add >>**.
11. In the **Available counters** list, expand **PhysicalDisk**, click **%Disk Time**, and then click **Add >>**.
12. Click **Avg. Disk Queue Length** and then click **Add >>**.
13. In the **Available counters** list, expand **System**, click **Processor Queue Length**, and then click **Add >>**.
14. In the **Available counters** list, expand **Network Interface**, click **Bytes Total/sec**, click **Add >>**, and then click **OK**.
15. On the **Which performance counters would you like to log?** page, in the **Sample interval** text box, type **1**, and then click **Next**.
16. On the **Where would you like the data to be saved?** page, click **Next**.
17. On the **Create the data collector set?** page, click **Save and close**, and then click **Finish**.
18. In **Performance Monitor**, in the **Results** pane, right-click **LON-SVR1 Performance**, and then click **Start**.

▶ Task 2: Create a typical workload on the server

1. Click **Start**, and then click **Windows PowerShell**.
2. At the command prompt, type the following command, and then press Enter:

```
Fsutil file createnew bigfile 104857600
```

3. At the command prompt, type the following command, and then press Enter:

```
Copy bigfile \\LON-dc1\c$
```

4. At the command prompt, type the following command, and then press Enter:

```
Copy \\LON-dc1\c$\bigfile bigfile2
```

5. At the command prompt, type the following command, and then press Enter:

```
Del bigfile*.*
```

6. At the command prompt, type the following command, and then press Enter:

```
Del \\LON-dc1\c$\bigfile*.*
```

7. Do not close the **Windows PowerShell** window.

▶ Task 3: Analyze the collected data

1. Switch to **Performance Monitor**.
2. In the navigation pane, right-click **LON-SVR1 Performance**, and then click **Stop**.
3. In **Performance Monitor**, in the navigation pane, expand **Reports**, expand **User Defined**, expand **LON-SVR1 Performance**, and then click **LON-SVR1_DateTime-000001**.
4. On the toolbar, on the **Change graph type** icon, click the down arrow, then click **Report**, and then review the report data.
5. Record the values that are listed in the report for later analysis. Recorded values include:
   - **Memory, Pages/sec**
   - **Network Interface, Bytes Total/sec**
   - **PhysicalDisk, %Disk Time**
   - **PhysicalDisk, Avg. Disk Queue Length**
   - **Processor, %Processor Time**
   - **System, Processor Queue Length**

Results: After this exercise, you should have established a baseline for performance-comparison purposes.

Exercise 2: Identifying the source of a performance problem

▶ Task 1: Capture performance data by using a data collector set

1. Switch to **Performance Monitor**.
2. In **Performance Monitor**, go to **Data Collector Sets**, **User Defined**, and in the results pane start the **LON-SVR1 Performance** data collector set.

▶ Task 2: Create additional workload on the server

1. On **LON-SVR1**, click **Start**, and then click **Windows PowerShell ISE**.
2. In **Windows PowerShell ISE**, click the **Open** button, and then open the following script:

```
E:\Labfiles\Mod12\StressTest.ps1
```

3. In **Windows PowerShell ISE**, click the **Run Script (F5)** button.
4. Wait until the script has finished running and then close **Windows PowerShell ISE**.

▶ Task 3: Remove the workload, and then review the performance data

1. Switch to **Performance Monitor**.
2. In the navigation pane, right-click **LON-SVR1 Performance**, and then click **Stop**.
3. In **Performance Monitor**, in the navigation pane, expand **Reports**, expand **User Defined**, expand **LON-SVR1 Performance**, and then click **LON-SVR1_DateTime-000002**.
4. On the toolbar, on the **Change graph type** icon, click the down arrow, click **Report**, and then review the report data.

   Record the following values:

   - **Memory, Pages/sec**
   - **Network Interface, Bytes Total/sec**
   - **PhysicalDisk, %Disk Time**
   - **PhysicalDisk, Avg. Disk Queue Length**
   - **Processor, %Processor Time**
   - **System, Processor Queue Length**

   Question: Compared with your previous report, which values have changed?

   Answer: Memory and disk activity are reduced, but processor activity has increased significantly.

   Question: What would you recommend?

   Answer: You should continue to monitor the server to ensure that the processor workload does not reach capacity.

Results: After this exercise, you should have used performance tools to identify a potential performance bottleneck.

Exercise 3: Viewing and configuring centralized event logs

▶ Task 1: Configure subscription prerequisites

1. On **LON-DC1**, click the **Search** button and then in the **Search the web and Windows** text box, type **Cmd** and press Enter.
2. At the command prompt, type the following command, and then press Enter:

```
winrm quickconfig
```

3. If prompted, type **Y,** and then press Enter.
4. In **Server Manager**, click **Tools**, and then click **Active Directory Users and Computers**.
5. In the **Active Directory Users and Computers** console, in the navigation pane, expand **Adatum.com**, and then click **Builtin**.

6. In the **results** pane, double-click **Administrators**.
7. In the **Administrators Properties** dialog box, click the **Members** tab.
8. Click **Add**, and in the **Select Users, Contacts, Computers, Service Accounts, or Groups** dialog box, click **Object Types**.
9. In the **Object Types** dialog box, select the **Computer**s check box, and then click **OK**.
10. In the **Select Users, Contacts, Computers, Service Accounts, or Groups** dialog box, in the **Enter the object names to select** box, type **LON-SVR1**, and then click **OK**.
11. In the **Administrators Properties** dialog box, click **OK**.
12. Switch to **LON-SVR1**.
13. Click the **Search** button, and then in the **Search the web and Windows** text box, type **Cmd** and press Enter.
14. At the command prompt, type the following command, and then press Enter:

```
Wecutil qc
```

15. When prompted, type **Y**, and then press Enter.

▶ Task 2: Create a subscription

1. On **LON-SVR1**, click the **Search** button, type **Eventvwr**, and then press Enter.
2. In **Event Viewer**, in the navigation pane, click **Subscriptions**.
3. Right-click **Subscriptions**, and then click **Create Subscription**.
4. In the **Subscription Properties** dialog box, in the **Subscription name** text box, type **LON-DC1 Events**.
5. Click **Collector initiated**, and then click **Select Computers**.
6. In the **Computers** dialog box, click **Add Domain Computers**.
7. In the **Select Computer** dialog box, in the **Enter the object name to select** text box, type **LON-DC1**, and then click **OK**.
8. In the **Computers** dialog box, click **OK**.
9. In the **Subscription Properties – LON-DC1 Events** dialog box, click **Select Events**.
10. In the **Query Filter** dialog box, in the **Logged** drop-down list, click **Last 7 days**.
11. Select the **Critical, Warning, Information**, **Verbose**, and **Error** check boxes.
12. In the **Event logs** drop-down list, expand **Applications and Services Logs**, expand **Microsoft**, expand **Windows**, expand **Diagnosis-PLA**, and then select the **Operational** check box.
13. Switch to the **Query Filter** dialog box, and then click **OK**.
14. In the **Subscription Properties – LON-DC1 Events** dialog box, click **OK**.

▶ Task 3: Configure a performance counter alert

1. Switch to the **LON-DC1** computer.
2. Open **Performance Monitor**.
3. In **Performance Monitor**, in the navigation pane, expand **Data Collector Sets**, and then click **User Defined**.

4. Right-click **User Defined**, point to **New**, and then click **Data Collector Set**.
5. In the **Create new Data Collector Set** wizard, in the **Name** text box, type **LON-DC1 Alert**.
6. Click **Create manually (Advanced)**, and then click **Next**.
7. On the **What type of data do you want to include?** page, click **Performance Counter Alert**, and then click **Next**.
8. On the **Which performance counters would you like to monitor?** page, click **Add**.
9. In the **Available counters** list, expand **Processor**, click **%Processor Time**, click **Add >>**, and then click **OK**.
10. On the **Which performance counters would you like to monitor?** page, in the **Alert when** list, click **Above**.
11. In the **Limit** text box, type **10**, and then click **Next**.
12. On the **Create the data collector set?** page, click **Finish**.
13. In the navigation pane, expand the **User Defined** node, and then click **LON-DC1 Alert**.
14. In the results pane, right-click **DataCollector01**, and then click **Properties**.
15. In the **DataCollector01 Properties** dialog box, in the **Sample interval** text box, type **1**, and then click the **Alert Action** tab.
16. Select the **Log an entry in the application event log** check box, and then click **OK**.
17. In the navigation pane, right-click **LON-DC1 Alert**, and then click **Start**.

▶ Task 4: Introduce additional workload on the server

1. On **LON-DC1**, click **Start**, and then click **Windows PowerShell ISE**.
2. In the **Windows PowerShell ISE**, click the **Open** button, and then open the following script:

```
E:\Labfiles\Mod12\StressTest.ps1
```

3. In **Windows PowerShell ISE**, click the **Run Script (F5)** button.
4. Wait until the script has finished running.
5. Close **Windows PowerShell ISE**.

▶ Task 5: Verify the results

1. Switch to **LON-SVR1**.
2. In **Event Viewer**, in the navigation pane, expand **Windows Logs**.
3. Click **Forwarded Events**.

Question: Are there any performance-related alerts?

Answer: Answers might vary, but there should be some events that relate to the workload imposed on **LON-DC1**. Events will have an ID of 2031. If you do not receive any events, proceed with the rest of the lab.

Results: At the end of this exercise, you should have successfully centralized event logs and examined these logs for performance-related events.

▶ Task 6: Prepare for course completion

When you are finished with the lab, revert all virtual machines to their initial state. To do this, perform the following steps:

1. On the host computer, start **Microsoft Hyper-V Manager**.
2. In the **Virtual Machines** list, right-click **20740A-LON-DC1**, and then click **Revert**.
3. In the **Revert Virtual Machines** dialog box, click **Revert**.
4. Repeat steps 2 and 3 for **20740A-LON-SVR1**.