

OFFICIAL MICROSOFT LEARNING PRODUCT

20414C

**Implementing an Advanced Server
Infrastructure**

Companion Content

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

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

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

© 2014 Microsoft Corporation. All rights reserved.

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

Product Number: 20414C

Released: 04/2014

MICROSOFT LICENSE TERMS MICROSOFT INSTRUCTOR-LED COURSEWARE

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

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

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

1. DEFINITIONS.

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

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

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

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

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

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

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

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

b. If you are a Microsoft Learning Competency Member:

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

c. If you are a MPN Member:

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

d. If you are an End User:

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

e. If you are a Trainer.

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

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

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

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

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

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

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

- a. **Pre-Release Licensed Content.** This Licensed Content subject matter is on the Pre-release version of the Microsoft technology. The technology may not work the way a final version of the technology will and we may change the technology for the final version. We also may not release a final version. Licensed Content based on the final version of the technology may not contain the same information as the Licensed Content based on the Pre-release version. Microsoft is under no obligation to provide you with any further content, including any Licensed Content based on the final version of the technology.
- b. **Feedback.** If you agree to give feedback about the Licensed Content to Microsoft, either directly or through its third party designee, you give to Microsoft without charge, the right to use, share and commercialize your feedback in any way and for any purpose. You also give to third parties, without charge, any patent rights needed for their products, technologies and services to use or interface with any specific parts of a Microsoft technology, Microsoft product, or service that includes the feedback. You will not give feedback that is subject to a license that requires Microsoft to license its technology, technologies, or products to third parties because we include your feedback in them. These rights survive this agreement.
- c. **Pre-release Term.** If you are an Microsoft IT Academy Program Member, Microsoft Learning Competency Member, MPN Member or Trainer, you will cease using all copies of the Licensed Content on the Pre-release technology upon (i) the date which Microsoft informs you is the end date for using the Licensed Content on the Pre-release technology, or (ii) sixty (60) days after the commercial release of the technology that is the subject of the Licensed Content, whichever is earliest (“**Pre-release term**”). Upon expiration or termination of the Pre-release term, you will irretrievably delete and destroy all copies of the Licensed Content in your possession or under your control.

- 4. SCOPE OF LICENSE.** The Licensed Content is licensed, not sold. This agreement only gives you some rights to use the Licensed Content. Microsoft reserves all other rights. Unless applicable law gives you more rights despite this limitation, you may use the Licensed Content only as expressly permitted in this agreement. In doing so, you must comply with any technical limitations in the Licensed Content that only allows you to use it in certain ways. Except as expressly permitted in this agreement, you may not:
- access or allow any individual to access the Licensed Content if they have not acquired a valid license for the Licensed Content,
 - alter, remove or obscure any copyright or other protective notices (including watermarks), branding or identifications contained in the Licensed Content,
 - modify or create a derivative work of any Licensed Content,
 - publicly display, or make the Licensed Content available for others to access or use,
 - copy, print, install, sell, publish, transmit, lend, adapt, reuse, link to or post, make available or distribute the Licensed Content to any third party,
 - work around any technical limitations in the Licensed Content, or
 - reverse engineer, decompile, remove or otherwise thwart any protections or disassemble the Licensed Content except and only to the extent that applicable law expressly permits, despite this limitation.
- 5. RESERVATION OF RIGHTS AND OWNERSHIP.** Microsoft reserves all rights not expressly granted to you in this agreement. The Licensed Content is protected by copyright and other intellectual property laws and treaties. Microsoft or its suppliers own the title, copyright, and other intellectual property rights in the Licensed Content.
- 6. EXPORT RESTRICTIONS.** The Licensed Content is subject to United States export laws and regulations. You must comply with all domestic and international export laws and regulations that apply to the Licensed Content. These laws include restrictions on destinations, end users and end use. For additional information, see www.microsoft.com/exporting.
- 7. SUPPORT SERVICES.** Because the Licensed Content is “as is”, we may not provide support services for it.
- 8. TERMINATION.** Without prejudice to any other rights, Microsoft may terminate this agreement if you fail to comply with the terms and conditions of this agreement. Upon termination of this agreement for any reason, you will immediately stop all use of and delete and destroy all copies of the Licensed Content in your possession or under your control.
- 9. LINKS TO THIRD PARTY SITES.** You may link to third party sites through the use of the Licensed Content. The third party sites are not under the control of Microsoft, and Microsoft is not responsible for the contents of any third party sites, any links contained in third party sites, or any changes or updates to third party sites. Microsoft is not responsible for webcasting or any other form of transmission received from any third party sites. Microsoft is providing these links to third party sites to you only as a convenience, and the inclusion of any link does not imply an endorsement by Microsoft of the third party site.
- 10. ENTIRE AGREEMENT.** This agreement, and any additional terms for the Trainer Content, updates and supplements are the entire agreement for the Licensed Content, updates and supplements.
- 11. APPLICABLE LAW.**
- a. United States. If you acquired the Licensed Content in the United States, Washington state law governs the interpretation of this agreement and applies to claims for breach of it, regardless of conflict of laws principles. The laws of the state where you live govern all other claims, including claims under state consumer protection laws, unfair competition laws, and in tort.

b. Outside the United States. If you acquired the Licensed Content in any other country, the laws of that country apply.

- 12. LEGAL EFFECT.** This agreement describes certain legal rights. You may have other rights under the laws of your country. You may also have rights with respect to the party from whom you acquired the Licensed Content. This agreement does not change your rights under the laws of your country if the laws of your country do not permit it to do so.
- 13. DISCLAIMER OF WARRANTY. THE LICENSED CONTENT IS LICENSED "AS-IS" AND "AS AVAILABLE." YOU BEAR THE RISK OF USING IT. MICROSOFT AND ITS RESPECTIVE AFFILIATES GIVES NO EXPRESS WARRANTIES, GUARANTEES, OR CONDITIONS. YOU MAY HAVE ADDITIONAL CONSUMER RIGHTS UNDER YOUR LOCAL LAWS WHICH THIS AGREEMENT CANNOT CHANGE. TO THE EXTENT PERMITTED UNDER YOUR LOCAL LAWS, MICROSOFT AND ITS RESPECTIVE AFFILIATES EXCLUDES ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT.**
- 14. LIMITATION ON AND EXCLUSION OF REMEDIES AND DAMAGES. YOU CAN RECOVER FROM MICROSOFT, ITS RESPECTIVE AFFILIATES AND ITS SUPPLIERS ONLY DIRECT DAMAGES UP TO US\$5.00. YOU CANNOT RECOVER ANY OTHER DAMAGES, INCLUDING CONSEQUENTIAL, LOST PROFITS, SPECIAL, INDIRECT OR INCIDENTAL DAMAGES.**

This limitation applies to

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

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

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

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

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

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

Cette limitation concerne:

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

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

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

Revised July 2013

Module 1

Overview of Management in an Enterprise Data Center

Contents:

Module Review and Takeaways	2
Lab Review Questions and Answers	3

Module Review and Takeaways

Review Question(s)

Question: Explain how System Center components are integrated, and list the benefits of integration.

Answer: System Center integrates the various components by using:

- Operations Manager Monitoring Management Packs
- Orchestrator integration packs
- System Center Cloud Services Process Pack
- Connectors

Integration provides the monitoring of the System Center environment and automation of several data center–related tasks. These tasks include provisioning virtual machines and creating incidents automatically in Service Manager by using alerts within Operations Manager. Additionally, you can use the Operations console to perform many of the tasks that you perform within individual consoles.

Question: Compared to physical machines, what additional high availability option can you use when you deploy virtual machines?

Answer: You can make the virtual machine highly available so that you can support applications that do not provide any other type of high availability.

Lab Review Questions and Answers

Lab: Considerations for Implementing an Enterprise Data Center

Question and Answers

Question: How do the requirements at A. Datum compare to your organization's requirements? What requirements are similar? What additional requirements do you have?

Answer: Answers will vary significantly. Probably, none of the students will have the same requirements, but there should be some overlap between the student requirements and the A. Datum requirements.

Question: What services and tools are you using to manage your data center? How well integrated are the tools?

Answer: Answers will vary. Most organizations use some tools that are not well integrated.

Module 2

Planning and Implementing a Server Virtualization Strategy

Contents:

Lesson 2: Planning and Implementing a Server Virtualization Host Environment	2
Module Review and Takeaways	7
Lab Review Questions and Answers	8

Lesson 2

Planning and Implementing a Server Virtualization Host Environment

Contents:

Question and Answers	3
Resources	3
Demonstration: Using the VMM Management Console	3
Demonstration: Configuring Host Groups	5
Demonstration: Managing VMM Libraries	5

Question and Answers

Question: Why would you want to create an equivalent object?

Answer: Equivalent objects help ensure that you can use a single template across multiple sites.

Question: What are five types of objects that a library might store?

Answer: Objects that a library may store include SQL Server scripts, Microsoft Web Deployment Tool packages, Microsoft Application Virtualization (Server App-V) packages, driver files, answer files, customer resources, and virtual disk drives.

Question: How could you prevent two web servers from running on the same host server?

Answer: You can prevent web servers from running on the same hosts by configuring custom properties on the virtual machines and hosts, and then creating a placement rule.

Resources

Adding Virtualization Hosts to VMM

 **Best Practice:** You should consider security requirements before adding other vendor hosts to your network. For example, you must decide how to implement certificates for virtualization hosts and you may want to determine how to use a Run As account.

 **Reference Links:** For more information, go to:

- System Requirements: VMware ESX Hosts <http://go.microsoft.com/fwlink/p/?linkId=285337>
- System Requirements: Citrix XenServer Hosts <http://go.microsoft.com/fwlink/p/?linkId=285261>

Deploying Hyper-V Hosts

 **Best Practice:** Some considerations for bare-metal deployment:

- You should ensure that your baseboard firmware is current. Consider updating all firmware before deployment.
- Make sure that you have enough space for the .vhd file on the physical server partition, because VMM will cache drivers during deployment.
- When creating the .vhd or .vhdx file, consider the size of the host page file. The host's RAM will determine this. After you deploy the server, remote administration will not be enabled. Consider creating Group Policy settings that enable remote administration.

Working with VMM Libraries

 **Additional Reading:** For more information, go to Configuring the Library Overview at <http://go.microsoft.com/fwlink/p/?linkId=285262>

Demonstration: Using the VMM Management Console

Demonstration Steps

1. On LON-VMM1, on the desktop, double-click **Virtual Machine Manager Console**.

2. In the **Connect to Server** dialog box, ensure that the **Use current Microsoft Windows session identity** check box is selected, and then click **Connect**. The Virtual Machine Manager console opens.
3. Click the **Fabric** workspace.
4. From the ribbon, click **Add Resources**, and then select **Hyper-V Hosts and Clusters**. The Add Resource Wizard starts.
5. On the **Resource location** page, click **Windows Server computers in a trusted Active Directory domain**, and then click **Next**.
6. On the **Credentials** page, click **Manually enter the credentials**, and then use the following credentials:
 - User name: **Adatum\Administrator**
 - Password: **Pa\$\$w0rd**
7. Click **Next**.
8. On the **Discovery scope** page, click **Specify Windows Server computers by names**, and in the **Computer names** field, type **LON-HOST1**, and then click **Next**.
9. On the **Target resources** page, click **lon-host1.adatum.com**, and then click **Next**. On the warning about the Hyper-V role, click **OK**.
10. On the **Host settings** page, click **All Hosts**, and then click **Next**.
11. On the **Summary** page, click **Finish**.
12. Review the status, and then close the Jobs window when the task finishes. A warning message may appear, related to multipath I/O not being enabled. You can ignore this message for this task.
13. Click the **VMs and Services** workspace.
14. On the ribbon, click **All Hosts** and then **Create Host Group**.
15. Under **All Hosts**, enter the name **Sydney Host Group**, and then press Enter.
16. On the ribbon, click **Create Cloud**.
17. On the **General** page of the Create Cloud Wizard, type **Sydney Cloud** in the name box, and then click **Next**.
18. On the Resources page, click **Sydney Host Group**, and then click **Next**.
19. On the **Logical Networks** page, mention that this is where you can add existing logical networks to the cloud, and then click **Next**.
20. On the **Load Balancers** page, mention that this is where you can add existing load balancers to the cloud, and then click **Next**.
21. On the **VIP Templates** page, mention that this is where you can add existing virtual IP (VIP) templates to the cloud, and then click **Next**.
22. On the **Port Classifications** page, mention that this is where you can add existing Port Classifications to the cloud, and then click **Next**.
23. On the **Storage** page, mention that this is where you can add existing storage classifications to the cloud, and then click **Next**.
24. On the **Library** page, mention that this is where you can add existing read-only library shares to the cloud, and then click **Next**.
25. On the **Capacity** page, mention that this is where you can configure the capacity for this cloud, and then click **Next**.

26. On the **Capability profiles** page, click **Hyper-V**, and then click **Next**.
27. On the **Summary** page, click **Finish**.
28. Click the **Close** icon to close the Jobs window.
29. Click the **Library** workspace, and then review the items on the ribbon.
30. Click the **Jobs** workspace, and then click **History**. Review the list of recent jobs and describe each item on the ribbon.
31. Click the **Settings** workspace, and then review the list of **Run As** accounts. Describe the items on the ribbon.

Demonstration: Configuring Host Groups

Demonstration Steps

1. On LON-VMM1, on the desktop, double-click **Virtual Machine Manager Console**.
2. In the **Connect to Server** dialog box, ensure that the **Use current Microsoft Windows session identity** check box is selected, and then click **Connect**. The Virtual Machine Manager console opens.
3. Click **VMs and Services**, and then in the navigation pane, click **All Hosts**.
4. On the ribbon, click **Create Host Group**.
5. Type **Classroom** for the host group name.
6. Right-click the host group that you created, and then click **Properties**. Discuss the options on the **General** properties page.
7. Click **Placement Rules**, and then discuss the options on this page.
8. Click **Host Reserves**, and then discuss the options on this page.
9. Click **Dynamic Optimization**, and then discuss the options on this page.
10. Click **Settings** in the **Power optimization** area, and then discuss these options. Click **Cancel** to close the dialog box.
11. Click **Network**, and then discuss the options on this page.
12. Click **Storage**, and then discuss the options on this page.
13. Click **Custom Properties**, and then discuss the options on this page.
14. Click **Cancel** to close the **Classroom Properties** dialog box.
15. Keep LON-DC1 and LON-VMM1 running, as they are required for the next demonstration in this lesson.

Demonstration: Managing VMM Libraries

Demonstration Steps

Configure a library and library share

1. On TOR-SVR1, on the Server Manager Dashboard, click **File and Storage Services**, and then click **Shares**. In the Shares workspace, click **Tasks**, click **New Share**, click **SMB Share – Quick**, click **Next** twice, type **TORVMMLibrary**, click **Next** three times, and then click **Create**.
2. Click **Close**.
3. On LON-VMM1, open the Virtual Machine Manager console, and then click **Library** in the bottom left of the screen. From the ribbon, click **Add Library Server**. On the **Enter Credentials** page, click

Enter a user name and password, and then enter the following credentials:

- User name: **Adatum\Administrator**
 - Password: **Pa\$\$w0rd**
4. Click **Next**, and then click **Search**.
 5. In the **Computer name** field, type **TOR-SVR1**, and then click **Search**.
 6. On the **Computer Search** page, click **tor-svr1.adatum.com**, click **Add**, click **OK**, and then click **Next**.
 7. Click the box next to **TORVMMLibrary**, and then click the box next to **Add Default Resources**.
 8. Click **Next**, and then click **Add Library Servers**.
 9. Review the job status, and then close the Jobs window.
 10. Keep all virtual machines running, as they are required for demonstrations in the next module.

Module Review and Takeaways

Question: Why would you use an equivalent object? What steps do you need to take after you create it to ensure that VMM placement algorithms use it?

Answer: You should use equivalent objects to store resources used in virtual machine templates so you can deploy them from nearby locations. You need to associate library servers with host groups to ensure that VMM placement algorithms use equivalent objects.

Question: What are some of the reasons for deploying more than one VMM management server?

Answer: Reasons can include bandwidth constraints and administrative issues, which you might encounter when you are working with multiple organizations or budgets.

Real-world Issues and Scenarios

When planning a virtualization project, there are a number of physical, data center, and host considerations. Server density can change, which will affect power consumption and the type of cooling required. For example, a fully populated blade chassis may change the cooling requirements for a data center if you wanted a farm of host servers with physical graphics processing units (GPUs) to provide Microsoft RemoteFX®. This could result in greater heat output, thereby increasing your cooling requirements.

Tools

- Microsoft Virtual Machine Converter Plug-in for VMware vSphere Client
- Microsoft Virtual Machine Servicing Tool 2012 at <http://go.microsoft.com/fwlink/p/?linkId=285267>
- Microsoft Assessment and Planning Toolkit at <http://go.microsoft.com/fwlink/p/?linkId=285265>
- System Center 2012 Virtual Machine Manager Component Add-ons and Extensions at <http://go.microsoft.com/fwlink/p/?linkId=285266>

Common Issues and Troubleshooting Tips

Common Issue	Troubleshooting Tip
Unable to add VMware ESX or Citrix XenServer hosts	<p>Check name resolution, check any firewalls, and verify certificates.</p> <p>Check that adequate permissions have been granted on the hosts. Ensure you use the correct RunAs account.</p>

Lab Review Questions and Answers

Lab: Planning and Implementing a Server Virtualization Strategy

Question and Answers

Question: Planning and Implementing a Server Virtualization Strategy

Answer: The network bandwidth is the factor that would influence a design the most.

Module 3

Planning and Implementing Networks and Storage for Virtualization

Contents:

Lesson 1: Planning a Storage Infrastructure for Virtualization	2
Lesson 2: Implementing a Storage Infrastructure for Virtualization	4
Lesson 3: Planning and Implementing a Network Infrastructure for Virtualization	9
Lesson 4: Planning and Implementing Network Virtualization	13
Module Review and Takeaways	16
Lab Review Questions and Answers	18

Lesson 1

Planning a Storage Infrastructure for Virtualization

Contents:

Resources

3

Resources

Planning High-Availability Options for Hyper-V Storage



Reference Links: For more information, go to The Microsoft Storage Team Blog at <http://go.microsoft.com/fwlink/?LinkID=285270>.

Lesson 2

Implementing a Storage Infrastructure for Virtualization

Contents:

Resources	5
Demonstration: Configuring iSCSI Storage for Virtualization	5
Demonstration: Configuring Storage in VMM	8

Resources

Managing Storage in VMM

 **Reference Links:** For a list of supported storage arrays, see Supported Storage Arrays for System Center 2012 VMM at: <http://social.technet.microsoft.com/wiki/contents/articles/16100.supported-storage-arrays-for-system-center-2012-vmm.aspx>.

Demonstration: Configuring iSCSI Storage for Virtualization

Demonstration Steps

Add virtual disks to LON-SVR1

1. On LON-HOST1, on the taskbar, click **File Explorer**.
2. Double-click **Local Disk (C:)**.
3. On the title bar, click the **New folder** icon.
4. Name the folder **StoragePool**.
5. Close File Explorer.
6. In Hyper-V Manager, right-click **20414C-LON-SVR1**, and then click **Settings**.
7. In the **Settings for 20414C-LON-SVR1 on LON-HOST1** dialog box, click **SCSI Controller**.
8. Click **Hard Drive**, and then click **Add**.
9. In the Media area, click **New**.
10. On the **Before You Begin** page of the New Virtual Hard Disk Wizard, click **Next**.
11. On the **Choose Disk Format** page, click **VHDX**, and then click **Next**.
12. On the **Choose Disk Type** page, click **Dynamically expanding**, and then click **Next**.
13. On the **Specify Name and Location** page, type **iSCSI1.vhdx**, and then click **Browse**.
14. Navigate to **C:\StoragePool**, and then click **Select Folder**.
15. On the **Specify Name and Location** page, click **Next**.
16. On the **Configure Disk** page, enter the size as **50 GB**, and then click **Finish**.
17. On the **Hard Drive** page, click **Apply**.
18. Repeat steps 7 to 17 to create disks **iSCSI2.vhdx** and **iSCSI3.vhdx**.
19. Click **OK** to close the **Settings for 20414C-LON-SVR1 on LON-HOST1** dialog box.
20. In the Actions pane, click **Start**.
21. Sign in to LON-SVR1 as **Adatum\Administrator** with the password **Pa\$\$w0rd**.

Add the iSCSI Target Server Role Service

1. On LON-SVR1, on the **Manage** menu in Server Manager, 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 (Installed)**, expand **File and iSCSI Services**, 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**.

Create a storage pool

1. In Server Manager, in the navigation pane, click **File and Storage Services**, and then click **Storage Pools**.
2. Confirm that the disks you have added are visible in the Physical Disks section. If they are not, in the Storage Pool section, click **Tasks**, and then click **Refresh**.
3. In the Storage Pool section, click **Tasks**, and then click **New Storage Pool**.
4. On the **Before You Begin** page, click **Next**.
5. In the **Storage Pool Name** page in the **Name** field, type **VMPool**, and then click **Next**.
6. On the **Physical Disks** page, select all three disks, and then click **Automatic** in Allocation. Note that you can assign a hot spare. Leave the selection as **Automatic**, and then click **Next**.
7. On the **Confirmation** page, click **Create**.
8. On the **Results** page, click **Create a virtual disk when this wizard closes**, and then click **Close**. The New Virtual Disk Wizard launches.
9. On the **Before you begin** page, click **Next**, and on the **Storage Pool** page, click **Next**. On the **Virtual Disk Name** page, in the **Name** field, type **VMStorage**, and then click **Next**.
10. On the **Storage Layout** page, click **Parity**, and then click **Next**. On the **Provisioning** page, click **Thin**, and then click **Next**.
11. On the **Size** page, in the **Specify size** text box, type **100**, and then click **Next**.
12. On the **Confirmation** page, review the settings, and then click **Create**.
13. On the **View results** page, click **Close**.
14. The New Volume Wizard launches. On the **Before You Begin** page, click **Next**. On the **Server and Disk** page, in the Disk area, click **VMStorage Virtual Disk**, and then click **Next**. On the **Size** page, leave the default (**99.9**) **GB**, and then click **Next**.
15. On the **Drive Letter or Folder** page, set the drive letter to **F**, and then click **Next**. On the **File System Settings** page, click the **Volume Label** field, and then type **VMStorage**. Click **Next**, review the settings, click **Create**, and then on the **Results** page, click **Close**.
16. In the File and Storage Services pane, click **iSCSI**.
17. In the iSCSI Virtual Disks pane, click **Tasks**, and then in the **Tasks** drop-down list box, 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 **F:**, and then click **Next**.
19. On the **Specify iSCSI virtual disk name** page, in the **Name** field type **LONHOST1-iSCSIDisk1**, and then click **Next**.

20. On the **Specify iSCSI virtual disk size** page, in the **Size** box, type **90**, in the drop-down list box, ensure **GB** is selected, click **Dynamically expanding**, and then click **Next**.
21. On the **Assign iSCSI target** page, click **New iSCSI target**, and then click **Next**.
22. On the **Specify target name** page, in the **Name** box, type **LON-HOST1**, and then click **Next**.
23. On the **Specify access servers** page, click **Add**.
24. In the **Add Initiator ID** dialog box, click **Browse**.
25. In the **Select Computer** dialog box, type **LON-HOST1**, click **Check Names**, and then click **OK**.
26. In the **Add initiator ID** dialog box, click **OK**.
27. On the **Specify access servers** page, click **Next**.
28. On the **Enable Authentication** page, click **Next**.
29. On the **Confirm selections** page, click **Create**.
30. On the **View results** page, wait until creation completes, and then click **Close**.
31. In the iSCSI Virtual Disks pane, click **Tasks**, and then in the **Tasks** drop-down list box, click **New iSCSI Virtual Disk**.
32. In the New iSCSI Virtual Disk Wizard, on the **Select iSCSI virtual disk location** page, under **Storage location**, click **C:**, and then click **Next**.
33. On the **Specify iSCSI virtual disk name** page, in the **Name** field type **iSCSIDisk2**, and then click **Next**.
34. On the **Specify iSCSI virtual disk size** page, in the **Size** box, type **5**, in the drop-down list box, ensure **GB** is selected, and then click **Next**.
35. On the **Assign iSCSI target** page, click **LON-HOST1**, and then click **Next**.
36. On the **Confirm selections** page, click **Create**.
37. On the **View results** page, wait until creation completes, and then click **Close**.

Configure iSCSI initiators

1. On LON-HOST1, in Server Manager, click **Tools**, and then click **iSCSI Initiator**. When prompted to start the Microsoft iSCSI service, click **Yes**.
2. On the **Targets** page, in the **Target** field, type **172.16.0.12**. Click **Quick connect**, click **Done**, and then click **OK** to close the page.
3. On LON-HOST1, right-click the **Start** menu, and then click **Disk Management**.
4. Find the new 90 GB disk, right-click the disk, and then click **Online**. Right-click again, click **Initialize Disk**, and then on the **Initialize disk** page, click **OK**.
5. Right-click the unallocated space, and then click **New Simple Volume**.
6. On the **Welcome** page, click **Next**, on the **Specify Volume Size** page, leave the default value, and then click **Next**.
7. On the **Assign Driver letter or Path** page, click the drop-down list box, and then select the letter **V**. Click **Next**.
8. On the **Format Partition** page, in the **Volume label** field, type **VMStorage**. Click **Next**, review the settings, and then click **Finish**.
9. Close **Disk Management**.

Demonstration: Configuring Storage in VMM

Demonstration Steps

Update the LON-HOST1 virtual machine placement path in VMM

1. On LON-VMM1, on the task bar, click **Virtual Machine Manager**. In the **Connect to Server** dialog box, click **Connect**.
2. Click the **Fabric** workspace, expand **Servers**, click **LON-HOST1.adatum.com** on the Managed Computers pane, and then click **Refresh** on the ribbon.
3. On the ribbon, click **Home**, click **Jobs**, wait for **Refresh host job** to complete, and then close the Jobs window.
4. Click **LON-HOST1.adatum.com**, and then click **Properties** on the ribbon.
5. Click **Placement Paths**, click **Add** next to Specify default virtual machine paths to be used during virtual machine placement, click **VMStorage**, and then click **OK**. Click **OK** again to close the **Properties** page.

Create storage classifications

6. In the Virtual Machine Manager console, click the **Fabric** workspace, and then click **Storage**.
7. On the ribbon, click **Create Storage Classification**, and in the **Name** field, type **Gold**. In the **Description** field, type **15K SAS Drives**, and then click **Add**.
8. On the ribbon, click **Create Storage Classification**, and in the **Name** field, type **Silver**. In the **description** field, type **7K SATA Drives**, and then click **Add**.
9. Expand Storage, Click the **Classification and Pools** node, and then note that there is no capacity available.

Add storage providers

10. On LON-VMM1, in the Virtual Machine Manager console, click **Fabric**, right-click **Storage**, and then click **Add Storage Devices**.
11. On the **Select Provider Type** page, click **Windows-based file server**, and then click **Next**.
12. Click the **Provider IP address or FQDN** field, type **lon-svr1.adatum.com**, and then click **Browse**.
13. On the **Select a Run As account** page, click **Administrator**, and then click **OK**.
14. On the **Specify Discovery Scope** page, click **Next**.
15. On the **Gather Information** page, review the discovery result, and then click **Next**.
16. On the **Select Storage Devices** page, click **Next**.
17. On the **Summary** page, click **Finish**, and then close the Jobs window.

Create file shares from VMM

18. On LON-VMM1, click **Fabric**, and then on the ribbon, click **Create File Share**.
19. On the **Create File Share** page, in the **Name** field, type **GoldDisks**. In the **Local path** field, type **F:**, and then click **Create**.
20. Keep all virtual machines running; you will use them for a demonstration in the next lesson.

Lesson 3

Planning and Implementing a Network Infrastructure for Virtualization

Contents:

Demonstration: Configuring Virtual Networks	10
Demonstration: Configuring Virtual Network Components in VMM	10

Demonstration: Configuring Virtual Networks

Demonstration Steps

Create a virtual network

1. On LON-HOST1, in Hyper-V Manager, in the left pane, right-click **LON-HOST1**, and then click **Virtual Switch Manager**.
2. In the left pane, click **New virtual network switch**, in the Create virtual switch section, click **External**, and then click **Create Virtual Switch**.
3. In the **Virtual Switch Properties**, in the **Name** field, type **Classroom demo**, and then select the check box next to **Allow Management Operating System to share this network adapter**.
4. Select the check box next to **Enable single-root I/O virtualization (SR-IOV)**.
5. Change the virtual switch type to **Internal network**, and then click **OK**.

Create a virtual network adapter

1. In the left pane, right-click **LON-HOST1**, click **New**, and then click **Virtual Machine**.
2. On the **Before You Begin** page, click **Next**, and on the **Specify Name and Location** page, in the **Name** field, type **demo1**, and then click **Next**. On the **Specify Generation** page, click **Next**.
3. On the **Assign Memory** page, click **Next**.
4. On the **Configure Networking** page, click the arrow in the **Connection** field, click **Classroom Demo**, and then then click **Finish**.

Review virtual network adapter settings

1. In the right pane, right-click the virtual machine named **demo1**, and then click **Settings**.
2. From the list of hardware that appears, click the **Network adapter**. On the right, you can see the switch currently in use, as well as the virtual local area network (VLAN) and Bandwidth Management settings.
3. Under **Network adapter** settings, click **Hardware Acceleration**, and then on the right, notice that you can see the Virtual Machine Queue, Internet Protocol Security (IPsec) task offloading, and the single-root I/O virtualization (SR-IOV) settings.
4. Under **Network adapter** settings, click **Advanced Features**, and on the right, review the features you can assign.
5. When finished reviewing the options, click **Cancel**.
6. In Hyper-V Manager, under Virtual Machines, right-click the **demo1** virtual machine, and then click **Delete**.
7. On the **Delete Selected Virtual Machines** page, click **Delete** to confirm.
8. Right-click **LON-HOST1**, and then click **Virtual Switch Manager**.
9. Click the **Classroom demo** virtual switch, on the bottom, click **Remove**, and then click **OK**.
10. Keep all virtual machines running. You will use them for the next demonstration in this lesson.

Demonstration: Configuring Virtual Network Components in VMM

Demonstration Steps

Create a logical network

1. On LON-VMM1, launch the Virtual Machine Manager console.

2. Click the **Fabric** workspace, click the **Servers** node, on the ribbon, click **Create**, and then click **Logical Network**.
3. On the **Name** page, in the **Name** field, type **Classroom1**, and then click **Allow new VM networks created on this logical network to use network virtualization**. Click **Next**.
4. On the **Network Site** page, click **Add**, and then in the Host groups that can use this network site section, select **All Hosts**.
5. In the Associated VLANs and IP subnets area, click **Insert row**, click the **VLAN** field, and type **3**. Click the **IP subnet** field, type **192.168.3.0/24**, click **Next**, and then click **Finish**.
6. Close the Jobs window.

Create a logical network IP Pool

1. Click the **Fabric** workspace, on the ribbon, click **Create**, and click **IP Pool**. On the **Name** page, in the **Name** field, type **Classroom1 IP Pool**, click the **Logical network** drop-down list box, click **Classroom1**, and then click **Next**.
2. On the **Network site** page, click **Use an existing network site**, and then ensure that **Classroom1_0** is selected. Click the **IP subnet** drop-down list box, select **192.168.3.0/24**, and then click **Next**.
3. On the **IP address range** page, review the options, and then click **Next**.
4. On the **Gateway** page, review the options, and then click **Next**.
5. On the **DNS** page, review the options, and then click **Next**. On the **WINS** page, review the options, click **Next**, on the **Summary** page, click **Finish**, and then close the Jobs window.

Create an uplink native port profile

1. On the ribbon, click **Create**, and then click **Hyper-V Port Profile**.
2. On the **General** page, click the **Name** field, and then type **Classroom1 Uplink**. Click **Uplink port profile**, and then click **Next**.
3. On the **Network configuration** page, under **Network sites**, click **Classroom 1_0**, click **Enable Hyper-V Network-Virtualization**, and then click **Next**.
4. On the **Summary** page, click **Finish**, and then close the Jobs window.

Create a logical switch

1. On the ribbon, click **Create**, and then click **Logical Switch**.
2. On the **Getting Started** page, click **Next**, on the **General** page, in the **Name** field, type **Classroom switch1**, and then click **Next**.
3. On the **Extensions** page, leave the default extensions, and then click **Next**.
4. On the **Uplink** page, click **Add**, click the **Port profile** drop-down list box, select **Classroom1 Uplink**, click **OK**, and then click **Next**.
5. On the **Virtual Port** page, click **Add**, and then on the **Add Virtual Port** page, click **Browse**.
6. On the **Select a Port Profile Classification** page, click **High Bandwidth**, and then click **OK**. Click **Include a virtual network adapter port profile in this virtual port**, click the **Native virtual network adapter port profile**, select **High Bandwidth Adapter**, click **OK**, and then click **Next**.
7. On the **Summary** page, click **Finish**.
8. Close the Jobs window.

Add a logical switch to a host server

1. From the Fabric workspace, click **LON-HOST1.adatum.com**, on the ribbon click **Properties**, click **Virtual Switches**, click **New Virtual Switch**, and then click **New Logical Switch**. Click **OK** when presented with the Virtual Machine Manager warning dialog box.
2. At this point, if you have another network adapter, you can assign the logical switch to a physical adapter.
3. On the **Properties** page, click **Hardware**, and then scroll down and expand **Network adapters**. Click your physical network adapter, and note that you can select or clear the adapter for virtual machine placement and management use. Click the logical network, and on the right, under **Logical network connectivity**, you can assign the logical networks and IP subnets.
4. Click **Cancel**.
5. Keep all virtual machines running, as they are required for the next demonstration in this lesson.

Lesson 4

Planning and Implementing Network Virtualization

Contents:

Resources	14
Demonstration: Configuring Network Virtualization in VMM	14

Resources

How Network Virtualization Works

 **Reference Links:** For a complete overview of network virtualization, go to <http://go.microsoft.com/fwlink/?LinkID=285279>.

Implementing Network Virtualization

 **Best Practice:** In most sections of the VMM console, you can filter the view by entering text in the search field. Keep this feature in mind and apply a good naming convention to all your virtual network components. This will help you and other administrators when you are working with and or troubleshooting virtual networking. This applies to everything you can label in VMM.

Demonstration: Configuring Network Virtualization in VMM

Demonstration Steps

Create the Test VM network

1. On LON-VMM1, open the Virtual Machine Manager console, click the **VMs and Services** workspace, and then on the ribbon, click **Create VM Network**.
2. On the **Name** page, click the **Name** field, and then type **Classroom1_Test**. Click the **Logical networks** drop-down list box, select **Classroom1**, and then click **Next**.
3. On the **Isolation** page, click **Isolate using Hyper-V network-virtualization**, and then click **Next**.
4. On the **VM Subnets** page, click **Add**, and in the **Name** field, type **Test Network**. In the **Subnet** field, type **192.168.3.0/24**, and then click **Next**.
5. On the **Connectivity** page, click **Next**. Review the summary, and then click **Finish**.
6. Close the Jobs window.

Create the Production VM network

1. On LON-VMM1, open the Virtual Machine Manager console, click the **VMs and Services** workspace, and then on the ribbon, click **Create VM Network**.
2. On the **Name** page, click the **Name** field, and then type **Classroom1_Production**. Click the **Logical networks** drop-down list box, select **Classroom1**, and then click **Next**.
3. On the **Isolation** page, click **Isolate using Hyper-V network-virtualization**, and then click **Next**.
4. On the **VM Subnets** page, click **Add**, and in the **Name** field, type **Production Network**. In the **Subnet** field, type **192.168.3.0/24**, and then click **Next**.
5. On the **Connectivity** page click **Next**. Review the summary, and then click **Finish**.
6. Close the Jobs window.

Create the VM Network IP pools

1. In the **VMs and Services** workspace, click **VM Networks**, click **Classroom1_Production**, and then right-click and click **Create IP Pool**.
2. On the **Name** page, click the **Name** field, and then type **Production VM Network IP Pool**. Make sure that the VM Network is set to **Classroom1_Production** and that the VM subnet is set to **Production Network (192.168.3.0/24)**, and then click **Next**.

3. On the **IP address range** page, note that the first IP address in the range is reserved, leave the defaults, and then click **Next**.
4. On the **Gateway** page, click **Next**, and then on the **DNS** page, click **Next**. On the **WINS** page, click **Next**, and then on the **Summary** page, click **Finish**. Close the Jobs window.
5. Repeat steps 1 through 4 for the **Classroom1_Test VM Network** using the name **Test VM Network IP Pool**, the **VM Network set to Classroom1_Test**, and the VM subnet set to **Test Network (192.168.3.0 /24)**.
6. Keep all virtual machines running. They are required for the demonstrations in the next module.

Module Review and Takeaways

Best Practice

Storage and networking bandwidth is crucial to the planning process. Always look for bottlenecks, and calculate the amount of data that will transfer point-to-point. For example, if you host 500 servers on a SAN, and schedule an antivirus sweep, what is the impact?

Review Question(s)

Question: What is a benefit of logical switches?

Answer: You can define logical switches in VMM and then use them across multiple Hyper-V hosts. This will help with consistency across your virtualization environment.

Real-world Issues and Scenarios

After creating various logical networks and virtual machine networks, you are unable to remove a VMM object due to an error with a dependency on a temporary template. If this happens, you can remove the template by using Windows PowerShell®. Follow this procedure:

In the VMM console, on the ribbon, click **Windows PowerShell**, at the command prompt, type the following command, and then press Enter:

Get-SCVMTemplate | where {\$_.Name -like "Temporary*"}

Review the output, and then confirm that the only listed item is the suspicious temporary template, and that you do not have valid templates with the name "Temporary" in them.

Remove the problematic template by typing the following command at the command prompt, and then pressing Enter:

Get-SCVMTemplate | where {\$_.Name -like "Temporary*" } | Remove-SCVMTemplate

This should clear the dependent template, which will allow you to delete objects, such as a virtual machine network.

Tools

Microsoft Assessment and Planning Toolkit (MAP)

<http://go.microsoft.com/fwlink/?LinkID=285277>

Common Issues and Troubleshooting Tips

Common Issue	Troubleshooting Tip
Virtual machines are all paused	They could have run out of disk space. Look for unneeded snapshots, and then calculate how much disk space you require to ensure that you do not run out again.
Random iSCSI connectivity issues	Check that you have configured the network switches and network adapters are correctly, and that all support the same feature sets that you are using.
Live migrations fail, poor connectivity to virtual machines	Confirm that sufficient bandwidth is available and that live migration is not flooding a network that is used by other traffic that hosts and virtual machines require.

Common Issue	Troubleshooting Tip

Lab Review Questions and Answers

Lab: Planning and Implementing Virtualization Networks and Storage

Question and Answers

Question: What type of business would benefit from network virtualization?

Answer: Hosting companies and service providers are most likely to benefit, as they need to onboard existing customer systems or allow customers to create their own networks.

Question: Which two workloads could you consolidate into a single cluster?

Answer: You can consolidate the Microsoft SQL Server® and Hyper-V workloads into a single SMB 3.0 failover cluster.

Question: What are the new SAN types available to Hyper-V and its virtual machines?

Answer: Hyper-V version 3.0 introduces virtual Fibre Channel.

Module 4

Planning and Deploying Virtual Machines

Contents:

Lesson 4: Planning and Implementing Hyper-V Replica	2
Module Review and Takeaways	5

Lesson 4

Planning and Implementing Hyper-V Replica

Contents:

Demonstration: Enabling Hyper-V Replica	3
Demonstration: Managing Hyper-V Replication and Failover	3

Demonstration: Enabling Hyper-V Replica

Demonstration Steps

1. On LON-HOST1, open the Hyper-V Manager console.
2. In Hyper-V Manager, right-click **LON-HOST1**, and then select **Hyper-V Settings**.
3. In Hyper-V Settings for LON-HOST1, 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. Click **This PC**, double-click **Local Disk (E)**, and then click **New folder**. Type **VMReplica** for the folder name, and then press Enter.
8. Select the **E:\VMReplica** folder, and then click **Select Folder**. (Note: The drive letter might change depending on your host hardware configuration).
9. In the Hyper-V Settings for LON-HOST1, click **OK**.
10. In the Settings window, read the notice, and then click **OK**.
11. Click to the **Start** screen, and then click **Control Panel**.
12. In the Control Panel, click **System and Security**, and then click **Windows Firewall**.
13. Click **Advanced settings**.
14. Click **Inbound Rules**, and in the right pane, in the rule list, right-click the rule **Hyper-V Replica HTTP Listener (TCP-In)**, and then click **Enable Rule**.
15. Close the Windows Firewall with Advanced Security console, and then close Windows Firewall.
16. Repeat steps one through 15 on LON-HOST2.

Demonstration: Managing Hyper-V Replication and Failover

Demonstration Steps

1. On LON-HOST1, open Hyper-V Manager. Click **LON-HOST1**, and then right-click **20414C-LON-CORE**.
2. Click **Enable Replication**, and then on the **Before You Begin** page, click **Next**.
3. On the **Specify Replica Server** page, click **Browse**.
4. In the Select Computer window, type **LON-HOST2**, click **Check Names**, click **OK**, and then click **Next**.
5. On the **Specify Connection Parameters** page, review the settings, make sure that **Use Kerberos Authentication (HTTP)** is selected, and then click **Next**.
6. On the **Choose Replication VHDs** page, make sure that **20414C-LON-CORE.avhdx** is selected, and then click **Next**.
7. On the **Configure Recovery History** page, click **Next**. On the **Configure Additional Recovery Points** page, click **Next**.
8. On the **Choose Initial Replication Method** page, click **Send initial copy over the network**, select **Start replication immediately**, and then click **Next**.
9. On the **Completing the Enable Replication wizard** page, click **Finish**.



Note: Wait approximately five to 10 minutes. You can monitor the progress of initial replication in the **Status** column in the Hyper-V Manager console on LON-HOST1. When it completes (progress reaches 100%), make sure that **20414C-LON-CORE** has appeared on LON-HOST2 in Hyper-V Manager.

10. On LON-HOST2, in Hyper-V Manager, right-click **20414C-LON-CORE**.
11. Select **Replication**, and then click **View Replication Health**.
12. Review the content of the window that appears, and then make sure that there are no errors.
13. Click **Close**.
14. On LON-HOST1, open Hyper-V Manager, and then verify that **20414C-LON-CORE** is turned off.
15. Right-click **20414C-LON-CORE**, select **Replication**, and then click **Planned Failover**.
16. In the Planned Failover window, make sure that **Start the replica virtual machine after failover** is selected, and then click **Fail Over**.
17. In the Planned Failover window, click **Close**.
18. On LON-HOST2, in Hyper-V Manager, make sure that **20414C-LON-CORE** is running.
19. On LON-HOST2, right-click **20414C-LON-CORE**, and then select **Shut Down**. In the **Shut Down Machine** dialog box, click **Shut Down**.
20. On LON-HOST1, right-click **20414C-LON-CORE**, point to **Replication**, and then click **Remove Replication**.
21. In the **Remove Replication** dialog box, click **Remove Replication**.

Module Review and Takeaways

Best Practice

Just as with most information technology (IT) projects, good planning and change control will help you achieve overall success during virtualization. Performance and resource monitoring are essential to maintaining the virtualization infrastructure. Therefore, your implementation and conversion strategy should include these factors to maintain performance levels and avoid scenarios where you run out of resources.

Review Question(s)

Question: You must implement a Hyper-V extended replication. You have confirmed that the initial replication from host A to host B has completed. However, when you right-click the virtual machine, there is no option to extend replication. Why might this occur?

Answer: Windows Server® 2012 R2 Hyper-V introduces extended replication. Therefore, it is possible that the Hyper-V hosts running replication are running Windows Server 2012 Hyper-V, which does not support the new feature.

Question: Which two bare-metal system types can you preconfigure and provision by using the Virtual Machine Manager console?

Answer: The Virtual Machine Manager console allows you to preconfigure and provision bare-metal Hyper-V hosts and Windows File Servers.

Tools

- Microsoft Assessment and Planning Toolkit
- Microsoft Virtual Machine Converter
- Migration Automation Toolkit
- Microsoft Virtual Machine Converter Plug-in for VMware vSphere Client
- Disk2vhd

Module 5

Planning and Implementing a Virtualization Administration Solution

Contents:

Lesson 1: Planning and Implementing Automation with System Center 2012	2
Lesson 2: Planning and Implementing System Center 2012 Administration	6
Lesson 3: Planning and Implementing Self-Service Options in System Center 2012	8
Module Review and Takeaways	11
Lab Review Questions and Answers	12

Lesson 1

Planning and Implementing Automation with System Center 2012

Contents:

Demonstration: Integrating Orchestrator and VMM	3
Demonstration: Creating a Basic Runbook	4

Demonstration: Integrating Orchestrator and VMM

Demonstration Steps

Install the System Center Integration Pack for VMM

1. On LON-OR1, right-click the **Start** icon, and then click **Run**. On the **Run** page, click the **Open** field, type `\\lon-dc1\labfiles\system_center_2012_orchestrator_integration_packs.exe`, and then click **OK**. On the **Choose Directory For Extracted File** page, leave the default directory, and then click **OK**. On the **Extraction Complete** page, click **OK**.
2. On LON-OR1, click **Start**, click the down arrow, and then click **Deployment Manager**.
3. In the Deployment Manager console, right-click **Integration Packs**, and then click **Register IP with the Orchestrator Management Server**.
4. On the **Welcome to the Integration Pack Registration Wizard** page, click **Next**, and then on the **Select Integration Packs or Hotfixes** page, click **Add**.
5. On the **Open** page, in the **File name** field, type `\\lon-dc1\labfiles\SC2012_Virtual_Machine_Manager_Integration_Pack.oip`. Click **Open**. The integration pack is now listed. Click **Next**, and then on the **Completing the Integration Pack Wizard** page, click **Finish**. In the **Microsoft Software License Terms** window, click **Accept**.
6. Wait until the registration is complete, click and expand **Orchestration Management Server**, and then click **Integration Packs**.
7. Right-click **System Center Integration Pack for System Center 2012 Virtual Machine Manager**, and then click **Deploy IP to Runbook Server or Runbook Designer**.
8. On the **Welcome to the Integration Pack Deployment Wizard** page, click **Next**, on the **Deploy Integration Packs or Hotfixes** page, select the check box next to **System Center Integration Pack for System Center 2012 Virtual Machine Manager**, and then click **Next**.
9. On the **Computer Selection** page, in the **Computer** field, type **LON-OR1**, click **Add**, and then click **Next**.
10. On the **Installation Options** page, click **Next**, and then on the **Completing the Integration Pack Deployment Wizard** page, click **Finish**.
11. Review the log entries, and then close the Orchestrator Deployment Manager.

Set the Windows PowerShell execution policy

1. On LON-OR1, on the task bar, right-click **Windows PowerShell**, and then under **Tasks**, click **Run as Administrator**.
2. At the Windows PowerShell® prompt, type `set-executionpolicy remotesigned`, press Enter, type **Y**, and then press Enter.
3. Close the Windows PowerShell window.
4. On LON-VMM1, on the task bar, right-click **Windows PowerShell**, and then under **Tasks**, click **Run as Administrator**.
5. At the Windows PowerShell prompt, type `set-executionpolicy remotesigned`, press Enter, type **Y**, and then press Enter.
6. Close the Windows PowerShell window.

Enable Remote Management Trusted Hosts

1. On LON-OR1, right-click the **Start** icon, and then click **Run**. On the **Run** page, in the **Open** field, type `gpedit.msc`, and then click **OK**. The Local Group Policy Editor Management console appears.

2. On the left side, under **Local Computer Policy**, click to expand **Computer Configuration**, expand **Administrative Templates**, scroll down and double-click **Windows Components**, and then double-click **Windows Remote Management (WinRM)**.
3. On the left, click **WinRM Client**, and then on the right, under **WinRM Client**, double-click **Trusted Hosts**.
4. On the **Trusted Hosts** page, click **Enabled**, in the **TrustedHostList** field, type **LON-VMM1**, and then click **OK**.
5. Close the Group Policy editor.

Configure the System Center Integration Pack for VMM

1. On LON-OR1, click **Start**, click **Down** arrow, and then click **Runbook Designer**.
2. On the menu at the top, click **Options**, and then click **SC 2012 Virtual Machine Manager**.
3. On the **Configurations** page, click **Add**, on the **Add Configuration** page, in the **Name** field, type **LON-VMM1**, and then click the browse (...) button.
4. On the **Item Selection** page, click **System Center Virtual Machine Manager**, and then click **OK**.
5. On the **Add Configuration** page, under **Properties**, in the **VMM Administrator console** field, type **LON-VMM1**, and in the **VMM Server** field, type **LON-VMM1**. In the **User** field, type **Adatum\Administrator**, delete the text in the **Domain** field, and then in the **Password** field, type **Pa\$\$w0rd**.
6. In the **Authentication Type (Remote only)** field, click **Browse**, click **Negotiate**, and then click **OK**.
7. Click **OK**, and then on the **Configurations** page, click **Finish**.
8. In the Runbook Designer console, in the Activities section on the right, click **SC 2012 Virtual Machine Manager**, and then review the activities.
9. Leave LON-DC1 and LON-VMM1 running because you will use them in the next demonstration.

Demonstration: Creating a Basic Runbook

Demonstration Steps

Create a basic runbook

1. On LON-OR1, click **Start**, click the down arrow, and then click **Runbook Designer**.
2. On the left, in the Connections pane, right-click **Runbooks**, click **New**, click **Folder**, on your keyboard, press the Delete key, type **20414 Runbooks**, and then press Enter.
3. Right-click the **20414 Runbooks** folder, click **New**, click **Runbook**, at the top of the central pane, right-click **New Runbook**, click **Rename**, click **Yes** to confirm that you are checking out this runbook, type **VMM Library Monitor**, and then press Enter.
4. On the right pane, under **Activities**, expand **File Management**, and then click and drag the **Monitor Folder** activity to the center of the central pane.
5. Right-click the **Monitor Folder** activity, click **Rename**, and then type **VMM Library Monitor**.
6. Right-click **VMM Library Monitor**, click **Properties**, and on the left, click **General**. On the **General Information** page, in the **Description** field, type **This Runbook monitors the VMM library for new virtual hard disks**.
7. On the left, click **Details**, in the folder to monitor section, in the **Path** field, type **\\LON-VMM1\MSSCVMLibrary**, and then click **Include sub-folders**.

8. In the File Filter section, click **Add**, on the **Filter Setting** page, click the **Name** drop-down list box, click **File Name**, and then in the **Value** field, type ***.vhd**, and then click **OK**.
9. On the left, click **Triggers**, and in the Trigger if section, select the check box next to **Number of files is**. Click the drop-down list box under **Number of files is**, select **greater than**, and then type **0**.
10. On the left, click **Authentication**, in the **User name** field, type **Adatum\Administrator**, in the **Password** field, type **Pa\$\$wOrd**, and then click **Finish**.
11. On the right, under **Activities**, click **Notification**, and then click and drag the **Send Event Log Message** activity to the central pane and to the right of the Virtual Machine Manager (VMM) Library Monitor activity.
12. Place the pointer over the VMM Library Monitor activity and a small arrow appears to the right. Place the pointer over the arrow and the pointer should change to a cross. Click the arrow and drag it to the **Send Event Log Message**. A link with an arrow should now appear between the two activities.
13. Right-click the link between the two activities, click **Properties**, when the **Link Properties** page appears, review the filter, and then click **Finish**.
14. Right-click the **Send Event Log Message**, click **Properties**, on the **Details** page, in the Properties section, click the **Computer** field, and then type **LON-OR1**. In the **Message** field, type **A virtual hard disk file was created or updated in the LON-VMM1 library**. In the Severity section, click **Warning**, and then click **Finish**.
15. On the ribbon, click **Check In**, and then click **Runbook Tester**. In **Confirm Check Out** dialog box, click **Yes**.
16. In the Runbook Tester, click **Run**.
17. On the Windows task bar, click the **File Explorer** icon. In the **address bar** field, type **\\lon-vm1\MSSCVMMLibrary\VHDs**, and then press Enter.
18. On the ribbon of the VHDs window, click **View**, and then select the checkbox next to **File name extensions**.
19. Right-click any of the **Blank Disk – Large.vhd** files, click **Copy**, right-click an empty space in the File Explorer window, and then click **Paste**. A new file is created called **Blank Disk – Large – Copy.vhd**.
20. Switch to the Runbook Tester. In the log section, wait until the **Activity name Send Event Log Message** appears.
21. Switch to the **Start** page, type **Event**, and then click **Event Viewer**. In the center, in the Summary of Administrative Events pane, expand **Warning**, and then you should see an Event ID with the ID of **1** and a Source of **Orchestrator Runbook**. Double-click **Orchestrator event**, and then review the event.
22. Close the Event Viewer, and then close the File Explorer window.
23. Close the Runbook Tester.

Lesson 2

Planning and Implementing System Center 2012 Administration

Contents:

Demonstration: Create a Delegated Administrator in VMM

7

Demonstration: Create a Delegated Administrator in VMM

Demonstration Steps

Configure delegated administration in VMM

1. On LON-VMM1, from the desktop, open the Virtual Machine Manager console.
2. In the **Connect to Server** dialog box, ensure that the **Use current Microsoft Windows session identity** check box is selected, and then click **Connect**. The Virtual Machine Manager (VMM) console opens.
3. In the VMM console, click the **Settings** workspace, and then on the ribbon, click **Create User Role**.
4. On the **Name and description** page, in the **Name** field, type **DevAdmin**, in the **Description** field, type **Development team administrators**, and then click **Next**.
5. On the **Profile** page, click **Fabric Administrator (Delegated Administrator)**, and then click **Next**.
6. On the **Members** page, click **Add**, in the **Select Users, Computers, or Groups** dialog box, in the **Enter the object names to select** field, type **Rob Cason**, click **OK**, and then click **Next**.
7. On the **Scope** page, click **All Hosts**, and then click **Next**.
8. On the **Library servers** page, click **Add**, select **LON-VMM1.Adatum.com**, click **OK**, and then click **Next**.
9. On the **Run As Accounts** page, click **Add**, select **Administrator**, click **OK**, and then click **Next**.
10. Review the summary, and then click **Finish**.
11. Close the Jobs window.

Lesson 3

Planning and Implementing Self-Service Options in System Center 2012

Contents:

Demonstration: Creating VMM Private Clouds

9

Demonstration: Creating VMM Private Clouds

Demonstration Steps

Create a private cloud

1. On LON-VMM1, from the desktop, open the Virtual Machine Manager console.
2. In the **Connect to Server** dialog box, ensure that the **Use current Microsoft Windows session identity** check box is selected, and then click **Connect**. The VMM console opens.
3. Click the **VMs and Services** workspace.
4. On the ribbon, click **Create Cloud**.
5. On the **General** page, in the **Name** field, type **London Development**, in the **Description** field, type **London Development Cloud**, and then click **Next**.
6. On the **Resources** page, select **All Hosts**, and then click **Next**.
7. On the **Logical Networks** page, select **External Network**, and then click **Next**.
8. On the **Load Balancers** page, select **Microsoft Network Load Balancing (NLB)**, and then click **Next**.
9. On the **VIP Templates** page, click **Next**.
10. On the **Port Classifications** page, click **Network load balancing**, click **Medium bandwidth**, click **Low bandwidth**, and then click **Next**.
11. On the **Storage** page, click **Next**.
12. On the **Library** page, in the **Read-only library shares** section, click **Add**. Select **MSSCVMMLibrary**, click **OK**, and then click **Next**.
13. On the **Capacity** page, review the capacity options. Clear the check box next to each selected resource, and then assign the following:
 - 8 virtual central processing units (CPUs)
 - 12 gigabytes (GB) memory
 - 250 GB storage
 - 15 Custom quota (points)
 - 8 virtual machines
14. Click **Next**.
15. On the **Capability Profiles** page, select **Hyper-V**, and then click **Next**.
16. Review the **Summary** page, and then click **Finish**.
17. Close the Jobs window.

Assign access to the London Development cloud

1. Click the **VMs and Services** workspace, right-click **Tenants**, and then click **Create User Role**.
2. On the **Name and description** page, in the **Name** field, type **DevSS**. In the **Description** field, type **London Development Team Self Service Role**, and then click **Next**.
3. On the **Profile** page, click **Application Administrator (Self-Service User)**, and then click **Next**.
4. On the **Members** page, click **Add**, on the **Select Users** page, type **anat**, click **OK**, and then click **Next**.

5. On the **Scope** page, click **London Development**, and then click **Next**.
6. On the **Quotas** page, review the Role and Member level quotas, and then click **Next**.
7. On the **Networking** page, click **Add**, on the **Select VM Networks** page, click **External Network**, click **OK**, and then click **Next**.
8. On the **Resources** page, click **Next**.
9. On the **Permissions** page, click **Select All**, and then click **Next**.
10. On the **Run As accounts** page, click **Add**, click **Administrator**, click **OK**, and then click **Next**.
11. On the **Summary** page, review the settings, and then click **Finish**.

Connect App Controller to VMM

1. On LON-VMM1, move the pointer to the bottom left corner until the Start icon appears, click the **Start** icon, and when the Windows user interface appears, click **App Controller**.
2. On the **App Controller Credentials** page, in the **User name** field, type **Adatum\Administrator**, in the **Password** field, type **Pa\$\$w0rd**, and then click **Sign In**.
3. On the **Overview** page, under **Status**, click **Connect a Virtual Machine Manager server and clouds**. On the **Add a new VMM connection** page, click the **Connection name** field, and then type **LON-VMM1.adatum.com**. In the **Description** field, type **London VMM Server access**. In the **Server name** field, type **LON-VMM1.adatum.com**, and then click **OK**.

Module Review and Takeaways

Review Question(s)

Question: What are some of the benefits of automation and self-service?

Answer: Automation can reduce human error by undertaking a task or series of tasks systematically. Automation can reduce the time that it takes for information technology (IT) staff to complete tasks. Additionally, you can use automation to allow the assignment of privileges to a runbook rather than to a user. For example, you can have a runbook that will add user accounts to a group, and then you allow self-service users to call this runbook.

Self-service can provide users and administrators with rapid access to resources in a controlled environment, without the need to log calls or wait for an administrator.

Lab Review Questions and Answers

Lab: Planning and Implementing an Administration Solution for Virtualization

Question and Answers

Question: If you receive a call from the Toronto developers informing you that there are no resources left, where can you see who is consuming all of the resources?

Answer: In the VMM console, click the VMs and Services workspace, expand clouds, and then click the Toronto Cloud. Click Overview on the ribbon. Then you then can see the quotas and drill down to individual assignments.

Question: Can Adam deploy a virtual machine?

Answer: Adam should be able to deploy a virtual machine, but only from an assigned template.

Module 6

Planning and Implementing a Server Monitoring Strategy

Contents:

Lesson 1: Planning Monitoring in Windows Server 2012	2
Lesson 2: Overview of Operations Manager	4
Lesson 3: Planning and Configuring Monitoring Components	8
Lesson 4: Configuring Integration with VMM	11
Module Review and Takeaways	13
Lab Review Questions and Answers	14

Lesson 1

Planning Monitoring in Windows Server 2012

Contents:

Resources

3

Resources

Options for Monitoring a Server Virtualized Environment



Reference Links:

You can review the Performance Tuning Guidelines for Windows Server 2012 document at <http://go.microsoft.com/fwlink/?LinkID=285313>.

Implementing a Windows PowerShell Desired State Configuration Solution



Additional Reading: For more information on Windows PowerShell, refer to the Windows PowerShell Desired State Configuration Overview at <http://go.microsoft.com/fwlink/?LinkID=392395>.

An online Hands on Lab about the DSC with Windows Server 2012 R2 is available from Microsoft TechEd North America 2013 at the following address: <http://go.microsoft.com/fwlink/?LinkID=392396>.

Lesson 2

Overview of Operations Manager

Contents:

Resources	5
Demonstration: Using the Operations Manager Console	5
Demonstration: Installing the Operations Manager Agent	7

Resources

Operations Manager Components

 **Reference Links:** For more information about distributed deployments of Operations Manager, see <http://go.microsoft.com/fwlink/?LinkID=285319>.

Options for Operations Manager Agent Installation

 **Reference Links:** For more information on the supported operating systems for the Operations Manager agent, see <http://go.microsoft.com/fwlink/?LinkID=285321> and search for "Operations Manager Agent – Windows-Based Computers" in the browser.

What Is Audit Collection Services?

Reference Links:

- For information on how to filter ACS events for UNIX and Linux computers, see <http://go.microsoft.com/fwlink/?LinkID=290803>
- For more information on the use of Dynamic Access Control with ACS in Operations Manager, see <http://go.microsoft.com/fwlink/?LinkID=285318>

Deploying Audit Collection Services

Reference Links:

- For more information on how to configure certificates for ACS Collector and Forwarder, see <http://go.microsoft.com/fwlink/?LinkID=285320>
- For more information on the ACS administration and the AdtAdmin.exe tool, see <http://go.microsoft.com/fwlink/?LinkID=285317>

Considerations for Deploying Operations Manager

 **Reference Links:** System Requirements: System Center 2012 R2- Operations Manager <http://technet.microsoft.com/en-us/library/dn249696.aspx>

Demonstration: Using the Operations Manager Console

Demonstration Steps

1. On LON-OM1, from the Desktop, in the Taskbar, click **Operations Console**.
2. Click the **Monitoring** workspace, expand the **Operations Manager** node, and then click **Active Alerts**. Explain that any alerts from servers in the Operations Manager infrastructure would display here.
3. In the Operations Manager node, click **Management Group Diagram**. Explain that the green check marks indicated that the component is healthy.
4. In the Management Group Diagram, expand the **Data Access Service** group. Explain that this shows all servers running that service.
5. Under the Data Access Services in the **Management Group Diagram**, click on the **Data Access Services** child node. Notice that the **Detail View** is populated.

6. In the Management Group Diagram, expand the **Audit Collection Services** node. Explain that nothing displays because ACS has not been deployed.
7. In the Operations Manager node, click **Management Group Health**. Explain that this is a dashboard view that contains information from three different views.
8. In the Operations console, in the bottom left pane, click **Authoring** to open the Authoring workspace.
9. In the Authoring pane, click **Groups**. Explain that groups are created when management packs are imported and populated based on the management packs' discovery rules.
10. In the Operations console, in the middle pane, right-click **Windows Server Computer Group**, and then click **View Group Members**. Explain that only two servers display because Operations Manager is currently monitoring only one server and itself.
11. Close the Managed Objects – Adatum – Operations Manager window.
12. In the Operations console, in the middle pane, right-click **Windows Server Computer Group**, and then click **View Diagram**.
13. In the Diagram View – Adatum – Operations Manager window, expand **LON-OM1.Adatum.com**, and then expand the **Healthy** node. Explain that Operations Manager monitors these components currently, and are reporting them as healthy. Expand the **Not monitored** node, and explain that Operations Manager is not currently monitoring these components.
14. Close the Diagram View – Adatum – Operations Manager window.
15. In the Authoring pane, expand **Management Pack Objects**. Explain the purpose of each type of management pack object.
16. In the Operations console, in the bottom left pane, click **Reporting** to open the Reporting workspace. Explain that this node displays reports that you use to review high-level or detailed information.
17. In the Operations console, in the bottom left pane, click **Administration** to open the Administration workspace.
18. In the Administration pane, click **Connected Management Groups**. Explain that you can add other management groups to the Operations Manager hierarchy through this node.
19. In the Administration pane, under the Device Management node, click **Management Servers**. Explain that this node displays all of the management servers that the Operations Manager hierarchy uses. Explain that the other nodes under **Device Management** are empty because Operations Manager is not configured to manage any servers.
20. In the Administration pane, click **Management Packs**. Explain that this is where you would import management packs from different vendors.
21. In the Management Packs pane, double-click **Network Management – Core Monitoring**.
22. In the **Network Management – Core Monitoring** dialog box, click the **Dependencies** tab. Explain that management packs build on top of each other.
23. Close the **Network Management – Core Monitoring** dialog box.
24. In the Operations console, in the bottom left pane, click **My Workspace**. Explain that My Workspace is different for each user who accesses the Operations console.
25. In the Operations console, in the bottom left pane, click **Monitoring** to open the Monitoring workspace.
26. In the Monitoring pane, under the Operations Manager node, right-click **Active Alerts**, and then click **Add To My Workspace**.

27. In the **Add To My Workspace** dialog box, in the **Name** box, type **OpsMgr -Active Alerts**, and then click **OK**.
28. In the Operations console, in the bottom left pane, click **My Workspace**, and then select the **OpsMgr -Active Alerts** node.



Note: Explain that the view you have just added is now available from My Workspace.

29. Leave the Operations console open for the next demonstration.

Demonstration: Installing the Operations Manager Agent

Demonstration Steps

1. Switch to LON-OM1.
2. In the Operations console, on the bottom left pane, click **Administration** to open the Administration workspace.
3. Under the Administration pane, click **Discovery Wizard**.
4. In the Computer and Device Management Wizard, on the **Discovery Type** page, ensure that **Windows computers** is selected, and then click **Next**.
5. On the **Auto or Advanced** page, ensure that **Advanced discovery** is selected, and then click **Next**.
6. On the **Discovery Method** page, click **Browse for, or type-in computer names**, and, in the box below, type **LON-SVR1, LON-SVR2**, and then click **Next**.
7. On the **Administrator Account** page, click **Discover**.
8. On the **Select Objects to Manage** page, click **Select All**, and then click **Next**.
9. On the Summary screen, click **Finish**.
10. In the Agent Management Task Status window, wait for the task to complete, and then close the window.
11. Switch to LON-SVR1.
12. In the Start screen, click **Administrative Tools**.
13. In the Administrative Tools window, double-click **Services**.
14. In the Services window, point out the **Microsoft Monitoring Agent** service.

Lesson 3

Planning and Configuring Monitoring Components

Contents:

Question and Answers	9
Demonstration: Importing Management Packs	9

Question and Answers

Discussion: Planning Monitoring with Operations Manager

Question: The CIO wants you to design a monitoring solution for all aspects of the company's IT infrastructure, client devices, and various networking devices, even those not running a Microsoft operating system. How can you use Operations Manager in these situations?

Answer: Operations Manager can monitor the company's IT infrastructure from end to end. This means that it can monitor applications, the operating system, the hardware on which the operating system relies, and the network devices that provide access to the application.

Question: The CIO wants to know if there is a way that he can use Operations Manager data to gauge the state of the overall IT infrastructure quickly. Is this possible, and how can you present high-level data views?

Answer: You can use Operations Manager to monitor performance and availability of the IT infrastructure. You can view the health status of computers and applications monitored by Operations Manager through performance, alert, and dashboard views. A dashboard view can quickly present high-level information on the overall status of the infrastructure. You can configure a dashboard view of the high-level data for the CIO that shows the information he requires in one overall screen shot.

Question: Contoso, Ltd. has a number of wireless LANs within their headquarters, all within the corporate firewall. Bandwidth is limited on the wireless LANs and many of the devices you wish to monitor over the wireless LANs have limited storage space and memory. Given these limitations, what are your options for monitoring the devices on this network?

Answer: Consider deploying agentless monitoring. This will consume fewer resources on the target devices than configurations where agents are running on the device and reporting back information. The information returned is not as in-depth as the agent information, but it should be sufficient for device monitoring in most situations where only basic information is required.

Demonstration: Importing Management Packs

Demonstration Steps

1. On **LON-OM1**, on the desktop, in the task bar, click **Operations Console**, if it is not already open. In the Operations console, in the left pane, click **Administration** to open the Administration workspace.
2. Under the Administration node, click **Management Packs**, and review the list of management packs deployed to Operations Manager.
3. In the Tasks pane, click **Import Management Packs**.
4. In the **Import Management Packs** dialog box, click **Add**, and then, in the **Add** drop-down list box, click **Add from disk**.
5. In the **Online Catalog Connection** dialog box, click **No**.
6. In the **Select Management Packs to import** dialog box, expand drive **C**, expand **Program Files (x86)**, expand **System Center Management Packs**, and then expand **System Center Monitoring Pack for SQL Server**. Click all SQL Server management pack files, and then click **Open**.



Note: Several management pack files are installed already, and have a Blue circle with a letter 'I' in it.

7. On the **Select Management Packs** page, click **Install**, wait about 15 minutes for the management packs to be imported, and then click **Close**.



Note: While you are waiting for the install to complete, consider moving to the Discussion topic at the end of this lesson. You can return to the demonstration when the management pack installation is complete, and finish the discussion at the designated time.

8. Scroll down the list of management packs to locate the management packs you installed.
9. On the bottom-left-hand pane, click **Monitoring** to open the Monitoring workspace.
10. Expand **Microsoft SQL Server**, and then click **Computers**. You may need to wait a few seconds before LON-OM1.Adatum.com displays. Explain that the discovery process for the SQL Server management pack is responsible for finding computers that are running Microsoft SQL Server.

Revert Virtual Machines

After you finish the demonstration, 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 **20414C-LON-DC1**, and then click **Revert**.
3. In the **Revert Virtual Machine** dialog box, click **Revert**.
4. Repeat steps 2 and 3 for **20414C-LON-SVR1**, **20414C-LON-SVR2** and **20410C-LON-OM1**.

Lesson 4

Configuring Integration with VMM

Contents:

Resources

12

Resources

What Is Performance and Resource Optimization?

- **Reference Links:** F5 PRO-enabled Management Pack for System Center

<http://go.microsoft.com/fwlink/?LinkID=285324>

- Citrix NetScaler PRO-Enabled Management Pack for System Center

<http://go.microsoft.com/fwlink/?LinkID=285315>

Module Review and Takeaways

Common Issues and Troubleshooting Tips

Common Issue	Troubleshooting Tip
<p>Management pack does not exist for a specific function. Difficult to update overrides for alerts.</p>	<p>In many cases, you could create a management pack to store overrides related to an imported management pack. A best practice in this case would be to create a management pack for overrides for each management pack that you've imported. This would simplify management.</p>

Lab Review Questions and Answers

Lab: Implementing a Server Monitoring Strategy

Question and Answers

Question: What is the purpose of the channel object when creating notifications?

Answer: Channels specify the type of messaging solution used for the notification. There are four types of channels that you can use:

- E-Mail. Use Simple Mail Transfer Protocol (SMTP) to send email messages.
- Instant Message. Use to send instant messages (IMs).
- Text Message. Use Short Message Service (SMS) to send text messages.
- Command. Use to run a custom command.

Question: Can you integrate System Center 2012 SP1 Operations Manager with System Center 2012 R2 Virtual Machine Manager?

Answer: No.

Module 7

Planning and Implementing High Availability for File Services and Applications

Contents:

Module Review and Takeaways

2

Module Review and Takeaways

Review Question(s)

Question: What are the prerequisites for a clustered storage space?

Answer: The prerequisites for a clustered storage space are:

- Connect all physical disks to the nodes through a serial-attached SCSI interface.
- Have at least three physical disks, with at least 4 GB each.
- Dedicate all physical disks to the storage pool.
- Ensure that Storage Spaces formatted in Resilient File System (ReFS) are not added to the CSV.
- Ensure that all physical disks pass the failover cluster validation tests.

Question: What is one important consideration when deploying NLB by using virtual machines?

Answer: You should ensure that the virtual machines are set to enable MAC address spoofing.

Question: What should you do to ensure that a group of shared files is available locally to users from different physical sites, and that all changes to the files are available in all sites?

Answer: You should use a DFS namespace with a different target server in each site, and configure DFS replication to replicate changes.

Question: Your company needs a SAN for a virtualization project. Management is looking at all possible solutions for a SAN due to budgets constraints. You are asked to provide a solution using Windows Server 2012 R2. What can you propose to create a SAN by using Windows Server 2012 R2 without buying a Fibre Channel SAN?

Answer: You can use a failover cluster with serial-attached SCSI drives. Add the drives to CSV and use clustered Storage Spaces. Virtual disks created in the pool can be exposed to the network by using an iSCSI target server. Redundancy can be provided by using multiple network adapters and MPIO. You can use a 10 Gigabits per second (Gbps) Ethernet network for iSCSI traffic.

Question: You have a server named Server1 that runs Windows Server 2012 R2. Server1 has a hardware RAID array containing 20 drives. The RAID array presents three physical drives to the operating system. Each drive is a RAID 5 array. One drive is used as a startup and system partition, the other drives are currently not used.

You add the two drives not currently used to a storage pool by using Storage Spaces. You need to create two virtual drives and provide availability of data in case up to two physical disks fail. What should you do?

Answer: Creating a two-way mirror would be the ideal solution here. Hardware RAID already supports failure of up to one disk (RAID 5). If a second disk fails, the RAID 5 array will not be available, but by using Storage Spaces and mirroring the data to another physical disk (the other RAID 5 array), the data will be available as long as one of the RAID 5 drives is available. Some students might suggest simple disk, since there is already RAID 5, but RAID 5 supports the failure of only one disk.

Question: You have a server named Server2 that runs Windows Server 2012 R2. Server2 has several hard drives directly attached to itself. Some of the hard drives are serial-attached SCSI drives, some are SATA drives, and some are solid-state drives. You will add all the attached drives to a storage pool, and you will use the pool to create Storage Spaces used for file sharing. You need to ensure that data that is frequently accessed is stored in physical hard drives that have a better read/write performance. What should you do?

Answer: You should use tiered storage in Storage Spaces. When available, it automatically detects frequently accessed data and moves it to solid-state drives. Students might suggest creating different pools, one with the serial-attached SCSI/SATA drives, another with the solid-state drives. Although this provides tiers, it is not automatic.

Module 8

Planning and Implementing a High Availability Infrastructure Using Failover Clustering

Contents:

Lesson 2: Implementing Failover Clustering	2
Lesson 3: Planning and Implementing Updates for Failover Clustering	6
Module Review and Takeaways	9
Lab Review Questions and Answers	11

Lesson 2

Implementing Failover Clustering

Contents:

Demonstration: Configuring the Scale-Out File Server Cluster	3
--	---

Demonstration: Configuring the Scale-Out File Server Cluster

Demonstration Steps

1. On LON-SVR1, in Server Manager, click **Dashboard**, and then click **Add roles and features**.
2. On the **Before You Begin** page, click **Next**.
3. On the **Select installation type** page, click **Next**.
4. On the **Select destination server** page, click **Next**.
5. On the **Select server roles** page, expand **File and Storage Services (Installed)**, expand **File and iSCSI Services (Installed)**, and then verify that **File Server** has been selected.
6. Click **Next**.
7. On the **Select features** page, select **Failover Clustering**, click **Add Features**, and then click **Next**.
8. On the **Confirm installation selections** page, click **Install**.
9. When the **Installation Succeeded** message appears, click **Close**.
10. Repeat steps one through nine on LON-SVR2.
11. On LON-SVR1, open Server Manager, click **Tools**, and then click **iSCSI Initiator**. At the **Microsoft iSCSI** prompt, click **Yes**.
12. Click the **Discovery** tab.
13. Click **Discover Portal**.
14. In the **IP address or DNS Name** box, type **172.16.0.10**, and then click **OK**.
15. Click the **Targets** tab, and then click **Refresh**.
16. In the Targets list, select **iqn.1991-05.com.microsoft:lon-dc1-dctarget1-target**, and then click **Connect**.
17. Select **Add this connection to the list of Favorite Targets**, and then click **OK**.
18. Click **OK** to close iSCSI Initiator Properties.
19. On LON-SVR2, open Server Manager, click **Tools**, and then click **iSCSI Initiator**.
20. In the **Microsoft iSCSI** dialog box, click **Yes**.
21. Click the **Discovery** tab.
22. Click **Discover Portal**, in the IP address or DNS name box, type **172.16.0.10**, and then click **OK**.
23. Click the **Targets** tab.
24. In the **Discovered Targets** list, select **iqn.1991-05.com.microsoft:lon-dc1-dctarget1-target**, and then click **Connect**.
25. Select **Add this connection to the list of Favorite Targets**, and then click **OK**.
26. Click **OK** to close iSCSI Initiator Properties.
27. On LON-SVR2, in the Server Manager window, click **Tools**, and then click **Computer Management**.
28. Expand **Storage**, and then click **Disk Management**.
29. Right-click **Disk 2**, and then click **Online**. (Note: Make sure that you do not click Disk 1, as it is the disk being used in the previously created cluster).
30. Right-click **Disk 2**, and then click **Initialize Disk**. In the **Initialize Disk** dialog box, click **OK**.

31. Right-click the unallocated space next to **Disk 2**, and then click **New Simple Volume**.
32. On the **Welcome** page, click **Next**.
33. On the **Specify Volume Size** page, click **Next**.
34. On the **Assign Drive Letter or Path** page, click **Next**.
35. On the **Format Partition** page, in the **Volume label** box, type **ClusterDisk**. Select the **Perform a quick format** check box, and then click **Next**.
36. Click **Finish**.
37. Right-click **Disk 3**, and then click **Online**.
38. Right-click **Disk 3**, and then click **Initialize Disk**. In the **Initialize Disk** dialog box, click **OK**.
39. Right-click the unallocated space next to **Disk 3**, and then click **New Simple Volume**.
40. On the **Welcome** page, click **Next**, and then on the **Specify Volume Size** page, click **Next**.
41. On the **Assign Drive Letter or Path** page, click **Next**.
42. On the **Format Partition** page, in the **Volume label** box, type **Quorum**. Select the **Perform a quick format** check box, and then click **Next**.
43. Click **Finish**.
44. Close Computer Management, and then cancel any prompts to format the disk.
45. On LON-SVR1, in Server Manager, click **Tools**, and then click **Computer Management**.
46. Expand **Storage**, and then click **Disk Management**.
47. Right-click **Disk Management**, and then click **Refresh**.
48. Right-click **Disk 3**, and then click **Online**. (Note: Make sure that you do not click Disk 2).
49. Right-click **Disk 4**, and then click **Online**.



Note: LON-SVR1 already has two disks that are marked as Disk 3 and Disk 4. However, please note that on LON-SVR2, the same disks are marked as Disk 2 and Disk 3.

50. Close Computer Management.
51. On LON-SVR1, in the Server Manager console, click **Tools**, and then click **Failover Cluster Manager**.
52. In Failover Cluster Manager, in the center pane, under **Management**, click **Create Cluster**.
53. In the Create Cluster Wizard on the **Before You Begin** page, read the information, and then click **Next**.
54. In the **Enter server name** box, type **LON-SVR1**, and then click **Add**. Type **LON-SVR2**, and then click **Add**.
55. Verify the entries, and then click **Next**.
56. On the **Validation Warning** page, click **No. I do not require support from Microsoft for this cluster**, and then click **Next**.
57. In the **Access Point for Administering the Cluster** page, in the **Cluster Name** box, type **FSCluster**.
58. In the **IP Address Name** box, under **Address**, type **172.16.0.127**, and then click **Next**.
59. In the **Confirmation** dialog box, verify the information, clear the check mark next to **Add all eligible storage to the cluster**, and then click **Next**.

60. In the **Create Cluster Wizard Summary** page, click **Finish**.
61. In the Failover Cluster Manager, expand **FSCluster.Adatum.com**, expand **Storage**, and then right-click **Disks**.
62. Click **Add Disk**.
63. In the **Add Disks to a Cluster** dialog box, verify that Cluster Disk 1 and Cluster Disk 2 are selected, and then click **OK**.
64. Verify that the disks appear available for cluster storage in **Failover Cluster Manager**.
65. Right-click **Cluster Disk 1** that is assigned to Available Storage, and then select **Add to Cluster Shared Volumes**.
66. Right-click **FSCluster.Adatum.com**, select **More Actions**, and then click **Configure Cluster Quorum Settings**. Click **Next**.
67. On the **Select Quorum Configuration Option** page, click **Use default quorum configuration**, and then click **Next**.
68. On the **Confirmation** page, click **Next**, and then on the **Summary** page, click **Finish**.
69. Right-click **Roles**, and then select **Configure Role**.
70. On the **Before You Begin** page, click **Next**.
71. On the **Select Role** page, select **File Server**, and then click **Next**.
72. On the **File Server Type** page, click **Scale-Out File Server for application data**, and then click **Next**.
73. On the **Client Access Point** page, in the **Name** box, type **AdatumFS**, and then click **Next**.
74. On the **Confirmation** page, click **Next**.
75. On the **Summary** page, click **Finish**.
76. On LON-SVR1, in the Failover Cluster Manager console, click **Roles**, and then in the central pane, right-click **AdatumFS**.
77. Select **Add File Share**. If you receive a message that the Client Access Point is not ready, wait for a minute, and then try again.
78. In the New Share Wizard, on the **Select the profile for this share** page, select **SMB Share-Applications**, and then click **Next**.
79. On the **Select the server and path for this share**, click **Select by volume**, and then click **Next**.
80. On the **Specify share name** page, in the **Share name** text box, type **TestShare**, and then click **Next**.
81. On the **Configure share settings** page, click **Next**.
82. On the **Specify permissions to control access** page, click **Next**.
83. On the **Confirm selections** page, click **Create**, and then click **Close**.

Lesson 3

Planning and Implementing Updates for Failover Clustering

Contents:

Question and Answers	7
Demonstration: Configuring CAU	7

Question and Answers

What Is CAU?

Question: How do you update cluster nodes in your environment?

Answer: Answers may vary. Some students might answer that they use scripts or other semi-manual procedures.

Demonstration: Configuring CAU

Demonstration Steps

1. On LON-DC1, in Server Manager, 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, make sure 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 list of features, click **Failover Clustering**. In the **Add features that are required for Failover Clustering?** dialog box, click **Add Features**. Click **Next**.
7. On the **Confirm installation selections** page, click **Install**.
8. When installation is complete, click **Close**.
9. On LON-DC1, in the Server Manager dashboard, click **Tools**, and then click **Cluster-Aware Updating**.
10. In the Cluster-Aware Updating window, in the Connect to a **failover cluster** drop-down list, select **FSCLUSTER**. Click **Connect**.
11. In the Cluster Actions pane, click **Preview updates for this cluster**.
12. In the FSCLUSTER-Preview Updates window, click **Generate Update Preview List**.
13. After several minutes, updates will appear in the list. Review updates, and then click **Close**.
14. In the Cluster Actions pane, click **Create or modify Updating Run Profile**.
15. Review and explain available options. Do not make any changes, and then click **Close** when you are finished.
16. Click **Apply updates to this cluster**.
17. On the **Getting Started** page, click **Next**.
18. On the **Advanced Options** page, review options for updating, and then click **Next**.
19. On the **Additional Update Options** page, click **Next**.
20. On the **Confirmation** page, click **Update**, and then click **Close**.
21. In the Cluster nodes pane, you can review the updating's progress. (Note: You should emphasize that one node of the cluster is in the Waiting state, while the other node is restarting after it is updated).
22. Wait until the process is finished. (Note: This may require restarting both nodes.)
23. Sign in to LON-SVR1 with the username **Adatum\Administrator** and the password **Pa\$\$w0rd**.
24. On LON-SVR1, in the Server Manager dashboard, click **Tools**, and then click **Cluster-Aware Updating**.

25. In the Cluster-Aware Updating window, in the **Connect to a failover cluster** drop-down list, select **FSCLUSTER**. Click **Connect**.
26. Click **Configure cluster self-updating options**.
27. On the **Getting Started** page, click **Next**.
28. On the **Add CAU Clustered Role with Self-Updating Enabled** page, click **Add the CAU clustered role, with self-updating mode enabled, to this cluster**, and then click **Next**.
29. In the **Specify self-updating schedule** area, click **Weekly**, select **4:00 AM** for **Time of day**, and then select **Sunday** for **Day of the week**. Click **Next**.
30. On the **Advanced Options** page, click **Next**.
31. On the **Additional Update Options** page, click **Next**.
32. On the **Confirmation** page, click **Apply**.

Module Review and Takeaways

Best Practices

- Try to avoid using a quorum model that depends on a disk alone.
- Use CSVs for Hyper-V high availability or Scale-Out File Server.
- Ensure that in case of one node failure, other nodes can handle the load.
- Plan multisite clusters carefully.
- Develop standard configurations before you implement highly available virtual machines. You should configure the host computers as identically as possible. To make sure that you have a consistent Hyper-V platform, you should configure standard network names, and use consistent naming standards for CSV volumes.
- Implement Virtual Machine Manager (VMM). VMM provides a management layer on top of Hyper-V and Failover Cluster Management that can prevent you from making mistakes when you manage highly available virtual machines. For example, it blocks you from creating virtual machines on storage that is inaccessible from all nodes in the cluster.

Review Question(s)

Question: What is the most important benefit of Scale-Out File Server?

Answer: The most important benefit of Scale-Out File Server, compared to clustered file server in previous Windows versions, is the addition of the scalability feature, or active/active operating mode.

Question: Does Live Migration require that you implement a cluster?

Answer: In Windows Server 2012, it is not mandatory to have a cluster for Live Migration to work.

Question: How do you replicate data between storage in a multisite cluster?

Answer: Multisite data replication can be synchronous or asynchronous. For example, synchronous replication does not acknowledge data changes made in Site A until the data successfully writes to Site B. With asynchronous replication, data changes made in Site A eventually write to Site B.

Tools

Tools	Use	Where to find
Failover Cluster Manager	Manages clusters	Administrative Tools
Windows PowerShell	Command-line management of Windows Server	Administrative Tools
VMM	Virtual environment management	Start menu
Hyper-V Manager	Virtual machines management	Administrative Tools

Common Issues and Troubleshooting Tips

Common Issue	Troubleshooting Tip
Virtual machine failover fails after I implement CSV and migrate the shared storage to CSV.	The CSV home folder is located on the host server system drive. You cannot move it. If the host computers use different system drives, the failovers will fail because the hosts cannot access the same storage location. All failover cluster nodes should use the same hard drive configuration.
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.	By default, virtual machines do not fail back to a host computer after they migrate to another host. You can enable failback on the virtual machine properties in Failover Cluster Management, or you can implement PRO in VMM.

Lab Review Questions and Answers

Lab: Planning and Implementing a Highly Available Infrastructure by Using Failover Clustering

Question and Answers

Question: What is the benefit of using CAU?

Answer: CAU is a feature that enables administrators to update cluster nodes automatically with little or no loss in availability during the update process.

Question: What are the main benefits of having Performance and Resource Optimization (PRO) implemented in VMM?

Answer: PRO is a very important component in managing server workloads in a virtualized environment. PRO integrates VMM and Operations Manager to deliver automation of some tasks that manage workloads on your infrastructure.

Module 9

Planning and Implementing a Business Continuity Strategy

Contents:

Lesson 1: Overview of Business Continuity Planning	2
Module Review and Takeaways	4
Lab Review Questions and Answers	6

Lesson 1

Overview of Business Continuity Planning

Contents:

Resources

3

Resources

Windows Azure Backup



Reference Links: For more information about Windows Azure Backup, go to <http://go.microsoft.com/fwlink/?LinkID=288908>



Additional Reading: For more information about Windows Azure Backup, go to <http://go.microsoft.com/fwlink/?LinkID=288908>

Module Review and Takeaways

Best Practice

You must test your backup and restore strategies before you deploy them in a production environment. Also, you should test your backup and restore strategies in production on a regular basis. However, be careful not to affect your production environment when testing. For testing, you should use a copy of the production data on an isolated, nonproduction environment.

Review Question(s)

Question: What is more convenient for organizations: using a centralized protection solution, such as DPM, or using separate products to protect different servers, data, and services?

Answer: The more convenient option depends on the technologies that the organization is using. The first step in planning should be determining if DPM supports the technologies that the organization is using. If so, then DPM can provide a centralized dashboard for managing backups and restores, and for reporting on different protection jobs and other relevant information. Having separate products is a convenient solution only when organizations use servers that run software that DPM does not support. Also, organizations that have a small number of servers might consider using Windows Server Backup for their backup and restore procedures.

Real-world Issues and Scenarios

Scenario 1:

Your organization has defined its backup and restore strategy. However, after several months of running successful backup jobs, your IT manager wants to test the restore of data located on a file server. No server failures have been detected so far. When performing restore, a backup administrator finds that no corporate data has been restored because the wrong folder from the file server has been configured for backup. Now your organization will have to conduct regular testing on the restore procedures to verify that the correct data will be restored if a failure occurs.

Scenario 2:

A. Datum has seven file servers. You decide to consolidate to a new virtual clustered file server.

You copy the first of several file server's data to the new virtual clustered file server. The initial backup takes nine hours, and incremental daily backups take around 20 minutes.

Over the following year, A. Datum transfers the data successfully from all the remaining file servers.

During restore testing, administrators notice that restores are slower than backups. During a disaster recovery planning meeting, they calculate the time it would take to recover the virtual file server fully to another site. They discover that it would take more than 24 hours, and determine this to be unacceptable. To resolve this issue, the company must invest in a storage infrastructure immediately to ensure that it can recover the corporate file server. They could have avoided this problem if they had calculated the time for backup and restore of the file servers before migrating the production systems.

Tools

- DPM Administrator Console. A GUI for configuring and managing DPM.
- DPM Management Shell. Windows PowerShell® for configuring and managing DPM.

Common Issues and Troubleshooting Tips

Common Issue	Troubleshooting Tip
--------------	---------------------

Common Issue	Troubleshooting Tip
DPM protection agent installation fails	Check technical documentation about specific types of installation that you plan to perform, such as physical machine, virtual machine, workgroup machine, because those deployments are different. Also, check if firewalls are separating computers that need to be protected, so that you can open the appropriate port, TCP Port 135.

Lab Review Questions and Answers

Lab: Implementing a Virtual Machine Backup Strategy with DPM

Question and Answers

Question: Why is it important to prepare a detailed backup and restore strategy for your organization?

Answer: If you prepare a detailed backup and restore strategy, your organization is ready to address any potential risk of losing business-critical data.

Question: Has an organization addressed potential risks by simply identifying them?

Answer: No. In the IT world, risks and threats are constantly evolving. Organizations should evaluate their backup and restore strategies regularly and thoroughly. They should change these strategies according to the latest developments in IT and changes to their business requirements.

Question: Why did you create separate protection groups for backup file server data and virtual machines?

Answer: Typically, file servers and virtual machines have different backup and restore strategies. Therefore, you created two protection groups so that you could apply these different strategies. For example, you would store file server protection group data on both hard disk and tape, while you would store virtual machines on a hard disk only. Also, backup schedules might differ between those two protection groups.

Question: Why do you need to install protection agents on a Hyper-V host computer?

Answer: You need to install a protection agent on a Hyper-V host computer when your organization's strategy is to back up virtual machine files and configuration settings. Therefore, backup jobs will make a copy of all virtual machine data necessary for a complete virtual machine restore. Installing a protection agent on a Hyper-V host computer is not necessary if your organization's strategy is to back up data within virtual machines but not the virtual machines themselves.

Module 10

Planning and Implementing a Public Key Infrastructure

Contents:

Lesson 1: Planning and Implementing Deployment of a Certification Authority	2
Lesson 2: Planning and Implementing Certificate Templates	5
Lesson 3: Planning and Implementing Certificate Distribution and Revocation	7
Module Review and Takeaways	9
Lab Review Questions and Answers	11

Lesson 1

Planning and Implementing Deployment of a Certification Authority

Contents:

Question and Answers	3
Demonstration: Deploying and Configuring a Stand-Alone Root CA	3

Question and Answers

Internal and Public CAs

Question: If you have already implemented a CA hierarchy in your environment, do you also use external certificate for some purposes? If yes, for what?

Answer: Answers may vary. Most commonly, some people will use external public certificates for web servers.

Guidelines for Designing a CA Hierarchy

Question: If you have deployed a CA hierarchy in your company, how many layers does it have? Why did you choose this design?

Answer: Answers may vary, but organizations deploy a two-tier hierarchy most often.

Demonstration: Deploying and Configuring a Stand-Alone Root CA

Demonstration Steps

1. Sign in to **LON-CA1** as **Administrator** with the password **Pa\$\$w0rd**.
2. In the Server Manager console, click **Add roles and features**.
3. On the **Before You Begin** page, click **Next**.
4. On the **Select installation type** page, click **Next**.
5. On the **Select destination server** page, click **Next**.
6. On the **Select server roles** page, select **Active Directory Certificate Services**. When the **Add Roles and Features Wizard** window displays, click **Add Features**, and then click **Next**.
7. On the **Select features** page, click **Next**.
8. On the **Active Directory Certificate Services** page, click **Next**.
9. On the **Select role services** page, ensure that **Certification Authority** is selected, and then click **Next**.
10. On the **Confirm installation selections** page, click **Install**.
11. On the **Installation progress** page, after installation completes successfully, click **Configure Active Directory Certificate Services on the destination server**.
12. In the AD CS Configuration Wizard, on the **Credentials** page, click **Next**.
13. On the **Role Services** page, select **Certification Authority**, and then click **Next**.
14. On the **Setup Type** page, select **Standalone CA**, and then click **Next**.
15. On the **CA Type** page, ensure that **Root CA** is selected, and then click **Next**.
16. On the **Private Key** page, ensure that **Create a new private key** is selected, and then click **Next**.
17. On the **Cryptography for CA** page, keep the default selections for cryptographic provider and hash algorithm, but set the **Key length** to **4096**, and then click **Next**.
18. On the **CA Name** page, in the **Common name for this CA** box, type **AdatumRootCA**, and then click **Next**.
19. On the **Validity Period** page, click **Next**.
20. On the **CA Database** page, click **Next**.
21. On the **Confirmation** page, click **Configure**.

22. On the **Results** page, click **Close**.
23. On the **Installation progress** page, click **Close**.
24. On LON-CA1, in the Server Manager console, click **Tools**, and then click **Certification Authority**.
25. In the certsrv – [Certification Authority (Local)] console, right-click **AdatumRootCA**, and then click **Properties**.
26. In the **AdatumRootCA Properties** window, click the **Extensions** tab.
27. In the **Extensions** tab, in the **Select extension:** drop-down list box, select **CRL Distribution Point (CDP)**, and then click **Add**.
28. In the **Location** text box, type **http://lon-svr1.adatum.com/CertData/**, and, in the **Variable** drop-down list box, click **<CaName>**, and then click **Insert**.
29. In the **Variable** drop-down list box, click **<CRLNameSuffix>**, and then click **Insert**. In the **Variable** drop-down list box, click **<DeltaCRLAllowed>**, and then click **Insert**.
30. In the **Location** text box, position the cursor at the end of the URL, type **.crl**, and then click **OK**.
31. Select the following options: **Include in the CDP extension of issued certificates** and **Include in CRLs. Clients use this to find Delta CRL locations**. Click **Apply**. In the **Certification Authority** pop-up window, click **No**.
32. In the **Select extension:** drop-down list box, click **Authority Information Access (AIA)**, and then click **Add**.
33. In the **Location** text box, type **http://lon-svr1.adatum.com/CertData/**, and, in the **Variable** drop-down list box, click **<ServerDNSName>**, and then click **Insert**.
34. In the **Location** text box, type an underscore (**_**), and, in the **Variable** drop-down list box, click **<CaName>**, and then click **Insert**.
35. In the **Variable** drop-down list box, click **<CertificateName>**, and then click **Insert**.
36. In the **Location** text box, position the cursor at the end of the URL, type **.crt**, and then click **OK**.
37. Select the **Include in the AIA extension of issued certificates** check box, and then click **OK**.
38. Click **Yes** to restart the Certification Authority service.
39. In the Certification Authority console, expand **AdatumRootCA**, right-click **Revoked Certificates**, point to **All Tasks**, and then click **Publish**.
40. In the **Publish CRL** window, click **OK**.

Lesson 2

Planning and Implementing Certificate Templates

Contents:

Question and Answers

6

Question and Answers

Designing Certificate Template Security

Question: To which role will you assign full access rights for one or more certificate templates?

Answer: Most often, you will assign full access on certificate templates to CA managers and people who design and create certificate templates. You should never assign it to people who just need to enroll for a certificate.

Lesson 3

Planning and Implementing Certificate Distribution and Revocation

Contents:

Question and Answers

8

Question and Answers

Certificate Enrollment Options

Question: How do you usually enroll for certificates in your environment? Do you use CA Web enrollment? Why or why not?

Answer: Answers may vary.

Module Review and Takeaways

Best Practices

- When deploying a CA infrastructure, deploy a stand-alone root CA—a root CA that is not joined to a domain—and an enterprise subordinate CA—the issuing CA). After the enterprise subordinate CA receives a certificate from the root CA, take the root CA offline.
- Issue a certificate for the root CA for an extended period of time, such as 15 or 20 years.
- Use autoenrollment for certificates that are used widely.
- Use a Restricted Enrollment Agent whenever possible.

Review Question(s)

Question: What is required for using autoenrollment for certificates?

Answer: You must have an enterprise CA and you must configure Group Policy options. Additionally, you must enable autoenrollment for the desired certificates, and then you must configure GPOs.

Tools

Tools	Use	Where to find
Certificate Authority console	Managing Certificate Authority	Administrative Tools
Certificate Template console	Managing certificate templates	CA console
Certificates console	Managing local certificate store	MMC snap-in
Certutil.exe	Managing CA and certificates	Command-line tool

Common Issues and Troubleshooting Tips

Common Issue	Troubleshooting Tip
The CA is not configured to include CRL distribution point locations in the extensions of issued certificates. Clients may not be able to locate a CRL to check the revocation status of a certificate and certificate validation may fail.	Use the Certification Authority snap-in to configure the CRL distribution point extension and to specify the network location of the CRL. The default locations of the CRL are added to the CRL distribution point extension settings during a CA installation. The CA is configured to include the default locations in the extensions of all issued certificates.
The CA was installed as an enterprise CA, but Group Policy settings for user autoenrollment have not been enabled. An enterprise CA can use autoenrollment to simplify certificate issuance and renewal. If autoenrollment is not enabled, certificate issuance and renewal may not occur as expected.	Use the Group Policy Management console to configure user autoenrollment policy settings. Then use the Certificate Templates snap-in to configure autoenrollment settings on the certificate template.

Common Issue	Troubleshooting Tip

Lab Review Questions and Answers

Lab: Planning and Implementing an Active Directory Certificate Services Infrastructure

Question and Answers

Question: Why is installing an enterprise root CA not recommended?

Answer: For security reasons, root CAs should be offline, without any network access. Root enterprise CAs cannot be offline, so there is no maximum protection for its key.

Question: What is the main benefit of OCSP versus CRL?

Answer: OCSP provides the status for a single certificate that clients request, instead of downloading the entire CRL and delta CRLs. Furthermore, OCSP responses are much faster and more reliable, because clients do not cache them.

Question: What must you do to recover private keys?

Answer: You must configure your CA to archive private keys for specific templates, and then you must issue a KRA certificate.

Module 11

Planning and Implementing an Identity Federation Infrastructure

Contents:

Lesson 1: Planning and Implementing an AD FS Server Infrastructure	2
Lesson 2: Planning and Implementing AD FS Claims Providers and Relying Parties	5
Lesson 3: Planning and Implementing AD FS Claims and Claim Rules	7
Lesson 4: Planning and Implementing Web Application Proxy	9
Module Review and Takeaways	13
Lab Review Questions and Answers	14

Lesson 1

Planning and Implementing an AD FS Server Infrastructure

Contents:

Resources	3
Demonstration: Preparing DNS and Installing the AD FS Server Role	3

Resources

Integrating AD FS with Online Services

 **Additional Reading:** For more information on integrating AD FS with the Windows Azure ACS, go to <http://go.microsoft.com/fwlink/?LinkID=285332>.

Demonstration: Preparing DNS and Installing the AD FS Server Role

Demonstration Steps

Prepare DNS

1. On LON-DC1, in Server Manager, click **Tools**, and then click **DNS**.
2. In the left pane, expand **LON-DC1**.
3. In the left pane, expand **Forward Lookup Zones**, and then click **Adatum.com**.
4. Right-click **Adatum.com**, and then click **New Host (A or AAAA)** from the context menu.
5. In the New Host window, type **adfs** in the **Name** text box and type **172.16.0.10** in the **IP address** text box.
6. Click **Add Host**. Click **OK**, and then click **Done**.
7. Close the DNS Manager.

Install the AD FS server role

1. On LON-DC1, click the Windows PowerShell® shortcut on the taskbar. At the Windows PowerShell prompt, run the **Add-KdsRootKey –EffectiveTime (Get-Date).AddHours(-10)** command.
2. Close the Windows PowerShell window.
3. In Server Manager, click **Manage**, and then click **Add Roles and Features**.
4. On the **Before you begin** page, click **Next**.
5. On the **Select installation type** page, click **Next**.
6. On the **Select destination server** page, click **Next**.
7. On the **Select server roles** page, select **Active Directory Federation Services**, and then click **Next**.
8. On the **Select features** page, click **Next**.
9. On the **AD FS** page, click **Next**.
10. On the **Confirm installation selections** page, click **Install**, and then wait for the installation to finish. Click **Close** when the installation completes.
11. In Server Manager, click the yellow notification icon, and then click the **Configure the federation service on this server** link.
12. On the **Welcome** page, ensure that **Create the first federation server in a federation server farm** is selected, and then click **Next**.
13. On the **Connect to Active Directory Domain Services** page, click **Next** to use the ADATUM\Administrator account.
14. On the **Specify Service Properties** page, select the **SSL certificate** that is named **adfs.adatum.com**. Enter **adfs.adatum.com** as the **Federation Service Display Name**, and then click **Next**.

15. On the **Specify Service Account** page, click **Use an existing domain user account or group Managed Service Account**.
16. Click **Select** to select the account name. In the Select User or Service Account window, type **ADFS-SVC** in the text box, and then click **OK**.
17. On the **Specify Service Account** page, type **Pa\$\$w0rd** in the **Account Password** field, and then click **Next**.
18. On the **Specify Configuration Database** page, ensure that the **Create a database on this server using Windows Internal Database** option is selected, and then click **Next**.
19. On the **Review Options** page, verify that the correct configuration settings are listed, and then click **Next**.
20. On the **Pre-requisite Checks** page, click **Configure**.
21. Wait for the configuration to finish (note that a service principal name registration error may occur), and then click **Close**.
22. On the LON-DC1 virtual machine, in Server Manager, click **Tools**, and then click **Windows PowerShell**.
23. At the Windows PowerShell prompt, type **set-ADFSProperties -AutoCertificateRollover \$False**, and then press Enter. You must perform this step so that you can modify the certificates that AD FS uses.
24. Close the Windows PowerShell window.
25. In Server Manager, click **Tools**, and then click **AD FS Management**.
26. In the AD FS console, in the left pane, expand **Service**, and then click **Certificates**.
27. Right-click **Certificates**, and then click **Add Token-Signing Certificate**.
28. In the **Select a token-signing certificate** dialog box, click the certificate with the name **adfs.adatum.com**, and then click **Click here to view certificate properties**.
29. Verify that the certificate purpose include **Ensures the identity of a remote computer**, and then click **OK**.
30. Click **OK** to close the **Windows Security** dialog box.
31. When the **AD FS Management** warning dialog box displays, click **OK**.
32. In the right pane, under **Certificates**, verify that the certificate has a subject of **CN=adfs.adatum.com**. If no name displays under the **Subject** when you add the certificate, delete the certificate, and then add the next certificate in the list.
33. Under **Token-signing**, right-click the newly added certificate, and then click **Set as Primary**. Review the warning message, and then click **Yes**.
34. Select the certificate that has just been superseded, right-click the certificate, and then click **Delete**. Click **Yes** to confirm the deletion.
35. Keep **LON-DC1** in a running state for use in a future demo.

Lesson 2

Planning and Implementing AD FS Claims Providers and Relying Parties

Contents:

Resources

6

Resources

Overview of AD FS Compatible Applications

 **Additional Reading:** For more information on WIF, go to Microsoft Developer Network (MSDN) at <http://go.microsoft.com/fwlink/?LinkID=285330>.

Options for Implementing Attribute Stores

 **Additional Reading:** For more information on custom attribute stores, go to MSDN at <http://go.microsoft.com/fwlink/?LinkID=285331>

Lesson 3

Planning and Implementing AD FS Claims and Claim Rules

Contents:

Resources

8

Resources

Creating Claim Rules by Using the Claims Rule Language



Additional Reading: For more information on the claims rule language, go to AD FS 2.0 Claims Rule Language Primer on TechNet at <http://go.microsoft.com/fwlink/?LinkID=285329>.

Lesson 4

Planning and Implementing Web Application Proxy

Contents:

Demonstration: Installing and Configuring the Web Application Proxy 10

Demonstration: Installing and Configuring the Web Application Proxy

Demonstration Steps

Install the Web Application Proxy role

1. On LON-SVR2, in Server Manager, click **Manage**, and then click **Add Roles and Features**.
2. In the Add Roles and Features Wizard, on the **Before you begin** page, click **Next**.
3. On the **Select installation type** page, click **Role-based or feature-based installation**, and then click **Next**.
4. On the **Select destination server** page, click **LON-SVR2.Adatum.com**, and then click **Next**.
5. On the **Select server roles** page, select the **Remote Access** check box, and then click **Next**.
6. On the **Select features** page, click **Next**.
7. On the **Remote Access** page, click **Next**.
8. On the **Select role services** page, select **Web Application Proxy**.
9. In the Add Roles and Features Wizard, click **Add Features**.
10. On the **Select role services** page, click **Next**.
11. On the **Confirm installation selections** page, click **Install**.
12. On the **Installation progress** page, click **Close**.

Configure certificates for the Web Application Proxy server

1. On LON-DC1, on the **Start** screen, type **mmc**, and then press **Enter**.
2. In the Microsoft Management Console, click **File**, and then click **Add/Remove Snap-in**.
3. In the Add or Remove Snap-ins window, in the **Available snap-ins** column, double-click **Certificates**.
4. In the Certificates snap-in window, click **Computer account**, and then click **Next**.
5. In the Select Computer window, click **Local Computer (the computer this console is running on)**, and then click **Finish**.
6. In the Add or remove Snap-ins window, click **OK**.
7. In the Microsoft Management Console, expand **Certificates (Local Computer)**, expand **Personal**, and then click **Certificates**.
8. Right-click the **adfs.adatum.com** certificate, point to **All Tasks**, and then click **Export**.
9. In the Certificate Export Wizard, click **Next**.
10. On the **Export Private Key** page, click **Yes, export the private key**, and then click **Next**.
11. On the **Export File Format** page, click **Next**.
12. On the **Security** page, select the **Password** check box.
13. In the **Password** and **Confirm password** boxes, type **Pa\$\$w0rd**, and then click **Next**.
14. On the **File to Export** page, in the **File name** box, type **C:\adfs.pfx**, and then click **Next**.
15. On the **Completing the Certificate Export Wizard** page, click **Finish**, and then click **OK** to close the success message.
16. Close the Microsoft Management Console, and then do not save the changes.
17. On LON-SVR2, on the **Start** screen, type **mmc**, and then press Enter.

18. In the Microsoft Management Console, click **File**, and then click **Add/Remove Snap-in**.
19. In the Add or Remove Snap-ins window, in the **Available snap-ins** column, double-click **Certificates**.
20. In the Certificates snap-in window, click **Computer account**, and then click **Next**.
21. In the Select Computer window, click **Local Computer (the computer this console is running on)**, and then click **Finish**.
22. In the Add or remove Snap-ins window, click **OK**.
23. In the Microsoft Management Console, expand **Certificates (Local Computer)**, and then click **Personal**.
24. Right-click **Personal**, point to **All Tasks**, and then click **Import**.
25. In the Certificate Import Wizard, click **Next**.
26. On the **File to Import** page, in the **File name** box, type `\\LON-DC1\c$\dfs.pfx`, and then click **Next**.
27. On the **Private key protection** page, in the **Password** box, type `Pa$$w0rd`.
28. Select the **Mark this key as exportable** check box, and then click **Next**.
29. On the **Certificate Store** page, click **Place all certificates in the following store**.
30. In the **Certificate store** box, select **Personal**, and then click **Next**.
31. On the **Completing the Certificate Import Wizard** page, click **Finish**, and then click **OK** to clear the success message.
32. Close the Microsoft Management Console, and then do not save the changes.

Configure the proxy to allow access to an internal web application

1. On LON-SVR2, click **Start**, click **Administrative Tools**, and then double-click **Remote Access Management**.
2. Click **Run the Web Application Proxy Configuration Wizard**.
3. On the **Welcome** page, click **Next**.
4. On the **Federation Server** page, type `dfs.adatum.com` in the **Federation service name** text box.
5. On the **Federation Server** page, type `administrator` in the **User name** text box, type `Pa$$w0rd` in the **Password** text box, and then click **Next**.
6. On the **AD FS Proxy Certificate** page, click the **Select a certificate to be used by the AD FS proxy** dropdown menu, and then click `dfs.adatum.com`. Click **Next**.
7. On the **Confirmation** page, click **Configure**.
8. On the **Results** page, click **Close**.
9. In the Remote Access Management console, in the right pane, click **Publish**.
10. On the **Welcome** page, click **Next**.
11. On the **Preauthentication** page, click **Pass-through**, and then click **Next**.
12. On the **Publishing Settings** page, type `AdatumTestApp` for the **Name**, type `https://lon-svr3.adatum.com/AdatumTestApp/` for the **External URL**, select `LON-DC1.Adatum.com` for the external certificate, and then click **Next**.
13. On the **Confirmation** page, click **Publish**.
14. On the **Results** page, click **Close**.

15. After the demonstration, revert all of the virtual machines used in the demos: LON-DC1, LON-SVR1, LON-SVR2, and LON-SVR3.

Module Review and Takeaways

Review Question(s)

Question: What is the difference between a claims provider trust and a relying party trust?

Answer: You create a claims provider trust in a resource partner to establish a relationship with the organization that is hosting the users who will be accessing the resources. A relying party trust specifies an application or another Federation Service that will consume the claims that your Federation Service produces.

Tools

- AD FS Management console. This console is available as part of the Remote Server Administration Tools or on AD FS servers.
- Public key infrastructure (PKI) certification authority. The PKI management tools are available as part of the Remote Server Administration Tools or on Certification Authority servers.
- Windows PowerShell. Windows PowerShell is available on Windows-based computers. You can add modules to manage specific roles such as AD FS.
- Server Manager. Server Manager is available on Windows-based servers. It is installed by default and can manage the local server and remote servers.

Lab Review Questions and Answers

Lab: Planning and Implementing AD FS Infrastructure

Question and Answers

Question: When does A. Datum's AD FS server act as an account federation server, and when does it act as a resource federation server?

Answer: When internal users at A. Datum are accessing web applications, and AD FS is providing SSO functionality, the A. Datum AD FS server is acting as both an account federation server and a resource federation server. When users from Trey Research are accessing the claims-aware web application at A. Datum, the A. Datum AD FS server is acting as a resource federation server, while the Trey Research AD FS server is acting as an account federation server.

Question: How could a proxy improve the security of A. Datum's AD FS deployment?

Answer: A federation server proxy would provide a connection endpoint for external users, which helps avoid exposing the federation server directly to the Internet.

Module 12

Planning and Implementing Data Access for Users and Devices

Contents:

Lesson 1: Planning and Implementing DAC	2
Lesson 3: Planning Work Folders	5
Module Review and Takeaways	7
Lab Review Questions and Answers	9

Lesson 1

Planning and Implementing DAC

Contents:

Demonstration: Creating Central Access Rules and Policies for DAC 3

Demonstration: Creating Central Access Rules and Policies for DAC

Demonstration Steps

1. On LON-DC1, on the taskbar, click **Server Manager**.
2. In Windows® 8 Server Manager, click **Tools**, and then click **Active Directory Administrative Center**.
3. In the Active Directory® Administrative Center console, in the navigation pane, click **Dynamic Access Control**.
4. Double-click **Claim Types**.
5. In the Tasks pane, click **New**, and then click **Claim Type**.
6. In the Create Claim Type window, in the Source attribute section, click the **Department** attribute.
7. In the **Display name** text box, type **Company Department**.
8. Select the **User** and **Computer** check boxes, and then click **OK**.
9. In the Tasks pane, click **New**, and then click **Claim Type**.
10. In the Create Claim Type window, in the Source attribute section, click the attribute **employeeType**.
11. In the **Display name** text box, type **Employee Type**.
12. Select the **User** and **Computer** check boxes, and then click **OK**.
13. Click **Dynamic Access Control**.
14. In the central pane, double-click **Resource Properties**.
15. In the **Resource Properties** list, locate and right-click **Department**, and then click **Enable**.
16. In the Active Directory Administrative Center console, in the navigation pane, click **Dynamic Access Control**.
17. Double-click **Central Access Rules**.
18. In the Tasks pane, click **New**, and then click **Central Access Rule**.
19. In the **Central Access Rule** dialog box, in the **Name** box, type **Department Match**.
20. In the Target Resource section, click **Edit**.
21. In the Central Access Rule window, click **Add a condition**.
22. Set a condition as **Resource-Department-Equals-Value-Research and Development**, and then click **OK**.
23. In the Permissions section, click **Use following permissions as current permissions**, and then click **Edit**.
24. Click **Administrators (ADATUM\Administrators)**, and then click **Remove**.
25. In **Advanced Security Settings for Permissions**, click **Add**.
26. In the **Permission Entry for Permissions** dialog box, click **Select a principal**.
27. In the **Select User, Computer, Service Account or Group** dialog box, type **Authenticated Users**, click **Check Names**, and then click **OK**.
28. In the Basic permissions section, click **Modify, Read and Execute, Read, and Write**.
29. Click **Add a condition**.
30. In the **Group** drop-down list box, click **Company Department**.

31. On the **Value** drop-down list box, click **Resource**.
32. On the last drop-down list box, click **Department**, and then click **OK** three times.



Note: As a result, you should have the following expression: **User-Company Department-Equals-Resource-Department**.

33. In the Active Directory Administrative Center console, click **Dynamic Access Control**, and then double-click **Central Access Policies**.
34. In the Tasks pane, click **New**, and then click **Central Access Policy**.
35. In the **Name** box, type **Department Match**, and then click **Add**.
36. Click the **Department Match** rule, and then click the **More (>>)** icon. Click **OK** twice.

Lesson 3

Planning Work Folders

Contents:

Demonstration: Configuring Work Folders

6

Demonstration: Configuring Work Folders

Demonstration Steps

1. On LON-SVR1, in Server Manager, expand **File and Storage Services**, and then click **Work Folders**.
2. In the **WORK FOLDERS** tile, click **Tasks**, and then click **New Sync Share**.
3. In the New Sync Share Wizard, on the **Before You Begin** page, click **Next**.
4. On the **Select the server and path** page, select **Select by file share**, ensure that the share you created in the preparation tasks. WF-Share, is highlighted, and then click **Next**.
5. On the **Specify the structure for user folders**, accept the default selection, user alias, and then click **Next**.
6. On the **Enter the sync share name** page, accept the default, and then click **Next**.
7. On the **Grant sync access to groups** page, note the default selection to disable inherited permissions and grant users exclusive access, and then click **Add**.
8. In the **Select User or Group** dialog box, in the **Enter the object names to select** field, type **WFsync**, click **Check Names**, and then click **OK**.
9. On the **Grant sync access to groups** page, click **Next**.
10. On the **Specify device policies** page, note the selections, accept the default selection, and then click **Next**.
11. On the **Confirm selections** page, click **Create**.
12. On the **View results** page, click **Close**.
13. Switch to LON-DC1, and then sign in as **Adatum\Administrator** with the password **Pa\$\$w0rd**.
14. Open **Server Manager**, click **Tools**, and then click **Group Policy Management**.
15. Expand **Forest: Adatum.com-Domains-Adatum.com**, click **Group Policy Objects**, right-click the **Group Policy Objects** container, and then click **New**.
16. In the New GPO window, type **Work Folders GPO** in the **Name** field, and then click **OK**.
17. Right-click **Work Folders GPO**, and then click **Edit**.
18. In the Group Policy Management Editor, expand **User Configuration/Policies/Administrative Templates/Windows Components**, and then click **Work Folders**.
19. Double-click **Specify Work Folders settings** in the details pane.
20. In the **Specify Work Folders settings** dialog box, click **Enabled**.
21. In the **Work Folders URL** text box, type **https://lon-svr1.adatum.com**, and then select **Force automatic setup**.
22. To close the **Specify Work Folders settings** dialog box, click **OK**, and then close the Group Policy Management Editor.
23. In the Group Policy Management Console, right-click the **Adatum.com** domain object, and then choose **Link an Existing GPO**.
24. In the Select GPO window, choose **Work Folders GPO**, and then click **OK**.
25. Close the Group Policy Management Console.

Module Review and Takeaways

Best Practices

- Use Central Access Policies instead of configuring conditional expressions on resources.
- Enable access-denied assistance settings.
- Always test changes that you have made to Central Access Rules and to Central Access Policies before implementing them.
- Use file classifications to assign properties to files.
- Use Work Folders to synchronize business data across devices.
- Always use HTTPS for Work Folders client connections.
- Use Workplace Join in BYOD scenarios.

Review Question(s)

Question: What is the BYOD concept?

Answer: BYOD is the policy of permitting employees to bring personal devices, such as laptops, tablets, and smart phones, to the workplace, and allowing employees to use those devices to access privileged company information and applications.

Question: What is the main purpose of access-denied assistance technology?

Answer: Access-denied assistance helps both administrators and end users to deal with access-denied errors when trying to access a resource. By using this technology, users are able to get a more accurate description of the reason for access denial and they are able to request access from a folder owner or administrator.

Question: What is the main benefit of Workplace Join for end users?

Answer: When using Workplace join, users can have a single sign-on (SSO) experience on devices that are not domain members.

Question: What is a claim?

Answer: A claim is information that Active Directory Domain Services (AD DS) states about a specific object, usually a user or a computer. Claims provide some information from a trusted source about an entity.

Question: What is the purpose of a Central Access Policy?

Answer: A Central Access Policy enables administrators to create a policy that is applied to one or more file servers in an organization. A Central Access Policy contains one or more Central Access Policy rules. Each rule contains settings that determine applicability and permissions.

Tools

Tool	Use	Location
Active Directory Administrative Center	Administering and creating claims, resource properties, rules, and policies	Administrative tools
Group Policy Management Console (GPMC)	Managing Group Policy	Administrative tools

Tool	Use	Location
Group Policy Management Editor	Editing Group Policy Objects (GPOs)	GPMC
Active Directory Federation Services (AD FS) Management Console	AD FS Management	Administrative tools
Web Application Proxy Console	Secure publishing of internal resources	Administrative tools
Work Folders administration interface	Work Folders provisioning and management	Server Manager

Common Issues and Troubleshooting Tips

Common Issue	Troubleshooting Tip
Claims are not populated with the appropriate values.	Verify that the correct attribute is selected for the claim. In addition, check that the attribute value for a specific object is populated.
A conditional expression does not allow access.	Verify that the expression is well defined. In addition, try using the Effective Access tab to troubleshoot the problem.
Work Folders do not sync on non-domain joined devices.	Ensure that a non-domain joined device trusts the certificate installed on the server that hosts Work Folders.

Lab Review Questions and Answers

Lab A: Implementing DAC and Access-Denied Assistance

Question and Answers

Question: What was your approach to the data access design?

Answer: Answers will vary.

Question: What was your approach to the DAC design?

Answer: Answer will vary.

Question: How does your organization implement data access for branch offices?

Answer: Answers will vary

Lab B: Implementing Work Folders

Question and Answers

Question: What is the purpose of implementing Web Application Proxy?

Answer: We implemented Web Application Proxy in this lab to publish Work Folders securely on an external network.

Question: Why did you implement AD FS in this lab?

Answer: We implemented AD FS to support the implementation of Web Application Proxy. We did not use it for authentication purposes, but we used it for pass-through authentication instead.

Question: Why do you need to accept security policies when configuring Work Folders on a non-domain joined device?

Answer: You should enforce security policies for device lock and encryption before the data sync starts. This provides better data security to devices that are non-domain joined.

Module 13

Planning and Implementing an Information Rights Management Infrastructure

Contents:

Lesson 1: AD RMS Overview	2
Lesson 2: Planning and Implementing an AD RMS Cluster	4
Lesson 3: Planning and Implementing AD RMS Templates and Policies	9
Lesson 4: Planning and Implementing External Access to AD RMS Services	12
Lesson 5: Planning and Implementing AD RMS Integration with Dynamic Access Control	14
Module Review and Takeaways	18
Lab Review Questions and Answers	19

Lesson 1

AD RMS Overview

Contents:

Question and Answers

3

Question and Answers

AD RMS Deployment Scenarios

Question: Have you implemented AD RMS in your environment? If yes, which deployment scenario are you using? If you are not using it currently, which deployment scenarios might you use in the future?

Answer: Answers will vary.

Lesson 2

Planning and Implementing an AD RMS Cluster

Contents:

Resources	5
Demonstration: Installing an AD RMS Cluster	5

Resources

Implementing an AD RMS Backup and Recovery Strategy

 **Additional Reading:** To restore a database, follow the regular procedures for a database restoration on SQL Server. See <http://go.microsoft.com/fwlink/?LinkID=285335> for a review of these procedures.

Demonstration: Installing an AD RMS Cluster

Demonstration Steps

Prepare the AD RMS infrastructure

1. On LON-DC1, in Server Manager, click **Tools**, and then select **Active Directory Users and Computers**.
2. In the console tree, expand **Adatum.com**.
3. Right-click **Users**, point to **New**, and then click **User**.
4. In the **New Object – User** dialog box, type **ADRMSSRVC** in the **First name** and **User logon name** boxes, and then click **Next**.
5. In the **New Object – User** dialog box, type **Pa\$\$w0rd** in the **Password** and **Confirm password** boxes. Clear the **User must change password at next logon** check box, click **Next**, and then click **Finish**.

 **Note:** You created the ADRMSSRVC account to use for installing and managing the AD RMS server deployment. To ensure that this account has the correct permissions to enable these tasks, including the ability to register the service connection point, you must make it a member of the Domain Admins group for the ADATUM.com domain. The AD RMS setup looks for the security identifier (SID) of the default Administrator account. The AD RMS service SID cannot match the SID of the default Administrator account.

Add ADRMSSRVC to the Domain Admins group

1. In the Active Directory Users and Computers console, click **Users**, and then double-click **Domain Admins**.
2. Click **Members**, and then click **Add**.
3. Type **adrmssrvc**, and then click **OK**.
4. Click **OK** to close Domain Admins Properties.

Add email addresses to user and group

1. Explain that we can use a user's or group's email address to set information rights from within an app, such as Microsoft Word. Therefore, we will add email addresses to some of the domain's security principal objects. In the Active Directory Users and Computers console, click the **Research** organizational unit (OU), and then double-click the **Hani Loza** account object.
2. On the **General** tab of the Hani properties sheet, in the **email** box, type **hani@adatum.com**, and then click **OK**.
3. Double-click the **Research** group within the **Research OU**.

4. On the **General** tab of the Research group properties, in the **email** box, type **Research@adatum.com**, and then click **OK**.
5. Close the Active Directory Users and Computers console.

Create a shared network folder that members of the Research group can modify

1. From the task bar, open File Explorer, and then right-click **Local Disk (C:)**.
2. Point to **New**, and then click **Folder**.
3. Type **ConfidentialResearch** for the new folder, and then press Enter.
4. Right-click **ConfidentialResearch**, point to **Share with**, and then click **Specific people**.
5. In the **Choose people on your network to share with** box, type **Research**, and then click **Add**.
6. In the list, click the arrow for **Permission Level** on the **Research** group, and then select **Read/Write**.
7. Click **Share**, and then click **Done**.

Create a share on LON-DC1 to store the AD RMS templates

1. From File Explorer, right-click **Local Disk (C:)**.
2. Point to **New**, and then click **Folder**.
3. Type **Public** for the new folder, and then press Enter.
4. Right-click **Public**, point to **Share with**, and then click **Specific people**.
5. In the Choose people on your network to share with window, click the arrow, select **Everyone**, and then click **Add**.
6. Click **Share**, and then click **Done**.
7. Close File Explorer.

Add the AD RMS server role

Windows Server 2012 includes the option to install AD RMS as a server role by using Windows Server 2012 Server Manager. The first server in an AD RMS environment is the root cluster, which has one or more AD RMS servers that you configure in a load-balancing environment.



Note: AD RMS is a server role of Windows Server 2012, so every user or device that accesses the server software requires a Windows Server 2012 client access license (CAL).

1. On LON-DC1, in the Dashboard console of Server Manager, click **Add roles and features**.
2. Click **Next** three times to get to the **Select Server roles** page.
3. On the **Select Server roles** page, select **Active Directory Rights Management Services**, click **Add Features**, and then click **Next**.
4. On the **Select features** page, click **Next**.
5. On the **Active Directory Rights Management Services** page, click **Next**.
6. In **Select role services** page, verify that **Active Directory Rights Management Server** is selected, and then click **Next**.
7. Click **Install** to add the role.
8. Allow the installation to complete, and then click **Close**.

Configure a new AD RMS root cluster

In Windows Server 2012, there are separate processes to add the AD RMS role and then configure a new AD RMS cluster. After you add the role, you must configure the role to deploy it.

To configure a new AD RMS root cluster:

1. In Server Manager, click the **Notifications** icon (the white flag next to **Manage**).
2. For the task event labeled **Configuration Required for Active Directory Rights Management Services at LON-DC1**, click **Perform additional configuration**. The AD RMS Configuration Wizard opens.
3. In the AD RMS Configuration Wizard, on the **AD RMS** page, click **Next**.
4. On the **Create or Join an AD RMS Cluster** page, accept the default selection (**Create a new AD RMS root cluster**), and then click **Next**.
5. On the **Select Configuration Database Server** page, click **Use Windows Internal Database on this server**, and then click **Next**.
6. In **Specify Service Account** page, click **Specify**, in the **Windows Security** dialog box, type the name **ADRMSSRV** and the password **Pa\$\$w0rd**, and then click **OK**.
7. Verify that the **Domain User Account** is set to **ADATUM\ADRMSSRV**, and then click **Next**.
8. For **Cryptographic Mode**, accept the default (**Cryptographic Mode 2**), and then click **Next**.
9. For **Cluster Key Storage**, accept the default setting (**Use AD RMS centrally managed key storage**), and then click **Next**.
10. For **Cluster Key Password**, type and confirm **Pa\$\$w0rd**, and then click **Next**.
11. For **Cluster Web Site**, accept the default setting (**Default Web Site**), and then click **Next**.
12. For **Cluster Address**, change the default setting—**Use an SSL-encrypted connection (https://)**—to **Use an unencrypted connection (http://)**. Close the yellow bar warning (that begins with “You cannot use an unencrypted...”). For **Fully Qualified Domain Name**, type **LON-DC1.adatum.com** (use the fully qualified domain name [FQDN], not just LON-DC1), and then click **Next**.
13. For **Licenser Certificate**, accept the default name (**LON-DC1** does not need to be the FQDN), and then click **Next**.
14. For **SCP Registration**, accept the default setting (**Register the SCP now**), and then click **Next**.
15. For **Confirmation**, review your installation selections, and then click **Install**.
16. Click **Close**.
17. Sign out of the server, and then sign in again to update the security token of the signed-in user account.



Note: You have installed and configured your AD RMS root cluster. Once you sign in again, you can manage AD RMS further by using the AD RMS console.

Open the Active Directory Rights Management Services console

1. On LON-DC1, in Server Manager, click **Tools**, and then click **Active Directory Rights Management Services**. If time permits, spend a few moments going over the various console tree nodes and settings.
2. Close the Active Directory Rights Management Services console.

From the console, you can configure trust and exclusion policies, and create rights policy templates.

The user account that is signed in when you install the AD RMS server role automatically becomes a member of the AD RMS Enterprise Administrators local group. A user must be a member of that group to administer AD RMS.

Tip: If using a self-signed certificate for the cluster, you can put a copy of that certificate in the Trusted Root-Certification Authorities store so that it will be trusted. You can also place a copy in that same certificates store on the client computer, so that the website is trusted.

If the Certificate Warning page appears, you can click Yes to load the website, or you can install the certificate in the Trusted Root Certification Authorities store. Do this for the local computer account.

Discuss the various nodes in the console tree. Explain how you can use the nodes in the console to configure trust and exclusion policies, and create rights policy templates.

Lesson 3

Planning and Implementing AD RMS Templates and Policies

Contents:

Question and Answers	10
Demonstration: Adding User Entities to an Exclusion Policy	10

Question and Answers

Options for Configuring AD RMS Rights Policy Templates

Question: Can an organization use AD RMS without using rights policy templates? If so, what are the limitations?

Answer: An organization can use AD RMS without using rights policy templates. The main limitation is that you must configure the authorized users manually. Then you must use rights each time you protect content with AD RMS.

Demonstration: Adding User Entities to an Exclusion Policy

Demonstration Steps

Add Domain Users Group to local Remote Desktop Users group

1. Sign in to LON-CL1 as **Adatum\administrator** with the password **Pa\$\$w0rd**.
2. From the Start screen, click the **Desktop** tile.
3. On the taskbar, click **File Explorer**.
4. In the **This PC** console tree, right-click **This PC**, and then select **Properties**.
5. In the **System** console tree, select **Remote** settings.
6. In the **System Properties** window, click **Select Users**.
7. In the **Remote Desktop Users** window, click the **Add** button.
8. In the **Select Users or Groups** window, in the **Enter the object names to select** text box, type **Domain Users**, and then click **OK** three times.
9. Close all open windows and sign out.

Exclude Rights Account Certificates (RACs)

1. Sign in to **LON-CL1** as **Adatum\hani** with the password **Pa\$\$w0rd**.
2. From the Start screen, click the **Desktop** tile.
3. From the desktop taskbar, click **Internet Explorer**.
4. In the URL bar, type **http://lon-dc1.adatum.com**.
5. Close any pop-up warnings.
6. Click the **gear** icon in the upper right of the Internet Explorer® window, and then click **Internet options**.
7. Click the **Security** tab, click **Local intranet**, and then click **Sites**.
8. Click **Advanced**, and in the **Add this website to the zone** text box, type **http://LON-DC1.adatum.com**, and then click **Add**.
9. Click **Close**, and then click **OK** two times.
10. Close Internet Explorer.
11. Click to the Start screen, and then type **Word**.
12. Click **Word 2013**. Click **Use recommended settings** in the **First things first** dialog box, and then click **Accept**.
13. In the **User Account Control** pop-up window, enter the domain administrator's credentials: **Adatum\administrator** with the password **Pa\$\$w0rd**. Click **Yes**.

14. In the **Office** dialog box, click **Next** three times, and then click **All done!**
15. Click the blank document in the **Word Recent** window.
16. In Microsoft Word, type **Research employees can read this document, but they cannot change, print, or copy it on the blank document page.**
17. From the File menu, on the **Info** page, click **Protect Document**, point to and click **Restrict Access**, and then click **Connect to Digital Rights Management Servers** to get templates. The templates will then download.



Note: You will not receive notification of the template download.

18. On the **Info** page, click **Protect Document**, point to and click **Restrict Access**, and then click **Restricted Access**.
19. In the **Permission** dialog box, select the **Restrict permission to this document** check box, and then in the **Read** box, type **Research@adatum.com**.
20. Click **OK** to close the **Permission** dialog box.
21. From the File menu, click **Save As**, click the **Browse** button, in the **File name** text box, type **\\LON-DC1\ConfidentialResearch\ADRMS-TST.docx**, and then click **Save**.
22. Close Microsoft Word, and then sign out of LON-CL1. Remember that the above steps ensure that a RAC has been created for Hani.

Exclude the restriction on a user

1. Switch back to LON-DC1, and in Server Manager, click **Tools**, and then click **Active Directory Rights Management Services**.
2. In the AD RMS console, expand **lon-dc1.adatum.com**.
3. Expand **Exclusion policies**, and then click **Users**.
4. In the Actions pane, click **Enable User Exclusion**.
5. In the Actions pane, click **Exclude RAC**.
6. On the **Add RAC to be excluded** page, ensure that **Use this option for excluding rights account certificates of internal users who have an Active Directory Domain Services account** is selected. Type **hani@adatum.com** in the **User name** box.
7. Click **Finish**. Hani's email address and public key should appear in the table in the **User Exclusion Information** page.
8. Close the Active Directory Rights Management Services console.

Lesson 4

Planning and Implementing External Access to AD RMS Services

Contents:

Question and Answers	13
Resources	13

Question and Answers

Options for Enabling External Users to Access AD RMS

Question: In what scenarios do you need to provide external access to AD RMS?

Answer: You need to provide external access to AD RMS if you want to distribute or accept AD RMS–protected documents from other organizations, or if you want to send AD RMS–protected content over the Internet.

Resources

Options for Enabling Application Access for AD RMS Clients

 **Additional Reading:** You can download these free from the Microsoft website, at <http://go.microsoft.com/fwlink/?LinkID=285336>.

Integrating AD RMS with AD FS

 **Additional Reading:** Windows Phone clients can use certain extended features, which the article at <http://go.microsoft.com/fwlink/?LinkID=285333> describes. All of these disparate client settings can increase support costs.

 **Additional Reading:** For more information, go to <http://go.microsoft.com/fwlink/?LinkID=285334>

 **Additional Reading:** For more information, go to <http://go.microsoft.com/fwlink/?LinkID=285334>.

Lesson 5

Planning and Implementing AD RMS Integration with Dynamic Access Control

Contents:

Demonstration: Deploy Encryption of Office Files

15

Demonstration: Deploy Encryption of Office Files

Demonstration Steps

Enable resource properties

1. On LON-DC1, open the Active Directory Administrative Center, and in the top of the console tree, click the **Tree View** icon.
2. Expand **Dynamic Access Control**, and then select **Resource Properties**.
3. In the Resource Properties details pane, scroll down to the **Impact** property in the **Display Name** column. Right-click **Impact**, and then click **Enable**.
4. Scroll down to the **Personally Identifiable Information** property in the **Display Name** column. Right-click **Personally Identifiable Information**, and then click **Enable**.
5. To publish the resource properties in the **Global Resource List**, in the left pane, click **Dynamic Access Control**, double-click **Resource Property Lists**, and then in the details pane, double-click **Global Resource Property List**.
6. In the Global Resource Properties List window, under **Resource Properties**, click **Add**, and then scroll down and click **Impact** to add it to the list. Do the same for **Personally Identifiable Information**. Click **OK** twice to finish.



Note: These resource properties may be listed already. If so, the OK button may be grayed out. If this is the case, simply verify that the resource properties are listed, and then click **Cancel**.

Use Windows PowerShell equivalent commands

The following Windows PowerShell® cmdlet or cmdlets perform the same function as the preceding procedure. You may demonstrate these cmdlets, but do not do so if you have already completed the actions above. Enter each cmdlet on a single line, even though they may appear word-wrapped across several lines here because of formatting constraint. Type the following, then press Enter:

```
Set-ADResourceProperty -Enabled:$true -Identity:"CN=Impact_MS,CN=Resource
Properties,CN=Claims Configuration,CN=Services,CN=Configuration,DC=adatum,DC=com"
Set-ADResourceProperty -Enabled:$true -Identity:"CN=PII_MS,CN=Resource
Properties,CN=Claims Configuration,CN=Services,CN=Configuration,DC=adatum,DC=com"
```

Create classification rules

1. Switch to LON-SVR1.
2. In Server Manager, click **Manage**, and then click **Add roles and features**.
3. Click **Next** three times until you reach the **Select server roles** page. Expand the **File And Storage Services (Installed)**, and then expand the **File And iSCSI Services (Installed)** nodes. Select the check box next to **File Server Resource Manager**. Click **Add Features**, click **Next** two times, and then click **Install**. When the installation is finished, click **Close**.
4. To refresh the Global Resource Properties, on the task bar, click the **Windows PowerShell** icon, in the Windows PowerShell window, type **Update-FSRMClassificationPropertyDefinition**, and then press Enter. Close Windows PowerShell.
5. To open File Server Resource Manager, in Server Manager, under **Tools**, click **File Server Resource Manager**.
6. In the left pane of File Server Resource Manager, expand **Classification Management**, and then select **Classification Rules**.

7. In the Actions pane, click **Configure Classification Schedule**. In the File Server Resource Manager Options window, on the **Automatic Classification** tab, select the **Enable fixed schedule** check box, select **Sunday**, and then select the **Allow continuous classification for new files** check box. Click **OK**.
8. In the Actions pane, click **Create Classification Rule**. This opens the **Create Classification Rule** dialog box.
9. In the **Rule Name** box, type **High Business Impact**.
10. In the **Description** box, type **Determines if the document has a high business impact based on the presence of the string Adatum Confidential**.
11. On the **Scope** tab, click the **Set Folder Management Properties** hyperlink, select **Folder Usage**, click **Add**, click **Browse**, and then browse to **C:\Finance Documents**. Click **OK**, select the value named **Group Files**, click **OK**, and then click **Close**. On the **Scope** tab, select **Group Files**.
12. Click the **Classification** tab, and under **Choose a method to assign a property to files**, select **Content Classifier** from the drop-down list box.
13. Under **Choose a property to assign to files**, select **Impact** from the drop-down list box.
14. Under **Specify a value**, select **High** from the drop-down list box.
15. Under **Parameters**, click **Configure**. In the **Classification Parameters** dialog box, in the **Expression Type** list, select **String**. In the **Expression** box, type **Adatum Confidential**, and then click **OK**.
16. Click the **Evaluation Type** tab. Click **Re-evaluate existing property values**, click **Overwrite the existing value**, and then click **OK** to finish.

Use Windows PowerShell equivalent commands

The following Windows PowerShell cmdlet or cmdlets perform the same function as the preceding procedure. You may demonstrate these cmdlets, but do not do so if you have already completed the actions above. Enter each cmdlet on a single line, even though they may appear word-wrapped across several lines here because of formatting constraints; type the following, then press Enter:

```
Update-FSRMClassificationPropertyDefinition
$date = Get-Date
$AutomaticClassificationScheduledTask = New-FsrmScheduledTask -Time $date -Weekly
@(3, 2, 4, 5,1,6,0) -RunDuration 0;
New-FSRMClassificationRule -Name "High Business Impact" -Property "Impact_MS" -
Description "Determines if the document has a high business impact based on the
presence of the string 'Contoso Confidential'" -PropertyValue "3000" -Namespace
@("C:\Finance Documents") -ClassificationMechanism "Content Classifier" -Parameters
@("StringEx=Min=1;Expr=Adatum Confidential") -ReevaluateProperty Overwrite
```

Protect documents with AD RMS

1. On LON-SVR1, open File Server Resource Manager, if it is not open already.
2. In the left pane, select **File Management Tasks**. In the Actions pane, click **Create File Management Task**.
3. In the **Task name** field, type **High Impact**. In the **Description** field, type **Automatic RMS protection for high impact documents**.
4. Click the **Scope** tab, and then select the **Group Files** check box.
5. Click the **Action** tab. Under **Type**, select **RMS Encryption**. In the **Read** box, type **Research@adatum.com**.
6. Click the **Condition** tab, and then click **Add**. Under **Property**, select **Personally Identifiable Information**. Under **Operator**, select **Equal**. Under **Value**, select **High**, and then click **OK**.

7. Click the **Schedule** tab. In the **Schedule** section, click **Weekly**, and then select **Sunday**. Running the task once a week ensures that you catch any documents that may have been missed due to a service outage or other disruptive event.
8. In the **Continuous operation** section, select **Run continuously on new files**, and then click **OK**. You now should have a file management task named **High Impact**.

Use Windows PowerShell equivalent commands

The following Windows PowerShell cmdlet or cmdlets perform the same function as the preceding procedure. You may demonstrate these cmdlets, but do not do so if you have already completed the actions above. Enter each cmdlet on a single line, even though they may appear word-wrapped across several lines here because of formatting constraints; type the following, then press Enter:

```
$fmjRmsEncryption = New-FSRMFmjAction -Type 'Rms' -RmsTemplate 'Adatum Finance Admin Only'
$fmjCondition1 = New-FSRMFmjCondition -Property 'PII_MS' -Condition 'Equal' -Value '5000'
$date = get-date
$schedule = New-FsrmscheduledTask -Time $date -Weekly @( 'Sunday' )
$fmj1=New-FSRMFileManagementJob -Name "High Impact" -Description "Automatic RMS protection for high PII documents" -Namespace @( 'C:\Finance Documents' ) -Action $fmjRmsEncryption -Schedule $schedule -Continuous -Condition @($fmjCondition1)
```

View the results

1. On LON-SVR1, in File Explorer, navigate to **C:\Finance Documents**.
2. Right-click the **Finance Memo** document, and then click **Properties**. Click the **Classification** tab, and then notice that the **Impact** property currently has no value. Click **Cancel**.
3. Switch to LON-CL1. Sign in as **Adatum\Hani** with the password **Pa\$\$wOrd**.
4. From the desktop, browse to the **\\LON-SVR1\Finance Documents** shared folder.
5. Open the **Finance Memo** document. Type **Adatum Confidential**. Save the document, and then close Microsoft Word.



Note: You may need to wait 30 seconds for the classification to occur.

6. Switch back to LON-SVR1. In File Explorer, navigate to **C:\Finance Documents**.
7. Right-click the **Finance Memo** document, and then click **Properties**. Click the **Classification** tab. Notice that the **Impact** property is now set to **High**. Click **Cancel**. If, after a minute or so, the classification does not change, take the following steps:
 - a. On LON-SVR1, open File Server Resource Manager, if it is not already open.
 - b. In the left pane, select **File Management Tasks**.
 - c. In the details pane, right-click the **High Impact** task, and then select **Run File Management Task Now...**
 - d. In the Run File Management Task pop-up window, click **Run the task in the background**, and then click **OK**.
 - e. Wait approximately 30 seconds, return to File Explorer, and then recheck the **Finance Memo.docx** properties. It should show an **Impact of High**.
8. Close all open windows and sign out of all virtual machines.

Module Review and Takeaways

Real-world Issues and Scenarios

If you enable the Super Users Group, you also enable success and failure auditing for Audit account management and Audit directory services access.

Tools

Tool	Where is it?
Active Directory Rights Management Service Administration Console	Server Manager, Tools
Active Directory Administrative Center	Server Manager, Tools
Windows PowerShell	Start Screen, Desktop Task Bar
File Services Resource Manager	Server Manager, Tools
Regedit.exe	Type in Run text box or command prompt

Common Issues and Troubleshooting Tips

Common Issue	Troubleshooting Tip
Be aware that you can use self-signed certificates, but you will need to add the server certificates from the AD RMS cluster servers to the Trusted Certification Authorities Store of any computer involved in IRM protection.	It is easier to acquire a commercial certificate or create one by using your own Trusted Certificate Authority, such as Active Directory Certificate Services (AD CS).
When you installed the AD RMS cluster in the lab, you used the Windows Internal database. However, if you intend to have multiple AD RMS servers in the cluster, you will need to use a full version of SQL Server to be able to add database items from multiple servers.	Do not use the Windows Internal Database in a normal production environment

Lab Review Questions and Answers

Lab: Planning and Implementing an AD RMS Infrastructure

Question and Answers

Question: How many AD RMS clusters do you need to deploy to satisfy the security requirements for both companies?

Answer: You must deploy one AD RMS cluster in the A. Datum forest and another in the Trey Research forest.

Question: What database solution should you deploy?

Answer: You should deploy the Windows Internal Database to reduce the number of servers that you have deployed. However, keep in mind that this will prevent you from deploying additional servers in each cluster.

Question: What service accounts, if any, do you need to create?

Answer: You need only one account, which will act as the service account. You cannot use the administrator's account, because the configuration of the AD RMS console requires an account other than the installing account to activate the database.

Question: What SSL certificate requirements do you have? How do you satisfy these requirements in both forests?

Answer: You can use self-signed certificates, and place the certificates in each computer's Trusted Certificate Authorities store.