Microsoft

OFFICIAL MICROSOFT LEARNING PRODUCT

20744B

Securing Windows Server 2016

Companion Content

Product Number: 20744B

Released: 06/2017

MICROSOFT LICENSE TERMS
MICROSOFT INSTRUCTOR-LED COURSEWARE

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

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

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

1. DEFINITIONS.

a. "Authorized Learning Center" means a Microsoft IT Academy Program Member, Microsoft Learning Competency Member, or such other entity as Microsoft may designate from time to time.

b. "Authorized Training Session" means the instructor-led training class using Microsoft Instructor-Led Courseware conducted by a Trainer at or through an Authorized Learning Center.

c. "Classroom Device" means one (1) dedicated, secure computer that an Authorized Learning Center owns or controls that is located at an Authorized Learning Center's training facilities that meets or exceeds the hardware level specified for the particular Microsoft Instructor-Led Courseware.

d. "End User" means an individual who is (i) duly enrolled in and attending an Authorized Training Session or Private Training Session, (ii) an employee of a MPN Member, or (iii) a Microsoft full-time employee.

e. "Licensed Content" means the content accompanying this agreement which may include the Microsoft Instructor-Led Courseware or Trainer Content.

f. "Microsoft Certified Trainer" or "MCT" means an individual who is (i) engaged to teach a training session to End Users on behalf of an Authorized Learning Center or MPN Member, and (ii) currently certified as a Microsoft Certified Trainer under the Microsoft Certification Program.

g. "Microsoft Instructor-Led Courseware" means the Microsoft-branded instructor-led training course that educates IT professionals and developers on Microsoft technologies. A Microsoft Instructor-Led Courseware title may be branded as MOC, Microsoft Dynamics or Microsoft Business Group courseware.

h. "Microsoft IT Academy Program Member" means an active member of the Microsoft IT Academy Program.

i. "Microsoft Learning Competency Member" means an active member of the Microsoft Partner Network program in good standing that currently holds the Learning Competency status.

j. "MOC" means the "Official Microsoft Learning Product" instructor-led courseware known as Microsoft Official Course that educates IT professionals and developers on Microsoft technologies.

k. "MPN Member" means an active Microsoft Partner Network program member in good standing.

l. "Personal Device" means one (1) personal computer, device, workstation or other digital electronic device that you personally own or control that meets or exceeds the hardware level specified for the particular Microsoft Instructor-Led Courseware.

m. "Private Training Session" means the instructor-led training classes provided by MPN Members for corporate customers to teach a predefined learning objective using Microsoft Instructor-Led Courseware. These classes are not advertised or promoted to the general public and class attendance is restricted to individuals employed by or contracted by the corporate customer.

n. "Trainer" means (i) an academically accredited educator engaged by a Microsoft IT Academy Program Member to teach an Authorized Training Session, and/or (ii) a MCT.

o. "Trainer Content" means the trainer version of the Microsoft Instructor-Led Courseware and additional supplemental content designated solely for Trainers' use to teach a training session using the Microsoft Instructor-Led Courseware. Trainer Content may include Microsoft PowerPoint presentations, trainer preparation guide, train the trainer materials, Microsoft One Note packs, classroom setup guide and Pre-release course feedback form. To clarify, Trainer Content does not include any software, virtual hard disks or virtual machines.

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

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

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

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

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

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

    provided you comply with the following:
iii. you will only provide access to the Licensed Content to those individuals who have acquired a valid license to the Licensed Content,
iv. you will ensure that each End User attending an Authorized Training Session has their own valid licensed copy of the Microsoft Instructor-Led Courseware that is the subject of the Authorized Training Session,
v. you will ensure that each End User provided with a hard-copy version of the Microsoft Instructor-Led Courseware will be presented with a copy of this agreement and each End User will agree that their use of the Microsoft Instructor-Led Courseware will be subject to the terms in this agreement prior to providing them with the Microsoft Instructor-Led Courseware. Each individual will be required to denote their acceptance of this agreement in a manner that is enforceable under local law prior to their accessing the Microsoft Instructor-Led Courseware,
vi. you will ensure that each Trainer teaching an Authorized Training Session has their own valid licensed copy of the Trainer Content that is the subject of the Authorized Training Session,
vii. you will only use qualified Trainers who hold the applicable Microsoft Certification credential that is the subject of the Microsoft Instructor-Led Courseware being taught for your Authorized Training Sessions,
viii. you will only use qualified MCTs who also hold the applicable Microsoft Certification credential that is the subject of the MOC title being taught for all your Authorized Training Sessions using MOC,
ix. you will only provide access to the Microsoft Instructor-Led Courseware to End Users, and
x. you will only provide access to the Trainer Content to Trainers.

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

i. Each license acquired on behalf of yourself may only be used to review one (1) copy of the Microsoft Instructor-Led Courseware in the form provided to you. If the Microsoft Instructor-Led Courseware is in digital format, you may install one (1) copy on up to three (3) Personal Devices. You may not install the Microsoft Instructor-Led Courseware on a device you do not own or control.

ii. For each license you acquire on behalf of an End User or Trainer, you may either:

1. distribute one (1) hard copy version of the Microsoft Instructor-Led Courseware to one (1) End User attending the Private Training Session, and only immediately prior to the commencement of the Private Training Session that is the subject matter of the Microsoft Instructor-Led Courseware being provided, **or**
2. provide one (1) End User who is attending the Private Training Session with the unique redemption code and instructions on how they can access one (1) digital version of the Microsoft Instructor-Led Courseware, **or**
3. you will provide one (1) Trainer who is teaching the Private Training Session with the unique redemption code and instructions on how they can access one (1) Trainer Content,

provided you comply with the following:

iii. you will only provide access to the Licensed Content to those individuals who have acquired a valid license to the Licensed Content,

iv. you will ensure that each End User attending an Private Training Session has their own valid licensed copy of the Microsoft Instructor-Led Courseware that is the subject of the Private Training Session,

v. you will ensure that each End User provided with a hard copy version of the Microsoft Instructor-Led Courseware will be presented with a copy of this agreement and each End User will agree that their use of the Microsoft Instructor-Led Courseware will be subject to the terms in this agreement prior to providing them with the Microsoft Instructor-Led Courseware. Each individual will be required to denote their acceptance of this agreement in a manner that is enforceable under local law prior to their accessing the Microsoft Instructor-Led Courseware,

vi. you will ensure that each Trainer teaching an Private Training Session has their own valid licensed copy of the Trainer Content that is the subject of the Private Training Session,

vii. you will only use qualified Trainers who hold the applicable Microsoft Certification credential that is the subject of the Microsoft Instructor-Led Courseware being taught for all your Private Training Sessions,

viii. you will only use qualified MCTs who hold the applicable Microsoft Certification credential that is the subject of the MOC title being taught for all your Private Training Sessions using MOC,

ix. you will only provide access to the Microsoft Instructor-Led Courseware to End Users, and

x. you will only provide access to the Trainer Content to Trainers.

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

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

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

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

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

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

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

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

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

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

a. **Pre-Release Licensed Content.** This Licensed Content subject matter is on the Pre-release version of the Microsoft technology. The technology may not work the way a final version of the technology will and we may change the technology for the final version. We also may not release a final version. Licensed Content based on the final version of the technology may not contain the same information as the Licensed Content based on the Pre-release version. Microsoft is under no obligation to provide you with any further content, including any Licensed Content based on the final version of the technology.

b. **Feedback.** If you agree to give feedback about the Licensed Content to Microsoft, either directly or through its third party designee, you give to Microsoft without charge, the right to use, share and commercialize your feedback in any way and for any purpose. You also give to third parties, without charge, any patent rights needed for their products, technologies and services to use or interface with any specific parts of a Microsoft technology, Microsoft product, or service that includes the feedback. You will not give feedback that is subject to a license that requires Microsoft to license its technology, technologies, or products to third parties because we include your feedback in them. These rights survive this agreement.

c. **Pre-release Term**. If you are an Microsoft IT Academy Program Member, Microsoft Learning Competency Member, MPN Member or Trainer, you will cease using all copies of the Licensed Content on the Pre-release technology upon (i) the date which Microsoft informs you is the end date for using the Licensed Content on the Pre-release technology, or (ii) sixty (60) days after the commercial release of the technology that is the subject of the Licensed Content, whichever is earliest ("**Pre-release term**"). Upon expiration or termination of the Pre-release term, you will irretrievably delete and destroy all copies of the Licensed Content in your possession or under your control.

4. **SCOPE OF LICENSE**. The Licensed Content is licensed, not sold. This agreement only gives you some rights to use the Licensed Content. Microsoft reserves all other rights. Unless applicable law gives you more rights despite this limitation, you may use the Licensed Content only as expressly permitted in this agreement. In doing so, you must comply with any technical limitations in the Licensed Content that only allows you to use it in certain ways. Except as expressly permitted in this agreement, you may not:
   - access or allow any individual to access the Licensed Content if they have not acquired a valid license for the Licensed Content,
   - alter, remove or obscure any copyright or other protective notices (including watermarks), branding or identifications contained in the Licensed Content,
   - modify or create a derivative work of any Licensed Content,
   - publicly display, or make the Licensed Content available for others to access or use,
   - copy, print, install, sell, publish, transmit, lend, adapt, reuse, link to or post, make available or distribute the Licensed Content to any third party,
   - work around any technical limitations in the Licensed Content, or
   - reverse engineer, decompile, remove or otherwise thwart any protections or disassemble the Licensed Content except and only to the extent that applicable law expressly permits, despite this limitation.

5. **RESERVATION OF RIGHTS AND OWNERSHIP**. Microsoft reserves all rights not expressly granted to you in this agreement. The Licensed Content is protected by copyright and other intellectual property laws and treaties. Microsoft or its suppliers own the title, copyright, and other intellectual property rights in the Licensed Content.

6. **EXPORT RESTRICTIONS**. The Licensed Content is subject to United States export laws and regulations. You must comply with all domestic and international export laws and regulations that apply to the Licensed Content. These laws include restrictions on destinations, end users and end use. For additional information, see www.microsoft.com/exporting.

7. **SUPPORT SERVICES**. Because the Licensed Content is "as is", we may not provide support services for it.

8. **TERMINATION.** Without prejudice to any other rights, Microsoft may terminate this agreement if you fail to comply with the terms and conditions of this agreement. Upon termination of this agreement for any reason, you will immediately stop all use of and delete and destroy all copies of the Licensed Content in your possession or under your control.

9. **LINKS TO THIRD PARTY SITES**. You may link to third party sites through the use of the Licensed Content. The third party sites are not under the control of Microsoft, and Microsoft is not responsible for the contents of any third party sites, any links contained in third party sites, or any changes or updates to third party sites. Microsoft is not responsible for webcasting or any other form of transmission received from any third party sites. Microsoft is providing these links to third party sites to you only as a convenience, and the inclusion of any link does not imply an endorsement by Microsoft of the third party site.

10. **ENTIRE AGREEMENT.** This agreement, and any additional terms for the Trainer Content, updates and supplements are the entire agreement for the Licensed Content, updates and supplements.

11. **APPLICABLE LAW.**
    a. United States. If you acquired the Licensed Content in the United States, Washington state law governs the interpretation of this agreement and applies to claims for breach of it, regardless of conflict of laws principles. The laws of the state where you live govern all other claims, including claims under state consumer protection laws, unfair competition laws, and in tort.

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

12. LEGAL EFFECT. This agreement describes certain legal rights. You may have other rights under the laws of your country. You may also have rights with respect to the party from whom you acquired the Licensed Content. This agreement does not change your rights under the laws of your country if the laws of your country do not permit it to do so.

13. DISCLAIMER OF WARRANTY. THE LICENSED CONTENT IS LICENSED "AS-IS" AND "AS AVAILABLE." YOU BEAR THE RISK OF USING IT. MICROSOFT AND ITS RESPECTIVE AFFILIATES GIVES NO EXPRESS WARRANTIES, GUARANTEES, OR CONDITIONS. YOU MAY HAVE ADDITIONAL CONSUMER RIGHTS UNDER YOUR LOCAL LAWS WHICH THIS AGREEMENT CANNOT CHANGE. TO THE EXTENT PERMITTED UNDER YOUR LOCAL LAWS, MICROSOFT AND ITS RESPECTIVE AFFILIATES EXCLUDES ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT.

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

This limitation applies to

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

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

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

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

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

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

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

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

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

Revised July 2013

Module 1

Attacks, breach detection, and Sysinternals tools

Contents:

Lesson 1

Understanding attacks

Contents:

Question and Answers

Question: Ask students to describe attacks that their organizations have experienced.

> **Answer:** Answers will vary. This question aims to elicit a discussion about the student's experiences with attacks.

Resources

Attack timelines

 **Additional Reading:** To learn more about pass the hash attacks, refer to: "Defending Against Pass-the-Hash Attacks" at http://aka.ms/yxwbip

Lesson 2

Detecting security breaches

Contents:

Question and Answers

Question: Discuss with students their experiences with detecting breaches and ask them what they look for when they suspect a breach has occurred in their environment.

Answer: Answers will vary. This discussion builds on the discussion that you began in lesson one.

Lesson 3

Examining activity with the Sysinternals tools

Contents:

Question and Answers

Question: Discuss with students whether they have used any of the Sysinternals tools and how they have used them.

> **Answer:** Answers will vary depending on the student's experience. This question allows the instructor to find out more about the students' knowledge of these tools.

Resources

System Monitor

Additional Reading: To learn more about Sysmon, refer to: "Sysmon v5.02" at http://aka.ms/Tigm98

Autoruns

Additional Reading: To learn more about the Autoruns tool, refer to: "Autoruns for Windows v13.7" at: http://aka.ms/Xnt6os

LogonSessions

Additional Reading: To learn more about the LogonSessions tool, refer to: "LogonSessions v1.4" at http://aka.ms/Ugnyh8

Process Explorer

Additional Reading: To learn more about the Process Explorer tool, refer to "Process Explorer v16.20" at: http://aka.ms/usw7c8

Process Monitor

Additional Reading: To learn more about Process Monitor, refer to "Process Monitor v3.32" at: http://aka.ms/Qc19u6

Sigcheck

Additional Reading: To learn more about Sigcheck, refer to "Sigcheck v2.54" at: http://aka.ms/Lsef33

Demonstration: Sysinternals tools

Demonstration Steps

1. Start **LON-DC1**. When this virtual machine has started, start **LON-SVR1**.
2. Sign in to **LON-SVR1** as **Adatum\Administrator** with the password **Pa55w.rd**.
3. On the taskbar, click **File Explorer**.

4. In File Explorer, double click on the **Allfiles (D:)** volume.
5. Double click the **Labfiles** folder.
6. Double click the **Mod01** folder.
7. In the **Mod01** folder, right click **LogonSessions.zip**, and then click **Extract All**.
8. In the **Extract Compressed (Zipped) Folders** dialog box, clear the **Show extracted files when complete** check box, and then click **Extract**.
9. Repeat steps 7 and 8 for **ProcessExplorer.zip** and **ProcessMonitor.zip**.
10. Close File Explorer.
11. Right-click **Start**, and then click **Computer Management**.
12. In the **Computer Management** console, expand **Local Users and Groups**, right-click **Users**, and then click **New User**.
13. In the **New User** dialog box, in the **User Name** textbox, enter **Attacker**.
14. In the **Password** and **Confirm password** textboxes, type **Pa55w.rd**.
15. Clear the **User must change password at next logon** check box, click **Create**, and then click **Close**.
16. In the **Users** list, right-click **Attacker**, and then click **Properties**.
17. In the **Attacker Properties** dialog box, on the **Member Of** tab, click **Add**.
18. In the **Select Groups** dialog box, enter **Administrators**, and then click **OK**.
19. To close the **Attacker Properties** dialog box, click **OK**.
20. Close the **Computer Management** console.
21. Right click **Start**, and then click **Run**.
22. In the **Run** dialog box, type **cmd.exe**, and then click **OK**.
23. In the **Administrator: C:\Windows\system32\cmd.exe** window, type the following command, and then press Enter:

```
runas /user:Attacker cmd.exe
```

24. At the **Enter the password for Attacker:** prompt, type **Pa55w.rd**, and then press Enter.
25. Snap the **cmd.exe (running as LON-SVR1\Attacker)** window to the right side of the screen.
26. Snap the **Administrator:c:\Windows\system32\cmd.exe** window to the left side of the screen
27. On the right side of the screen, in the **LON-SVR1\Attacker command prompt** window, type the following command, and then press Enter:

```
ftp.exe
```

28. On the left side of the screen, in the **Administrator** window, type the following commands, pressing Enter after each:

```
D:
Cd labfiles\Mod01\LogonSessions
Logonsessions -p
```

29. In the **LogonSessions License Agreement** dialog box, click **Agree**.
30. Review the output of the logonsessions tool.

Note: Note the processes and IDs that are running under the logon session for **ADATUM\Administrator** and the processes and IDs that are running under the logon session for **LON-SVR1\Attacker**. You should see that ftp.exe is running.

31. In the **Administrator** command prompt, on the left side of the screen, type the following commands, and then press Enter:

```
Cd D:\Labfiles\Mod01\ProcessExplorer
procexp
```

32. In the **Process Explorer License Agreement** dialog box, click **Agree**.
33. Snap the **Process Explorer** window to the left of the screen.
34. In Process Explorer, under the cmd.exe process, locate the ftp.exe process.
35. To close the ftp session, in the right **cmd.exe** window, at the **ftp>** prompt, type **bye**, and then press Enter.

Note: The ftp.exe item is removed from Process Explorer.

36. In the right **cmd.exe** window, type **notepad newfile1.txt**, press Enter, and then click **Yes**.

Note: A new notepad.exe item appears in Process Explorer.

37. In the **Notepad** window, enter some random text and note the changes in Process Explorer window. Close Notepad without saving.
38. In the **Administrator** command prompt, on the left side of the screen, type the following commands, and then press Enter after each one:

```
Cd D:\Labfiles\Mod01\ProcessMonitor
Procmon
```

39. In the **Process Monitor License Agreement** dialog box, click **Agree**, and then snap the **Process Monitor** window to the left side of the screen.
40. In the right **cmd.exe** window, type **ftp.exe**, and then press Enter.
41. Scroll through the **Process Monitor** window until you locate the FTP.exe process name.
42. Right click on the **ftp.exe** process name, and then click **Highlight 'ftp.exe'**.
43. Scroll through the **Process Monitor** window, and notice that all instances of the ftp.exe process name are now highlighted.
44. On the **Process Monitor** toolbar, click the **Filter** icon.
45. In the **Process Monitor Filter** dialog box, click the **Architecture** drop-down menu, and then click **Process Name**.
46. In the textbox. type **ftp.exe**, click **Add**, and then click **OK**.
47. In the right-hand **cmd.exe** window, at the **ftp>** prompt, type **bye**, and then press Enter.
48. Review the changes in the **Process Monitor** window.
49. On the **Process Monitor** toolbar, click the **Filter** icon.

50. In the list of filters, clear the check next to **Process Name is ftp.exe**, click the **Architecture** drop-down menu, and then click **Process Name**.
51. In the textbox, type **cmd.exe**, click **Add**, and then click **OK**
52. In the right-hand **cmd.exe** window, type **notepad newfile2.txt**, press Enter, click **Yes**, enter some random text, and then close the file without saving.
53. Review the additional activity recorded in process monitor based on the cmd.exe filter.
54. Click the **File** menu, and then click **Save**.
55. In the **Save To File** dialog box, accept the defaults, and then click **OK**.

Module Review and Takeaways

Review Question

Question: Which of the attack types that this module covers have you seen in your own environment?

Answer: Answers will vary depending on the student's environment and experience.

Lab Review Questions and Answers

Lab: Basic breach detection and incident response strategies

Question and Answers

Question: What switch do you use with LogonSessions to view processes that are in use in each session?

Answer: You use the **-p** switch to view processes that are in use in each session.

Question: What is the main difference between Process Explorer and Process Monitor?

Answer: Process Explorer is a tool designed to allow you to view activity in real time. Process Monitor allows you to record activity for later analysis.

Module 2

Protecting credentials and privileged access

Contents:

Lesson 1

Understanding user rights

Contents:

Question and Answers

Question: Ask students about their model for assigning privileges to administrative accounts. Are there accounts that have privileges to multiple separate systems, such as Exchange and Configuration Manager, or are there separate accounts for each set of administrative tasks?

Answer: Answers will vary depending on each student's individual organizational practices.

Resources

Principle of least privilege

 **Additional Reading:** For more information, refer to: "Implementing Least-Privilege Administrative Models" at: http://aka.ms/Hw2tr3

Protected users, authentication policies, and authentication-policy silos

 **Additional Reading:** For more information, refer to: "Authentication Policies and Authentication Policy Silos" at: http://aka.ms/J0abq2

Demonstration: Configuring user rights and account-security options

Demonstration Steps

1. Sign in to **LON-DC1** as **Adatum\Administrator** with the password **Pa55w.rd**.
2. In the **Server Manager** console, on the **Tools** menu, click **Active Directory Administrative Center**.
3. In the **Active Directory Administrative Center** console, double-click **Adatum (local)**, and then double-click the **IT** organizational unit (OU).
4. In the **IT** OU, double-click **Dante Dabney**. This will open the **Dante Dabney** dialog box.
5. In the **Dante Dabney** dialog box, click **Log on to**.
6. In the **Log on to** dialog box, click **The following computers**, type **LON-SVR2**, and then click **Add**.
7. Click **OK** to close the **Log on to** dialog box.
8. Click **OK** to close the **Dante Dabney** dialog box.
9. Switch to **LON-SVR1**, and then try to sign in as **Adatum\Dante** with the password **Pa55w.rd**.
10. Review the message that informs you that the account is configured to prevent you from using this PC, and then click **OK**.
11. Switch to **LON-SVR2**, and then try to sign in as **Adatum\Dante** with the password **Pa55w.rd**.
12. After you sign in successfully, click **Start**, click **Dante Dabney**, and then click **Sign out**.
13. Sign in to **LON-SVR2** as **Adatum\Administrator** with the password **Pa55w.rd**.
14. Right-click **Start**, and then click **Run**.
15. In the **Run** dialog box, type **gpedit.msc**, and then click **OK**.
16. In the **Local Group Policy** editor, under **Computer Configuration**, expand **Windows Settings**, expand **Security Settings**, expand **Local Policies**, and then select **User Rights Assignment**.
17. Double-click the **Deny log on locally** policy.

18. On the **Deny log on locally Properties** dialog box, click **Add User or Group**.
19. In the **Select Users, Computers, Service Accounts, or Groups** dialog box, type **Dante**, click **Check Names**, and then click **OK** twice.
20. Close **Local Group Policy Editor**.
21. Right-click **Start**, and then click **Run**.
22. In the **Run** dialog box, type **gpupdate /force**, and then click OK.
23. Click **Start**, click **Administrator**, and then click **Sign Out**.
24. Attempt to sign in to **LON-SVR2** as **Adatum\Dante** with the password **Pa55w.rd**. Note that the sign-in method is not allowed.

Demonstration: Delegating privileges

Demonstration Steps

1. Ensure that you are signed in to **LON-DC1** as **Adatum\Administrator** with the password **Pa55w.rd**.
2. On the **Tools** menu of the **Server Manager** console, click **Active Directory Users and Computers**.
3. Right-click the **Marketing** OU, and then click **Delegate Control**.
4. In **Delegation of Control Wizard**, on the **Welcome to the Delegation of Control Wizard** page, click **Next**.
5. On the **Users or Groups** page, click **Add**.
6. On the **Select Users, Computers, or Groups** page, type **IT**, click **Check Names**, click **OK**, and then click **Next**.
7. On the **Tasks to Delegate** page, select **Reset user passwords and force password change at next logon**, and then click **Next**.
8. Click **Finish** to close the **Delegation of Control Wizard**.
9. Sign in to **LON-SVR1** as **Adatum\Administrator** with the password **Pa55w.rd**.
10. Click **Start**, and then click **Server Manager**. In the **Server Manager** console, click **Manage**, and then click **Add Roles and Features**.
11. In the **Add Roles and Features Wizard,** on the **Before you begin** page, click **Next**.
12. On the **Select Installation Type** page, click **Role-based or feature-based installation**, and then click **Next**.
13. On the **Select destination server** page, click **Next**.
14. On the **Select Server Roles** page, click **Next**.
15. On the **Select Features page**, expand **Remote Server Administration Tools**, expand **Role Administration Tools**, select **AD DS and AD LDS Tools**, click **Next**, click **Install**, and then click **Close**.
16. Right-click **Start**, click **Shut down or sign out**, and then click **Sign out**.
17. Sign in to **LON-SVR1** as **Adatum\Beth** with the password **Pa55w.rd**.
18. Click **Start**, and then click **Server Manager**.
19. In the **Server Manager** console, on the **Tools** menu, click **Active Directory Users and Computers**.
20. Under **Adatum.com**, click the **Marketing** OU. Right-click **Ada Russell**, and then click **Reset Password**.

21. On the **Reset Password** dialog box, type the password **Pa55w.rd2** twice, and then click **OK** twice. This verifies that you can reset passwords in the Marketing OU by using Beth's account.
22. Click **Managers OU**, right-click the **Art Odum** user account, and then click **Reset Password**.
23. On the **Reset Password** dialog box, type the password **Pa55w.rd2** twice, and then click **OK**.
24. Note that the Windows operating system cannot complete the password change for **Art Odum** because access is denied.

Lesson 2

Computer and service accounts

Contents:

Question and Answers

Question: Ask students how they manage service accounts in their organization

> **Answer:** Answers will vary depending on how the student's organization manages service accounts.

Demonstration: Creating and managing group Managed Service Accounts

Demonstration Steps

1. Ensure that you are signed in to **LON-DC1** as **Adatum\Administrator** with the password **Pa55w.rd**.
2. Right-click **Start**, and then click **Windows PowerShell (Admin)**.
3. At the Windows PowerShell command prompt, type the following command, and then press Enter:

```
Add-KdsRootKey -EffectiveTime ((get-date).addhours(-10))
```

4. To create the new group Managed Service Account named **LON-SVRS-GMSA**, type the following command, and then press Enter:

```
New-ADServiceAccount LON-SVRS-GMSA
-DNSHOSTNAME LON-SVRS-GMSA.adatum.com
```

5. Switch to **LON-SVR1**, sign out from the Beth account, and then sign in as **Adatum\Administrator** with the password **Pa55w.rd**.
6. Right-click **Start**, and then click **Windows PowerShell (Admin)**.
7. At the Windows PowerShell command prompt, type the following command, and then press Enter:

```
Install-WindowsFeature RSAT-AD-PowerShell
Set-ADServiceAccount -Identity LON-SVRS-GMSA -
PrincipalsAllowedToRetrieveManagedPassword LON-SVR1$
Install-ADServiceAccount LON-SVRS-GMSA
```

8. Right-click **Start**, and then click **ComputerManagement**.
9. Expand **Services and Applications**, and then click **Services**.
10. Right-click the **Windows Internal Database** service, and then click **Properties**.
11. On the **Log On** tab, click **This Account**, and then click **Browse**.
12. On the **Select User** dialog box, click **Locations**.
13. On the **Locations** dialog box, click **Entire Directory**, and then click **OK**.
14. In the **Select User or Service Account** dialog box, type **LON-SVRS-GMSA**, and then click **OK**.
15. Clear the **Password** and **Confirm password** text boxes, and then click **OK**.
16. When prompted that the account has been granted the Log On As Service right, click **OK**.

Lesson 3

Protecting credentials

Contents:

Question and Answers

Question: What should an organization do before it institutes NTLM blocking?

> **Answer:** An organization should audit NTLM usage prior to disabling the authentication protocol.

Resources

Configuring Credential Guard

Additional Reading: For more information, refer to: "Protect derived domain credentials with Credential Guard" at: http://aka.ms/Vwpgdp

NTLM blocking

Additional Reading: For more information, refer to: "Introducing the Restriction of NTLM Authentication" at: http://aka.ms/Ynbr7l

Demonstration: Locating problematic accounts

Demonstration Steps

1. Ensure that you are signed in to **LON-DC1** as **Adatum\Administrator** with the password **Pa55w.rd**.
2. In the **Server Manager** console, on the **Tools** menu, click **Active Directory Administrative Center**.
3. Maximize the **Active Directory Administrative Center** window, and then click **Global Search**.
4. Click the **down arrow** in the circle, and then click **Add Criteria**.
5. Select **Users whose password has an expiration date/no expiration date**, and then click **Add**.
6. Click **Search**. Note that 255 items are found.
7. Click **Clear All**.
8. Click **Add criteria**.
9. Select **Users with enabled accounts who have not logged on for more than a given number of days**, and then click **Add**.
10. Click the underlined setting **15 after number of days**, and then click **90**.
11. Click **Search**.
12. Note that 250 items are found.

Lesson 4

Privileged Access Workstations and jump servers

Contents:

Question and Answers

Question: Ask students if they use Privileged Access Workstations or jump servers in their environment, and why?

Answer: Answers will vary depending on the student's environment.

Resources

Jump servers

Additional Reading: For more information, refer to: "Privileged Access Workstations" at: http://aka.ms/Rd5xkn

Securing domain controllers

Additional Reading: For more information, refer to: "Securing Domain Controllers Against Attack" at: http://aka.ms/H84erd

Lesson 5

Local administrator password solution

Contents:

Question and Answers

Question: How do you manage local administrator account passwords in your organization?

> **Answer:** Answers will vary. Some students will indicate that their organizations have no technology in place. Other students will have a solution, including some who use LAPS.

Demonstration: Configuring and deploying LAPS

Demonstration Steps

1. Ensure that you are signed in to **LON-DC1** as **Adatum\Administrator** with the password **Pa55w.rd**.
2. In the **Server Manager** console, on the **Tools** menu, click **Active Directory Users and Computers**.
3. In the **Active Directory Users and Computers** console, right-click the **Adatum.com** domain, click **New**, and then click **Organizational Unit**.
4. In the **New Object – Organizational Unit** dialog box, type the name **Sydney_Computers**, and then click **OK**.
5. Under adatum.com, click the **Computers** container, right-click **LON-SVR2**, and then click **Move**.
6. In the **Move** dialog box, click **Sydney_Computers**, and then click **OK**.
7. Right-click **Start**, and then click **Run**.
8. In the **Run** dialog box, type **\\LON-SVR1\d$\Labfiles\Mod02**, and then click **OK**.
9. In the **Mod02** window, double-click **LAPSx64.msi**.
10. In the **Local Administrator Password Solution Setup** wizard, on the **Welcome** page, click **Next**.
11. On the **End-User License Agreement** page, click **I accept the terms in the License Agreement**, and then click **Next**.
12. On the **Custom Setup** page, remove the selection next to the **AdmPwd GPO Extension**, select **Management Tools**, **Fat client UI**, **PowerShell module** and **GPO Editor** templates, click **Next**, and then click **Install**.
13. When the installation completes, click **Finish**.
14. Right-click **Start**, and then click **Windows PowerShell (Admin)**.
15. In the **Administrator: Windows PowerShell** window, type the following commands, and then press Enter after each command:

```
Import-Module admpwd.ps
Update-AdmPwdADSchema
Set-AdmPwdComputerSelfPermission -Identity “Sydney_Computers”
```

16. In the **Server Manager** console, on the **Tools** menu, click **Group Policy Management**.
17. In the **Group Policy Management** console, expand **Forest: Adatum.com**, expand **Domains**, expand **Adatum.com**, right-click the **Sydney_Computers** OU, and then click **Create a GPO in this domain, and Link it here**.
18. In the **Name input** box of the **New GPO** dialog box, type **LAPS_GPO**, and click **OK**.
19. In the **Group Policy Management** window, under **Sydney_Computers**, right-click **LAPS_GPO**, and then click **Edit**.
20. In the **Group Policy Management Editor** window, under **Computer Configuration**, expand the **Policies** and **Administrative Templates** nodes, and then select **LAPS**.
21. Double-click the **Enable local admin password management** policy.

22. In the **Enable local admin password management** window, click **Enabled**, and then click **OK**.
23. Double-click the **Password Settings** policy.
24. In the **Password Settings policy** dialog box, click **Enabled**, configure **Password Length** to **20**.
25. Verify that the **password Age** is configured to **30**, and then click **OK**.
26. Close **Group Policy Management Editor**.
27. Sign in to **LON-SVR2** as **Adatum\Administrator** with the password **Pa55w.rd**.
28. Right-click **Start**, and then click **Run**.
29. In the **Run** dialog box, type **\\LON-SVR1\d$\Labfiles\Mod02**, and then click **OK**.
30. In the **Mod02** window, double-click **LAPSx64.msi**.
31. In the **Local Administrator Password Solution Setup Wizard**, on the **Welcome** page, click **Next**.
32. On the **End-User License Agreement** page, click **I accept the terms of the License Agreement**, click **Next** twice, and then click **Install**.
33. Click **Finish** to close the **Local Administrator Password Solution Setup Wizard**.
34. Right-click **Start**, and then click **Run**.
35. In the **Run** dialog box, type **gpupdate /force** and then click **OK**.
36. Restart **LON-SVR2**.
37. Switch to **LON-DC1**.
38. Click **Start,** click LAPS, and then click **LAPS UI**.
39. In the **LAPS UI** dialog box, in the **ComputerName** text box, type **LON-SVR2**, and then click **Search**.
40. Review the **Password** and the **Password expires** values, and then click **Exit**.
41. In the **Windows PowerShell** window, type the following command, and then press Enter:

```
Get-AdmPwdPassword LON-SVR2 | Out-Gridview
```

42. Review the password assigned to **LON-SVR2**.

Module Review and Takeaways

Review Question

Question: Members of which security groups can, by default, use the LAPS user interface (UI) app or Windows PowerShell to retrieve the local Administrator password of a computer configured to use LAPS?

Answer: Members of the Domain Admins and Enterprise Admins group can retrieve the local Administrator password of a computer configured to use LAPS by using the LAPS UI app or Windows PowerShell.

Lab Review Questions and Answers

Lab A: Implementing user rights, security options, and group Managed Service Accounts

Question and Answers

Question: How can you block certain groups of users from signing in to sensitive servers?

Answer: You can use the deny log on locally policy to block certain groups of users from signing in to sensitive servers.

Question: Which privilege would you delegate if you wanted to allow a specific team within your organization to create, delete, and manage groups?

Answer: You would delegate the Create, delete, and manage groups privilege to the team's group by using the Delegation of Privilege Wizard.

Lab B: Configuring and deploying LAPS

Question and Answers

Question: Which Windows PowerShell cmdlet do you use to configure a specific OU so that computers within that OU can use LAPS?

Answer: You use the **Set-AdmPwdComputerSelfPermission** cmdlet to configure a specific OU so that computers that have accounts within that OU can use LAPS.

Question: Which Windows PowerShell cmdlet do you use to retrieve the local Administrator password from AD DS when a computer is configured to use LAPS?

Answer: You use the **Get-AdmPwdPassword** cmdlet to retrieve the local Administrator password from AD DS when a computer is configured to use LAPS.

Module 3

Limiting administrator rights with Just Enough Administration

Contents:

Lesson 1

Understanding JEA

Contents:

Question and Answers

Question: Which filename extension does a JEA role capability file use?

( ) .psrc

( ) .psd1

( ) .pssc

Answer:

(√) .psrc

( ) .psd1

( ) .pssc

Feedback:

JEA role-capability files use the **.psrc** extension. The **.pssc** extension is used for session-configuration files. The **.psd1** extension is used for module manifests.

Demonstration: Creating a role-capability file

Demonstration Steps

1. On **LON-DC1**, click the **Start** hint, and then click **Windows PowerShell ISE**.
2. Maximize the **Windows PowerShell ISE** window.
3. In the **Windows PowerShell** pane, type the following commands, and press Enter after each:

```
Cd 'c:\Program Files\WindowsPowerShell\Modules'
Mkdir DNSOps
Cd DNSOps
New-ModuleManifest .\DNSOps.psd1
Mkdir RoleCapabilities
Cd RoleCapabilities
New-PSRoleCapabilityFile -Path .\DNSOps.psrc
Ise DNSOps.psrc
```

4. In the **DNSOps.psrc** script pane of the **Windows PowerShell ISE**, navigate to and place the cursor under the line that starts with **# VisibleCmdlets =**, and then type the following:

```
VisibleCmdlets = @{ Name = 'Restart-Service'; Parameters = @{ Name='Name';
ValidateSet = 'DNS'}}
```

5. Navigate to and place the cursor under the line that starts with **# VisibleFunctions =**, and then type the following:

```
VisibleFunctions = 'Add-DNSServerResourceRecord', 'Clear-DNSServerCache','Get-
DNSServerResourceRecord','Remove-DNSServerResourceRecord'
```

6. Navigate to and place the cursor under the line that starts with # **VisibleExternalCommands =**, and then type the following:

```
VisibleExternalCommands = 'C:\Windows\System32\whoami.exe'
```

7. Click **Save**.

Demonstration: Creating a session-configuration file

Demonstration Steps

1. On **LON-DC1**, in the **Windows PowerShell** pane of the **Windows PowerShell ISE**, type the following commands, and press Enter after each:

```
New-PSSessionConfigurationFile -Path .\DNSOps.pssc -Full
Ise DNSOps.pssc
```

2. In the **DNSOps.pssc** script pane of **Windows PowerShell ISE**, navigate to the line that is **SessionType = 'Default'**, and then change it to **SessionType = 'RestrictedRemoteServer'**.
3. Navigate to the line that is **#RunAsVirtualAccount = $true**, and then remove the **#** so that the line is **RunAsVirtualAccount = $true**.
4. Navigate to the line that starts with **# RoleDefinitions**, place the cursor under this line, and then type the following:

```
RoleDefinitions = @{ 'ADATUM\DNSOps' = @{ RoleCapabilities = 'DNSOps' };}
```

5. Click **Save**.

Demonstration: Creating a JEA endpoint

Demonstration Steps

1. In the **Windows PowerShell** pane of the **Windows PowerShell ISE**, type the following commands, and press Enter after each:

```
Register-PSSessionConfiguration -Name DNSOps -Path .\DNSOps.pssc
Restart-Service WinRM
Get-PSSessionConfiguration
```

2. Verify that **DNSOps** is listed as a Windows PowerShell endpoint.

Lesson 2

Verifying and deploying JEA

Contents:

Question and Answers

Question: Is it better to create one JEA endpoint with multiple role capabilities or to create multiple JEA endpoints, each linked to a separate role capability?

Answer: Answers will vary depending on student opinions.

Feedback: By creating separate JEA endpoints, it is simpler to delegate separate operations tasks to different people. If you create a single JEA endpoint linked to multiple role capabilities, you might inadvertently assign administrative privileges that are not necessary to one or more groups of users.

Demonstration: Connecting to a JEA endpoint

Demonstration Steps

1. If not signed in already, sign on to **LON-SVR1** as **Adatum\Administrator** by using **Pa55w.rd** as the password.
2. Click **Start**, and then click **Windows PowerShell**.
3. In the **Windows PowerShell** window, type the following commands, and press Enter after each:

```
Enter-PSSession -ComputerName LON-DC1
 (get-command).count
Whoami
Exit-PSSession
```

4. Sign out of **LON-SVR1**.
5. Sign in to **LON-SVR1** as **Adatum\Beth** by using **Pa55w.rd** as the password.
6. Click **Start**, and then click **Windows PowerShell**.
7. In the **Windows PowerShell** window, type the following commands, and press Enter after each command:

```
Enter-PSSession -ComputerName LON-DC1 -ConfigurationName DNSOps
 (Get-Command).count
WhoAmI
Get-DNSServerResourceRecord -zonename Adatum.com
Add-DNSServerResourceRecord -zonename “Adatum.com” -A -Name “MEL-SVR1” -IPv4Address
“172.16.0.101”
Get-DNSServerResourceRecord -zonename Adatum.com
Restart-Service DNS
Restart-Service WinRM
```

Note: Note that you will get an error message when attempting to restart the Windows Remote Management (WinRM) service because the JEA endpoint is not configured to allow this.

```
Exit-PSsession
```

Demonstration: Deploying JEA configuration to another computer

Demonstration Steps

1. If not signed in already, sign on to **LON-SVR2** as **Adatum\Administrator** by using **Pa55w.rd** as the password.
2. Right-click the **Start** hint, and then click **Run**.

3. In the **Run** dialog box, type **\\LON-DC1\c$**, and then click **OK**.
4. In **File Explorer**, navigate to the **Program Files\WindowsPowerShell\Modules** folder.
5. Copy the **DNSOps** folder to the local **c:\Program Files\WindowsPowerShell\Modules** folder.
6. Click **Start**, and then click **Windows PowerShell**.
7. In the **Windows PowerShell** window, type the following commands, and then press Enter after each:

```
Cd 'c:\Program Files\WindowsPowerShell\Modules\DNSOps\RoleCapabilities'
Register-PSSessionConfiguration -Name DNSOps -Path .\DNSOps.pssc
Restart-Service WinRM
Get-PSSessionConfiguration
```

8. Verify that **DNSOps** is listed as a Windows PowerShell endpoint.

Module Review and Takeaways

Review Question

Question: Which element of JEA configuration allows you to specify which tasks can be performed when connecting to a JEA endpoint?

Answer: The role-capability file allows you to specify which tasks can be performed when connecting to a JEA endpoint.

Lab Review Questions and Answers

Lab: Limiting administrator privileges with JEA

Question and Answers

Question: How do you add additional DNS server-maintenance functions to the JEA configuration?

Answer: You modify the role-capability file to add additional DNS server-maintenance functions to the JEA configuration.

Question: Which command allows you to verify if a virtual account is being used in a JEA session?

Answer: You can use the **whoami.exe** command to verify that a virtual account is being used in a JEA session.

Module 4

Privileged access management and administrative forests

Contents:

Lesson 1

ESAE forests

Contents:

Question and Answers

Question: Should you consider deploying an ESAE forest in your environment as a method of securing accounts used for administrative tasks?

Answer: Answers will vary depending on your environment.

Lesson 2

Overview of Microsoft Identity Manager

Contents:

Question and Answers

Question: Ask the students if they have deployed MIM or Forefront Identity Manager (FIM) to manage identity in their environment.

Answer: Answers will vary, depending on the particulars of the student's environment.

Resources

MIM requirements

 **Additional Reading:** For more information about MIM requirements, refer to "Supported platforms for MIM 2016": http://aka.ms/Armxl4

Lesson 3

Overview of JIT administration and PAM

Contents:

Question and Answers

Question: Other than the host server operating system, which two Microsoft products do you need to deploy before you deploy MIM 2016?

Answer: You need to deploy SharePoint and SQL Server prior to deploying MIM 2016.

Demonstration: Configuring the PAM trust relationship

Demonstration Steps

1. On **SYD-MIM**, ensure that you are signed in as **Adatumadmin\MIMAdmin** with the password **Pa$$w0rd**, and then open the **Windows PowerShell** window.
2. In the **Windows PowerShell** window, type the following command, and then press Enter:

```
$ca = get-credential  –UserName Adatum\Administrator –Message "Adatum forest domain
admin credentials"
```

3. At the prompt, sign in by using **Pa$$w0rd** as the password, and then click **OK**.
4. In the **Windows PowerShell** window, type the following commands, pressing Enter after each command (some commands may take several minutes to complete executing depending on the speed of your virtual machines):

```
New-PAMTrust -SourceForest "adatum.com" -Credentials $ca
New-PAMDomainConfiguration -SourceDomain "adatum" -Credentials $ca
Test-PAMTrust -SourceForest "adatum.com" -CorpCredentials $ca
Test-PAMDomainConfiguration -SourceDomain "adatum" -Credentials $ca
```

5. Switch to **MEL-DC1**. From the **Server Manager** console, click tools, and then click **Active Directory Users and Computers**.
6. In the **Active Directory Users and Computers** console, right-click **Adatum.com**, and then click **Delegate Control**.
7. On the **Welcome to the Delegation of Control Wizard** page of the **Delegation of Control Wizard**, click **Next**.
8. On the **Users or Groups** page, click **Add**.
9. On the **Select Users, Computers, or Groups** page, click **Locations**.
10. In the **Locations** dialog box, click **ADATUMADMIN.COM**, and then click **OK**.
11. In the **Select Users, Computers, or Groups** dialog box, type **Domain Admins**, and then click **Check Names**.
12. in the **Enter Network Credentials** dialog box, provide the following credentials, and click **OK**:
    - Username: **adatumadmin\administrator**
    - Password: **Pa$$w0rd**
13. In the **Select Users, Computers, or Groups** dialog box, after Domain Admins, type **Mimmonitor**, click **Check Names**, and then click **OK**.
14. On the **Users or Groups** page, click **Next**.
15. On the **Tasks to Delegate** page, select **Read All User Information**, click **Next**, and then click **Finish**.

Demonstration: Creating user and shadow principals

Demonstration Steps

1. Ensure that you are signed on to **MEL-DC1** as **ADATUM\Administrator** by using **Pa$$w0rd** as the password.
2. Click on the **Windows PowerShell** icon on the taskbar.
3. In the **Windows PowerShell** window, type the following commands, pressing Enter after each command:

```
New-ADGroup –name CorpAdmins –GroupCategory Security –GroupScope Global –
SamAccountName CorpAdmins
New-ADUser –SamAccountName Wayne –name Wayne
$jp = ConvertTo-SecureString 'Pa$$w0rd' –asplaintext –force
Set-ADAccountPassword –identity Wayne –NewPassword $jp
Set-ADUser –identity Wayne –Enabled 1 -DisplayName "Wayne"
```

 **Note:** This will create a new group named CorpAdmins and a new user named Wayne, which will be used later to demonstrate PAM.

4. Switch to **SYD-MIM**. You should be signed in as **adatumadmin\mimadmin** by using **Pa$$w0rd** as the password.
5. In the **Windows PowerShell** window, type the following commands, pressing Enter after each command:

```
$sj = New-PAMUser –SourceDomain adatum.com –SourceAccountName Wayne
$jp = ConvertTo-SecureString 'Pa$$w0rd' –asplaintext –force
Set-ADAccountPassword –identity priv.Wayne –NewPassword $jp
Set-ADUser –identity priv.Wayne –Enabled 1
$ca = get-credential –UserName Adatum\Administrator –Message "Adatum forest domain
admin credentials"
```

6. In the dialog box, sign in by using **Pa$$w0rd** as the password, and then click **OK**.
7. In the **Windows PowerShell** window, type the following commands, pressing Enter after each command:

```
$pg = New-PAMGroup –SourceGroupName "CorpAdmins" –SourceDomain adatum.com –SourceDC
mel-dc1.adatum.com –Credentials $ca
$pr = New-PAMRole –DisplayName "CorpAdmins" –Privileges $pg –Candidates $sj
```

8. Switch to **SYD-DC1**.
9. From **Server Manager**, click **Tools**, and then click **Active Directory Users and Computers**.
10. Open the **PAM Objects** container and verify that the **Adatum.CorpAdmins** group and **PRIV.Wayne** user are present.
11. If one is not already open, open a **Windows PowerShell** window and type the following commands, pressing Enter after each command:

```
Get-ADGroup -identity Adatum.corpadmins -properties SIDHistory
Get-ADGroup -server mel-dc1.adatum.com -identity corpadmins
```

 **Note:** The SID value of the Adatum group and the SID History value of the ADATUMADMINS group are the same.

Demonstration: Configuring and requesting privileged access

Demonstration Steps

1. Ensure that you are signed in to **MEL-SVR1** as **Adatum\administrator** by using **Pa$$w0rd** as the password.
2. Click the File Explorer icon on the taskbar and then double-click **DVD Drive (D:) MIM2016-EVAL**.
3. Double click the .htm file and in the **Internet Explorer** dialog box, click **Yes**.
4. On the **Microsoft Identity Manager** page, click **Install Add-ins and Extensions, 64-bit**.
5. In the **Do you want to run or save setup.exe?** dialog box, click **Run**.
6. On the **Welcome to the Microsoft Identity Manager Add-ins and Extensions Setup Wizard** page of the **Microsoft Identity Manager 2016 Wizard**, click **Next**.
7. On the **End-User License Agreement** page, click **I accept the terms in the License Agreement**, and then click **Next**.
8. On the **MIM Customer Experience Improvement Program** page, click **I don't want to join the program at this time**, and click **Next**.
9. On the **Custom Setup** page, click **MIM Add-in for Outlook**, and then click **Entire feature will be unavailable**.
10. On the **Custom Setup** page, click **MIM Password and Authentication**, and then click **Entire feature will be unavailable**.
11. On the **Custom Setup** page, click **PAM Client**, and then click **Entire Feature Will Be Installed On Local Hard Drive**, and then click **Next**.
12. On the **Configure MIM PAM Service Address** page, configure the following settings, and then click **Next**:
    - PAM Server Address: **syd-mim.adatumadmin.com**
    - Port: **5725**
13. Click **Install**, and then, when the installation finishes, click **Finish**.
14. Right-click **Start**, and then click **Computer Management**.
15. In the **Computer Management** console, expand **Local Users** and **Groups**, and then click **Groups**. Double-click the **Administrators** group.
16. In the **Administrators Properties** dialog box, click **Add**.
17. In the **Select Users, Computers, Service Accounts, or Groups** dialog box, type **adatumadmin\adatum.corpadmins** and click Check Names.
18. Enter the credentials **adatumadmin\administrator** and the password **Pa$$w0rd** and click **OK** three times.
19. Right-click **Start**, click **Shut Down or Sign Out**, and then click **Restart**. Provide the reason **Lab**.
20. Sign in to **MEL-SVR1** as **Adatum\Wayne** by using **Pa$$w0rd** as the password.
21. On the **Taskbar**, click **Windows PowerShell**, and then, in the **Windows PowerShell** window, type the following command, and then press Enter:

```
Whoami /groups
```

22. Verify that the **Wayne** account is not a member of the **CorpAdmins** group.

23. On the **Taskbar**, click **Server Manager**.
24. On the **Manage** menu of the **Server Manager** console, click **Add Roles and Features**.
25. On the **Before you begin** page, click **Next** four times.
26. On the **Select Features** page, click **WINS Server**. In the **Add Roles and Features** dialog box, click **Add Features**.
27. Click **Next**, and then click **Install**.
28. Review the message that informs you that you do not have adequate user rights to make changes to the target computer, and then click **Close**.
29. Right-click **Start**, click **Shut down or sign out**, and click **Sign out**.
30. Sign into **MEL-SVR1** as **ADATUMADMIN\priv.Wayne** by using **Pa$$w0rd** as the password.
31. On the **Taskbar**, click **Windows PowerShell**, and then, in the **Windows PowerShell** window, type the following command, and then press Enter:

```
Whoami /groups
```

32. Verify that the account is not a member of the **CorpAdmins** group.
33. On the **Taskbar**, click on **Server Manager**.
34. On the **Manage** menu of the **Server Manager** console, click **Add Roles and Features**.
35. On the **Before you begin** page, click **Next** four times.
36. On the **Select Features** page, click **WINS Server**.
37. In the **Add Roles and Features** dialog box, click **Add Features**, click **Next**, and then click **Install**.
38. Review the message that informs you that you do not have adequate user rights to make changes to the target computer, and then click **Close**.
39. In the **Windows PowerShell** window, type the following commands, and then press Enter after each command:

```
Import-Module MIMPAM
Get-PAMRoleForRequest
```

Note: This will show a list of roles for which the **priv.Wayne** account can apply. Note the TTL for the role listed.

40. In the **Windows PowerShell** window, type the following commands, and then press Enter after each command:

```
New-PamRequest -RoleDisplayName CorpAdmins
```

Note: The request status is set to **Processing**.

41. Right-click **Start**, click **Shut down or sign out**, and then click **Sign out**.
42. Sign into **MEL-SVR1** as **ADATUMADMIN\priv.Wayne** by using **Pa$$w0rd** as the password.
43. On the **Taskbar**, click **Windows PowerShell**, in the **Windows PowerShell** window, type the following command, and then press Enter:

```
Whoami /groups
```

44. Verify that the account is a member of the **CorpAdmins** group.
45. On the **Taskbar**, click **Server Manager**.
46. On the **Manage** menu of the **Server Manager** console, click **Add Roles and Features.**
47. On the **Before you begin** page, click **Next** four times.
48. On the **Select Features** page, click **WINS Server**.
49. In the **Add Roles and Features** dialog box, click **Add Features**, click **Next**, and then click **Install**.
50. When the feature installs, click **Close**.

Demonstration: Managing PAM roles

Demonstration Steps

1. Switch to **MEL-DC1**, and verify that you are signed on as **ADATUM\Administrator**.
2. In the **Windows PowerShell** window, type the following commands, pressing Enter after each command:

```
New-ADUser –SamAccountName Gavin –name Gavin
$jp = ConvertTo-SecureString 'Pa$$w0rd' –asplaintext –force
Set-ADAccountPassword –identity Gavin –NewPassword $jp
Set-ADUser –identity Gavin –Enabled 1 -DisplayName "Gavin"
```

 **Note:** This set of commands allows you to create a new user named Gavin that you will enable for PAM.

3. Switch to **SYD-MIM**, and ensure that you are signed on as **ADATUMADMIN\MIMAdmin**.
4. In the **Windows PowerShell** window, type the following commands, pressing Enter after each command:

```
$sj = New-PAMUser –SourceDomain adatum.com –SourceAccountName Gavin
$jp = ConvertTo-SecureString 'Pa$$w0rd' –asplaintext –force
Set-ADAccountPassword –identity priv.Gavin –NewPassword $jp
Set-ADUser –identity priv.Gavin –Enabled 1
```

5. Start **Internet Explorer**, and navigate to **http://syd-mim.adatumadmin.com:82/IdentityManagement/default.aspx**.
6. If prompted, sign in as **ADATUMADMIN\Mimadmin** by using **Pa$$w0rd** as the password.
7. In the **Microsoft Identity Manager** console, click **PAM Roles** under **Privileged Access Management**.
8. In the list of **Privileged Access Management** roles, click **CorpAdmins**.
9. In the **General** tab of the **Corpadmins** dialog box, change the **PAM Role TTL(sec)** from **3600** to **600**, and then click **OK**, and then click **Submit**.

 **Note:** When performing this demonstration, you can also describe the function of the other fields.

10. In the list of **Privileged Access Management** roles, click **Corpadmins**.
11. On the **Candidates** tab of the **Corpadmins** dialog box, click **Browse**.
12. In the **Select Users** dialog box, click the magnifying glass next to Search. Wayne and Adatum.Wayne should already be selected. Select **ADATUM.Gavin** and **Gavin**, and then click **OK** twice, and then click **Submit**.
13. Click **OK** to close the **CorpAdmins** dialog box.
14. Under **Privileged Access Management**, click **PAM Requests**.
15. Review the **PAM Requests**.
16. Click on **PRIV.Wayne**, and review the details of when the request was made, when the request expires, and the role requested.

Module Review and Takeaways

Review Question

Question: What is the minimum number of forests required to deploy PAM?

Answer: You need a minimum of two forests to deploy PAM, including the administrative forest in which you deploy PAM and the production forest.

Lab Review Questions and Answers

Lab: Limiting administrator privileges with PAM

Question and Answers

Question: What step would you take to ensure that a user requesting a PAM role had access to that role for two hours rather than one?

Answer: You would change the TTL of the role to two hours.

Question: Where can you view the users that have been granted PAM roles?

Answer: You can use the PAM Requests section, under the Privileged Access Management area, in the MIM console.

Module 5

Mitigating malware and threats

Contents:

Lesson 1

Configuring and managing Windows Defender

Contents:

Question and Answers

Question: What are some of the scan options that are available when you use Windows Defender?

Answer: The following table describes the scanning options.

Scan options	Description
Quick	Checks the areas that malware, including viruses, spyware, and unwanted software, are most likely to infect.
Full	Checks all files on your hard disk and all running programs.
Custom	Enables users to scan specific drives and folders.

Demonstration: Using Windows Defender

Demonstration Steps

1. Switch to **LON-CL1**.
2. Right-click **Start**, and then click **Control Panel**.
3. Click **View by**, select **Large Icons**, and then click **Windows Defender**.
4. Click **Close** on the **What's new** dialog box.
5. On the Windows Defender **Home** tab, ensure that the **Quick** scan option is selected.
6. Click **Scan now**, and then review the results.
7. Close Windows Defender.
8. Open File Explorer, and then go to **C:\Files**.
9. In the **Files** folder, open **sample.txt** in Notepad. The **sample.txt** file contains a text string to test malware detection.
10. In the **sample.txt** file, delete both instances of **<remove>**, including the brackets and any extra lines or blank spaces.
11. Save and close the file. Immediately, Windows Defender detects a potential threat.
12. Windows Defender then removes **sample.txt** from the **Files** folder.
13. Right-click **Start**, and then click **Control Panel**.
14. Click **Windows Defender**.
15. In Windows Defender, click the **History** tab.
16. Click **View details**, and then review the results.
17. Select the check box for **Virus:DOS/EICAR_Test_File**, and then click **Remove**.
18. Close all open windows.

Lesson 2

Restricting software

Contents:

Resources

What is AppLocker?

 **Additional Reading:** For more information about AppLocker, refer to AppLocker Overview: http://aka.ms/Amf8jf

Demonstration: Creating AppLocker rules

Demonstration Steps

Create a Group Policy Object (GPO) to enforce the default AppLocker Executable rules

1. On **LON-DC1**, in Server Manager, click **Tools**, and then click **Group Policy Management**.
2. In the **Group Policy Management Console (GPMC)**, go to **Forest: Adatum.com\Domains\Adatum.com**.
3. Click **Group Policy Objects**, right-click **Group Policy Objects**, and then click **New**.
4. In the **New GPO** window, in the **Name** text box, type **WordPad Restriction Policy**, and then click **OK**.
5. Right-click **WordPad Restriction Policy**, and then click **Edit**.
6. In the **Group Policy Management Editor** window, go to **Computer Configuration\Policies\Windows Settings\Security Settings\Application Control Policies\AppLocker**.
7. Click **Executable Rules**, right-click **Executable Rules**, and then select **Create New Rule**.
8. On the **Before You Begin** page, click **Next**.
9. On the **Permissions** page, click **Deny**, and then click **Next**.
10. On the **Conditions** page, click **Publisher**, and then click **Next**.
11. On the **Publisher** page, click **Browse**, and then click **This PC**.
12. On the **Open** page, double-click **Local Disk (C:)**.
13. On the **Open** page, double-click **Program Files**, double-click **Windows NT**, double-click **Accessories**, click **wordpad.exe**, and then click **Open**.
14. Move the slider up to the **File name** position, and then click **Next**.
15. Click **Next** again, and then click **Create**.
16. If prompted to create default rules, click **Yes**.
17. In the **Group Policy Management Editor** window, go to **Computer Configuration\Policies\Windows Settings\Security Settings**.
18. Expand **Application Control Policies**, right-click **AppLocker**, and then select **Properties**.
19. On the **Enforcement** tab, under **Executable rules**, select the **Configured** check box, click **Enforce rules**, and then click **OK**.
20. In the **Group Policy Management Editor** window, go to **Computer Configuration\Policies\Windows Settings\Security Settings**.
21. Click **System Services**, and then double-click **Application Identity**.

22. In the **Application Identity Properties** dialog box, above **Select service startup mode**, click **Define this policy setting**, click **Automatic**, and then click **OK**.
23. Close the **Group Policy Management Editor** window.

Apply the GPO to the domain

1. In the **GPMC**, expand **Forest: Adatum.com**, expand **Domains**, expand **Adatum.com**, and then expand **Group Policy Objects**.
2. In the **GPMC**, right-click **Adatum.com**, and then click **Link an Existing GPO**.
3. In the **Select GPO** window, in the **Group Policy Objects** window, click **WordPad Restriction Policy**, and then click **OK**.
4. Close the **GPMC**.
5. Switch to the **Start** screen, type **cmd**, and then press Enter.
6. In the **Command Prompt** window, type **gpupdate /force**, and then press Enter. Wait for the policy to update.

Test the AppLocker rule

1. Sign in to **LON-CL1** as **Adatum\Beth** with the password **Pa55w.rd**.
2. In the **Search** text box, type **cmd**, and then press Enter.
3. In the **Command Prompt** window, type **gpupdate /force**, and then press Enter. Wait for the policy to update.
4. In the **Search** text box, type **WordPad**, and then press Enter. Notice that WordPad does not start.

 **Note:** It will take a few minutes for the gpupdate to take effect. If WordPad launches, wait a minute and try again.

Lesson 3

Configuring and using the Device Guard feature

Contents:

Resources

Implementing Device Guard policies

Additional Reading: For more information, refer to "Configurable Code Integrity Policy for Windows PowerShell" at http://aka.ms/U0nker

Code-integrity file rules

Additional Reading: For more information, refer to Add unsigned app to code integrity policy: http://aka.ms/Tkie2j

Reference Links: To download a copy of the **signtool.exe**, refer to SignTool at: http://aka.ms/S4ihkk

Demonstration: Creating code-integrity file rules

Demonstration Steps

1. On **LON-DC1**, open the **Start** screen, select **Windows PowerShell**.
2. In Windows PowerShell, type the following commands, pressing Enter after each line:

```
$CIPolicyPath=$env:userprofile+"\Desktop\"
$InitialCIPolicy=$CIPolicyPath+"InitialScan.xml"
$CIPolicyBin=$CIPolicyPath+"DeviceGuardPolicy.bin"
```

3. Scan your device for installed applications. Create a new code-integrity policy by typing the following command and then pressing Enter:

```
New-CIPolicy -Audit -Level Hash -FilePath $InitialCIPolicy -UserPEs -Fallback Hash 3>
Warningslog.txt
```

4. Convert the code-integrity policy to a binary format by typing the following command and then pressing Enter:

```
ConvertFrom-CIPolicy $InitialCIPolicy $CIPolicyBin
```

5. After you complete these steps, close Windows PowerShell. The Device Guard policy file (**DeviceGuardPolicy.bin**) and the original .xml file (**InitialScan.xml**) will be available on your desktop.
6. Open the **Initalscan.xml** file located on the desktop. You can open the file by clicking the File Explorer icon on the taskbar, typing **C:\Users\Administrator\Desktop\Initialscan.xml** into the **Quick Access** box, and then pressing Enter.

   You will notice that the current rules for the **SIPolicy** are set with **Audit Mode** enabled.
7. On the Start screen, select **Windows PowerShell**.
8. In the **Windows PowerShell** window, type the following cmdlet and parameter to review the rule options:

```
Set-RuleOption -Help
```

9. Review the output of the command, and then notice that **Audit Mode** is defined in rule 3.

10. In Windows PowerShell, type the following commands, pressing Enter after each line:

```
# Initialize the variables that will be used
$CIPolicyPath=$env:userprofile+"\Desktop\"
$InitialCIPolicy=$CIPolicyPath+"InitialScan.xml"
$CIPolicyBin=$CIPolicyPath+"DeviceGuardPolicy.bin"
$EnforcedCIPolicy=$CIPolicyPath+"EnforcedPolicy.xml”
$CIEnforceBin = $CIPolicyPath + “EnforceDeviceGuardPolicy.bin”
# Copy the initial file to maintain the original copy
cp $InitialCIPolicy $EnforcedCIPolicy
# Remove the audit mode
Set-RuleOption -Option 3 -FilePath $EnforcedCIPolicy -Delete
# Cover the new code policy to binary format
ConvertFrom-CIPolicy $EnforcedCIPolicy $CIEnforceBin
```

11. Open the **EnforcedPolicy.xml** file located on the desktop, and then ensure that the file no longer contains **Audit Mode**.

Lesson 4

Deploying and using the EMET

Contents:

Demonstration: Protecting applications with EMET

Demonstration Steps

1. On **20744B-LON-DC1**, install the **EMET Setup.msi** file located at **E:\Labfiles\Mod05**.
2. After the installation is complete, select **Configure Manually Later**, click **Finish**, and then click **Close**.
3. In the notification area in the lower-right corner, right-click the icon, and then select **Open EMET**.
4. Click **Apps** on the top menu bar, and then review the applications that are configured in the EMET.
5. Close the **Application Configuration** window.
6. Click **Import** in the upper-left corner of the EMET. Review the three options available. Select **Recommended Software.xml**, and then click **Open**.
7. Click **Apps** on the top menu bar, and then review the applications that are configured in the EMET.
8. Notice that the Windows PowerShell executable is not included. Click **Add Application**. In the **File name** text box, enter **C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe**.
9. Click **Open**, and then click **OK**.
10. Click **Start**. Click the **Windows PowerShell** icon. After the application loads, minimize it to the notification area.
11. On the **Enhanced Mitigation Experience Toolkit** page, click **Refresh**. You now should see **PowerShell – Windows PowerShell** under **Running Processes**.

Module Review and Takeaways

Best Practice

When using the EMET in your organization, you should use GPOs to deploy consistent configurations throughout your environment.

Review Question

Question: What is the best way to deploy the EMET in a large enterprise environment?

> **Answer:** Use Group Policy or Microsoft System Center Configuration Manager. The current versions have built-in support for Group Policy and System Center Configuration Manager.

Real-world Issues and Scenarios

There are new reports of malware being used to exploit organizations throughout the world. It is important that you review the latest Microsoft Security Bulletin Summary to learn which vulnerabilities might exist in your system and how you can stay current on antimalware technologies and updates.

Tools

There are a number of tools that you can use to exploit vulnerabilities on a Windows system. Kali Linux is distributed freely and it includes several tools that Windows administrators can use to test their system's security.

Lab Review Questions and Answers

Lab: Securing applications with AppLocker, Windows Defender, Device Guard Rules, and the EMET

Question and Answers

Question: The lab included several options that you could use to help prevent malware. Which solution uses security-mitigation technologies to make exploitation as difficult as possible?

Answer: The EMET. It makes exploitation very difficult, but these security-mitigation technologies do not guarantee that malicious hackers cannot exploit vulnerabilities.

Question: Which of the technologies introduced in this module work together to help prevent malware?

Answer: Windows Defender, AppLocker, the EMET, and Device Guard are designed to work together to help fight malware on a Windows system.

Module 6

Analyzing activity with advanced auditing and log analytics

Contents:

Lesson 1

Overview of auditing

Contents:

Demonstration: Locate events in the security log

Demonstration Steps

1. On LON-SVR1, on the taskbar, click **File Explorer**.
2. In the Navigation pane, click **This PC**.
3. Double-click **Allfiles (D:)**.
4. Right-click **Labfiles**, and then click **Properties**.
5. Click the **Sharing** tab, and then click **Share**.
6. In the box, type **Abbi**, and then click **Add**.

Note: Abbi Skinner should be given read access.

7. Click **Share**.
8. Click **Change settings**, click **Done**, and then click **Close**.
9. Right-click **Labfiles**, click **Properties**, click the **Security** tab, and then click **Advanced**.
10. Select the **Auditing** tab, and then click **Add**.
11. Click **Select a principal**. In the box, type **Everyone**, and then click **OK**.
12. Under **Type**, select **All**, and then click **OK**.
13. Click **OK** twice.
14. On LON-DC1, from Server Manager, click **Tools**, and then select **Group Policy Management**.
15. Expand **Forest:Adatum.com**, expand **Domains**, expand **Adatum.com**, select and right-click **Default Domain Policy**, and then click **Edit**.
16. Expand Computer Configuration, expand Policies, expand Windows Settings, expand Security Settings, and then expand Local Policies.
17. Click Audit Policy.
18. Double-click Audit object access, and then select the Define these policy settings check box.
19. Select both **Success** and **Failure**, and then click **OK**.
20. Open a Windows command prompt, type the following, and then press Enter.

```
GPUpdate /Force
```

Note: You can also configure this in advanced audit policy configuration, which is located in **Computer** > **Policies** > **Windows Settings** >**Security Settings** > **Advanced Audit Policy**. **Configuration**.

21. Sign in to LON-CL1 as **Abbi** with the password as **Pa55w.rd**.
22. Using File Explorer, browse to and open \\lon-svr1\Labfiles\Mod01\logonSessions.zip.
23. Sign out of LON-CL1.
24. Sign in to LON-CL1 as **Beth** with the password as **Pa55w.rd**.
25. Using File Explorer, attempt to browse to and open **\\lon-svr1\Labfiles\.**

26. Click Close at the error message.
27. On LON-DC1, from **Server Manager**, click **Tools**, and then select **Event Viewer**.
28. Expand **Windows Logs**, and then click **Security**.
29. Review several events, including success and failure events (if available).

Lesson 2

Advanced auditing

Contents:

Resources

Audit Collection Services

Additional Reading: For more information on ACS, refer to How to Install an Audit Collection Services (ACS) Collector and Database: http://aka.ms/Jwghcp

Demonstration: Configuring advanced auditing

Demonstration Steps

1. On LON-DC1, in Server Manager, click **Tools**, and then click **Group Policy Management**.
2. In Group Policy Management, double-click **Forest: Adatum.com**, double-click **Domains**, double-click **Adatum.com**, right-click **Group Policy Objects**, and then click **New**.
3. In the **New GPO** window, type **File Audit** in the **Name** box, and then press Enter.
4. Double-click the **Group Policy Objects** container, right-click **File Audit**, and then click **Edit**.
5. In the Group Policy Management Editor, under **Computer Configuration**, expand **Policies**, expand **Windows Settings**, expand **Security Settings**, expand **Advanced Audit Policy Configuration**, expand **Audit Policies**, and then click **Object Access**.
6. Double-click **Audit Detailed File Share**.
7. In the **Properties** window, select the **Configure the following audit events** check box.
8. Select the **Success** and **Failure** check boxes, and then click **OK**.
9. Double-click **Audit Removable Storage**.
10. In the **Properties** window, select the **Configure the following audit events** check box.
11. Select the **Success** and **Failure** check boxes, and then click **OK**.
12. Close the Group Policy Management Editor.
13. Close Group Policy Management.

Demonstration: Event log forwarding

Demonstration Steps

1. On LON-SVR1, click Start and then click **Windows PowerShell**.
2. Type the following commands, and then press Enter:

```
winrm quickconfig
```

3. Connect to LON-DC1, and then click **Start**.
4. Click **Windows PowerShell**, and type the following command, and then press Enter:

```
Wecutil qc
```

5. Type Y when prompted by The service startup mode will be changed to Delay-Start. Would you like to proceed?
6. Type the following commands, and then press Enter after each command:

```
Winrm id -remote:lon-svr1
Winrm enumerate winrm/config/listener
```

7. Connect to LON-SVR1; Select the **Windows PowerShell** window, type the following commands, and then press Enter after each command:

```
Winrm id -remote:lon-dc1
Winrm enumerate winrm/config/listener
Shutdown -r
```

8. Switch to LON-DC1 and continue using **Windows PowerShell**; type the following commands, and then press Enter after each command:

```
net localgroup "event log readers" LON-DC1$ /add
shutdown -r
```

9. After LON-SVR1 reboots, sign back in as **adatum\administrator** with the password **Pa55w.rd**.
10. After LON-DC1 reboots, sign back in as **adatum\administrator** with the password **Pa55w.rd**.
11. On LON-DC1, wait for the **Server Manager** to open.
12. Click **Tools**, and then select **Event Viewer**.
13. In the console tree, click **Subscriptions;** if prompted, click **Yes**.
14. On the **Actions** menu, click **Create Subscription**.
15. In the **Subscription Name** box, type **LogDemo** as the name for the subscription.
16. In the **Description** box, type an optional description.
17. In the **Destination Log** box, ensure that the log file specifies the default **ForwardedEvents** log.
18. Click **Select Computers**.
19. Click **Add Domain Computers**, type **LON-SVR1**, click **Check Names**, and then click **OK** twice.
20. Click **Select Events** to display the **Query Filter** dialog box.
21. Use the controls in the **Query Filter** dialog box to specify the criteria that events must meet to be collected (**Critical**, **Warning**, **Error**) for this demo, next to **Event Logs**, select **Application** and **Security**. Click **OK**.
22. In the **Subscription Properties** dialog box, click **OK**. The subscription is added to the **Subscriptions** pane, and if the operation was successful, the status of the subscription is **Active**.
23. On LON-SVR1, right-click **Start**, and then click **Windows PowerShell (Admin)**.
24. Type the following command, and then press Enter.

```
Eventcreate /id 999 /t error /l application /d “Error test event”
```

25. After a few minutes, return to LON-DC1, and then review the events being forwarded from LON-SVR1. You can find the events under **Forwarded Events** in the **Windows Logs** node.

Note: The events may take 15 – 20 minutes to show up on LON-DC1.

Lesson 3

Windows PowerShell auditing and logging

Contents:

Demonstration: Managing auditing by using Windows PowerShell

Demonstration Steps

1. Open Server Manager, click **Tools**, and then select **Event Viewer**.
2. Review the Windows logs under **System**.
3. Click **Start**, and then select **Windows PowerShell**.
4. Type the following, and then press Enter after each line.

```
Get-EventLog Security -newest 20
Get-EventLog System -newest 20 | Format-List
Get-EventLog "Windows PowerShell" | Group-Object eventid | Sort-Object Name
```

Demonstration: Configuring transcript, module, and script block logging

Demonstration Steps

1. If necessary, sign in to LON-DC1 as **Adatum\Administrator** with the password **Pa55w.rd**.
2. Switch to the **Windows PowerShell** window.
3. Type the following, and then press Enter:

```
Get-Module Microsoft.* |
Select Name, LogPipelineExecutionDetails
```

4. Review the output, and notice the status of **LogPipelineExecutionDetails**.
5. Type the following, and then press Enter after each command:

```
Get-Module Microsoft.* | ForEach {
  $_.LogPipelineExecutionDetails = $True
}
Get-Module Microsoft.* |
Select Name, LogPipelineExecutionDetails
```

6. Review the output, and then type the following, and then press Enter after each command:

```
Get-EventLog Security -Newest 100
Get-ChildItem -Path C:\inetpub\wwwroot
```

7. Review the event log.
8. Navigate back to Windows PowerShell, and then type the following, and then press Enter:

```
Get-WinEvent -FilterHashtable @{LogName='Windows PowerShell';Id ='800'} -MaxEvents 1
|
Select -Expand Message
```

9. Open Server Manager, click **Tools**, and then select **Group Policy Management**.
10. Right-click **Default Domain Policy**, and then click **Edit**.
11. Open the **Group Policy Management Editor**.
12. Expand **Computer Configuration**, expand **Policies**, expand **Administrative Templates**, expand **Windows Components**, click **Windows PowerShell**, and then examine the GPO settings shown on the main screen.
13. Collapse the GPO nodes.

14. Expand **Computer Configuration**, expand **Preferences**, expand **Window Settings**, right-click **Environment**, point to **New**, and then select **EnvironmentVariable**. Enter the following information:
    - Name: **PSLogScriptBlockExecution**
    - Value: **0**
15. Click **OK**, right-click **Environment**, point to **New**, and then select **EnvironmentVariable**. Enter the following information, and then click **OK**:
    - Name: **PSLogScriptBlockExecutionVerbose**
    - Value: **0**
16. Close the Group Policy Management Editor.
17. Click **Start**, select **Server Manager**, click **Tools**, and then click **Event Viewer**.
18. Review the Windows logs under **System**.
19. Locate the Event Tracing for Windows (ETW) logs under the following file path: **Applications and Services/Microsoft/Windows, PowerShell/Operational**.
20. Close all open windows.

Module Review and Takeaways

Best Practice

Windows Server 2016 has several auditing enhancements that increase the level of detail in security auditing logs and simplify the deployment and management of auditing policies.

Auditing is an ongoing activity on your network that is one of the critical security practices in your organization. By auditing events related to security, you can obtain early notice of potential malicious activity and evidence if a breach occurs.

Review Question

Question: You have configured an audit policy by using Group Policy to apply it to all of the file servers in your organization. After enabling the policy and confirming that the Group Policy settings are being applied, you discover that audit events are not being recorded in the event logs. What is the most likely reason for this?

> **Answer:** To audit file access, you must configure the files or folders to audit specific events. If you do not do so, the audit events will not be recorded.

Real-world Issues and Scenarios

When you review the Forwarded Events log, if the Event Log Reader permission is skipped, the collector might show the following message: **The description for Event ID 111 from source Microsoft-Windows-EventForwarder cannot be found. Either the component that raises this event is not installed on your local computer or the installation is corrupted. You can install or repair the component on the local computer. If the event originated on another computer, the display information had to be saved with the event.**

Lab Review Questions and Answers

Lab: Configuring advanced auditing

Question and Answers

Question: What is the reason for applying audit policies across an entire organization?

Answer: If you are trying to pinpoint a general problem, or if you are unsure where a specific event is occurring, targeting a large group of servers might be necessary for you to capture the event. In this case, you can use event filtering to search for a specific audit event. After pinpointing a problem, it is a good practice to narrow the scope of the auditing or disable the auditing to reduce the number of generated logs, to reduce performance impacts on computers, and to make it easier to read the logs on a regular basis.

Module 7

Deploying and configuring Advanced Threat Analytics and Microsoft Operations Management Suite

Contents:

Lesson 1

Deploying and configuring ATA

Contents:

Question and Answers

Question: You need to configure port mirroring when you configure an ATA Lightweight Gateway.

( ) True

( ) False

Answer:

( ) True

(√) False

Feedback:

Installing an ATA Lightweight Gateway on a domain controller removes the need to configure port mirroring.

Question: Which ATA Gateways should you configure as domain synchronizer candidates?

( ) All ATA Gateways

( ) Remote site ATA Gateways

( ) ATA Gateways that are installed on read-only domain controllers

( ) Any ATA Gateway that is not a read-only domain controller or serving as a remote site ATA Gateway.

Answer:

( ) All ATA Gateways

( ) Remote site ATA Gateways

( ) ATA Gateways that are installed on read-only domain controllers

(√) Any ATA Gateway that is not a read-only domain controller or serving as a remote site ATA Gateway.

Feedback:

By default, only ATA Gateways are set as domain synchronizer candidates. We recommend disabling any remote site ATA Gateways from being domain synchronizer candidates. If your domain controller is read only, do not set it as a domain synchronizer candidate.

Resources

Understanding ATA

 **Additional Reading:** For more information, refer to the datasheet "Microsoft Advanced Threat Analytics" at: https://aka.ms/ul0xra

ATA deployment requirements

 **Additional Reading:** For more information on directory object permissions, refer to "View or Set Permissions on a Directory Object" at: http://aka.ms/Bgxyha

Demonstration: ATA deployment and configuration

Demonstration Steps

1. On **LON-SVR1**, click **Start**, and then click **Server Manager**.
2. In Server Manager, click **Tools**, and then click **Internet Information Services (IIS) Manager**.
3. In the IIS Manager, expand **LON-SVR1**, expand **Sites**, and then click **Default Web Site**.
4. In the **Actions** pane, click **Bindings**.
5. Select **https**, and then click **Remove**. Click **Yes**, and then close all open windows.
6. On **LON-SVR1**, right-click the network icon on the taskbar, and then click **Open Network and Sharing Center**.
7. Click **Change Adapter Settings**, right-click **Ethernet**, and then click **Properties**.
8. Select **Internet Protocol Version 4 (TCP/IPv4)**, and then click **Properties**.
9. In the **Internet Protocol Version 4 Properties** dialog box, click **Advanced**.
10. In the **Advanced TCP/IP Settings** dialog box, on the **IP Settings** tab, under **IP addresses**, click the **Add** button.
11. In the **IP address** text box, type **172.16.0.13**. Verify that the **Subnet mask** defaults to **255.255.0.0**. Click **Add**, click **OK** twice, and then click **Close**.
12. On **LON-SVR1**, on the taskbar, click the **File Explorer** icon.
13. Browse to **D:\LabFiles\Mod07**, right-click **ATA1.7.iso**, and then select **Mount**.
14. Verify that you now see a new DVD drive with **Microsoft ATA Center Setup.exe**.
15. Right-click the .exe file, and then click **Run as administrator**.
16. The first page prompts you to select your language. By default, **English** is selected. Click **Next** to accept the default setting.
17. Review the Microsoft Software License Terms, select the **I accept the Microsoft Software License Terms** check box, and then click **Next**.
18. On the next page, where you can select the Microsoft update option, leave the default, and then click **Next**.
19. Review the **ATA Center Configuration** page, and confirm that you have different IP addresses for the **Center Service IP Address** and the **Console IP Address**. The first should be **172.16.0.11** and the **Console IP Address** should be **172.16.0.13**.
20. Click **Install**.
21. Open Server Manager, and then on the **Tools** menu, click **Computer Management**.
22. Under **System Tools**, expand **Local Users and Groups**, and then select **Groups**.
23. Right-click **Microsoft Advanced Threat Analytics Administrators**, and then click **Add to Group**.
24. Click the **Add** button, in the text box, type **Beth**, click **Check Names**, and then click **OK**.
25. Click **Add**, in the text box, type **ATARead**, click **Check Names**, and then click **OK**.
26. Click **OK** to close the **Microsoft Advanced Threat Analytics Administrators Properties** dialog box.
27. Close **Computer Management**.
28. After the installation is complete, click **Launch**.

29. At the security notification, click **Continue to this website**.
30. After a few moments, when the **Sign-in** page displays, type **Beth** as the username and **Pa55w.rd** as the password, and then click **Sign in**.
31. In the upper-right corner of the form, click the ellipses (**...**) button, and then click **Configuration**.
32. On the left under **Data Sources**, click **Directory Services**.
33. For the **Username**, type **ATARead**.
34. For the **Password**, type **Pa55w.rd**.
35. For the **Domain**, type **adatum.com**, and then click **Save**.
36. In the blue header, click **Download Gateway setup and install the first Gateway**.
37. Click **Download Gateway Setup**.
38. Save the file at **D:\Labfiles\Mod07**.

 **Note:** The download step above does not require an internet connection. The download is created from the bits already on the server.

39. Open File Explorer, and then browse to **D:\Labfiles\Mod07**.
40. Copy the **Microsoft ATA Gateway Setup.zip** file, and paste it to **\\LON-DC1\E$\Labfiles\Mod07**. Replace the existing file if necessary.
41. Close File Explorer.
42. On **LON-DC1**, open File Explorer, and then browse to **E:\Labfiles\Mod07**.
43. Right-click **Microsoft ATA Gateway Setup.zip**, and then select **Extract All**.
44. In the **Files will be extracted to this folder** text box, type **E:\Labfiles\Mod07\Gateway**, and then click **Extract**.
45. In **E:\Labfiles\Mod07\Gateway**, right-click **Microsoft ATA Gateway Setup.exe**, and then select **Run as administrator**.
46. The first page prompts you to select your language. By default, **English** is selected. Click **Next** to accept the default setting.
47. Review the ATA Gateway deployment type. Point out to students that because this is a domain controller, ATA Lightweight Gateway is already selected. Click **Next**.
48. In the **User Name** text box, type **ATARead**. In the **Password** text box, type **Pa55w.rd**, and then click **Install**.
49. After the installation completes, click **Finish**.

Lesson 2

Deploying and configuring Microsoft Operations Management Suite

Contents:

Question and Answers

Question: Which Microsoft Operations Management Suite service helps you collect and analyze data that resources in your cloud and on-premises environments generate?

( ) Log Analytics

( ) Data Analytics

( ) Microsoft Operations Management Suite data connectors

( ) Network data connectors

Answer:

(√) Log Analytics

( ) Data Analytics

( ) Microsoft Operations Management Suite data connectors

( ) Network data connectors

Feedback:

Log Analytics is a service in Microsoft Operations Management Suite that helps you collect and analyze data that resources in your cloud and on-premises environments generate.

Question: Log Analytics requires local resources that analyze collected data.

( ) True

( ) False

Answer:

( ) True

(√) False

Feedback:

The deployment requirements for Log Analytics are minimal because the Azure cloud hosts the central components. The components include the repository and the services that allow you to correlate and analyze collected data. You can access the Microsoft Operations Management Suite portal from any browser, so there is no requirement for client software.

Microsoft Operations Management Suite security and auditing functions

Question: Which non-Microsoft product does Microsoft Operations Management Suite allow you to manage and help protect?

( ) AWS

( ) VMware

( ) Linux

( ) OpenStack

Answer:

(√) AWS

(√) VMware

(√) Linux

(√) OpenStack

Feedback:

Microsoft Operations Management Suite allows you to manage and help protect Azure or AWS, Windows Server or Linux, and VMware or OpenStack.

Resources

Microsoft Operations Management Suite usage and deployment scenarios

Additional Reading: To learn more about Azure Automation with runbooks, refer to "Getting Started With Azure Automation – Runbook Management: at: http://aka.ms/Cz3zbw

Demonstration: Microsoft Operations Management Suite deployment and configuration

Demonstration Steps

1. If needed, create a Microsoft Account and Azure account as outlined in the Lab Exercise, "Preparing and deploying Microsoft Operations Management Suite," tasks 1 and 2.
2. Sign in to **LON-CL1**, and then click **Start**. In the search bar, type **Internet Explorer**, and then start the program.
3. In Microsoft Internet Explorer, type the following URL, and then press Enter: **https://www.microsoft.com/en-us/server-cloud/operations-management-suite/overview.aspx**.
4. Click **Create a free account**.
5. Click **Get started**.
6. If you are not already signed in, sign in by using your Microsoft account.
7. Fill out the **Create New Workspace** form using the email you used to create your Microsoft account, and then click **CREATE**.
8. Select the desired Azure Subscription, and then click **LINK**.
9. Verify that the **Microsoft Operations Management Suite** page now appears.
10. On the **Microsoft Operations Management Suite** home page, click **Solutions Gallery**.
11. Review the available solutions.
12. Click the house icon on the left side.
13. On the home page, click **Settings**.
14. Click **Connected Sources**, and ensure that **Windows Servers** is selected.
15. Click the Windows **Start** button.
16. Type **Notepad**, and then press Enter.
17. Switch back to **Microsoft Internet Explorer**, and look for **WORKSPACE ID** and **PRIMARY KEY** in the right pane.
18. Copy, and paste both the **WORKSPACE** and **PRIMARY KEY** IDs in Notepad.
19. Save the Notepad file as **D:\WorkspaceID.txt**, in case you need it later.
20. Click **Download Windows Agent (64 bit)** to download **MMASetup-AMD64.exe**.
21. Click **Save**, then click **Run**.

22. In the **Welcome to the Microsoft Monitoring Agent Setup Wizard**, click **Next**.
23. If a **User Account Control** dialog box displays, click **Yes**.
24. Read the Microsoft Software License Terms, and then click **I Agree**.
25. Accept the default destination folder by clicking **Next**.
26. Select **Connect the agent to Azure Log Analytics (OMS)**, and then click **Next**.
27. Enter the **Workspace ID** and the **Primary Key** that you copied to Notepad, and then click **Next**.
28. If you are prompted for Microsoft Updates, click **Next**.
29. Click **Install**, and then click **Finish**.
30. Open Control Panel on LON-CL1.
31. In Control Panel, click **System and Security**, and then click **Microsoft Monitoring Agent**.
32. If a **User Account Control** dialog box displays, click **Yes**
33. Click the **Azure Log Analytics (OMS)** tab, select the listed item, and then click **Edit**. This will allow you to update the **Workspace Key** if needed. Click **Cancel**.
34. Click **Cancel**.
35. Return to the Microsoft Operations Management Suite website, and then refresh your browser. Show students that you can now review the **Usage**, and can now see data for **LON-CL1**.

 **Note:** In some cases, it can take a while for the usage data to display. This could be something that you can show prior to the Microsoft Operations Management Suite lab.

Module Review and Takeaways

Best Practice

In larger environments, you should consider scaling out and using multiple ATA Gateways.

Review Questions

Question: Which security domains can you examine in Microsoft Operations Management Suite?

Answer: You can examine the following domains in Microsoft Operations Management Suite:

- Malware Assessment
- Update Assessment
- Identity and Access

Question: Explain how to use ATA to improve security.

Answer: ATA benefits include:

- Detect threats with behavior analytics. There is no need to create rules, deploy agents, or fine tune or monitor a flood of security reports.
- Adapt as fast as malicious users. ATA continuously learns from organizational entity behavior (users, devices, and resources), and adjusts itself to reflect changes in your rapidly evolving enterprise.
- Focus on what is important by using the simple attack timeline. The attack timeline is a clear, efficient, and convenient feed that displays the right things on the timeline, giving you the power of perspective on the who, what, when, and how of your enterprise.
- Reduce the fatigue of false positives. Alerts only occur after suspicious activities are contextually aggregated.
- Prioritize and plan for next steps. For each identified suspicious activity or known attack, ATA provides recommendations for investigation and remediation.

Some of ATA's key features include:

- Mobility support. Witness all authentication and authorization to organizational resources within the organizational perimeter or on mobile devices.
- Integration with SIEM. ATA works with SIEM and provides options to forward security alerts to your SIEM or to send emails to specific people.
- Seamless deployment. ATA functions as an application and uses port mirroring to allow seamless deployment.

Question: Explain how to use Microsoft Operations Management Suite to improve security.

Answer: Microsoft Operations Management Suite security and compliance features help you identify, assess, and mitigate security risks in your infrastructure. These features are implemented through multiple solutions in Log Analytics that analyze log data and the configuration from the agent systems to assist you in ensuring the ongoing security of your environment.

- The Security and Audit solution collects and analyzes security events on managed systems to identify suspicious activity.
- The Antimalware solution reports on the status of antimalware protection on managed systems.

- The System Updates solution analyzes security updates and other updates on your managed systems so that you easily identify systems that require updates.

Real-world Issues and Scenarios

ATA Center capacity planning:

- The required disk space for an ATA database can vary on a per–domain controller basis.
- If you have multiple domain controllers, sum up the required disk space per domain controller to calculate the full amount of space that is necessary for the ATA database.
- To calculate ATA Center sizing precisely based on your requirements, refer to http://aka.ms/atasizing.

Tools

Wireshark is a network protocol analyzer that lets you examine your network at a precise level. Although Wireshark can be of great value, remember not to install it on the servers that you use for ATA Gateways or ATA Centers.

Common Issues and Troubleshooting Tips

Common Issue	Troubleshooting Tip
Some users report seeing event ID 1013 in the Microsoft ATA event log in the ATA Center.	This issue is often tied to system backups, when disks are not able to provide enough input/output (I/O) operations per second (IOPS) during the backup process.

Lab Review Questions and Answers

Lab: Deploying ATA and Microsoft Operations Management Suite

Question and Answers

Question: What is the advantage of using an ATA Lightweight Gateway?

Answer: You do not need to configure port mirroring for an ATA Lightweight Gateway.

Question: What are some of the requirements to install ATA?

Answer: Some requirements include a domain user account, a list of subnets that have a short Time to Live (TTL), a honeytoken account, Wireshark, and Microsoft Message Analyzer.

Module 8

Secure Virtualization Infrastructure

Contents:

Lesson 1

Guarded fabric

Contents:

Question and Answers

Question: Which service provides the transport keys that are needed to unlock and run shielded VMs on affirmatively attested (or healthy) Hyper-V hosts?

Answer: KPS

Resources

Nano Server as a TPM-attested guarded host

 **Additional Reading:** For more information, refer to Prepare Nano Server Script for Guarded Fabric: http://aka.ms/V2thr5

Lesson 2

Shielded and encryption-supported virtual machines

Contents:

Question and Answers

Question: What are some of the differences between encryption-supported VMs and shielded VMs?

> **Answer:** Like shielded VMs, encryption-supported VMs make use of Secure Boot, virtual Trusted Platform Modules (vTPM), and encrypted VM states. However, with encryption-supported VMs, these settings can be configured. In shielded VMs, they are enforced. In addition, the **Virtual Machine Connection** console is set to **On** for encryption-supported VMs but is disabled in shielded VMs. Finally, COM/serial ports are disabled in shielded VMs, and you cannot attach a debugger to the VM process.

Resources

Troubleshooting shielded and encryption-supported VMs

 **Additional Reading:** For more information, refer to Shielded VMs and Guarded Fabric Troubleshooting Guide for Windows Server 2016: https://aka.ms/ehnloq

Module Review and Takeaways

Best Practice

Although it is possible to use one domain to configure a guarded fabric, we recommend that the HGS have a unique forest.

Review Question

Question: What trusts are needed between domains, and which domain should the guarded host be a member of?

> **Answer:** The HGS server needs to have a one-way trust with the organization's domain. The guarded host should be a member of the organization domain and not a member of the HGS forest.

Common Issues and Troubleshooting Tips

Common Issue	Troubleshooting Tip
A shielded VM fails to start after turning on vTPM.	Verify that the guarded host has been added to the correct security group.

Lab Review Questions and Answers

Lab: Guarded fabric with Admin-trusted attestation and shielded VMs

Question and Answers

Question: Describe the critical components of the guarded fabric.

Answer: Shielded VMs and the guarded fabric enable cloud service providers or enterprise private cloud administrators to provide a more secure environment for tenant VMs. A guarded fabric is comprised of one HGS, which typically consists of a cluster of three nodes, one or more guarded hosts, and a set of shielded VMs.

Question: In the lab, you created an environment that was comprised of the HGS and the guarded host, and you added an HGS group to the corporate domain. Which of these roles needs to be a physical server?

Answer: The guarded host, because it cannot run in a virtualized environment.

Module 9

Securing application development and server-workload infrastructure

Contents:

Lesson 1

Using SCM

Contents:

Question and Answers

Question: SCM 4.0 has which of the following default product baselines?

( ) Internet Explorer 6 and Internet Explorer 7

( ) Microsoft Exchange Server 2007 SP1

( ) Windows 8

( ) Windows Server 2008 SP1

( ) Windows Server 2012

Answer:

( ) Internet Explorer 6 and Internet Explorer 7

( ) Microsoft Exchange Server 2007 SP1

(√) Windows 8

( ) Windows Server 2008 SP1

(√) Windows Server 2012

Feedback:

SCM 4.0 does not have a baseline template for systems and apps that were created before Windows Server 2012, Internet Explorer 8, and Microsoft Exchange Server 2010.

Resources

Managing security baselines

Additional Reading: For more information, refer to Security baseline for Windows 10 v1607 ("Anniversary edition") and Windows Server 2016: https://aka.ms/hhsdmo

Deploying security configurations

Additional Reading: You can download the standalone LGPO.EXE tool at: https://aka.ms/kkvmk5

Demonstration: Installing SCM

Demonstration Steps

Install SCM

1. On **LON-SVR1**, click **File Explorer** on the taskbar.
2. In **File Explorer**, go to **D:\Labfiles\Mod09**.
3. Double-click **Security_Compliance_Manager_Setup.exe**.

   A command prompt window opens and starts the prerequisites for SCM.
4. When the **Microsoft Visual C++ 2010 x86 Redistributable Setup** window appears, select **I have read and accept the license terms**, and then click **Install**.
5. When the **Installation is Complete** page appears, click **Finish**.

6. The **Microsoft Security Compliance Manager Setup Wizard** then starts. On the **Welcome** page, clear **Always check for SCM and baseline updates**, and then click **Next**.

Note: There are several new baselines for Windows 10, Windows Server 2016, Internet Explorer 11, and so on. However, you must download and import them separately. Because you do not have Internet access on the course virtual machines (VMs), you cannot download these baselines. This is the reason why you cleared the **Always check for SCM and baseline updates** check box.

7. On the **License Agreement** page, click **I accept the terms of the license agreement**, and then click **Next**.
8. On the **Installation Folder** page, click **Next**.
9. On the **SQL Instances found** page, select **Create a new SQL express instance,** and then click **Next.**
10. On the **Microsoft SQL Server 2008 Express** page, click **Next**.
11. On the **SQL Server 2008 Express License Agreement** page, select **I accept the terms of the license agreement**, and then click **Next**.
12. On the **Ready to Install** page, click **Install**.
13. When the **Installation Successful** page opens, click **Finish**.
14. The **SCM** console opens and imports several baselines automatically. Leave the console open for the next demonstration.

Demonstration: Configuring and managing security baselines

Demonstration Steps

Install the Windows Server 2016 GPOs

1. On **LON-SVR1**, in the **SCM** console, in the **Actions** pane, click **Import – GPO Backup (folder)**.
2. In the **Browse for folder** window, go to **D:\Labfiles\Mod09\Windows 10 RS1 and Server 2016 Security Baseline\GPOs**, select the first GPO globally unique identifier (GUID) listed, and then click **OK**.
3. In the **GPO Name** window, note the GPO name, and then click **OK**.
4. In the **SCM Log** window, click **OK**.
5. Repeat steps 1 through 4 for the other 10 GPO GUIDs in the **GPOs** folder.

Associate and merge the Windows Server 2016 GPO with the Windows Server 2012 Member Server baseline

1. In the **SCM** console, in the console tree, expand **Custom baselines** (if not expanded already), and then expand **GPO import**.
2. In the list of baselines, select the **SCM Windows Server 2016 - Member Server Baseline – Computer 0.0**.
3. In the **Actions** pane, under **Baseline**, click the **Associate** hyperlink.
4. In the **Associate Product with a GPO** window, in the **Product name** list, select **Windows Server 2012**, and then click **Associate**.
5. In the **Baseline name** text box, type **Associated Server 2012-2016**, and then click **OK**.

6. In the **SCM** console tree, if not already selected, select the **Associated Server 2012-2016** under **Custom Baselines**, and then, in the **Actions** pane, under **Baseline**, click the **Compare/Merge** hyperlink.
7. In the **Compare Baselines** window, expand **Windows Server 2012**, and from the expanded list, select **WS2012 Member Server Security Compliance 1.0**, and then click **OK**.
8. Explain the information that is presented in the **Compare Baselines** window. Explain the settings in both the **Settings that differ** and **Settings that match** areas.
9. In the **Compare Baselines** window, click **Merge Baselines.**
10. In the **Merge Baselines** window, explain the **Merge conflicts to resolve** items, and then click **OK**.
11. In the **Specify a name for the merged baseline** text box, type **Member Server Merged 2012-2016**, and then click **OK**.
12. Explain why students would select one baseline setting versus another. Note that students can see a setting's full name by sliding the separator bar in the headings row.
13. In the details pane, scroll down until you reach the **Session Configuration** area under the **Name** column.
14. Double-click the item named **Interactive Logon: Message title for users attempting to log on**, and clear the **Not Defined** check box. In the **Customize setting value** text box, type **Welcome to A. Datum Corporation!**, and then click **Collapse**.
15. While still in the **Session Configuration** area, under the **Name** column, double-click the item named **Interactive Logon: Message text for users attempting to log on**. Clear the **Not Defined** check box, and in the **Customize setting value** text box, type **This device uses the Member Server Merged 2012-2016 Baseline.**, and then click **Collapse**.
16. In the **Actions** pane, under **Export**, click the **GPO Backup (folder)** hyperlink.
17. In the **Browse For Folder** window, expand **Allfiles (D:)**, expand **Labfiles**, select **Mod09**, and then click **OK**.
18. Close the **File Explorer** window.

Demonstration: Deploying a security baseline to a remote server

Demonstration Steps

Import an SCM GPO backup into the Group Policy Management Console

1. On **LON-DC1**, on the taskbar, select **File Explorer**.
2. In **File Explorer**, in the **URL** text box, type **\\LON-SVR1\D$\Labfiles\Mod09**, and then press Enter.
3. Right-click and then copy the GUID folder (Example: {bed88c04-5ffe-4857-aff6-be595c53ad41}).
4. In **File Explorer**, on **LON-DC1**, go to **Allfiles (E:\)\Labfiles**.

   In the details pane, right-click and then click **Paste**. Close **File Explorer**.
5. In **Server Manager**, on the **Tools** menu, click **Group Policy Management**.
6. In the **Group Policy Management Console** tree, expand **Forest: Adatum.com**, expand **Domains**, expand **Adatum.com**, and then select the **Group Policy Objects** node.
7. Right-click in the empty space in the details pane, and then click **New**.
8. In the **New GPO** window, in the **Name** text box, type **Member Server 2012-2016 Baseline**, and then click **OK**.

9. In the details pane, right-click the **Member Server 2012-2016 Baseline** item, and then click **Import Settings**.
10. In the **Import Settings Wizard**, on the **Welcome** page, click **Next**.
11. On the **Backup GPO** page, click **Next**.
12. On the **Backup location** page, in the **Backup folder** text box, type **E:\Labfiles**, and then click **Next**.
13. On the **Source GPO** page, ensure that the **Member Server Merged 2012-2016** item is selected, and then click **Next**.
14. On the **Scanning Backup** page, click **Next**.
15. On the **Migrating References** page, explain how you can use a migration table to map the settings to a destination GPO. However, because you do not have a migration table, you must accept the default settings, and then click **Next**.
16. On the **Completing the Import Settings Wizard** page, click **Finish**, and then, when the import succeeds, click **OK**.
17. Right-click the **Member Server 2012-2016 Baseline** item in the details pane, and then click **Edit**.
18. Maximize the **Group Policy Management Editor** window.
19. In the **Group Policy Management Editor** window, in the console tree, under the **Computer Configuration** node, expand **Policies**, expand **Windows Settings**, expand **Security Settings**, and then expand **Local Policies**.
20. Under **Local Policies**, select **Security Options**.
21. In the details pane of **Security Options**, scroll down to the setting item labeled **Interactive Logon: Message title for users attempting to log on**, and then double-click it.
22. Note that **Welcome to A. Datum Corporation!** is defined for this policy setting.
23. Do the same for the **Interactive Logon: Message text for users attempting to log on** item, ensuring that it is set to **This device uses the Member Server Merged 2012-2016 Baseline**.
24. Close the **Group Policy Management Editor** window, and then minimize the **Group Policy Management Console**.

Create the Member Server OU, move LON-SVR2 into it, and then link the Member Server 2012-2016 Baseline GPO to the OU

1. On **LON-DC1**, in **Server Manager**, on the **Tools** menu, select **Active Directory Users and Computers**.
2. In **Active Directory Users and Computers**, in the console tree, expand **Adatum.com**.
3. Right-click **Adatum.com**, click **New**, and then click **Organizational Unit**.
4. In the **New Object – Organizational Unit** window, in the **Name** text box, type **Member Servers**, and then click **OK**.
5. In the console tree, select the **Computers** node.
6. In the details pane, right-click **LON-SVR2**, and then click **Move**.
7. In the **Move** window, select the **Member Servers** OU, and then click **OK**.
8. In the console tree, select **Member Servers**, and then verify that **LON-SVR2** is in this OU.
9. Close the **Active Directory Users and Computers** console.
10. Maximize the **Group Policy Management Console**.

11. In the console tree, select **Adatum.com**, and then click the **Refresh** icon.
12. You should now see the **Member Servers** OU under **Adatum.com**. Select the OU.
13. Right-click **Member Servers**, and then click **Link an existing GPO**.
14. In the **Select GPO** window, select the **Member Server 2012-2016 Baseline** GPO, and then click **OK**.
15. Close the **Group Policy Management Console**.

Start LON-SVR2, and then observe the Interactive Logon message title and text

1. In **Hyper-V Manager** on the host computer, double-click **20744B-LON-SVR2**, and then, in the **Virtual Machine Connection** window, click **Start**.
2. When the VM starts, you should see the **Interactive Logon** screen before the **Sign in** screen.
3. Click **OK** on this screen, and then sign in to **LON-SVR2** as **Adatum\Administrator** by using **Pa55w.rd** as the password.
4. Close all open windows, and then sign out of all VMs.

Lesson 2

Introduction to Nano Server

Contents:

Question and Answers

Sequencing Activity

Question: The following are the steps to apply DSC to a Nano Server. Put the following steps in the correct order.

	Steps
	Create a configuration script for DSC on Nano Server.
	Copy the configuration script to the Nano Server.
	Ensure any necessary DSC resources are imported and available.
	Run the configuration script on the Nano Server to create the MOF file.
	Use the Start-DscConfiguration command in Windows PowerShell to deploy DSC against the MOF file.
	Verify that DSC has deployed and the configuration is set as expected.

Answer:

	Steps
1	Create a configuration script for DSC on Nano Server.
2	Copy the configuration script to the Nano Server.
3	Ensure any necessary DSC resources are imported and available.
4	Run the configuration script on the Nano Server to create the MOF file.
5	Use the Start-DscConfiguration command in Windows PowerShell to deploy DSC against the MOF file.
6	Verify that DSC has deployed and the configuration is set as expected.

Resources

Why is Nano Server more secure?

Additional Reading: For more information, refer to Introducing Server management tools at: https://aka.ms/mwe46x

Preparing, deploying, and managing Nano Server

Additional Reading: You can download Nano Server Image Builder at: http://aka.ms/NanoServerImageBuilder

Demonstration: Deploying and managing Nano Server

Demonstration Steps

Copy the required Windows PowerShell scripts

1. On **LON-HOST1**, right-click **Start**, and then click **Windows PowerShell (Admin)**.
2. In the **Windows PowerShell** window, type **cd**, and then press Enter.
3. In the **Windows PowerShell** window, type **md Nano**, and then press Enter.
4. In the **Windows PowerShell** window, type the following command, and then press Enter:

```
copy X:\NanoServer\NanoServerImageGenerator\*.ps* c:\nano
```

Note: Replace *X* in the above step with the drive letter that is assigned for the mounted .iso file.

Import Windows PowerShell modules

1. In the **Windows PowerShell** window, type the following command, and then press Enter:

```
Import-Module c:\nano\NanoServerImageGenerator.psm1
```

2. In the **Windows PowerShell** window, type the following command, and then press Enter:

```
New-NanoServerImage -Edition Standard -mediapath X:\ -Basepath c:\nano -targetpath
c:\nano\nano-svr1.vhdx -DeploymentType Guest -computername NANO-SVR1 -storage -
package Microsoft-NanoServer-DSC-Package -Compute
```

Note: Replace *X* in the above step with the drive letter that is assigned for the mounted .iso file.

3. At the **AdministratorPassword** prompt, sign in by using **Pa55w.rd** as the password, and then press Enter.
4. When the process completes, on the taskbar, click **File Explorer**, go to **C:\Nano**, and then examine the files listed. Verify that **nano-svr1.vhdx** exists.

Create a Hyper-V VM from nano-svr1.vhdx

1. On **LON-HOST1**, open **Hyper-V Manager**.
2. In the **Hyper-V** console, in the **Actions** pane, click **New**, and then click **Virtual Machine**.
3. In the **New Virtual Machine Wizard**, on the **Welcome** page, click **Next**.
4. On the **Specify Name and Location** page, in the **Name** text box, type **NANO-SVR1**, select **Store the virtual machine in a different location**, and then click **Browse**.
5. In the **Select Folder** window, in the **URL** text box, type **C:\nano**, press Enter, and then click **Select Folder**.
6. On the **Specify Name and Location** page, click **Next**.
7. On the **Specify Generation** page, select **Generation 2**, and then click **Next**.
8. On the **Assign Memory** page, click **Next**.

9. On the **Configure Networking** page, in the **Connection** drop-down list, select **Internal Network**, and then click **Next**.
10. On the **Connect Virtual Hard Disk** page, click **Use an existing virtual hard drive**, and then click **Browse**.
11. In the **Open** window, in the **URL** text box, type **C:\nano**, press Enter, select the **nano-svr1.vhdx** item, and then click **Open**.
12. On the **Connect Virtual Hard Disk** page, click **Next**.
13. On the **Completing the New Virtual Machine Wizard** page, click **Finish**.
14. In **Hyper-V Manager**, on **LON-HOST1**, double-click the **NANO-SVR1** item on the **Virtual Machines** pane.
15. In the **NANO-SVR1 on LON-HOST1 – Virtual Machine Connection** window, click **Start**.

Sign in to the NANO-SVR1 VM and view basic settings

1. On **NANO-SVR1**, in the **User name** text box, type **Administrator**, and then press the Tab key.
2. In the **Password** text box, sign in using **Pa55w.rd** as the password, and then press Enter.
3. On **NANO-SVR1**, in the **Nano Server Recovery Console**, note that the computer name is **NANO-SVR1** and that the computer is in a workgroup. Press the Tab key until **Networking** is selected, and then press Enter.
4. At the **Ethernet** prompt, press Enter.
5. In **Network Adapter Settings**, notice that DHCP is providing the IP configuration.
6. Make a note of the IP address.
7. Press Esc twice.

Add NANO-SVR1 to the domain

1. Switch to **LON-DC1**.
2. Right-click **Start**, then click **Windows PowerShell (Admin)**.
3. At the command prompt, type the following command, and then press Enter:

```
djoin.exe /provision /domain adatum /machine nano-svr1 /savefile C:\odjblob
```

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

4. At the command prompt, type the following cmdlet, and then press Enter. Your IP address will be different:

```
Set-Item WSMan:\localhost\Client\TrustedHosts "172.16.0.X"
```

5. Type **Y**, and when prompted, press Enter.
6. At the command prompt, type the following cmdlet, and then press Enter. Your IP address will be different:

```
$ip = "172.16.0.X"
```

7. At the command prompt, type the following cmdlet, and then press Enter:

```
Enter-PSSession -ComputerName $ip -Credential $ip\Administrator
```

8. In the **Windows PowerShell credential request** dialog box, in the **Password** text box, type **Pa55w.rd**, and then click **OK**.
9. At the command prompt, type the following cmdlet, and then press Enter:

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

10. At the command prompt, type the following cmdlet, and then press Enter:

```
Exit-PSSession
```

11. At the command prompt, type the following command, and then press Enter. Your IP address will be different:

```
net use z: \\172.16.0.X\c$
```

12. At the command prompt, type **Z:**, and then press Enter.
13. At the command prompt, type the following command, and then press Enter:

```
copy c:\odjblob
```

14. At the command prompt, type the following cmdlet, and then press Enter:

```
Enter-PSSession -ComputerName $ip -Credential $ip\Administrator
```

15. In the **Windows PowerShell credential request** dialog box, in the **Password** text box, type **Pa55w.rd**, and then click **OK**.
16. At the command prompt, type **cd**, and then press Enter.
17. At the command prompt, type the following cmdlet, and then press Enter:

```
djoin /requestodj /loadfile c:\odjblob /windowspath c:\windows /localos
```

18. At the command prompt, force Nano Server to restart by typing the following cmdlet, and then pressing Enter:

```
shutdown /r /t 5
```

19. Do not close Windows PowerShell. You will use it in the next demonstration.
20. Switch to **NANO-SVR1**.
21. In the **User name** text box, type **Administrator**, and then press the Tab key.
22. In the **Password** text box, type **Pa55w.rd**, and then press Tab.
23. In the **Domain** text box, type **Adatum**, and then press Enter.
24. In the **Nano Server Recovery Console**, observe that the computer is in the **adatum.com** domain.

Demonstration: Configuring Nano Server security by using DSC

Demonstration Steps

Review the DSC script

1. On **LON-DC1**, on the taskbar, click **File Explorer**.

2. In **File Explorer**, in the console tree, select **This PC**, and then, under **This PC**, expand **C:\Labfiles\Mod09**.
3. Right-click the **Demo2DscNanoConfig.ps1** file, and then click **Edit**. This will open the script in the Windows PowerShell Integrated Scripting Environment (ISE).
4. Briefly explain the main parts of the script. The relevant part is the block that calls Service. It checks to see if the **Hyper-V Virtual Machine Management Service (vmms)** is running.
5. Close **Windows PowerShell ISE** without altering or saving the script. Do not close **File Explorer**.

Deploy the DSC script to NANO-SVR1

1. Return to the **Windows PowerShell** window.
2. The drive Z that you mapped in the last demonstration should still be mapped. If it is not, type the following, substituting *X* with the same value that you used in the previous demonstration, and then press Enter:

```
net use z: \\172.16.0.X\c$
```

Note: You can ignore any message that states: "Command 'z:' was not run as the session in which it was intended to run was either closed or broken." The drive will still be properly mapped.

3. In **Windows PowerShell**, type the following commands, pressing Enter after each line:

```
z:
md demo
cd demo
copy c:\Labfiles\Mod09\Demo2DscNanoConfig.ps1
```

4. In **Windows PowerShell**, type the following command, and then press Enter:

```
Get-Command -Module PSDesiredStateConfiguration
```

   The output shows that the DSC package installed successfully as a module in the previous demonstration, and then shows all the commands that are available in the module.

5. In **Windows PowerShell**, type the following command, and then press Enter:

```
Get-DscResource
```

   This command's output shows the various resources that DSC can manipulate in Nano Server.

6. At the command prompt, type the following cmdlet, replacing the *X* with your IP address's last octet, and then press Enter:

```
$ip = "172.16.0.X"
```

7. At the command prompt, type the following command, and then press Enter:

```
$cred = Get-Credential
```

8. In the **Windows PowerShell Credential Request** window, in the **User name** text box, type **Adatum\administrator**, and in the **Password** text box, type **Pa55w.rd**, and then click **OK**.
9. At the command prompt, type the following command, and then press Enter:

```
Enter-PSSession -ComputerName $ip -Credential $Cred
```

10. At the command prompt, type the following command, and then press Enter:

```
Cd C:\demo
```

11. At the command prompt, type the following command, and then press Enter:

```
.\Demo2DscNanoConfig.ps1 -nodes localhost
```

    The script will return an .MOF file named **NANO-SVR1.MOF**.

12. At the command prompt, type the following command, and then press Enter:

```
Start-DscConfiguration -ComputerName "NANO-SVR1" -Wait -Force -Verbose -Path
.\NanoConfig
```

13. The **Wait** parameter stops for a few seconds to run the node. The command runs successfully, which verifies that the vmms service is running on NANO-SVR1.

14. At the command prompt, type the following command, and then press Enter:

```
Exit-PSSession
```

15. Close all open windows, and then sign out of **LON-DC1**.

Lesson 3

Understanding containers

Contents:

Question and Answers

Categorize Activity

Question: Categorize each item below.

Items	
1	Provides an operating-system environment
2	Only features a user mode
3	Provides an extra isolation boundary that has its own copy of the operating system binaries
4	Much of the user interface, the application stack, and the traditional .NET Framework is removed
5	You can use this image multiple times to deploy apps without changing the underlying layers
6	Automatically creates a Hyper-V virtual machine by using a base image
7	You can use it as a platform for a Windows container
8	Uses a shared kernel
9	Provides the isolation required to allow untrusted apps to run on the same host

Category 1		Category 2		Category 3
Nano Server		A Windows Server container		A Hyper-V container

Answer:

Category 1		Category 2		Category 3
Nano Server		A Windows Server container		A Hyper-V container
Provides an operating-system environment Much of the user interface, the application stack, and the traditional .NET Framework is removed You can use it as a platform for a Windows container		Only features a user mode You can use this image multiple times to deploy apps without changing the underlying layers Uses a shared kernel		Provides an extra isolation boundary that has its own copy of the operating system binaries Automatically creates a Hyper-V virtual machine by using a base image Provides the isolation required to allow untrusted apps to run on the same host

Demonstration: Deploying and managing Windows Server containers

Demonstration Steps

Examine the Microsoft Docker Image Repository

1. On **LON-HOST1**, if necessary, right-click **Start**, and then click **Windows PowerShell (Admin)**.
2. In the **Windows PowerShell** window, type the following to view the downloaded images, and then press Enter:

```
Docker search Microsoft
```

Download a prebuilt Docker images

1. Type the following command, and then press Enter to view the images available on the Docker Hub:

```
Docker images
```

2. In the **Windows PowerShell** window, type the following command to download the sample IIS image, and then press Enter:

```
docker run hello-world:nanoserver
```

3. Wait a few minutes for the image to download. Review the text on the screen that explains this image.

Note: The cmdlet takes about 2 minutes to run, and returns the following lines:

```
Hello from Docker!
This message shows that your installation appears to be working correctly.
To generate this message, Docker took the following steps:
 1. The Docker client contacted the Docker daemon.
 2. The Docker daemon pulled the "hello-world" image from the Docker Hub.
 3. The Docker daemon created a new container from that image which runs the
    executable that produces the output you are currently reading.
 4. The Docker daemon streamed that output to the Docker client, which sent it
    to your terminal.
```

4. In the **Windows PowerShell** window, type the following to verify the downloaded image, and then press Enter:

```
docker images
```

5. You should see three Docker images:
   a. microsoft/iis
   b. microsoft/nanoserver
   c. hello-world

Deploy a new container with the prebuilt image

- In the **Windows PowerShell** window, type the following to deploy the **IIS** container, and then press Enter:

```
docker run -d -p 80:80 microsoft/iis ping -t localhost
```

Note: This command runs the **IIS** image as a background service (**-d**). It also configures networking such that port 80 of the container host maps to port 80 of the container.

Manage the container

1. In the **Windows PowerShell** window, type the following to view the running containers, and then press Enter:

```
docker ps
```

2. Note the data from the first column under **Container ID** heading, which is a long string of characters (for example, fd85c4dbffba). You can use this to stop the container. In the **Windows PowerShell** window, type the following to view the running containers, and then press Enter:

```
Docker stop <Container ID>
```

Note: Replace <Container ID> shown above with the string returned from the **Docker ps** cmdlet you ran in Step 1.

Demonstration: Deploying Hyper-V containers

Demonstration Steps

1. In **Windows PowerShell** on **LON-HOST1**, type the following commands, and then press Enter:

```
Ipconfig
hostname
```

2. Note the IP Address and hostname are for **LON-HOST1**.
3. In **Windows PowerShell**, type the following command, and then press Enter:

```
docker run -it --isolation=hyperv microsoft/nanoserver cmd
```

4. After the above command completes, note that within the **Windows PowerShell** console, a command console with a black background will open. At the prompt, type the following commands, and then press Enter:

```
Ipconfig
hostname
```

5. Note the **IP Address** is not the same as that noted in Step 2 above, and the hostname is a long string of characters. This is the nanoserver you just created.
6. On **LON-HOST1**, click Start, and then click **Windows PowerShell**. This will open an additional **Windows PowerShell** console.
7. In the new **Windows PowerShell** window, type the following to view the running containers, and then press Enter:

```
docker ps
```

8. Note the data from the first column under **Container ID** heading, which is a long string of characters (for example, fd85c4dbffba). In the new **Windows PowerShell** window, type the following to stop the running container, and then press Enter:

```
Docker stop <Container ID>
```

9. Replace with the Container ID from the Docker ps cmdlet in step 7 above.
10. Close all open windows.

Module Review and Takeaways

Best Practices

- After installing SCM 3.0 on the main client computer or server, share the **LocalGPO** folder so that standalone and workgroup devices can access it easily.
- For a full graphical experience, manage Docker on Nano Server from a remote system that has GUI capabilities.
- If you want to share persistent data between containers, or you want to use data from nonpersistent containers, you should create a named Data Volume Container, and then mount the data from it.

Review Question

Question: What is the most secure processing environment you can have: Nano Server, Windows Containers, or Hyper-V Containers?

> **Answer:** Hyper-V containers are more secure than Windows containers, which are more secure than a traditionally deployed server operating system. You can host containers on Nano Server, which provides a quick and easy way of deploying a container, but using a Hyper-V Container on a Nano Server provides the best security of the three options.

Tools

Tool	Purpose	Where to find
SCM	Create, manage, and deploy security baselines for various Windows products and operating systems.	Free download from Microsoft.com
Docker Enterprise Edition for Windows Server 2016	Docker allows containers to run as isolated processes in user space on the host operating system, regardless of the operating system.	https://aka.ms/y6lgzc
GitHub	Deploy Hyper-V containers on Windows Server	https://aka.ms/puavgj

Lab Review Questions and Answers

Lab A: Using SCM

Question and Answers

Question: If **LON-SVR2** is a standalone server in a workgroup, what must you do to apply the security settings that you created in the **Member Server Merged 2012-2016** baseline to it?

Answer: You can use the LGPO.exe command-line tool. Otherwise, you must add the security settings manually.

Question: What should you do to merge two different product baselines in SCM?

Answer: You must associate the products first.

Lab B: Deploying and configuring Nano Server

Question and Answers

Question: What does the Windows PowerShell command shown below do?

```
Docker search Microsoft
```

Answer: It lists all the different prebuilt functions and roles for Windows containers that Microsoft created.

Question: What does the Windows PowerShell command shown below do?

```
Get-Command -Module PSDesiredStateConfiguration
```

Answer: It shows that the DSC package was installed successfully as a module, and then shows all the commands that are available in the module.

Module 10

Planning and protecting data

Contents:

Lesson 1

Planning and implementing encryption

Contents:

Question and Answers

Question: You need a public key to decrypt an EFS-encrypted file.

( ) True

( ) False

Answer:

( ) True

(√) False

Feedback:

The public key is for encrypting the file. For decrypting the file, you need a private key.

Question: If users have an appropriate private key, can they always decrypt an EFS-encrypted file?

( ) True

( ) False

Answer:

( ) True

(√) False

Feedback:

Users can decrypt the file only if they can access it. If they do not have file permissions to access the file, they cannot decrypt the file.

Question: You need a CA in your network to encrypt files by using EFS.

( ) True

( ) False

Answer:

( ) True

(√) False

Feedback:

A CA is not required to use EFS. We recommend that you use CA-issued certificates for EFS, but you also can use self-signed certificates.

Overview of EFS

Question: Does EFS use symmetric encryption or public key encryption?

Answer: EFS uses a combination of both encryption methods. It uses symmetric encryption to encrypt the file's contents, and it uses public key encryption to encrypt and protect the symmetric key that is used for file encryption.

Question: Who can open a file that is encrypted by using EFS?

Answer: To open an EFS-encrypted file, the user must have file permissions to access the file. However, the user also must have the appropriate private key, with which they decrypt the symmetric key. The user then uses the symmetric key to decrypt and open the encrypted file. If the user has an appropriate private key, this process is transparent, and they can open the file as if it were not encrypted. If the user does not have the appropriate private key, the user will see an Access denied error.

EFS and certificates

Question: Why must users have certificates before they can encrypt files by using EFS?

> **Answer:** EFS uses the user's public key to encrypt the symmetric key that is randomly generated for encrypting each file. If a user does not have a public key, EFS is not able to encrypt and protect the symmetric key. In this scenario, EFS will obtain the user certificate and then perform encryption.

Question: Can you share EFS-encrypted files with other users?

> **Answer:** Yes, you can share EFS-encrypted files with other users. To do this, however, the user's public key must be available. This is because EFS uses their public key to encrypt the symmetric key.

Recovering EFS-encrypted files

Question: How it is possible for the data recovery agent to decrypt any EFS-encrypted file?

> **Answer:** If you configure the data recovery agent in the environment, EFS encrypts a copy of the symmetric key with the public key of the recovery agent and adds it to the file during encryption. The data recovery agent can use their private key to decrypt their copy of the symmetric key and use it to decrypt the file.

Question: If you do not have the appropriate private key to decrypt the file, can you copy an EFS-encrypted file from the device on which it was encrypted to the dedicated workstation of the data recovery agent?

> **Answer:** No. If you do not have the appropriate private key to decrypt the file, you cannot copy the EFS-encrypted file between the workstations. The copy operation includes a read operation of the original file. If you do not have the appropriate private key, you cannot open and read the file. You should back up the encrypted files and restore them on the dedicated workstation of the data recovery agent.

Resolving common EFS issues

Question: How can a user who lost their private key transfer EFS-encrypted files to the dedicated workstation of the data recovery agent?

> **Answer:** The user does not have the appropriate private key, so they cannot copy encrypted files. However, the user can back up encrypted files and then transfer the backup to the dedicated workstation of the data recovery agent.

Question: How long after you add the new data recovery agent will they need to wait before they will be able to decrypt files?

> **Answer:** The Data Recovery Field (DRF) of the already encrypted files does not update automatically. The DRF of the encrypted files is updated when a user with the appropriate private key views their properties or runs the cipher **/U** command.

Resources

Overview of EFS

Additional Reading: For more information, refer to: How EFS Works at: http://aka.ms/Uw9drx

Recovering EFS-encrypted files

Additional Reading: For more information, refer to Key Recovery vs Data Recovery Differences at: http://aka.ms/Frtdxi

Demonstration: Using EFS to secure data

Demonstration Steps

1. On **LON-CL1**, in the taskbar, click the **Start** icon, type **certmgr.msc**, and then press Enter.
2. In the **Certificates - Current User** console, in the navigation pane, click **Personal**, and then in the details pane, verify that there are no items to show in this view.
3. In the taskbar, click the **File Explorer** icon.
4. In File Explorer, in the navigation pane, expand **This PC**, expand **Local Disk (C:)**, expand **Labfiles**, and then select **Mod10**. In the details pane, right-click **Adam1**, select **Properties**, and then click **Advanced**.
5. In the **Advanced Attributes** dialog box, point out that the **Details** button is dimmed and unavailable, as the file is not yet encrypted. Select the **Encrypt contents to secure data** check box, and then click **OK**. Click **Apply**, select the **Encrypt the file only** option, and then click **OK**.
6. Wait a few seconds and then explain that encryption of the user's first file takes a few seconds, because EFS must obtain a user certificate before encrypting the file.
7. In the **Adam1 Properties** dialog box, click **Advanced**, and then click **Details**. Point out that Adam Hobbs can access the file and that the Administrator has a recovery certificate for the file.
8. Click **Add**, and in the **Encrypting File System** dialog box, point out that only Adam Hobbs is listed, and then explain that Adam is the only user who currently has a public key. Click **Cancel** four times.
9. In File Explorer, point out that the file **Adam1** has a small key lock icon because it is protected by EFS. Point out that other files in the folder do not have a key lock icon.
10. In the **Certificates - Current User** console, refresh the view by pressing the **F5** key. In the navigation pane, expand **Personal**, and then click **Certificates**. In the details pane, point out that one certificate is listed, and show that it is issued to Adam Hobbs is for encrypting the file system.
11. On the taskbar, click the **Start** icon, click **Adam Hobbs**, and then click **Switch account**.
12. Sign in to **LON-CL1** as the user **ADATUM\Dawn** with the password **Pa55w.rd**.
13. On the taskbar, click the **File Explorer** icon.
14. In File Explorer, in the navigation pane, expand **This PC**, expand **Local Disk (C:)**, expand **Labfiles**, and then select **Mod10**.
15. In the details pane, double-click **Adam1**, and point out that you get an "Access denied" error, as Dawn does not have Adam's private key to unencrypt the file. Click **OK**, and then close Notepad.

16. In File Explorer, in the details pane, right-click **Don1**, and then select **Properties**.
17. In the **Properties** dialog box, click **Advanced**. Select the **Encrypt contents to secure data** check box, click **OK**, and then click **OK**. Select **Encrypt the file only**, select the **Always encrypt only the file** check box, and then click **OK**.
18. Wait a few seconds and point out that this is the first file that Dawn is encrypting. Explain that because of that, EFS must obtain a user certificate and encryption takes a bit longer than when a user already has EFS certificate.
19. In the **Don1 Properties** dialog box, click **Advanced**, and then click **Details**. Point out that Dawn Williamson can access the file and that Administrator has a recovery certificate for the file.
20. Click **Add**, select **Adam Hobbs**, and then click **OK**. Point out that now Adam Hobbs and Dawn Williamson can access the file, and then click **OK** three times.
21. On the taskbar, click the **Start** icon, click **Dawn Williamson**, and then select **ADATUM\Adam**.
22. Sign in to **LON-CL1** as user **ADATUM\Adam** with the password **Pa55w.rd**.
23. In File Explorer, double-click **Don1**. Verify that the file opens and that you can read the content. Explain that Dawn provided Adam with access to the encrypted file.
24. Close Notepad.

Lesson 2

Planning and implementing BitLocker

Contents:

Question and Answers

Question: To use BitLocker, your device must have a TPM.

( ) True

( ) False

Answer:

( ) True

(√) False

Feedback:

Windows 10 enables you to use BitLocker without a TPM.

Question: BitLocker-protected drives from Windows 8.1 can be unlocked on Windows 10.

( ) True

( ) False

Answer:

( ) True

(√) False

Feedback:

BitLocker from earlier Windows versions is compatible with Windows 10. In Windows 10 version 1511 and newer, you can use the new BitLocker encryption mode, which is not backward-compatible.

Question: When you turn on BitLocker for drive C, you can also specify to store the recovery key in AD DS.

( ) True

( ) False

Answer:

( ) True

(√) False

Feedback:

When you turn on BitLocker for a drive, you can specify where to store the recovery drive, but you can select only a USB flash drive, a file, a Microsoft account, or to print it. You cannot store the BitLocker recovery key to AD DS in a wizard. You can do that only by using Group Policy.

Overview of BitLocker

Question: Can you use BitLocker to encrypt only confidential data on the volume, leaving other data on the volume unencrypted?

Answer: No. When you turn on BitLocker on each volume, all the volume data is encrypted.

Question: Can you use BitLocker to encrypt all volumes on a Windows device?

Answer: No. BitLocker cannot encrypt system volumes, but it can encrypt all other volumes, regardless of the file system.

BitLocker and TPMs

Question: How can you configure BitLocker to work on a device without a TPM?

> **Answer:** By default, BitLocker requires a TPM. If a device does not have a TPM, you can use Group Policy to allow BitLocker without a TPM. In such case, you must provide a USB startup key for BitLocker to encrypt a volume.

Question: What is a disadvantage of running BitLocker on a Windows device that does not have a TPM?

> **Answer:** You can still encrypt volumes on Windows device, even if it does not have a TPM. However, Windows devices without TPMs will not be able to use the system-integrity verification during startup.

Configuring and managing BitLocker

Question: Which tools can you use for configuring and managing BitLocker?

> **Answer:** You can configure and manage BitLocker by using the BitLocker Drive Encryption tool in Control Panel, Windows PowerShell cmdlets, BitLocker Drive Encryption Configuration Tool (Manage-bde.exe), and also the MBAM tool, if your company is licensed to use the MDOP.

Question: You enabled the **Store BitLocker recovery information in Active Directory Domain Services (Windows Server 2008 and Windows Vista)** Group Policy setting on a Windows 10 device. Is the BitLocker recovery information stored in AD DS when you enable BitLocker?

> **Answer:** No. This Group Policy setting applies only to Windows Server 2008 and Windows Vista; it does not apply to Windows 10. If you want to store a BitLocker recovery key on a Windows 10 device, you must enable the **Choose how BitLocker-protected operating system drives can be recovered**, **Choose how BitLocker-protected fixed drives can be recovered**, or **Choose how BitLocker-protected removable drives can be recovered Group Policy** options.

Recovering a BitLocker-encrypted drive

Question: When turning on BitLocker on a device with a TPM, what is the purpose of saving the recovery password?

> **Answer:** If the TPM ever changes or cannot be accessed, if there are changes to key system files, or if someone tries to start the device from a startup media to circumvent the operating system, the device will switch to the recovery mode and will remain there until the user provides the recovery password. Storing the recovery password so that it is accessible to the user allows the user to complete the startup process.

Question: What is the difference between the recovery password and the password ID?

> **Answer:** The recovery password is a 48-digit password that unlocks a BitLocker-protected drive. The recovery password is unique to a particular BitLocker encryption, and you can store it in AD DS, on a USB flash drive, or to a file. A password ID is a 32-character ID that is unique to an encrypted drive. You can find the password ID on the **BitLocker Recovery** tab on the property page for computer object in Active Directory Users and Computers.

Managing BitLocker by using Microsoft BitLocker Administration and Monitoring

Question: How can you use MBAM to reduce the time that the help desk spends recovering a BitLocker unlock key for a remote user?

> **Answer:** Administrators can enable the MBAM Self-Service Portal to allow users to recover a BitLocker recovery password without having to call their help desk.

Question: Your company uses only Windows 10 devices that are protected by BitLocker and managed by Microsoft Intune. Can you deploy MBAM in your company?

> **Answer:** MBAM requires AD DS and SQL Server. Because your company is using only Windows 10 devices, it does not meet the prerequisites and you cannot deploy MBAM in the company.

Resources

Overview of BitLocker

Additional Reading: For more information, refer to BitLocker Overview at: http://aka.ms/eiaxj5

Configuring and managing BitLocker

Additional Reading: For more information, refer to BitLocker: Use BitLocker Drive Encryption Tools to manage BitLocker at: http://aka.ms/kyndxu

Additional Reading: For more information, refer to BitLocker Group Policy Settings at: http://aka.ms/Bvxso5

Managing BitLocker by using Microsoft BitLocker Administration and Monitoring

Additional Reading: For more information, refer to Microsoft BitLocker Administration and Monitoring at http://aka.ms/L3su1s

Demonstration: Using BitLocker

Demonstration Steps

1. On **LON-CL1**, on the taskbar, click the **Start** icon, type **gpedit.msc**, and then press Enter.
2. In the Local Group Policy Editor, in the navigation pane, expand **Computer Configuration**, expand **Administrative Templates**, expand **Windows Components**, and then expand **BitLocker Drive Encryption**.
3. In the navigation pane, click **Operating System Drives**, and then in the details pane, double-click **Require additional authentication at startup**.
4. In the **Require additional authentication at startup** dialog box, click **Enabled**. Verify that the **Allow BitLocker without a compatible TPM** check box is selected, and then click **OK**.

Note: Explain that this configuration is necessary only if the device does not have a TPM.

5. In the navigation pane, click the **Fixed Data Drives** node, and then in the details pane, double-click **Choose how BitLocker-protected fixed drives can be recovered**.
6. In the **Choose how BitLocker-protected fixed drives can be recovered** dialog box, click **Enabled**, and then click **OK**.
7. On **LON-CL1**, on the taskbar, click the **File Explorer** icon.

8. In File Explorer, in the navigation pane, expand **This PC**, click **Data (E:)**, right-click the empty space in the details pane, select **New**, click **Text Document**, type your name, and then press Enter.
9. In File Explorer, in the navigation pane, right-click **Data (E:)**, and then click **Turn on BitLocker**.
10. In the **BitLocker Drive Encryption (E:)** dialog box, select the **Use a password to unlock the drive** check box, in the **Enter your password** and **Reenter your password** text boxes, type **Pa55w.rd**, and then click **Next**.
11. On the **How do you want to back up your recovery key?** page, click **Save to a file**.
12. In the **Save BitLocker recovery key as** dialog box, in the navigation pane, click **This PC**, in the details pane, scroll down, double-click **Floppy Disk Drive (A:)**, click **Save**, and then click **Next**.
13. On the **Choose which encryption mode to use** page, click **Next**, and then click **Start encrypting**.
14. In File Explorer, in the navigation pane, point out that Local Disk (E:) has a small key lock icon.
15. In the **20744B-LON-CL1 Virtual Machine Connection** window, click the **File** menu, and then click **Settings**.
16. In the **Settings for 20744B-LON-CL1** window, in the navigation pane, below SCSI Controller, click **Hard Drive Disk1.vhd**, in the details pane, click **Remove**, and then click **OK**.
17. In the **20744B-LON-CL2 Virtual Machine Connection** window, click the **File** menu, and then click **Settings**.
18. In the **Settings for 20744B-LON-CL2** dialog box, in the navigation pane, click **SCSI Controller**, in the details pane, click **Hard Drive**, click **Add**, click **Browse**, navigate to **D:\Program Files\Microsoft Learning\20744\Drives**, click **Disk1.vhd**, click **Open**, and then click **OK**.
19. On the taskbar, click the **File Explorer** icon. In the navigation pane, point out that drive E is listed as **Local Disk (E:)** and that it has a small key lock icon.
20. In File Explorer, in the navigation pane, click **Local Disk (E:)**. The **BitLocker (E:)** dialog box opens.
21. In the **BitLocker (E:)** dialog box, in the text box, enter **Pa55w.rd**, and then click **Unlock**.
22. In File Explorer, in the navigation pane, point out that drive E appears as Data (E:) and no longer as Local Disk (E:).

 **Note:** In the details pane, point out that you can see the file with your name.

23. On **LON-DC1**, on the taskbar, click the **Server Manager** icon.
24. In Server Manager, click **Tools**, and then click **Active Directory Users and Computers**.
25. In Active Directory Users and Computers, in the navigation pane, expand **Adatum.com**, and then click **Computers**.
26. In the details pane, right-click **LON-CL1**, and then click **Properties**.
27. In the **LON-CL1 Properties** dialog box, click the **BitLocker Recovery** tab.

 **Note:** Point out that the BitLocker recovery password for the encrypted disk on **LON-CL1** is displayed.

Module Review and Takeaways

Review Questions

Question: Can you encrypt a whole volume by using EFS file encryption?

Answer: You can enable EFS at the file or folder level, but not at the volume level. However, you can enable EFS on all folders and files in the volume root folder, which would encrypt everything on that volume.

Question: Can you encrypt Windows system files by using EFS?

Answer: No. You cannot encrypt files that have the System attribute set by using EFS file encryption.

Question: Can you perform a full wipe of a lost Windows device?

Answer: No. Windows devices support only selective wipe. You can perform a selective wipe of a Windows device if the device is managed by Microsoft Intune, Microsoft System Center Configuration Manager, or some other mobile device management solution.

Lab Review Questions and Answers

Lab: Protecting data by using encryption and BitLocker

Question and Answers

Question: Why was the administrator on **LON-CL2** not able to open the **Adam1.txt** file although the account is a data recovery agent?

Answer: The administrator's data recovery certificate is stored only on the first domain controller by default. Because they did not have their data recovery certificate on **LON-CL2**, they were not able to open the file. After you imported the data recovery certificate, they were able to open the file.

Question: Why did you have to configure **LON-CL1** to allow BitLocker without a compatible TPM?

Answer: Virtual machines do not have a TPM. BitLocker requires a TPM by default and without modifying this requirement, you cannot use BitLocker on **LON-CL1**.

Module 11

Optimizing and securing file services

Contents:

Lesson 1

File Server Resource Manager

Contents:

Question and Answers

Question: Are quotas something that you would implement across all data or only in select locations?

> **Answer:** Answers might vary. However, quotas applied across all data might result in unintended consequences. You should undertake careful planning of quota settings before implementing quotas.

Question: In your environment, would you implement file screening?

> **Answer:** Answers will vary. However, you should carefully consider the implications of file screening before deploying it.

Demonstration: Installing and configuring FSRM

Demonstration Steps

Install the FSRM role service

1. If not already signed in, sign in to **LON-SVR1** as **Adatum\Administrator** with the password **Pa55w.rd**.
2. Click **Start**, and then click **Server Manager**, click **Manage**, and then click **Add Roles and Features**.
3. In the **Add Roles and Features Wizard**, click **Next**.
4. Confirm that **Role-based or feature-based installation** is selected, and then click **Next**.
5. Confirm that **LON-SVR1.Adatum.com** is selected, and then click **Next**.
6. On the **Select server roles** page, expand **File and Storage Services (2 of 12 Installed)**, expand **File and iSCSI Services (1 of 11 Installed)**, and then select the **File Server Resource Manager** check box.
7. In the **Add Roles and Features Wizard**, click **Add Features**.
8. Click **Next** twice to confirm role service and feature selection.
9. On the **Confirm installation selections** page, click **Install**.
10. When the installation completes, click **Close**.

Specify FSRM configuration options

1. In **Server Manager**, click **Tools**, and then click **File Server Resource Manager**.
2. In the **File Server Resource Manager** console, in the navigation pane, right-click **File Server Resource Manager (Local)**, and then click **Configure Options**.
3. In the **File Server Resource Manager Options** dialog box, click the **File Screen Audit** tab, and then select the **Record file screening activity in auditing database** check box.
4. Click **OK** to close the **File Server Resource Manager Options** dialog box. Close the **File System Resource Manager management** console.

Use Windows PowerShell to manage FSRM

1. In **Server Manager**, click **Tools**, and then click **Windows PowerShell**.
2. At the **Windows PowerShell** command prompt, type the following command, and then press Enter.

```
set-FSRMSetting -SMTPServer "SMTPServer" –AdminEmailAddress "fileadmin@adatum.com" –
FromEmailAddress "Lon-SVR1@adatum.com"
```

3. Close the **Windows PowerShell** window.

4. Open the **File Server Resource Manager** management console.
5. In the **File Server Resource Manager** window, in the navigation pane, right-click **File Server Resource Manager (Local)**, and then click **Configure Options**.
6. On the **Email Notifications** tab, review the configured options to confirm that they are the same as the options specified in the **Set-FSRMSetting** command.
7. Close all open windows.

Demonstration: Monitoring quota usage

Demonstration Steps

Create a quota

1. If not already signed in, sign in to **LON-SVR1** as **Adatum\Administrator** with the password **Pa55w.rd**.
2. Click **Start**, and then click **Server Manager**.
3. In **Server Manager**, click **Tools**, and then click **File Server Resource Manager**.
4. In **File Server Resource Manager**, expand the **Quota Management** node, and then click **Quota Templates**.
5. Right-click the **100 MB Limit** template, and then click **Create quota from template**.
6. In the **Create Quota** window, click **Browse**.
7. In the **Browse for Folder** window, expand **Allfiles (D:)**, expand **Labfiles**, expand **Mod11**, click **Data**, and then click **OK**.
8. In the **Create Quota** window, click **Create**.
9. In the **File Server Resource Manager** window, click **Quotas** to view the newly created quota.

Test a quota

1. Click **Start**, and then click the **Windows PowerShell** icon.
2. In the **Windows PowerShell** window, type the following two commands, and then press Enter after each command.

```
cd D:\labfiles\Mod11\data
Fsutil file createnew largefile.txt 130000000
```

3. Notice that the following message displays: **Error: There is not enough space on the disk**.
4. Close the **Windows PowerShell** window.

Demonstration: Implementing a file screen

Demonstration Steps

Create a file screen

1. In the **File Server Resource Manager** window, expand the **File Screening Management** node, and then click **File Screen Templates**.
2. Right-click the **Block Image Files** template, and then click **Create File Screen from Template**.
3. In the **Create File Screen** window, click **Browse**.

4. In the **Browser for Folder** window, expand **Allfiles (D:)**, expand **Labfiles**, expand **Mod11**, click **Data**, and then click **OK**.
5. In the **Create File Screen** window, click **Create**.

Test a file screen

1. Open **File Explorer**.
2. In the **File Explorer** window, expand **This PC**, and then expand **Allfiles (D:)**, expand **Labfiles**, and then click **Mod11**.
3. In **File Explorer**, click the **Home** tab, click **New Item**, and then click **Bitmap Image**.
4. Type **testimage**, and then press Enter.
5. Confirm that the file was successfully created.
6. Right-click **testimage**, and then click **Copy**.
7. Right-click **Data**, and then click **Paste**.
8. You will receive a message that you need permission to perform this action. Click **Cancel** to close the message box.
9. Close **File Explorer**.

Demonstration: Generating on-demand storage reports

Demonstration Steps

Generate a storage report

1. In **File Server Resource Manager**, in the navigation pane, click and right-click **Storage Reports Management**, and then click **Generate Reports Now**.
2. In the **Storage Reports Task Properties** dialog box, select the **Large Files** check box.
3. Click the **Scope** tab, and then click **Add**.
4. In the **Browse for Folder** window, click **Allfiles (D:)**, and then click **OK**.
5. In the **Storage Reports Task Properties** dialog box, click **OK**.
6. In the **Generate Storage Reports** dialog box, verify that **Wait for reports to be generated and then display them** is selected, and then click **OK** to generate the report.
7. In **File Explorer**, in the **Interactive** folder, right-click the html file, click **Open with**, click **Internet Explorer**, click **OK**, and examine the report.
8. Close the report window.
9. Close the **File Explorer** window.
10. Close the **File Server Resource Manager** window.
11. Close the **Server Manager** window.

Lesson 2

Implementing classification and file management tasks

Contents:

Question and Answers

Question: How could you use automatic classification in your environment?

> **Answer:** Answers will vary; some students might want to tie in automatic classification with AD RMS to provide a basic data loss prevention solution.

Demonstration: Configuring file classification

Demonstration Steps

Create a classification property

1. On **LON-SVR1**, click **Start**, and then click the **Server Manager** icon.
2. In the **Server Manager** console, click **Tools**, and then click **File Server Resource Manager**.
3. In **File Server Resource Manager**, expand **Classification Management**, click and then right-click **Classification Properties**, and then click **Create Local Property**.
4. In the **Create Local Classification Property** window, in the **Name** text box, type **Documents**, in the **Property Type** drop-down list, ensure that **Yes/No** is selected, and then click **OK**.

Create a classification rule

1. In **File Server Resource Manager**, expand **Classification Management**, click **Classification Rules**, and then, in the **Action** pane, click **Create Classification Rule**.
2. In the **Create Classification Rule** window, on the **General** tab, in the **Rule name** text box, type **Corporate Documents Rule**, and ensure that the **Enable** check box is selected.
3. In the **Create Classification Rule** window, in the **Scope** tab, click **Add**.
4. In the **Browse For Folder** window, expand **Allfiles (D:\)**, expand **Labfiles**, expand **Mod11**, click the **Documents** folder, and then click **OK**.
5. In the **Create Classification Rule** window, on the **Classification** tab, in the **Classification method** drop-down list, click **Folder Classifier**. In the **Property-Choose a property to assign to files** drop-down list, click **Documents**, and then, in the **Property-Specify a value** drop-down list, click **Yes**.
6. In the **Create Classification Rule** window, on the **Evaluation type** tab, click **Re-evaluate existing property values**, ensure that the **Aggregate the values** option button is selected, and then click **OK**.
7. In **File Server Resource Manager**, in the **Action** pane, click **Run Classification With All Rules Now**.
8. In the **Run classification** window, select the **Wait for classification to complete** radio button, and then click **OK**.
9. Review the **Automatic classification report** that displays in Windows Internet Explorer, and ensure that the report lists the same number of files that were classified in the **Documents** folder. There will be three files.
10. Close Internet Explorer.

Demonstration: Configuring file management tasks

Demonstration Steps

Create a file

1. On **LON-SVR1**, on the taskbar, click the **File Explorer** icon.
2. Go to **D:\Labfiles\Mod11\Documents**, right-click **Strategy1.txt** and then click **Copy**. Right-click in the right pane, and then click **Paste**.

Create a file management task

1. On **LON-SVR1**, click **Start**, and then click the **Server Manager** shortcut.
2. In **Server Manager**, click **Tools**, and then click **File Server Resource Manager**.
3. In **File Server Resource Manager**, select and then right-click the **File Management Tasks** node, and then click **Create File Management Task**.
4. In the **Task name** text box, type **Expire Documents**.
5. In the **Description** text box, type **Move old documents to another folder**.
6. Click the **Scope** tab.
7. In the **Scope** section, click **Add**.
8. Expand **Allfiles (D:)**, expand **Labfiles**, expand **Mod11**, click **Documents**, and then click **OK**.

Configure a file management task to expire documents

1. In the **Create File Management Task** window, click the **Action** tab.
2. On the **Action** tab, under Type, select **File expiration**.
3. In **Expiration directory**, type **D:\Labfiles\Mod11\Data**.
4. In the **Create File Management Task** window, click the **Condition** tab.
5. On the **Condition** tab, select the **File name patterns** check box, and then type ***Copy*** in the text box.
6. In the **Create File Management Task** window, click the **Schedule** tab.
7. Select **Monthly**, and then select the **Last** check box.
8. In the **Create File Management Task** window, click **OK**.
9. Right-click the **Expire Documents** task, and then click **Run File Management Task Now**.
10. In the **Run File Management Task** window, choose **Wait for task to complete**, and then click **OK**.
11. View the generated report, and confirm that one file was moved.
12. Click the **Expiration directory** link in the report header, and then expand the directories to view the expired file.
13. Open the **D:\Labfiles\Mod11\Documents** folder, and view the contents. The **Strategy1 - Copy.txt** file will not be there.
14. Close all open windows.

Lesson 3

Dynamic Access Control

Contents:

Question and Answers

Question: Which technologies are a requirement if you want to use Dynamic Access Control?

( ) Active Directory Domain Services

( ) Kerberos

( ) AD CS

( ) AD RMS

( ) AD FS

Answer:

(√) Active Directory Domain Services

(√) Kerberos

( ) AD CS

( ) AD RMS

( ) AD FS

Feedback:

Only AD DS and Kerberos are requirements for Dynamic Access Control, although file classification can use AD RMS.

Question: Dynamic Access Control in Windows Server 2016 supports both user and computer claims.

( ) True

( ) False

Answer:

(√) True

( ) False

Feedback:

Dynamic Access Control supports user and computer claims. The claims are based on attributes in AD DS and the values in those attributes.

Resources

Foundation technologies for Dynamic Access Control

Additional Reading: For more information on the changes in Kerberos v5 regarding Kerberos armoring, refer to: http://aka.ms/v54k6z

Implementing and configuring central access policies

Additional Reading: Download the Microsoft Data Classification Toolkit at: http://aka.ms/alw15o

Additional Reading: To troubleshoot Dynamic Access Control if your users are not receiving correct access, download the "Understand and Troubleshoot Dynamic Access Control in Windows Server 2012" guide at: http://aka.ms/w2d2fo

Demonstration: Configuring Dynamic Access Control

Demonstration Steps

Prepare AD DS for Dynamic Access Control

1. On **LON-DC1**, in **Server Manager**, click **Tools**, and then click **Active Directory Users and Computers**.
2. In the **Active Directory Users and Computers** window, right-click **Adatum.com**, click **New**, and then click **Organizational Unit**.
3. In the **New Object – Organizational Unit** dialog box, in the **Name** text box, type **DAC-Protected computers**, and then click **OK**.
4. Click the **Computers** container, right-click **LON-SVR1**, and then click **Move**.
5. In the **Move** window, click **DAC-Protected computers**, and then click **OK**.
6. Switch to the **Server Manager** window, click **Tools**, and then click **Group Policy Management**.
7. Expand **Forest: Adatum.com**, expand **Domains**, expand **Adatum.com**, and then click the **Group Policy Objects** container.
8. In the results pane, right-click **Default Domain Controllers Policy**, and then click **Edit**.
9. In **Group Policy Management Editor**, under **Computer Configuration**, expand **Policies**, expand **Administrative Templates**, expand **System**, and then click **KDC**.
10. In the details pane, double-click **KDC support for claims, compound authentication and Kerberos armoring**.
11. In the **KDC support for claims, compound authentication and Kerberos armoring** window, select **Enabled**, and in the **Options** section, from the drop-down list, select **Always provide claims**, and then click **OK**.
12. Close **Group Policy Management Editor** and **Group Policy Management Console**.
13. Click **Start**, and then click **Windows PowerShell**.
14. In the **Windows PowerShell** window, type **gpupdate /force**, and then press Enter. After Group Policy updates, close **Windows PowerShell**.
15. Switch to the **Active Directory Users and Computers** window.
16. In the navigation pane, click the **Research** OU, and in the content pane, right-click **Connie Vaughn**, and then click **Properties**.
17. In the **Connie Vaughn Properties** window, click the **Organization** tab. Ensure that the **Department** text box is populated with the value **Research**, and then click **Cancel**.
18. Close **Active Directory Users and Computers**.

Configure claims, resource properties, and central access rules

1. In **Server Manager**, click **Tools**, and then click **Active Directory Administrative Center**.
2. In the **Active Directory Administrative Center**, in the navigation pane, click **Dynamic Access Control**, and then double-click **Claim Types**.
3. In the **Tasks** pane, click **New**, and then click **Claim Type**.
4. In the **Create Claim Type** window, in the **Source Attribute** section, locate and select **department**.
5. In the **Display name** text box, type **Company Department**.

6. Select both **User** and **Computer**, and then click **OK**.
7. In the **Active Directory Administrative Center**, click **Dynamic Access Control**, and then double-click **Resource Properties**.
8. In the **Resource Properties** list, right-click **Department**, and then click **Enable**.
9. Double-click **Department**.
10. Scroll down to the **Suggested Values** section, and then click **Add**.
11. In the **Add a suggested value** window, in both the **Value** and **Display name** text boxes, type **Research**, and then click **OK** two times.
12. Click **Dynamic Access Control**, and then double-click **Resource Property Lists**.
13. In the central pane, double-click **Global Resource Property List**, ensure that **Department** displays, and then click **Cancel**. If it does not display, click **Add**, and then add the property, and click **OK**.
14. In the navigation pane, click **Dynamic Access Control**, and then double-click **Central Access Rules**.
15. In the **Tasks** pane, click **New**, and then click **Central Access Rule**.
16. In the **Create Central Access Rule** dialog box, in the **Name** text box, type **Department Match**.
17. In the **Target Resources** section, click **Edit**.
18. In the **Central Access Rule** dialog box, click **Add a condition**.
19. In the last drop-down list, select **Research**. Verify that the condition is **Resource-Department-Equals-Value-Research**, and then click **OK**.
20. In the **Permissions** section, select **Use following permissions as current permissions**, and then click **Edit**.
21. Select the permission entry for **OWNER RIGHTS**, and then click **Remove**. Repeat this step for the **Administrators (ADATUM\Administrators)** and **SYSTEM** groups.
22. In the **Advanced Security Settings for Permissions** dialog box, click **Add**.
23. In the **Permission Entry for Permissions** dialog box, click **Select a principal**.
24. In the **Select User, Computer, Service Account, or Group** window, type **Authenticated Users**, click **Check Names**, and then click **OK**.
25. In the **Basic permissions** section, select **Modify**, **Read & Execute**, **Read**, and **Write**.
26. Click **Add a condition**.
27. From the **Group** drop-down list box, select **Company Department**, and from the **Value** drop-down list box, select **Resource**, and from the last drop-down list box, select **Department**, and then click **OK** three times.

Classify files manually

1. Switch to **LON-SVR1**.
2. Click **Start**, and then click **Server Manager**.
3. In **Server Manager**, click **Tools**, and then click **File Server Resource Manager**.
4. In **File Server Resource Manager**, expand **Classification Management**, click **Classification Properties**, right-click **Classification Properties**, and then click **Refresh**.
5. Verify that the **Department** property is listed.
6. In the taskbar, click the **File Explorer** icon.

7. In the **File Explorer** window, in the address bar, type **D:\Labfiles\Mod11**, press Enter, and in the content pane, right-click the **Research** folder, and then click **Properties**.
8. Click the **Classification** tab, click **Department**, and in the **Value** section, click **Research**, and then click **OK**.

Configure and deploy a central access policy

1. Switch to **LON.DC1**.
2. In the **Active Directory Administrative Center**, in the navigation pane, click **Dynamic Access Control**, and then double-click **Central Access Policies**.
3. In the **Tasks** pane, click **New**, and then click **Central Access Policy**.
4. In the **Name** text box, type **Department Match**, and then click **Add**.
5. Click the **Department Match** rule, click **>>**, and then click **OK** twice.
6. Close the **Active Directory Administrative Center**.
7. In **Server Manager**, click **Tools**, and then click **Group Policy Management**.
8. In **Group Policy Management Console**, right-click **DAC-Protected computers**, and then click **Create a GPO in this domain, and link it here**.
9. In the **New GPO** dialog box, in the **Name** text box, type **DAC Policy**, and then click **OK**.
10. Right-click **DAC Policy**, and then click **Edit**.
11. In the **Group Policy Management Editor** window, under Computer Configuration, expand **Policies**, expand **Windows Settings**, expand **Security Settings**, expand **File System**, right-click **Central Access Policy**, and then click **Manage Central Access Policies**.
12. Click **Department Match**, click **Add**, and then click **OK**.
13. Close **Group Policy Management Editor** and **Group Policy Management Console**.
14. Switch to **LON-SVR1**.
15. On **LON-SVR1**, click **Start**, and then click **Windows PowerShell**.
16. At the **Windows PowerShell** command prompt, type the following command, and then press Enter.

```
gpupdate /force
```

17. Close **Windows PowerShell**.
18. Switch to the **File Explorer** window.
19. In the **File Explorer** window, right-click the **Research** folder, and then click **Properties**.
20. In the **Research Properties** dialog box, click the **Security** tab, and then click **Advanced**.
21. In the **Advanced Security Settings for Research** window, click the **Central Policy** tab, and then click **Change**.
22. From the drop-down list box, select **Department Match**, and then click **OK** twice.

Demonstration: Configuring access-denied assistance

Demonstration Steps

1. Switch to **LON-DC1**.
2. On **LON-DC1**, in **Server Manager**, click **Tools**, and then click **Group Policy Management**.

3. In **Group Policy Management Console**, right-click **DAC Policy**, and then click **Edit**.
4. In the **Group Policy Management Editor** window, **under Computer Configuration**, expand **Policies**, expand **Administrative Templates**, expand **System**, and then click **Access-Denied Assistance**.
5. In the details pane, double-click **Customize message for Access Denied errors**.
6. In the **Customize message for Access Denied errors** window, click **Enabled**.
7. In the **Display the following message to users who are denied access** text box, type **You are denied access because of permission policy. Please request access**.
8. Select **Enable users to request assistance**, review other options, but do not make any changes, and then click **OK**.
9. In the details pane of **Group Policy Management Editor**, double-click **Enable access-denied assistance on client for all file types**, click **Enabled**, and then click **OK**.
10. Close **Group Policy Management Editor** and **Group Policy Management Console**.

Module Review and Takeaways

Best Practices

- Use quota templates to control and monitor the amount of data that groups store.
- Use file classification to identify and provide more granular control over certain types of data.

Review Questions

Question: How do FSRM templates for quotas and file screens provide a more efficient FSRM management experience?

> **Answer:** Templates enable administrators to create quotas and file screens quickly, based on predefined templates. You also can use templates to manage child quotas in a one-to-many manner. To change the file size for several quotas created from the template, you only need to change the template.

Question: How does access-denied assistance enhance the user experience?

> **Answer:** When the access-denied assistance feature is configured with easy-to-understand explanations and up-to-date contact information, it helps users understand why they cannot access a particular resource, and it enables you to direct them to the right contact who can provide them access.

Tools

Tool	What it is used for	Where to find it
File Server Resource Manager	Managing quotas, file screens, classification management, and storage reports	• Add FSRM role service from the **Add Roles and Features Wizard**, or by using **Windows PowerShell**. • Server Manager - Tools
Windows PowerShell	Manage FSRM	Windows PowerShell: `import-module FileServerResourceManager`

Common Issues and Troubleshooting Tips

Common Issue	Troubleshooting Tip
When you try to run a file management task at a command prompt, you might receive an error specifying that the task could not be found.	This occurs because the task name in the file server interface does not match the task name required by the command prompt. For example, you might create a task named Task1, but the name required by the command prompt is *FileManagement-Task1*.

Lab Review Questions and Answers

Lab A: Quotas and file screening

Question and Answers

Question: What criteria do you need to meet to use FSRM for managing a server's file structure?

Answer: The servers must be running Windows Server 2003 SP1 or newer to use FSRM. If you want to use FCI, you must be running Windows Server 2008 R2 or newer. Additionally, you must format the volumes on which you perform FSRM operations with NTFS.

Question: In what ways can classification management and file-management tasks decrease administrative overhead when dealing with a complex file and folder structure?

Answer: Classification management and file-management tasks can allow administrators to automate the manual classification and modification of files on a file server. Rather than inspecting files manually and performing manual file operations, administrators can set up FCI to classify files, and then perform the necessary operations on those files by using file management tasks.

Lab B: Implementing Dynamic Access Control

Question and Answers

Question: How do file classifications enhance Dynamic Access Control usage?

Answer: When you use file classifications, you can set attributes on files automatically, and then use those attributes in conditional expressions when you implement Dynamic Access Control.

Question: Can you implement Dynamic Access Control without central access policy?

Answer: Yes, you can set conditional expressions directly on resources.

Module 12

Securing network traffic with firewalls and encryption

Contents:

Lesson 1

Understanding network-related security threats

Contents:

Question and Answers

Discussion: Common network-related security threats

Question: What are some of the security threats that you are familiar with?

Answer: Answers might vary but might include phishing emails, spyware, and ransomware.

Resources

Well-known ports

 **Additional Reading:** For a complete list of well-known ports and registered ports, refer to Service Name and Transport Protocol Port Number Registry: https://aka.ms/ivsdso

Lesson 2

Understanding Windows Firewall with Advanced Security

Contents:

Question and Answers

Question: What are the benefits of using a host-based firewall, such as Windows Firewall with Advanced Security?

Answer: Windows Firewall with Advanced Security provides the following benefits:

- Computers have improved protection from attacks on the internal network. This can help to prevent malware from moving through the internal network by blocking unsolicited inbound traffic.
- Inbound rules help to prevent network scanning to identify hosts on the network. The simplest network scanners ping hosts on a network in an attempt to identify them. Windows Firewall with Advanced Security helps to prevent member servers from responding to ping requests. Domain controllers do respond to ping requests.
- When you enable outbound rules, they can prevent malware from spreading by preventing the malware from communicating on the network. In the case of a virus outbreak, you can configure computers with a specific outbound rule that helps to prevent the virus from communicating over the network.
- Connection security rules allow you to create sophisticated firewall rules that use computer and user-authentication information to limit communication with high-security computers.

Demonstration: How to use Windows Firewall to manage network traffic

Demonstration Steps

Create an inbound firewall rule

1. On **LON-DC1**, open a **Command Prompt** window, type the following, and then press Enter.

```
Ping LON-SVR2
```

Note: The result should be "Request timed out."

2. Switch to **LON-SVR2**, open a **Windows PowerShell** window, type the following, and then press Enter.

```
Test-Connection LON-DC1
```

Note: The ping to **LON-DC1** should be successful.

3. Click the **Start** button, and then click **Control Panel**.
4. Click **System and Security**, and then click **Windows Firewall**.
5. In the **Windows Firewall** window, click the **Advanced settings** link on the left side to open the **Windows Firewall with Advanced Security** management console.
6. Under **Windows Firewall with Advanced Security on Local Computer**, in the navigation pane, click **Inbound Rules**.
7. Right-click **Inbound Rules**, and then click **New Rule**.
8. In the **New Inbound Rule Wizard**, on the **Rule Type** page, click **Custom**, and then click **Next**.
9. On the **Program** page, click **All programs**, and then click **Next**.

10. On the **Protocol and Ports** page, in the **Protocol type** list, click **ICMPv4**, and then click **Next**.
11. On the **Scope** page, click **Next**.
12. On the **Action** page, click **Allow the connection**, and then click **Next**.
13. On the **Profile** page, click **Next**.
14. On the **Name** page, in the **Name** text box, type **Allow Ping Rule**, and then click **Finish**.
15. In the navigation pane, expand **Monitoring**, and then click **Firewall**.
16. Verify that the **Allow Ping Rule** was created.

Test the inbound firewall rule

- Switch to **LON-DC1**, type the following in the **Command Prompt** window, and then press Enter.

```
Ping LON-SVR2
```

 **Note:** The ping to **LON-SVR2** should be successful.

Create an outbound firewall rule

1. Switch to **LON-SVR2**, and then click **Outbound Rules**.
2. Right-click **Outbound Rules**, and then click **New Rule**.
3. In the **New Outbound Rule Wizard**, on the **Rule Type** page, click **Custom**, and then click **Next**.
4. On the **Program** page, click **All programs**, and then click **Next**.
5. On the **Protocol and Ports** page, in the **Protocol type** list, click **ICMPv4**, and then click **Next**.
6. On the **Scope** page, click **Next**.
7. On the **Action** page, click **Block the connection**, and then click **Next**.
8. On the **Profile** page, click **Next**.
9. On the **Name** page, in the **Name** text box, type **Prevent Ping Rule**, and then click **Finish**.
10. In the navigation pane, expand **Monitoring**, and then click **Firewall**.
11. Verify that the **Prevent Ping Rule** was created.

Test the outbound firewall rule

- In the **Windows PowerShell** window, type the following, and then press Enter.

```
Test-Connection LON-DC1
```

 **Note:** The result should be "Test-Connection : Testing connection to computer 'LON-DC1' failed: Unknown error (0x2b2a)."

Reset the firewall rules on LON-SVR2

1. Switch to the **Windows Firewall with Advanced Security** console, and then in the navigation pane, click **Windows Firewall with Advanced Security on Local Computer**.
2. In the **Actions** pane, click **Restore Default Policy**.
3. In the **Windows Firewall with Advanced Security** dialog box, click **Yes**, and then click **OK**.

4. Switch to the **Windows PowerShell** window, type the following, and then press Enter.

```
Test-Connection LON-DC1
```

Note: The ping to **LON-DC1** should be successful.

Lesson 3

Configuring IPsec

Contents:

Question and Answers

Question: In your environment, are you using IPsec, or would you use it?

> **Answer:** Answers will vary. To start the discussion, you can suggest using IPsec for perimeter zone systems or for VPN tunnels that traverse the public Internet.

Resources

What is IPsec?

Additional Reading: For more information, refer to What Is IPSec?: http://aka.ms/G0crt8

Demonstration: Creating and configuring connection security rules

Demonstration Steps

Allow ICMP traffic on LON-SVR1 if secure

1. Switch to **LON-SVR1**.
2. Open Server Manager, click **Tools**, and then click **Windows Firewall with Advanced Security**.
3. In **Windows Firewall with Advanced Security**, click and then right-click **Inbound Rules**, and then click **New Rule**.
4. In the **New Inbound Rule Wizard** dialog box, click **Custom**, and then click **Next**.
5. On the **Program** page, click **Next**.
6. On the **Protocols and Ports** page, in the **Protocol type** list, click **ICMPv4**, and then click **Next**.
7. On the **Scope** page, click **Next**.
8. On the **Action** page, click **Allow the connection if it is secure**, and then click **Next**.
9. On the **Users** page, click **Next**.
10. On the **Computers** page, click **Next**.
11. On the **Profile** page, click **Next**.
12. On the **Name** page, in the **Name** box, type **ICMPv4 allowed**, and then click **Finish**.

Create a server–to-server rule on connecting servers

1. On **LON-SVR1**, in **Windows Firewall with Advanced Security**, click and then right-click **Connection Security Rules**, and then click **New Rule**.
2. In the **New Connection Security Rule Wizard**, click **Server-to-server**, and then click **Next**.
3. On the **Endpoints** page, click **Next**.
4. On the **Requirements** page, click **Require authentication for inbound and outbound connections**, and then click **Next**.
5. On the **Authentication Method** page, click **Advanced**, and then click **Customize**.
6. In the **Customize Advanced Authentication Methods** dialog box, under **First authentication methods**, click **Add**.
7. In the **Add First Authentication Method** dialog box, click **Preshared Key**, type **secret**, and then click **OK**.

8. In the **Customize Advanced Authentication Methods** dialog box, click **OK**.
9. On the **Authentication Method** page, click **Next**.
10. On the **Profile** page, click **Next**.
11. On the **Name** page, in the **Name** box, type **Adatum-Server-to-Server**, and then click **Finish**.

Create a server-to-server rule on LON-CL1

1. Switch to **LON-CL1**.
2. If required, sign in as **Adatum\administrator** with the password **Pa55w.rd**.
3. In Cortana, type **Windows Firewall**, and then click **Windows Firewall with Advanced Security**.
4. Click and then right-click **Connection Security Rules**, and then click **New Rule**.
5. In the **New Connection Security Rule Wizard**, click **Server-to-server**, and then click **Next**.
6. On the **Endpoints** page, click **Next**.
7. On the **Requirements** page, click **Require authentication for inbound and outbound connections**, and then click **Next**.
8. On the **Authentication Method** page, click **Advanced**, and then click **Customize**.
9. In the **Customize Advanced Authentication Methods** dialog box, under **First authentication methods**, click **Add**.
10. In the **Add First Authentication Method** dialog box, click **Preshared Key**, type **secret**, and then click **OK**.
11. In the **Customize Advanced Authentication Methods** dialog box, click **OK**.
12. On the **Authentication Method** page, click **Next**.
13. On the **Profile** page, click **Next**.
14. On the **Name** page, in the **Name** box, type **Adatum-Server-to-Server**, and then click **Finish**.

Test the rule

1. In Cortana, type **cmd.exe**, and then press Enter.
2. At the command prompt, type **ping 172.16.0.11**, and then press Enter.
3. Switch to Windows Firewall with Advanced Security.
4. Expand **Monitoring**, expand **Security Associations**, and then click **Main Mode**.
5. In the **Main Mode** pane, double-click the listed item.
6. View the information in **Main Mode**, and then click **OK**.
7. Click **Quick Mode**.
8. In the **Quick Mode** pane, double-click the listed item.
9. View the information in **Quick Mode**, and then click **OK**.

Lesson 4

Datacenter Firewall

Contents:

Question and Answers

Question: In your environment, do you foresee using Datacenter Firewall or NSGs?

Answer: Answers will vary depending on the complexity of the networks the students work on.

Module Review and Takeaways

Review Questions

Question: When you configure a firewall rule to allow access to an application on a specific port, which network profile or profiles should the rule apply to?

Answer: The rule should apply to a network profile from which the traffic is expected.

Question: What are the advantages of using Datacenter Firewall in a private network environment?

Answer: Several advantages might be mentioned:

- It provides a software-based firewall solution that is integrated with Microsoft System Center Virtual Machine Manager; it can be managed by tenants or administrators; and it can be scaled to help small and large deployments of virtual machines.
- Firewall policies that are assigned to the virtual machines move along with the virtual machines when they are moved to a new host. This is possible because:
  - Datacenter Firewall is deployed as a vSwitch port host agent firewall.
  - Datacenter Firewall policies assigned by service provider tenants are independent of other tenants' firewall settings.
  - Each vSwitch port is configured independently of the host on which the virtual machine is running.
- It provides protection features for tenant virtual machines that are independent of the tenant guest operating system.

Question: For what scenarios do you use IPsec?

Answer: Answers will vary, but you can use IPsec for:

- Securing host-to-host traffic
- Securing traffic to servers
- Using L2TP
- Site-to-site (gateway-to-gateway) tunneling
- Enforcing logical networks

Question: You need to ensure that traffic is encrypted and authenticated as it passes between a computer in the perimeter network and a computer in your internal network. The computer in the perimeter network is not a member of your AD DS forest. What authentication methods can you use if you attempt to establish an IPsec rule between these two computers?

Answer: You cannot use Kerberos authentication because the perimeter computer is not in the forest. Therefore, you can use certificates or a preshared key.

Lab Review Questions and Answers

Lab: Configuring Windows Firewall with Advanced Security

Question and Answers

Question: You want to introduce a new application that needs to use specific ports. What information do you need to configure Windows Firewall with Advanced Security, and from which source can you get that information?

> **Answer:** You need to know which ports and IP addresses the application will use so that the application can run while still being protected from security threats. You can get this information from the application vendor.

Question: Explain why **LON-CL1** can connect to both **LON-SVR1** and **LON-SVR2** in the lab, but **LON-SVR2** cannot connect to **LON-SVR1**.

> **Answer: LON-SVR1** is configured for server isolation, and therefore only those computers that use IPsec to secure network traffic can connect to it. Because **LON-CL1** is in the Secure Clients OU, the Request Security policy is applied to it, and therefore it will request IPsec when connecting to another server. **LON-SVR2** does not have any security configured, so **LON-CL1** can connect to it without using IPsec. **LON-SVR2** cannot connect to **LON-SVR1** because **LON-SVR2** is not configured to request security, and **LON-SVR1** refuses all unsecured connections.

Module 13

Securing network traffic

Contents:

Lesson 1

Configuring advanced DNS settings

Contents:

Question and Answers

Question: DNS policies and RRL are new in Windows Server 2016. How would you use these new features in your environment?

> **Answer:** Answers will vary based on the student's approach to network security. Students with public-facing Windows DNS servers typically will implement RRL.

Resources

DNS policies

 **Additional Reading:** For more information, refer to Set-DnsServerQueryResolutionPolicy: http://aka.ms/D9e1pv

Demonstration: Configuring DNSSEC

Demonstration Steps

Configure DNSSEC

1. If you have not done so already, sign in to **LON-DC1** as **Adatum\Administrator** with the password **Pa55w.rd**.
2. In **Server Manager**, click **Tools**, and then in the drop-down list box, click **DNS**.
3. In **DNS**, expand **LON-DC1**, expand **Forward Lookup Zones**, and then select and right-click **Adatum.com**.
4. On the menu, click **DNSSEC>Sign the Zone**.
5. In the **Zone Signing Wizard**, click **Next**.
6. Click **Customize zone signing parameters**, and then click **Next**.
7. On the **Key Master** page, click **The DNS server LON-DC1 is the Key Master**, and then click **Next**.
8. On the **Key Signing Key (KSK)** page, click **Next**.
9. On the **Key Signing Key (KSK)** page, click **Add**.
10. On the **New Key Signing Key (KSK)** page, click **OK**.
11. On the **Key Signing Key (KSK)** page, click **Next**.
12. On the **Zone Signing Key (ZSK)** page, click **Next**.
13. On the **Zone Signing Key (ZSK)** page, click **Add**.
14. On the **New Zone Signing Key (ZSK)** page, click **OK**.
15. On the **Zone Signing Key (ZSK)** page, click **Next**.
16. On the **Next Secure (NSEC)** page, click **Next**.
17. On the **Trust Anchors (TAs)** page, select the **Enable the distribution of trust anchors for this zone** check box, and then click **Next**.
18. On the **Signing and Polling Parameters** page, click **Next**.
19. On the **DNS Security Extensions** page, click **Next**, and then click **Finish**.
20. In **DNS Manager**, expand **Trust Points**, expand **com**, and then click **Adatum**. Ensure that the DNSKEY resource records exist and that their status is valid.

21. In **Server Manager**, click **Tools**, and then in the drop-down list box, click **Group Policy Management**.
22. In the **Group Policy Management Console**, expand **Forest: Adatum.com**, expand **Domains**, expand **Adatum.com**, right-click **Default Domain Policy**, and then click **Edit**.
23. In the **Group Policy Management Editor**, under **Computer Configuration**, expand **Policies**, expand **Windows Settings**, and then click the **Name Resolution Policy** folder.
24. In the **Create Rules** section, in the **Suffix** field, type **Adatum.com** to apply the rule to the suffix of the namespace.
25. Select both the **Enable DNSSEC in this rule** and the **Require DNS clients to check that the name and address data has been validated by the DNS server** check boxes, and then click **Create**.
26. Scroll down, and then click **Apply**.
27. Close all open windows.

Demonstration: Configuring DNS policies and RRL

Demonstration Steps

Configure DNS policies

1. On **LON-DC1**, click **Start**, and then click **Windows PowerShell**.
2. To create a new client subnet for the London clients, type the following command at the Windows PowerShell command prompt, and then press Enter:

```
Add-DnsServerClientSubnet -Name "LondonSubnet" -IPv4Subnet "172.16.0.0/16" -PassThru
```

3. To create a new client subnet for the Paris clients, type the following command at the Windows PowerShell command prompt, and then press Enter:

```
Add-DnsServerClientSubnet -Name "ParisSubnet" -IPv4Subnet "172.17.0.0/16" -PassThru
```

4. To create a new zone scope for England, type the following command at the Windows PowerShell command prompt, and then press Enter:

```
Add-DnsServerZoneScope -ZoneName "adatum.com" -Name "adatum_england" -PassThru
```

5. To create a new zone scope for France, type the following command at the Windows PowerShell command prompt, and then press Enter:

```
Add-DnsServerZoneScope -ZoneName "adatum.com" -Name "adatum_france" -PassThru
```

6. To create a resource record to find the web server in England, type the following command at the Windows PowerShell command prompt, and then press Enter:

```
Add-DnsServerResourceRecord -ZoneName “adatum.com” -A -Name “www” -IPv4Address
172.16.0.11 -ZoneScope “adatum_england” -PassThru
```

7. To create a resource record to find the web server in France, type the following command at the Windows PowerShell command prompt, and then press Enter:

```
Add-DnsServerResourceRecord -ZoneName “adatum.com” -A -Name “www” -IPv4Address
172.17.0.11 -ZoneScope “adatum_france” -PassThru
```

8. To create the DNS policy for England, type the following command at the Windows PowerShell command prompt, and then press Enter:

```
Add-DnsServerQueryResolutionPolicy -Name “EnglandPolicy” -Action ALLOW -ClientSubnet
‘eq,LondonSubnet’ -ZoneScope ‘adatum_england,1’ -ZoneName “adatum.com” -PassThru
```

9. To create the DNS policy for France, type the following command at the Windows PowerShell command prompt, and then press Enter:

```
Add-DnsServerQueryResolutionPolicy -Name “FrancePolicy” -Action ALLOW -ClientSubnet
‘eq,ParisSubnet’ -ZoneScope ‘adatum_france,2’ -ZoneName “adatum.com” -PassThru
```

10. To view the defined DNS policies, type the following command at the Windows PowerShell command prompt, and then press Enter:

```
Get-DnsServerQueryResolutionPolicy -ZoneName adatum.com
```

11. To verify that name resolution is working, type the following command at the Windows PowerShell command prompt, and then press Enter:

```
Ping www.adatum.com
```

Note: The address www.adatum.com should resolve to 172.16.0.11.

12. To configure a time-based policy, type the following command at the Windows PowerShell command prompt, change the time range so that Paris is used 90 percent of the time from 9:00 AM to 5:00 PM, and then press Enter:

```
Add-DnsServerQueryResolutionPolicy -Name AdatumPeakPolicy -Action ALLOW -ZoneScope
‘adatum_england,1;adatum_france,9’ –TimeOfDay ‘EQ,09:00-17:00’ -ZoneName adatum.com -
ProcessingOrder 1 -PassThru
```

Note: Ensure that you include the current time in the **-TimeofDay** value.

13. To test name resolution, type the following command at the Windows PowerShell command prompt, and then press Enter:

```
Ping www.adatum.com
```

Note: The address www.adatum.com will resolve to 172.17.0.11 90 percent of the time. If it does not do so the first time, flush the DNS cache by typing **ipconfig /flushdns** at a command prompt, and then try again.

Configure RRL

1. To enable RRL with default settings, type the following command at the Windows PowerShell command prompt, and then press Enter:

```
Set-DNSServerRRL
```

2. When prompted to **Confirm** the command, type **Y**, and then press Enter.
3. Read the warning that displays.
4. To view the RRL settings, type the following command at the Windows PowerShell command prompt, and then press Enter:

```
Get-DNSServerRRL | FL
```

5. Verify that the RRL settings display.

Lesson 2

Examining network traffic with Message Analyzer

Contents:

Question and Answers

Question: For what types of troubleshooting issues would Message Analyzer be most helpful to use?

( ) Access denied to a file

( ) Access denied to a share

( ) Access denied to a website

( ) Slow connections

( ) All of the above

Answer:

( ) Access denied to a file

( ) Access denied to a share

( ) Access denied to a website

( ) Slow connections

(√) All of the above

Feedback:

Message Analyzer evaluates more than just network traffic, including Windows Event logs and text-based log files.

Demonstration: Installing Message Analyzer

Demonstration Steps

1. Switch to **LON-SVR1**.
2. Click **Start**, and then click **File Explorer**. In **File Explorer**, expand **This PC**, expand **Allfiles (D:)**, expand **Labfiles**, and then click the **Mod13** folder.
3. In the **Mod13** folder, double-click **MessageAnalyzer64.msi**.
4. In the **Microsoft Message Analyzer Setup Wizard**, on the **Welcome to the Microsoft Message Analyzer Setup Wizard** page, click **Next**.
5. On the **End-User License Agreement** page, select the **I accept the terms in the License Agreement** check box, and then click **Next**.
6. On the **Microsoft Message Analyzer Optimization** page, click **Next**.
7. On the **Ready to install Microsoft Message Analyzer** page, click **Install**.
8. On the **Completed the Microsoft Message Analyzer Setup Wizard** page, click **Finish**.
9. When the installation is complete, close all open windows and then restart **LON-SVR1**.
10. After the server restarts, sign in as **Adatum\Administrator** with the password **Pa55w.rd**.

Demonstration: Capturing and analyzing traffic with Message Analyzer

Demonstration Steps

Capture unencrypted network traffic

1. On **LON-SVR1**, click **Start**, expand the **Microsoft Message Analyzer** folder, and then click **Microsoft Message Analyzer**.

2. In the **Welcome to Microsoft Message Analyzer** dialog box, click both **Do not update items** and **No, I do not want to participate**, and then click **OK**.
3. Review the start page, and then click **Start Local Trace**.
4. After the capture begins, switch to **LON-CL1**.
5. On **LON-CL1**, click **Start**, type **\\lon-svr1\d$\Labfiles\Mod13**, and then press Enter:
6. Copy the **MessageAnalyzer64.msi** file to the local desktop.
7. Switch to **LON-SVR1**.
8. In the **Microsoft Message Analyzer**, click **Session**, and then click **Stop**.

Examine the Analysis tools

1. In the **Filter** field, type the following filter, and then click **Apply**:

```
*address==172.16.0.40
```

2. Click the **Module** header to sort by module.
3. Scroll through the traffic, and then show the various types of traffic captured.

Note: Tip: If you hover over a module name, a tool tip will display the full name.

4. If any **DiagnosisTypes** display, click one, and then show the error.
5. Scroll down until you see **SMB2** in the **Module** column.
6. Add a filter by right-clicking **SMB2** in the **Module** column, and then clicking **Add 'Module' to Filter**.
7. In the filter, change **OR** to **AND**, and then click **Apply**.
8. Examine the SMB2 traffic.

Enable IPsec in a Group Policy Object (GPO)

1. Switch to **LON-DC1**, and then open **Server Manager**.
2. In **Server Manager**, click **Tools**, and then click **Group Policy Management**.
3. In the **Group Policy Management Console**, expand **Forest: Adatum.com**, expand **Domains**, expand **Adatum.com**, right-click **Default Domain Policy**, and then click **Edit**.
4. In the **Group Policy Management Edito**r, under **Computer Configuration**, expand **Policies**, expand **Windows Settings**, expand **Security Settings**, and then click the **IP Security Policies on Active Directory (ADATUM.COM)**.
5. Right-click **Server (Request Security)**, and then click **Assign**.
6. Close all open windows.
7. Switch to **LON-SVR1**
8. Click **Start**, and then click **Windows PowerShell**.
9. At the Windows PowerShell command prompt, type the following command, and then press Enter:

```
GPUDPATE /Force
```

10. When the update completes, close the Windows PowerShell command prompt.
11. Switch to **LON-CL1**.

12. Click **Start**, type **Windows PowerShell**, and then click **Windows PowerShell**.
13. At the Windows PowerShell command prompt, type the following command, and then press Enter:

```
GPUDPATE /Force
```

14. When the update completes, close all open windows.

Capture encrypted network traffic

1. On **LON-SVR1**, in the **Global toolbar**, click **New Session**.
2. In the **New Session** dialog box, click **Live trace**, click **Select Scenario**, and then click **Local Network Interfaces (Win 8.1 and later)**.
3. Click **Start**.
4. After the capture begins, switch to **LON-CL1**.
5. On **LON-CL1**, click **Start**, type **\\lon-svr1\d$\Labfiles\Mod13**, and then press Enter.
6. Copy the **MessageAnalyzer64.msi** file to the local desktop. When prompted, choose to replace the file on the desktop.
7. Switch to **LON-SVR1**.
8. In the **Microsoft Message Analyzer**, click **Session**, and then click **Stop**.

Examine the Analysis tools

1. In the **Filter** field, type the following filter, and then click **Apply**:

```
*address==172.16.0.40
```

2. Click the **Module** header to sort by module.
3. Note that most of the captured traffic is of module ESP (IP Encapsulating Security Payload).
4. If any **DiagnosisTypes** display, click one, and then show the error.
5. Close all open windows.

Disable IPsec in the GPO

1. Switch to **LON-DC1**, and then open Server Manager.
2. In Server Manager, click **Tools**, and then click **Group Policy Management**.
3. In the **Group Policy Management Console**, expand **Forest: Adatum.com**, expand **Domains**, expand **Adatum.com**, right-click **Default Domain Policy**, and then click **Edit**.
4. In the Group Policy Management Editor, under **Computer Configuration**, expand **Policies**, expand **Windows Settings**, expand **Security Settings,** and then click the **IP Security Policies on Active Directory (ADATUM.COM)**.
5. Right-click **Server (Request Security)**, and then click **Un-Assign**.
6. Close all open windows.
7. Switch to **LON-SVR1**.
8. Click **Start**, and then click **Windows PowerShell**.
9. At the Windows PowerShell command prompt, type the following command, and then press Enter:

```
GPUDPATE /Force
```

10. When the update completes, close all open windows.
11. Switch to **LON-CL1**.
12. In Cortana, type **Windows PowerShell**, and then click **Windows PowerShell**.
13. At the Windows PowerShell command prompt, type the following command, and then press Enter:

```
GPUDPATE /Force
```

14. When the update completes, close all open windows.

Lesson 3

Securing and analyzing SMB traffic

Contents:

Question and Answers

Question: What is the risk associated with leaving SMB 1.x enabled in your environment?

> **Answer:** SMB 1.x is not a secure protocol. If it is enabled in your environment, you could be vulnerable to attacks that take advantage of SMB 1.x.

Resources

Understanding SMB 3.1.1 protocol security

 **Additional Reading:** For more information, refer to Microsoft Open Specifications Support Team Blog: http://aka.ms/Aldg7y

Demonstration: Disabling SMB 1.0, and configuring SMB encryption on shares

Demonstration Steps

Disable SMB 1.x on Windows 10

1. Switch to **LON-CL1**.
2. Click **Start**, type **Windows PowerShell**, and then click **Windows PowerShell**.
3. At the **Windows PowerShell command prompt**, type the following command, and then press Enter:

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

4. When prompted, press **Y**, and then press Enter.
5. Close all open windows.

Disable SMB 1.x on Windows Server 2016

1. Switch to **LON-SVR1**.
2. Click **Start**, and then click **Windows PowerShell**.
3. At the Windows PowerShell command prompt, type the following command, and then press Enter:

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

4. When prompted, press **Y**, and then press Enter.

Configure a share for SMB encryption

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

```
New-SmbShare –Name “Mod13” -Path “D:\Labfiles\Mod13” –EncryptData $true
```

2. At the Windows PowerShell command prompt, to provide full control permission on the share to Everyone, type the following command, and then press Enter:

```
Grant-FileShareAccess –Name Mod13 -AccountName “Everyone” -AccessRight Full
```

Capture encrypted SMB traffic

1. On **LON-SVR1**, click **Start**, expand the **Microsoft Message Analyzer** folder, and then click **Microsoft Message Analyzer**.
2. On the **Start** page, click **Start Local Trace**.
3. After the capture begins, switch to **LON-CL1**.
4. On **LON-CL1**, click **Start**, type **\\lon-svr1\Mod13**, and then press Enter.
5. Copy the **MessageAnalyzer64.msi** file to the local desktop. When prompted, choose to replace the file on the desktop.
6. Switch to **LON-SVR1**.
7. In the **Microsoft Message Analyzer,** click **Session**, and then click **Stop**.

Examine the Analysis tools

1. In the **Filter** filter, type the following filter, and then click **Apply**:

```
(*address==172.16.0.40) and (SMB2)
```

2. Click the **Summary** header to sort by module.
3. Note that most of the captured SMB2 traffic is **TransformMessage, Encrypted**.

Module Review and Takeaways

Review Questions

Question: In what scenarios would you consider using Message Analyzer as a troubleshooting tool?

> **Answer:** Answers will vary, but you can use Message Analyzer to identify illegitimate network traffic, and troubleshoot application or network issues.

Question: What are the risks if you disable SMB 1.0 communications? What are the risks if you do not disable this older protocol?

> **Answer:** SMB 1.0 is an old protocol that was developed without the same concern for security as SMB 3 or later. SMB 1.0 does not enforce encryption and is less secure. However, some old applications might still require this protocol, so these applications could fail if you disable SMB 1.0. If you do not disable SMB 1.0, you do not get the security features available with SMB 3 or later.

Lab Review Questions and Answers

Lab A: Securing DNS

Question and Answers

Question: Why did only Main Mode monitoring show that encryption was being used?

Answer: Encryption was configured for only the ICMPv4 protocol, and the quick mode session does not use ICMPv4.

Question: Why would you create a separate zone to use for DNSSEC?

Answer: Answers will vary. One reason would be to allow for different settings for different zones, so that if one zone is compromised, the other zones will not necessarily be compromised.

Lab B: Microsoft Message Analyzer and SMB encryption

Question and Answers

Question: With IPsec applied to all traffic, does a network capture provide any clues as to the traffic's purpose?

Answer: No. All the IPsec-protected traffic shows as ESP traffic, and there are no indicators as to what is in the packets.

Question: For your environment, would the IPsec or SMB 3.1.1 encryption method work better?

Answer: Answers will vary. You can configure IPsec to encrypt all network traffic, while SMB 3.1.1 only encrypts SMB traffic from Windows 10 or Windows Server 2016 shares.

Module 14

Updating Windows Server

Contents:

Lesson 1

Overview of WSUS

Contents:

Question and Answers

Question: Which of the following products can WSUS update?

( ) Microsoft Visual Studio 2010

( ) Microsoft Security Essential

( ) Microsoft Office 2010

( ) Microsoft Silverlight

( ) Windows RT

Answer:

(√) Microsoft Visual Studio 2010

(√) Microsoft Security Essential

(√) Microsoft Office 2010

(√) Microsoft Silverlight

(√) Windows RT

Feedback:

WSUS supports a wide variety of Microsoft products.

Resources

WSUS server deployment options

 **Additional Reading:** For more information, refer to: Determine Capacity Requirements at: http://aka.ms/Scktfu

Lesson 2

Deploying updates with WSUS

Contents:

Question and Answers

Question: Do you use multiple computer groups in your WSUS environment?

> **Answer:** Answers will vary. Some students might manually test updates and deploy them automatically after approval. Others might use an automated deployment for testing before a wider automated deployment.

Resources

WSUS troubleshooting

 **Additional Reading:** For more information, refer to: Windows Server Update Services Tools and Utilities at: http://aka.ms/Erqdqk

Demonstration: Approving updates by using WSUS

Demonstration Steps

1. On **LON-SVR1**, click **Start**, click **Windows Administrative tools**, and then click the **Windows Server Update Services** console.
2. In **Windows Server Update Services**, expand **LON-SVR1**, expand **Updates**, click **Critical Updates**, in the **Status** drop-down list, select **Any**, and then click **Refresh**.
3. Right-click **Update for Windows 10 Version 1607 for x64-based Systems (KB3199209)**, and then click **Approve**.
4. In the **Approve Updates** window, in the **All Computers** drop-down list, select **Approved for Install**.
5. Click **OK**, and then click **Close**.
6. Verify that the **Approval** column shows **Install**.
7. Close the **Update Services** console.

Module Review and Takeaways

Review Questions

Question: Your manager has asked if all updates to the Windows operating system should apply automatically when they are released. Do you recommend an alternative process?

> **Answer:** All updates should be tested before they are applied in a production environment. That is, you should first deploy updates to a set of test computers by using WSUS.

Question: Your organization implements several apps that are not Microsoft apps. A colleague has proposed using WSUS to deploy app and operating system updates. Are there any potential issues with using WSUS?

> **Answer:** Yes. WSUS is an excellent tool for deploying updates for Microsoft apps such as the Microsoft Office System and Windows operating system updates. However, WSUS does not deploy updates for all Microsoft apps, and it does not deploy updates for non-Microsoft apps. Microsoft System Center 2012 Configuration Manager is a better choice when you need to deploy updates for non-Microsoft apps.

Question: Why is WSUS easier to manage in an Active Directory Domain Services (AD DS) domain?

> **Answer:** WSUS takes advantage of the AD DS organizational unit (OU) structure for deploying client settings through Group Policy. You can also use Group Policy settings to configure client-side targeting to determine the WSUS group membership of a client computer.

Tools

The following table includes the tools that are needed for this module.

Tool	Use	Where to find it
WSUS Administration console	Administer WSUS	**Server Manager** - Tools
Windows PowerShell WSUS cmdlets	Administer WSUS from the command-line interface	Windows PowerShell

Lab Review Questions and Answers

Lab: Implementing update management

Question and Answers

Question: You created a separate group for the Research department. Why would you configure a separate group for part of your organization's computers?

Answer: The Research department might have special considerations or security practices that require a different process for testing and approving updates than the rest of the organization. Additionally, other departments might have administrators that have been delegated the responsibility for managing the update approval process.

Question: What is the advantage of configuring a downstream WSUS server?

Answer: If a slow wide area network (WAN) connection links the main WSUS server and the downstream server, the downstream WSUS server only downloads the updates once for the client computers it services, instead of each client computer downloading the update individually over the WAN connection from the main WSUS server.