Microsoft

OFFICIAL MICROSOFT LEARNING PRODUCT

20703-1B
Administering System Center Configuration Manager

Companion Content

Product Number: 20703-1B

Released: 04/2019

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

Managing computers and mobile devices in the enterprise

Contents:

Lesson 1

Overview of systems management by using enterprise management solutions

Contents:

Question and Answers

Question: Considering your environment, which features from Configuration Manager are you planning on implementing?

> **Answer:** Some of the students may have implemented Configuration Manager; some may be new to the product. Use this question to have a short conversation about how the students are planning on using Configuration Manager.

Resources

Overview of System Center and Enterprise Mobility + Security

Additional Reading: For more information about licensing System Center products, refer to: https://aka.ms/xq41ya

Lesson 2

Overview of the Configuration Manager architecture

Contents:

Question and Answers

Question: When deploying a stand-alone Configuration Manager site in a large organization, how can you support remote offices?

( ) Deploy secondary sites in the larger remote locations.

( ) Deploy additional primary sites in the larger remote locations.

( ) Deploy management points and distribution points in the smaller remote locations.

( ) Deploy a central administration site in the headquarters location and a single site for all the remote locations.

( ) Deploy a Service Connection point in each location to provide the local users with services.

Answer:

(√) Deploy secondary sites in the larger remote locations.

( ) Deploy additional primary sites in the larger remote locations.

(√) Deploy management points and distribution points in the smaller remote locations.

( ) Deploy a central administration site in the headquarters location and a single site for all the remote locations.

( ) Deploy a Service Connection point in each location to provide the local users with services.

Resources

Configuration Manager site server and site database requirements

Additional Reading: For more information, refer to: “Configuration Manager on Azure” at: https://aka.ms/ypz23o

Additional Reading: Additional roles have additional prerequisites. Before installing any additional roles, check the requirements at: Supported operating systems for Configuration Manager site system servers, refer to: http://aka.ms/ipxutw

Additional Reading: For more information, refer to: http://aka.ms/u0vhhq

Additional Reading: For more information, refer to: http://aka.ms/jdkx5i

Lesson 3

Overview of the Configuration Manager administrative tools

Contents:

Question and Answers

Categorize each item below.

Items	
1	Devices
2	Applications
3	Active Alerts
4	User Collections
5	Global Conditions
6	Queries
7	User State Migration
8	Automatic Deployment Rules
9	Deployments
10	Asset Intelligence
11	Driver Packages
12	Client Activity
13	Endpoint Protection
14	Servicing Plans
15	Site Servicing Status

Category 1		Category 2		Category 3
Assets and Compliance		Software Library		Monitoring

Answer:

Category 1		Category 2		Category 3
Assets and Compliance		Software Library		Monitoring
Devices User Collections User State Migration Asset Intelligence Endpoint Protection		Applications Global Conditions Automatic Deployment Rules Driver Packages Servicing Plans		Active Alerts Queries Deployments Client Activity Site Servicing Status

Demonstration: Exploring the nodes of the Configuration Manager console

Demonstration Steps

1. Sign in to LON-CFG as **Adatum\Administrator** with the password **Pa55w.rd**.
2. On the taskbar, click the **Configuration Manager console** icon.
3. Briefly discuss each node of the **Assets and Compliance** workspace, and explain how they are used.
4. Click the **Software Library** workspace.
5. Briefly discuss each node of the Software Library workspace, and explain how they are used.
6. Click the **Monitoring** workspace.
7. Briefly discuss each node of the Monitoring workspace, and explain how they are used.
8. Click the **Administration** workspace.
9. Briefly discuss each node of the Administration workspace, and explain how they are used.
10. When the demonstration is complete, close the **Configuration Manager console**.

Lesson 4

Tools for monitoring and troubleshooting a Configuration Manager site

Contents:

Question and Answers

Question: In your environment, which of these components would you regularly use to monitor your environment?

> **Answer:** Answers will vary, encourage the students to discuss the merits of each of the monitoring method discussed.

Demonstration: Viewing Site Status and Component Status

Demonstration Steps

View Site Status

1. If you are not already signed in to LON-CFG, sign in as **Adatum\Administrator** with the password **Pa55w.rd**.
2. On the taskbar, click the **Configuration Manager console** icon.
3. Click the **Monitoring** workspace, and expand the **System Status** folder.
4. Click the **Site Status** node.
5. Discuss the information that displays in the results pane.
6. Right-click the **Management point** status line, click **Show Messages**, and then click **All**.
7. In the **Status Messages: Set Viewing Period** dialog box, click **OK**.
8. Discuss the status messages, and demonstrate how to read the description by hovering the mouse pointer over a description.
9. Right-click one of the status messages, and click **Detail**.
10. Discuss the information in the **Status Message Details** dialog box, and close the **Status Message Details** dialog box.
11. Close the **Configuration Manager Status Message Viewer for <S01> <Adatum Site>** dialog box.

View Component Status

1. Click the **Component Status** node.
2. Discuss the information shown in the results pane, and point out how the component status differs from the site status.
3. Right-click the **SMS_EXECUTIVE** status line, click **Show Messages**, and then click **All**.
4. In the **Status Messages: Set Viewing Period** dialog box, click **OK**.
5. Discuss the messages, and then close all the open dialog boxes.

Demonstration: Using reports to view site information

Demonstration Steps

1. If you are not already signed in to LON-CFG, sign in to LON-CFG as **Adatum\Administrator** with the password **Pa55w.rd**.
2. If Configuration Manager is not already open, on the taskbar, click the **Configuration Manager console** icon.
3. Click the **Monitoring** workspace, and expand the **Reporting** folder.
4. Expand the **Reports** node, and click the **Administrative Security** folder.

5. In the results pane, right-click **Security roles summary**, and then to display the Security roles summary report, click **Run**.
6. Review the report, and close it.
7. Click the **Internet Explorer** icon.
8. In the Internet Explorer Address bar, type **http://LON-cfg/reports**, and then press Enter.
9. On the **SQL Server Reporting Services Home** page, click **ConfigMgr_S01**.
10. On the **SQL Server Reporting Services ConfigMgr_S01** page, click **Administrative Security**.
11. On the **SQL Server Reporting Services Administrative Security** page, click the **Administrative users security assignments** report.
12. Review the report, and close Internet Explorer.

Module Review and Takeaways

Best Practice

Supplement or modify the following best practices for your own work situations:

- Make sure you clearly differentiate between upgrading, updating, and installing. Best practices have changed to favor upgrade over migration, and each process is different with distinct uses. Be sure to review the mobile device management methods, as each method has distinct architectural and managerial requirements, advantages, and disadvantages.

Review Questions

Question: What are the three types of sites in Configuration Manager?

Answer: The three types of sites in Configuration Manager are:

- Central administration site
- Primary site
- Secondary site

Question: What is the difference between attributes and attribute values?

Answer: Attributes are the types of data collected, whereas attribute values are the actual values collected.

Question: What is the difference between a data query and a status message query?

Answer: You can use data queries to find any data in the Configuration Manager tables and to build collections. You can use status message queries to query only the stored status messages and to assist in the monitoring and troubleshooting of Configuration Manager.

Question: How many reporting services points can you have in your hierarchy? How many should you have in your hierarchy?

Answer: Answers will vary. You can have one or more reporting services points per primary site and central administration site. You should have at least one reporting services point in the central administration site, and at least one reporting services point in each primary site where local administrators need to view reports that include data from their site only.

Tools

Following are the tools you can use in Configuration Manager.

Tool	Use for	Where to find it
Configuration Manager Trace Log tool	Viewing log files	*InstallationPath*\Microsoft Configuration Manager\tools

Common Issues and Troubleshooting Tips

Common Issue	Troubleshooting Tip
Search results don’t seem to match your request	Try modifying your search slightly, and widen the search to experiment. Searching for a space can be helpful if a wide search shows no results.

Common Issue	Troubleshooting Tip
Console may not show objects after an operating system upgrade	Permissions on Configuration Manager files and folders should not be changed manually. WMI tools can also be helpful to reveal object access issues.

Lab Review Questions and Answers

Lab: Exploring the Configuration Manager tools

Question and Answers

Question: When would you use a local search?

Answer: Answers will vary. One possible answer is to find a single or related group of devices inside a collection.

Question: What is the benefit of saving a search?

Answer: Answers will vary. One possible answer is that when you conduct a complex search, you might want to save the results if you intend to refer to them frequently. In such cases, you do not have to recreate the search each time.

Question: What is the difference between Site Status messages and Component Status messages?

Answer: Site Status messages include all the status messages related to a particular role, which would include the status messages from all the components that are involved. Component Status messages contain only the status messages for that component.

Question: Why were some of the components in a stopped state?

Answer: Some components, such as the site backup, run only when they have work to perform.

Question: Why were there so many more entries between the milestones in the log file and the same milestones in the status messages?

Answer: Status messages generate only for significant events, such as milestones and errors, while the log files record every event that occurs, including milestones and errors.

Module 2

Analyzing data using queries, reports, and CMPivot

Contents:

Lesson 1

Introduction to queries

Contents:

Resources

What is a query?

Additional Reading: For more information, refer to: “Querying with WQL” at: https://aka.ms/xt617i

Demonstration: Creating and running queries

Demonstration Steps

Create a data query

1. On **LON-CFG**, if the **Configuration Manager** console is not open already, on the taskbar, click the **Configuration Manager Console** icon.
2. Click the **Monitoring** workspace, and then click **Queries**.
3. Right-click the **Queries** node, and then click **Create Query**.
4. In the **Create Query Wizard**, on the **General** page, in the **Name** box, type **All LON Systems**.
5. Click **Edit Query Statement**, and in the **All LON Systems Query Statement Properties** dialog box, on the **General** tab, click **New** (✳).
6. In the **Result Properties** dialog box, click **Select**.
7. In the **Select Attribute** dialog box, click the **Attribute** drop-down list, click **Active Directory Site Name**, and then click **OK**.
8. In the **Result Properties** dialog box, click **OK**.
9. In the **All LON Systems Query Statement Properties** dialog box, on the **General** tab, click **New** (✳).
10. In the **Result Properties** dialog box, click **Select**.
11. In the **Select Attribute** dialog box, click the **Attribute** drop-down list, click **IP Addresses**, and then click **OK**.
12. In the **Result Properties** dialog box, click **OK**.
13. In the **All LON Systems Query Statement Properties** dialog box, on the **General** tab, click **New** (✳).
14. In the **Result Properties** dialog box, click **Select**.
15. In the **Select Attribute** dialog box, click the **Attribute** drop-down list, click **Last Logon User Name**, and then click **OK**.
16. In the **Result Properties** dialog box, click **OK**.
17. In the **All LON Systems Query Statement Properties** dialog box, on the **Criteria** tab, click **New** (✳).
18. In the **Criterion Properties** dialog box, click **Select**.
19. In the **Select Attribute** dialog box, in the **Attribute class** list, click **System Resource**.
20. In the **Select Attribute** dialog box, in the **Attribute** list, click **Name**, and then click **OK**.
21. In the **Criterion Properties** dialog box, in the **Operator** drop-down list, click **is like**.
22. In the **Value** box, type **%LON%**, and then click **OK**.

23. In the **All LON Systems Query Statement Properties** dialog box, click **OK**.
24. In the **Create Query Wizard**, on the **General** page, click **Next**.
25. On the **Summary** page, click **Next**.
26. On the **Completion** page, click **Close**.

Run the data query

1. Right-click the **All LON Systems** query, and then click **Run**.
2. Review the results. Explain why the **Name** attribute does not display in the results pane.

Examine the Smsprov.log

1. Open File Explorer, and then browse to **C:\Program Files\Microsoft Configuration Manager\Logs**.
2. Scroll down, and then double-click the **Smsprov.log** file.
3. Click **Tools**, and then click **Find**. In the **Find** box, type **%LON%**, and then click **Find**.
4. Press the F3 key until the line containing the **Execute WQL =** … statement is selected.
5. Point out the attributes selected for the WMI query.
6. Select the line containing the **Execute SQL =** … statement, and examine the SQL query.
7. Close the Configuration Manager Trace Log tool.

Lesson 2
Configuring SQL Server Reporting Services

Contents:

Question and Answers

Installing a reporting services point

Question: In a multisite hierarchy, in which site should you install a reporting services point so that you can view reports about all sites in the hierarchy?

> **Answer:** You should install the reporting services point in the central administration site. This is because the database in the central administration site contains the data from every site within the hierarchy. A primary site only contains the data related to it and any secondary child sites.

Demonstration: Installing a reporting services point

Demonstration Steps

1. On **LON-CFG**, click **Start**, expand **Microsoft SQL Server 2016**, and then click **Reporting Services Configuration Manager**.
2. In the **Reporting Services Configuration Connection** dialog box, click **Connect**.
3. In **Reporting Services Configuration Manager:LON-CFG\MSSQLSERVER**, click the **Service Account** node.
4. Verify that the reporting services are configured to use the **Network Service** account.
5. Click the **Web Service URL** node, and then review the default settings. Click **Apply**.
6. On the **Database** page, click **Change Database**.
7. On the **Action** page, select **Create a new report server database**, and then click **Next**.
8. On the **Database Server** page, click **Next**.
9. On the **Database** page, click **Next**.
10. On the **Credentials** page, click **Next**.
11. On the **Summary** page, click **Next**.
12. On the **Progress and Finish** page, click **Finish**.
13. In **Reporting Services Configuration Manager:LON-CFG\MSSQLSERVER**, click the **Web Portal URL** node. Click **Apply**.
14. In **Reporting Services Configuration Manager:LON-CFG\MSSQLSERVER**, click **Exit**.
15. If necessary, open the **Configuration Manager** console.
16. Click the **Administration** workspace, and then expand **Site Configuration**.
17. Click **Servers and Site Systems Roles**.
18. Right-click **\\LON-CFG.Adatum.com**, and then click **Add Site System Roles**.
19. In the **Add Site System Roles Wizard**, on the **General** page, click **Next**.
20. On the **Proxy** page, click **Next**.
21. On the **System Role Selection** page, select the **Reporting services point** check box, and then click **Next**.
22. On the **Reporting services point** page, click **Verify**.
23. On the **Reporting Services Point** page, click **Set**, and then click **New Account**.
24. In the **User name** box, type **Adatum\Administrator**, in the **Password** and **Confirm password** boxes, type **Pa55w.rd**, and then click **OK**.

25. On the **Reporting services point** page, click **Next**.
26. Review the **Summary** page, click **Next**, and then on the **Completion** page, click **Close**.
27. In the **Monitoring** workspace, expand the **Reporting** node, and then click the **Reports** node. You might have to refresh the console until all the reports appear.

Note: Note that this might take several minutes to complete.

28. Right-click the **Reports** node, and then click **Report Options**. Review the **Report Options** dialog box, and then click **OK**.
29. In the **Search** box, type **Windows**, and then click **Search**.
30. Right-click the **Windows Server computers** report, and then click **Run**.
31. In the **Windows Server computers** window, click **Values**, click **All Systems**, and then click **OK**.
32. Click **View Report**.
33. Close the **Windows Server Computers** window, and then minimize the **Configuration Manager** console.
34. Open Internet Explorer, and then navigate to **http://LON-CFG/Reports**.
35. Click the **ConfigMgr_S01** link. Review the different report folders, and then open one or two folders to view the reports in them.

Lesson 3

Analyzing the real-time state of a device by using CMPivot

Contents:

Demonstration: Using CMPivot for Data Analysis

Demonstration Steps

1. On **LON-CFG**, if the **Configuration Manager** console is not already open, on the taskbar, click the **Configuration Manager Console** icon.
2. Click the **Assets and Compliance** workspace, and then click **Device Collections**.
3. In the center panel, right-click **All Desktop and Server Clients**, and then click **Start CMPivot**.
4. In the **CMPivot (All Desktop and Server Clients)** window, click the **Query** tab.
5. On the **Query** tab, in the text box, type **Service**.
6. Click the **Run Query** button.
7. Review the results.
8. On the **Query** tab, in the text box, type **Service | where StartMode == 'Disabled'**.
9. Run the Query and then review the results.
10. Leave the **CMPivot (All Desktop and Server Clients)** window open.
11. In the **CMPivot (All Desktop and Server Clients)** window, Click **Create Collection**.
12. In the **Create Device Collection Wizard**, on the **General** page, in the **Name** text box, type **Computers with disabled service**.
13. Click **Next**.
14. On the **Membership Rules** page, notice that **LON-CFG** is listed with the **Direct** type.
15. Clear the **Schedule a full update on this collection** check box.
16. Click **Summary**.
17. On the **Summary** page, click **Next**.
18. On the **Completed** page, click **Close**.
19. In the **CMPivot (All Desktop and Server Clients)** window, on the **Query** tab, click **Export,** and then click **To File**.
20. In the **Export to File** window, under **Quick access** links, click **Desktop**.
21. In the **File name** text box, type **Disabled services by computer**, and then click **Save**.
22. On the computer's desktop, double-click the **Disabled services by computer.csv** file.
23. In the **How do you want to open this file?** window, select **Notepad**, and then click **OK**.
24. Notice that these results are the same as the results listed in the CMPivot results pane.
25. Close Notepad.
26. On the taskbar, click the **Configuration Manager Trace Log Tool** icon.
27. Click **File**, and then click **Open**.
28. Browse to **C:\Program Files\Microsoft Configuration Manager\Logs**, select **BgbServer.log**, and then click **Open**.
29. Toward the end of the log file, locate the text **Starting to send push task**.
30. Make note of the TaskGUID value on this line.
31. Click **File**, and then click **Open**.

32. Browse to **C:\Program Files\SMS_CCM\Logs**, select **CcmNotificationAgent.log**, and then click **Open**.
33. Scroll to the end of the log file. Notice that **Receive task from server with pushid=** will be listed for the time when CMPivot was executed.
34. Make note of the taskguid value on this line.
35. Compare the previous TaskGUID value to this taskguid value. This will match and show that you are reviewing the correct CMPivot entry.
36. Click **File**, and then click **Open**.
37. Select the **Scripts.log** file, and then click **Open**.
38. Scroll to the last line of the log file.
39. Approximately 14 lines from the last line, locate the text **Script Guid: 7DC6B6F1-E7F6-43C1-96E0-E1D16BC25C14**. This is the start of the execution for the **CMPivot** script.
40. Review the following lines to locate the text **Creating state message…** . In the line that follows this text, notice that the states message is being sent by using the fast method.
41. Compare the previous taskguid value to the guid value listed between the curly braces (**{}**) in this line. They will match and show that CMPivot is complete.
42. Close Configuration Manager Trace Log Tool.

Module Review and Takeaways

Best Practice

Supplement or modify the following best practices for your own work situations:

Report subscription scheduling. Whenever possible, schedule report subscription processing to run outside of normal office hours. This will reduce the load on the Configuration Manager site database server and improve availability for immediate report requests.

Use Collection Evaluation viewer (CEviewer.exe) to location optimize your collection queries. This tool is found within the **<*Install Folder*>\tools\ServerTools** folder on your site server.

Review Questions

Question: What is the difference between attributes and attribute values?

> **Answer:** Attributes are the types of data collected, and attribute values are the actual values collected.

Question: What is the difference between a data query and a status message query?

> **Answer:** You can use data queries to find any data in the Configuration Manager tables and to build collections. You can use status message queries to query only the stored status messages and to assist in the monitoring and troubleshooting of Configuration Manager.

Question: How many reporting services points can you have in your hierarchy? How many should you have in your hierarchy?

> **Answer:** Answers will vary. You can have one or more reporting services points per primary site and the central administration site. You should have at least one reporting services point in the central administration site. Additionally, you should have at least one reporting services point in each primary site where the local administrators need to view reports that include data only from their site.

Real-world Issues and Scenarios

Management users at an organization want to view reports from within Configuration Manager, but typically do not have any configured roles in Configuration Manager. What can you do to allow them to read reports from Configuration Manager?

Answer: Create a custom Configuration Manager security role, which grants them the minimum permission needed to read reports in SSRS.

Tools

The following are tools that you can use in Configuration Manager.

Tool	Use for	Where to find it
Configuration Manager Trace Log tool	Viewing log files	*InstallationPath*\Microsoft Configuration Manager\tools
SQL Server Data tools	Creating custom models for reports	SQL Server https://aka.ms/e10m8m

Common Issues and Troubleshooting Tips

Common Issue	Troubleshooting Tip
Queries not returning results	Data might not exist in the database. When setting the criteria for queries, use the **Values** button to be sure that the data exists in the database. Additionally, when using multiple criteria for a query, be careful not to create a query statement so complex that no objects can match the query.
Reports not showing up in the **Configuration Manager** console	Ensure that SSRS has been configured. In particular, when using the default settings, ensure that you clicked **Apply** for the **Web Service URL** and the **Report Manager URL**.

Lab Review Questions and Answers

Lab A: Creating and running queries

Question and Answers

Question: Which operator would you use for the query to return either the Sales users or the Research users?

> **Answer:** In this case, you are querying only for two security groups. Therefore, you can use the **LIST** operator or the **OR** operator. However, if you are querying for more than two items, the **List** operator is better. If you use the **AND** operator, it will return users who are in both groups. To find the users who are either Sales users or Research users, you must use the **OR** or **List** operator.

Question: Why would you use a subselect query in your work environment?

> **Answer:** Answers will vary. Some of the possible answers are:
>
> - The most popular reason is to locate all computers without a particular software title or version.
> - Another reason is to locate all the users who are not within a particular security group, organizational unit (OU), or Configuration Manager site.

Question: Why would you import an existing query to create a new query?

> **Answer:** Answers will vary. One possible answer is that it is easier to modify an existing query than to build a new query.

Lab B: Configuring SSRS

Question and Answers

Question: What is the difference between a WQL query and an SQL query?

> **Answer:** WMI Query Language (WQL) is based on Windows Management Instrumentation (WMI)—Microsoft's implementation of Web-Based Enterprise Management (WBEM)—which is a standard technology for accessing management information. SQL is a special-purpose programming language used to manage databases. While WQL has some similarities to SQL, you cannot use WQL to query a database directly.

Question: What account should you use for the SSRS service account?

> **Answer:** You should use the **Network Service** account or an account that has administrative rights to the reporting database.

Question: Which Configuration Manager security role do users need to view reports on the SQL Server Reporting Services website?

> **Answer:** Users will need any one of the built-in security roles, except Remote Tools Operators, to view some or all of the Configuration Manager reports.

Lab C: Analyzing the real-time state of a device by using CMPivot

Question and Answers

Question: What type of collection membership is created from CMPivot results?

> **Answer:** A direct collection membership is created from CMPivot results.

Question: While creating a collection from CMPivot results, when will the results get updated?

Answer: The collection is created with a direct membership. Therefore, the collection membership results will never get updated.

Question: What is the error generated by changing “where” to “Where” in the queries?

Answer: The error is **Failed to parse query**.

Module 3

Preparing the Configuration Manager management infrastructure

Contents:

Lesson 1

Configuring boundaries and boundary groups

Contents:

Question and Answers

Question: What does client roaming allow a Configuration Manager client to do?

( ) Move to another Configuration Manager site hierarchy and be discovered.

( ) Join an Active Directory domain.

( ) Move to another site and use management points in those other sites for content location and service requests.

( ) Allow internet-managed, Mac, and mobile devices to move to another site and communicate with management points there.

( ) Apply the Network Discovery method to those clients.

Answer:

( ) Move to another Configuration Manager site hierarchy and be discovered.

( ) Join an Active Directory domain.

(√) Move to another site and use management points in those other sites for content location and service requests.

( ) Allow internet-managed, Mac, and mobile devices to move to another site and communicate with management points there.

( ) Apply the Network Discovery method to those clients.

Feedback:

Option 1 is incorrect, because clients can roam to other sites but not to other site hierarchies—that is, site codes. Option 2 is incorrect, because joining a domain is not part of Configuration Manager. Option 3 is correct. Option 4 is incorrect, because these three specific client types cannot communicate with any management points except their own. Option 5 is incorrect, because client roaming is not a factor of the Network Discovery method.

Demonstration: Configuring a boundary and a boundary group

Demonstration Steps

Enable the Active Directory Forest Discovery method

1. On LON-CFG, open the Configuration Manager console, click the **Administration** workspace, and then expand **Hierarchy Configuration**.
2. Click **Discovery Methods**, and then click **Active Directory Forest Discovery**.
3. On the ribbon, click **Properties**.
4. In the **Active Directory Forest Discovery Properties** dialog box, select the following check boxes:
    - **Enable Active Directory Forest Discovery**
    - **Automatically create Active Directory site boundaries when they are discovered**
    - **Automatically create IP address range boundaries for IP subnets when they are discovered**
5. To close the **Active Directory Forest Discovery Properties** dialog box, click **OK**.
6. In the **Configuration Manager** dialog box, click **Yes.**

Configure a boundary

1. Click the **Boundaries** node.

2. To manually create a boundary, right-click the **Boundaries** node, and then click **Create Boundary**.
3. In the **Create Boundary** dialog box, in the **Description** box, type **VPN boundary**.
4. In the **Type** list, click the list. Review the four boundary types in the **Type** list.
5. Select the **IP subnet**, type the following information, and then click **OK**:
    - Network: **10.10.3.0**
    - Subnet mask: **255.255.255.0**
6. In the **Administration** workspace, click the **Boundary Groups** node.

Note: Notice that the London boundary group displays in the results pane. This is configured for the labs in this course.

7. Right-click **London**, and then click **Properties**. Notice that the AdatumHQ boundary belongs to this group.
8. Click the **References** tab, and notice that this boundary group is used for site assignment for all clients that are part of the AdatumHQ boundary. Additionally, notice that LON-CFG.Adatum.com is configured to provide policy and content location services for all boundary members.
9. Click the **Relationships** tab, and notice that there are no fallback relationships currently configured.
10. Click the **Options** tab, and notice that **Allow peer downloads in this boundary group** is configured by default.
11. To close the **London Properties** dialog box, click **OK**.

Configure a boundary group

1. Right-click **Boundary Groups**, and then click **Create Boundary Group**.
2. In the **Name** box, type **VPN Boundary Group**, and then click **Add**.
3. In the **Add Boundaries** dialog box, click **10.10.3.0**, and then click **OK**.
4. To close the **Create Boundary Group** dialog box, click **OK**.

Configure a boundary group relationship and options

1. Right-click **VPN Boundary Group**, and then click **Properties**.
2. Click the **Relationships** tab.
3. Click **Add**.
4. On the **Fallback Boundary Groups** dialog box, select **London**.
5. Under **Fallback times**, next to **Distribution point**, change **120** minutes to **10** minutes.
6. Click **OK**.
7. Click the **Options** tab. Remove the check mark next to **Allow peer downloads in this boundary group**. Click **OK**.

Verify Active Directory Forest Discovery

1. Under the **Hierarchy Configuration** node, click **Active Directory Forests**.
2. Click **Adatum.com**, and then in the details pane, click **Discovery Status**.

Note: Note that you must look on the **Discovery Status** tab, because no new information is actually collected, and the main details pane item is not updated.

3. Verify that the discovery status of **S01 – Adatum Site** has occurred in the last few minutes.

Lesson 2

Configuring resource discovery

Contents:

Question and Answers

Categorize each item into the appropriate category. Indicate your answer by writing the category number to the right of each item.

Items	
1	Can be set to discover only computers signed in to the domain for a specific period of time
2	Can use SNMP devices
3	Has the default Active Directory attribute when created
4	Retrieves information about computer accounts
5	Returns operating system version information
6	Retrieves information about user accounts
7	Can be set to discover only computers with a current Active Directory password
8	Uses DHCP servers to discover DHCP clients
9	Has the default Active Directory attribute "mail"

Category 1		Category 2		Category 3
The Active Directory System Discovery method		The Network Discovery method		The Active Directory User Discovery method

Answer:

Category 1		Category 2		Category 3
The Active Directory System Discovery method		The Network Discovery method		The Active Directory User Discovery method

Category 1		Category 2		Category 3
Can be set to discover only computers signed in to the domain for a specific period of time Retrieves information about computer accounts Can be set to discover only computers with a current Active Directory password		Can use SNMP devices Returns operating system version information Uses DHCP servers to discover DHCP clients		Has the default Active Directory attribute when created Retrieves information about user accounts Has the default Active Directory attribute "mail"

Demonstration: Configuring Active Directory discovery methods

Demonstration Steps

Configure and run the Active Directory System Discovery method

1. On LON-CFG, in the Configuration Manager console, click the **Administration** workspace, and then expand **Hierarchy Configuration**.
2. Click the **Discovery Methods** node, and then double-click **Active Directory System Discovery**.
3. In the **Active Directory System Discovery Properties** dialog box, verify that the **Enable Active Directory System Discovery** check box is selected.
4. Click **New**, and then note the available options.
5. Click **Browse**.
6. In the **Select New Container** dialog box, click the **Toronto Clients** container, and then click **OK**.
7. Verify that the **Recursively search Active Directory child containers** check box is selected, and then click **OK**.

Note: You should either disable this option or configure exclusions if you have objects in child organizational units (OUs) that you do not want to discover.

8. On the **Polling Schedule** tab, click **Schedule**.
9. In the **Custom Schedule** dialog box, set the **Recur every** value to **5 days**, and then click **OK**.
10. Verify that the **Enable delta discovery** check box is selected and set to an interval of **5 minutes**.
11. On the **Active Directory Attributes** tab, verify the Active Directory attributes that will be discovered by default.
12. On the **Options** tab, note the options used to exclude computers from discovery, and then click **OK**.
13. Right-click **Active Directory System Discovery**, and then click **Run Full Discovery Now**.
14. In the Configuration Manager message box, to run full discovery as soon as possible, click **Yes**.

Configure and run the Active Directory User Discovery method

1. On LON-CFG, in the Configuration Manager console, click the **Administration** workspace, and then expand **Hierarchy Configuration**.
2. Click the **Discovery Methods** node, and then double-click **Active Directory User Discovery**.

3. In the **Active Directory User Discovery Properties** dialog box, verify that the **Enable Active Directory User Discovery** check box is selected.
4. Click **New**, and then note the available options.
5. Click **Browse**.
6. In the **Select New Container** dialog box, click the **Adatum** container, and then click **OK**.
7. Verify that the **Recursively search Active Directory child containers** check box is selected, and then click **OK**.
8. On the **Polling Schedule** tab, click **Schedule**, configure the recurrence to take place every three days, and then click **OK**.
9. Verify that the **Enable delta discovery** check box is selected and has an interval of **5 minutes**.
10. On the **Active Directory Attributes** tab, note the attributes that are discovered by default, and then click **OK**.
11. With **Active Directory User Discovery** selected, on the ribbon, click **Run Full Discovery Now**.
12. In the **Configuration Manager** message box, to run a full discovery as soon as possible, click **Yes**.

Examine the discovered system and user resources

1. Click the **Assets and Compliance** workspace, and then click the **Devices** node. Notice that several devices are listed.
2. In the results pane, right-click **LON-CL2**, and then click **Properties**. Notice that the system was discovered by using the SMS_AD_SYSTEM_DISCOVERY_AGENT agent.
3. In the results pane, click **Close**.
4. In the **Assets and Compliance** workspace, click the **Users** node. Notice that users that have been discovered in the Adatum domain.
5. In the results pane, right-click **ADATUM\Adam (Adam Hobbs)**, and then click **Properties**. Notice that the user account was discovered by using the SMS_AD_USER_DISCOVERY_AGENT agent.
6. Close the **ADATUM\Adam (Adam Hobbs) Properties** dialog box.

Lesson 3

Organizing resources using device and user collections

Contents:

Demonstration: Creating collections

Demonstration Steps

Create a collection by using a direct rule

1. On LON-CFG, on the taskbar, click the **Configuration Manager Console** icon and when the Configuration Manager console opens, click the **Assets and Compliance** workspace, and then click **Devices**.
2. In the results pane, select **LON-CL1**, press and hold the Ctrl key, and then click **LON-CL2**.
3. Right-click one of the selected devices, point to **Add Selected Items**, and then click **Add Selected Items to New Device Collection**.
4. In the **Create Device Collection Wizard**, on the **General** page, type or select the following information, and then click **Next**:
   - Name: **London Test Collection**
   - Limiting collection: **All Systems** (Click **Browse** and select).
5. Review the **Membership Rules** page, and then click **Next**.
6. On the **Summary** page, click **Next**, and then click **Close**.
7. In the navigation pane, click **Device Collections**.
8. Double-click **London Test Collection**, and then verify that the two resources LON-CL1 and LON-CL2 are members of London Test Collection.

Create a query-based collection

1. In the **Assets and Compliance** workspace, right-click the **Device Collections** node, and then click **Create Device Collection**.
2. In the Create Device Collection Wizard, on the **General** page, type the following information, and then click **Next**:
   - Name: **Windows Servers**
   - Limiting collection: **All Systems** (Click **Browse** and select).
3. On the **Membership Rules** page, click **Add Rule**, and then click **Query Rule**.
4. In the **Query Rule Properties** dialog box, in the **Name** box, type **Windows Servers**.
5. Click **Edit Query Statement**.
6. In the **Query Statement Properties** dialog box, on the **Criteria** tab, click **New**.
7. In the **Criterion Properties** dialog box, click **Select**.
8. In the **Select Attribute** dialog box, in the **Attribute Class** list, click **System Resource**.
9. In the **Attribute** list, click **Operating System Name and Version**, and then click **OK**.
10. In the **Criterion Properties** dialog box, in the **Operator** list, click **is like**. In the **Value** box type **%Server%**, and then click **OK**.
11. To close the **Query Statement Properties** dialog box, click **OK**.
12. To close the **Query Rule Properties** dialog box, click **OK**.
13. On the **Membership Rules** page, click **Next** on each page of the wizard until you reach the **Completion** page, and then click **Close**.

14. Click **Device Collections** node, right-click the **Windows Servers** device collection, and then click **Show Members**.
15. Verify that **LON-CFG** is listed as a member.

Create a collection by using Windows PowerShell (Optional)

1. Click **Start**, right-click the **Windows PowerShell** icon, and then click **Run ISE as Administrator**.
2. In the Administrator: Windows PowerShell ISE window, type the following cmdlet, and then press Enter.

```
Import-Module “C:\Program Files (x86)\Microsoft Configuration
Manager\AdminConsole\bin\ConfigurationManager.psd1”
```

3. In the Administrator: Windows PowerShell ISE window, type the following cmdlet, and then press Enter.

```
CD S01:
```

4. In the Administrator: Windows PowerShell ISE window, type the following cmdlet, and then press Enter.

```
New-CMuserCollection -Name "Managers" -LimitingCollectionName "All Users"
```

5. Discuss the results, noting that nothing is listed for **CollectionRules** and that **MemberCount** shows **0**.
6. In the Administrator: Windows PowerShell ISE window, type the following cmdlet, and then press Enter.

```
Add-CMUserCollectionQueryMembershipRule -CollectionName "Managers" -QueryExpression
"select
SMS_R_USER.ResourceID,SMS_R_USER.ResourceType,SMS_R_USER.Name,SMS_R_USER.UniqueUserNa
me,SMS_R_USER.WindowsNTDomain from SMS_R_User where SMS_R_User.UserOUName like
'%MANAGERS%'" -RuleName "Managers"
```

7. In the Administrator: Windows PowerShell ISE window, type the following cmdlet, and then press Enter.

```
Get-CMUserCollection –Name Managers
```

8. Discuss the results, and point out that **CollectionRules** now shows **{Managers}** and that **MemberCount** shows **31**. It may take a few minutes for the membership count to update.

Demonstration: Create and apply maintenance windows and power management plans

Demonstration Steps

Configure a maintenance window for Windows 10 workstations

1. If the Configuration Manager console is not already open, on LON-CFG, on the taskbar, click the **Configuration Manager Console** icon in the Taskbar.
2. In the System Center Configuration Manager console, click the **Assets and Compliance** workspace, and then click the **Device Collections** node.
3. Right-click the **All Windows 10 Workstations** node, and then click **Properties**.
4. In the **All Windows 10 Workstations Properties** dialog box, click the **Maintenance Windows** tab.

5. On the **Maintenance Windows** page, click **New**.
6. In the **<new> Schedule** dialog box, in the **Name** box, type **Deployment Window**.
7. Configure the schedule as follows, and then click **OK**:
    - Start: **8 P.M.**
    - End: **4 A.M.**
    - Recurrence pattern: **Daily**
8. On the **General** tab, in the **Comment** box, type **Maintenance Windows: 8 P.M. to 4 A.M.**
9. In the **All Windows 10 Workstations Properties** dialog box, click **OK**.

Configure power management for the All Windows 10 Workstations collection

1. On LON-CFG, on the taskbar, click **Configuration Manager Console**.
2. In the Configuration Manager console, click the **Administration** workspace, and then click **Client Settings**.
3. Right-click **Client Settings**, and then click **Create Custom Client Device Settings**.
4. In the **Create Custom Client Device Settings** dialog box, in the **Name** box, type **Windows 10 Power Management Settings**.
5. Select the **Power Management** check box.
6. Click **Power Management**, configure the following options, and then click **OK**:
    - Allow power management of devices: **Yes**.
    - Allow users to exclude their device from power management: **Yes**.
7. Right-click **Windows 10 Power Management Settings**, and then click **Deploy**.
8. In the **Select Collection** dialog box, click **All Windows 10 Workstations**, and then click **OK**..
9. In the preview pane, click the **Deployments** tab. Verify that the **All Windows 10 Workstations** collection has been assigned **Windows 10 Power Management Settings**.
10. In the System Center Configuration Manager console, click the **Assets and Compliance** workspace, and then click **Device Collections**.
11. In the results pane, click **all Windows 10 Workstations**.
12. On the ribbon, click the **Home** tab, and then click **Properties**. The **All Windows 10 Workstations Properties** dialog box opens.
13. Click the **Power Management** tab, and then click **Specify power management settings for this collection**.
14. Under the **Peak hours** section, configure the following:
    - Start: **7 AM**
    - End: **5 PM**
15. Next to **Peak plan**, click the **Peak plan** list, and then select **High Performance (ConfigMgr)**.
16. Next to **Non-peak plan**, click the **Non-Peak plan** list, and then select **Power Saver (ConfigMgr)**.
17. Select the **Wakeup time (desktop computers)** check box, and then configure the **Wakeup time** to be **2:00 AM**.
18. To close the **All Windows 10 Workstations Properties** dialog box click **OK**.

Module Review and Takeaways

Review Questions

Question: What is the purpose of the Heartbeat Discovery method?

> **Answer:** The Heartbeat Discovery method is a client-side process that refreshes the discovery data for a Configuration Manager client. If the Heartbeat Discovery method is not enabled, all devices will show as inactive, and you will not be able to run site maintenance tasks to manage stale data in your database.

Question: You change an attribute on an Active Directory user object. You expect Active Directory Delta Discovery to identify the change within five minutes. However, Active Directory Delta Discovery does not discover the change. What might be the problem?

> **Answer:** The attribute that you changed is not a replicated attribute. Active Directory Delta Discovery discovers only replicated Active Directory attribute changes. However, when the full discovery cycle takes place, Active Directory Delta Discovery will discover this change.

Question: Which two critical services do boundary groups provide?

> **Answer:** Boundary groups provide site assignment and content-location services.

Question: The Active Directory System Discovery method does not discover several computer resources. You verify that the computer accounts are in AD DS. What else should you check?

> **Answer:** You should verify that the computer accounts are not disabled and that each computer account has a corresponding DNS record that is registered.

Lab Review Questions and Answers

Lab A: Configuring boundaries and resource discovery

Question and Answers

Question: You notice that the All User Groups built-in collection lists no members, even though you want this collection to be populated. What should you do?

> **Answer:** You should verify that you have enabled and run the Active Directory Group Discovery method.

Question: Which discovery method automatically creates IP subnet boundaries when it discovers them?

> **Answer:** The Active Directory Forest Discovery method automatically creates IP subnet boundaries when it discovers them.

Lab B: Configuring user and device collections

Question and Answers

Question: You need to create a collection that includes a static list of members. Which rule type should you use?

> **Answer:** You should use a direct rule to create a static list of members in a collection.

Question: You need to create a collection with workstations that do not have Office installed. How can you accomplish this?

> **Answer:** You can create a collection that includes all the workstations that have Office installed. Then create a second collection that is based on All Desktop and Server clients but that excludes the collection that contains the workstations with Office installed.

Question: You need to ensure that applications do not automatically install during working hours. What can you do?

> **Answer:** You can configure a maintenance window to ensure that application installations take place only during a specific time.

Module 4

Deploying and managing the Configuration Manager client

Contents:

Lesson 1

Overview of the Configuration Manager client

Contents:

Question and Answers

Question: The Configuration Manager settings that apply to a user or computer override any GPO settings.

( ) True

( ) False

Answer:

( ) True

(√) False

Feedback:

Any GPO settings that apply to a user or computer will override the settings applied by using Configuration Manager.

Exploring the properties of the Configuration Manager client

Question: Based on your organizational requirements, how would you change these settings if you find that you configured something incorrectly during the client's installation?

Answer: Answers will vary. However, they might include reinstalling the client with the correct settings or by changing client settings in the Configuration Manager console.

Question: How would you troubleshoot the issue of a user being unable to connect to the Configuration Manager infrastructure from home?

Answer: Answers will vary but might include using the Configuration Manager Control Panel item to verify that the user's computer is configured for Internet-based management and has a certificate installed. If the computer is configured properly for Internet-based management, you then would validate that the computer has a certificate that meets the requirements for Internet-based management.

Demonstration: Exploring the properties of the Configuration Manager client

Demonstration Steps

1. On LON-CFG, right-click Start, and then click **Control Panel**.
2. In Control Panel, click **System and Security**, and then click **Configuration Manager**.
3. Explain that the **General** tab contains basic information about the client. Review how you can use this information for troubleshooting:
    - For example, if a user brought a laptop home for the first time and cannot connect to the Configuration Manager infrastructure through the Internet, you might see that the user has only a self-signed certificate that is configured for "**Always intranet**."
    - You also can use this tab to identify whether the client is connected to the correct site (or to any site) and is running the correct version of the Configuration Manager client.
4. Click the **Components** tab, and explain how to use this tab to determine whether the client has received a policy:
    - You can use the **Components** tab to verify that components have installed successfully, and that a client is receiving a policy. Explain how the Enabled, Disabled, or Installed status of the components indicates that a policy has been downloaded.

- You can compare the Enabled or Disabled status to the client settings that a client should receive from the site.

5. Click the **Actions** tab. Review why you would initiate client actions manually, rather than waiting for the next scheduled interval.
    - For example, you might force an agent to run instead of waiting for a change to be applied during the next polling cycle.
6. Click the **Site** tab. Review why you would configure a client to use a different site. Perform the following:
    - Mention that automatic site assignment only occurs once.
    - Click the **Configure Settings** button and review how to change the site code.
7. Click the **Cache** tab, and then click **Configure Settings**. Review why you would change the size of the cache for a client. Explain that you set the cache size during client installation or you can also use client settings, and the default size is 5,120 megabytes (MB). Perform the following steps:
    - Click the **Change Location** button, review how to change the cache location, and then click **Cancel**.
    - Click the **Delete Files** button, explain the **Delete persisted cache content** check box, and then click **No**.
8. Click the **Configurations** tab. Discuss configuration baselines, and explain that you use the **Evaluate** and **View Report** buttons to check the client machine immediately in comparison to a baseline. Examine how to use the **Evaluate** and **View Report** buttons.
9. Click the **Network** tab, and then review why you would change a client to an Internet-based client.
10. Click the **Configure Settings** button, and then review how you would use these settings to convert a client to an Internet-based client.
11. Click **Cancel**, and then close Control Panel.

Lesson 2

Deploying the Configuration Manager client

Contents:

Question and Answers

Question: You can assign client devices either to a secondary site or to a central administration site.

( ) True

( ) False

Answer:

( ) True

(√) False

Feedback:

You can assign client devices to any primary site. However, you cannot assign client devices either to a secondary site or to a central administration site.

Resources

Overview of the client installation process for Windows-based clients

Additional Reading: For more information about the client installation properties in Configuration Manager, refer to "About client installation properties in System Center Configuration Manager" at https://aka.ms/bmz5p0

Demonstration: Installing the client software by using client push installation

Demonstration Steps

1. On LON-CFG, on the taskbar, click **Configuration Manager Console**.
2. In the Configuration Manager console, click the **Administration** workspace, expand **Site Configuration**, and then click **Servers and Site System Roles**.
3. In the preview pane, right-click the **Management point** role, and then click **Properties**.
4. Select the **Generate alert when the management point is not healthy** check box.
5. In the **Management point Properties** dialog box, click **OK**.
6. Right-click **Sites**, and then click **Hierarchy Settings**.
7. In the **Hierarchy Settings Properties** dialog box, select the **Use a fallback site** check box, and then click **OK**.
8. In the **Administration** workspace, click the **Sites** node.
9. On the ribbon, click **Settings**, click the **Client Installation Settings** drop-down list box, and then click **Client Push Installation**.
10. Click the **Accounts** tab.
11. Verify that **Adatum\ClientInstall** is configured as a Client Push Installation account. This was configured for the lab tasks.
12. Click the **Installation Properties** tab.
13. On the **Installation Properties** tab, in the **Installation properties** box, after **SMSSITECODE=S01** type the following on one line each separated by a space:

```
FSP=LON-CFG DISABLESITEOPT=True SMSCACHEDIR=Cache SMSCACHEFLAGS=MAXDRIVE
```

14. In the **Client Push Installation Properties** dialog box, click **OK**.
15. Click the **Assets and Compliance** workspace, and then click **Devices**.
16. Right-click **LON-CL1**, and then click **Install Client**.
17. In the Install Configuration Manager Client Wizard, on the **Before You Begin** page, click **Next**.
18. Review the **Installation Options** page, and then click **Next**.
19. Review the **Summary** page, verify that one resource is going to be installed, and then click **Next**.
20. On the **Completion** page, click **Close**.
21. Minimize the Configuration Manager console.

Lesson 3

Configuring and monitoring client status

Contents:

Question and Answers

Question: What would happen if you set a very low value for the alert thresholds?

Answer: The alerts would not trigger until a large number of clients reported issues.

Question: To view the client health rules that the Client Health evaluation engine is using, you can look in the *client location*\ccmeval.xml file.

( ) True

( ) False

Answer:

(√) True

( ) False

Configuring client status settings

Question: If you decide to change the default settings for the activity monitors, would you set them to a greater or less number of days?

Answer: Answers will vary.

Using the Configuration Manager console to monitor client health and client activity

Question: In your environment, how often would you monitor the Client Status page?

Answer: Answers will vary.

Demonstration: Configuring client status settings

Demonstration Steps

1. On LON-CFG, on the taskbar, open the Configuration Manager console.
2. Click the **Monitoring** workspace, and then click the **Client Status** node.
3. Right-click the **Client Status** node, and then click **Client Status Settings**.
4. In the **Client Status Settings Properties** dialog box, under **Evaluation periods to determine client activity**, review the following considerations:
   - If the clients do not have activity for the specified task within the specified number of days, the client displays in the monitor as inactive.
   - Do not configure these settings for less than the scheduled interval. For example, if hardware inventory is scheduled to run every 14 days, do not leave its activity monitor at the default 7 days. This could cause it to show as inactive most of the time.
5. Discuss the **Retain client status history for the following number of days** setting.

Explain that this setting is concerned primarily with health data, and the activity results show the last time a client was active, but not the frequency of activity.

6. In the **Client Status Settings Properties** dialog box, click **OK**.

Demonstration: Using the Configuration Manager console to monitor client health and client activity

Demonstration Steps

1. On LON-CFG, ensure that the Configuration Manager console still displays in the Monitoring workspace, with the **Client Status** node selected.
2. On the **Client Status** page, in the Statistics section, click the **Browse** button.

Explain that from here you can choose the collection whose health and activity you want to examine.

3. In the **Select Collection** dialog box, click the **All Desktop and Server Clients** collection, and then click **OK**.
4. Click the **Active clients that passed client check or no results :1** link, and briefly discuss the results.

Note: Note that a temporary node is created in the Assets and Compliance workspace, and that it displays in the console. In addition, note the name of the collection, which is **Active clients that passed client check or no results from All Desktop and Server Clients**.

5. In the Active clients that passed client check or no results from All Desktops and Server Clients collection window, click **LON-CFG**.
6. Examine the preview pane:
   - Explain that the **Summary** tab information contains an overview of that client's status, and other general information.
   - Click the **Client Activity Detail** tab. Explain that this tab shows the last time the client performed monitored activity, and the management point with which it last communicated.
   - Click the **Client Check Detail** tab. Explain that this tab displays the health checks the client has failed over the past 31 days (by default), or the last time the client passed all the health checks.
7. Close the Configuration Manager console. This will remove all temporary nodes that you created during the last open console session.
8. From the taskbar, open the Configuration Manager console.
9. In the Configuration Manager console, click the **Assets and Compliance** workspace, and then click the **Devices** node.
10. Note that the temporary nodes that you created in the previous steps are now removed. Point out that to remove these nodes manually from the **Devices** node, you can use the right-click menu, or you could use the ribbon.

Lesson 4

Managing client settings and performing management operations

Contents:

Question and Answers

Question: By default, anyone that creates a script can immediately run the script against a device or collection.

( ) True

( ) False

Answer:

( ) True

(√) False

Feedback:

After a script is created, it must be approved before it can be run against a device or collection. Also, if permissions are set as recommended, anyone creating a script will not be able to run a script as these required different security roles.

Demonstration: Configuring Default Client Settings

Demonstration Steps

1. On LON-CFG, on the taskbar, click **Configuration Manager Console**.
2. In the Configuration Manager console, click the **Administration** workspace, and then click the **Client Settings** node.
3. Right-click **Default Client Settings**, and then click **Properties**.
4. In the **Default Settings** dialog box, click the **Client Policy** setting. Explain that the **Client policy polling interval (minutes)** value controls how often the client will request settings from a management point:
    a. Verify that the Client policy polling interval (minutes) is set to **5** minutes. Notice that this is for demonstration purposes, and that you should not use this setting in a production environment.
    b. Note that this configuration also reduces the number of supported clients on the management point by 75 percent. Therefore, instead of supporting 25,000 clients per management point, approximately 6,000 clients only are supported.
5. Click the **State Messaging** setting. The **State message reporting cycle (minutes)** value controls how often the client sends state messages to a management point:
    a. Set the **State message reporting cycle (minutes)** to **5** minutes. Note that this is for demonstration purposes only, and you should not use this setting in a production environment.
    b. Note that configuring this short of a cycle could cause a backlog of state messages, especially during a software-update scan cycle.

Note: The other settings and values are set in a similar manner. Students will learn more about these settings in subsequent modules.

6. Click **OK** to accept changes, and close the **Default Settings** dialog box.

Demonstration: Configuring custom client settings

Demonstration Steps

1. In the Configuration Manager console, ensure that you are still in the **Client Settings** node in the **Administration** workspace.
2. Right-click the **Client Settings** node, and then click **Create Custom Client Device Settings**.
3. In the **Custom Device Settings** dialog box, in the **Name** text box, type **LON Server Systems**.
4. In the **Description** text box, type **Client settings for all LON server systems**.
5. In the Select and then configure the custom settings for client devices section, select the **State Messaging** check box.
6. Click the **State Messaging** setting, take note of the value displayed, and then set the **State message reporting cycle (minutes)** to **15** minutes.
7. Click **OK** to create the custom client device setting policy. Note the priority of the newly created **LON Server Systems** client setting.
8. Right-click the **LON Server Systems** client setting, and then click **Deploy**.
9. In the **Select Collection** dialog box, click **All Windows Servers**, and then click **OK**.
10. In the preview pane, click the **Deployments** tab. Point out to students the client deployment that you just created, and point out that you can assign the client setting to more than one collection.
11. Right-click **Client Settings**, and then click **Create Custom Client Device Settings**.
12. In the **Custom Device Settings** dialog box, in the **Name** text box, type **Windows 10 Client Systems**.
13. In the **Description** text box, type **Client settings for all Windows 10 client systems**.
14. In the Select and then configure the custom settings for client devices section, select the **Client Policy** check box.
15. Click the **Client Policy** setting, and take note of the value that displays. Set the **Client policy polling interval (minutes)** value to **30** minutes, and then click **OK**.

Demonstration: Running scripts on target devices

Demonstration Steps

1. In the Configuration Manager console, click the **Administration** workspace.
2. Expand **Site Configuration**, and then select **Sites**.
3. In the Ribbon, click **Hierarchy Settings**.
4. On the **General** tab, remove the check mark next to **Script authors require additional script approver**. Describe that this is only done in this demonstration so that the administrator can approve the script manually.
5. Click **OK** to close the **Hierarchy Settings Properties** box.
6. In the Configuration Manager console, click the **Software Library** workspace.
7. Click the **Scripts** node and then on the ribbon, click **Create Script**.
8. In the Create Script wizard, next to **Script name** enter **OS Version**.
9. In the Script window, type the following and then click **Next**:

```
Write-Output (Get-WmiObject -Class Win32_operatingSystem).Caption
```

10. On the **Summary** page, click **Next** and then click **Close**. Notice that the **Approval State** shows **Waiting for approval**.
11. Select the **OS Version** script and then in the ribbon click **Approve/Deny**. **The Approve or Deny Script** wizard starts. Click **Next**.
12. On the **Script Approval** page, select **Approve** and then click **Next**.
13. On the **Summary** page, click **Next** and then click **Close**.
14. In the Configuration Manager console, click the **Assets and Compliance** workspace.
15. Click the **Devices** node.
16. Select **LON-CFG**, right click **LON-CFG** and then click **Run Script**.
17. In the Run Script wizard, select the **OS Version** script and then click **Next**.
18. On the **Summary** page, click **Next**.
19. Take note of the Script status. Describe the results of the Script output and then click **Close**.
20. Click the **Monitoring** workspace and then click **Script Status**.
21. Select the **OS Version** script and notice its Overall Script Execution State.
22. In the ribbon click **Show Status** to view the script details.
23. Click **OK** to close the status information.

Module Review and Takeaways

Best Practices

- Always deploy at least one fallback status point.
- Do not rely on a single client installation method.

Review Questions

Question: Which site systems would you deploy to support Internet-based clients?

> **Answer:** Answers will vary. However, all answers should include a management point and a distribution point.

Question: Why would you want to assign multiple client device settings to a collection?

> **Answer:** You would assign multiple client device settings to a collection so you can create different client device-settings objects for separate Configuration Manager feature sets. For example, you might have one client device settings object for software deployment, and another client device settings object for hardware inventory.

Question: In a multiple domain forest, how will the client installation process obtain local administrative rights on all the client systems?

> **Answer:** Answers will vary. One possible solution is to use a client installation account from each domain that has administrative rights within that domain.

Question: Different groups or departments need different installation options. How can you accommodate these needs?

Common Issues and Troubleshooting Tips

Common Issue	Troubleshooting Tip
Certificate trust issues are occurring	Ensure that all systems trust the issuing CA.
Typographical errors are discovered on the command line for client.msi installation	Review the CCMSetup.log to find the error.
Nothing happens during an installation attempt	Check if Windows Firewall is blocking the deployment.
Clients are not receiving the intended settings	Validate the order in which the client settings are being applied.

Lab Review Questions and Answers

Lab A: Deploying the Configuration Manager client software

Question and Answers

Question: Which optional site system should you use to identify unmanaged clients?

> **Answer:** The fallback status point assists in identifying unmanaged clients.

Question: What is the simplest way of verifying that the Configuration Manager client is installed?

> **Answer:** Open Control Panel and verify if the Configuration Manager client displays as an item.

Lab B: Configuring and monitoring client status

Question and Answers

Question: In your environment, for what interval will you configure the client status settings?

> **Answer:** Answers will vary.

Question: In your environment, what threshold values will you set for alerts?

> **Answer:** Answers will vary.

Lab C: Managing client settings

Question and Answers

Question: How can you quickly verify that a custom setting has been applied to a client?

> **Answer:** You can review clients in client settings to determine if the setting has been applied.

Question: How can you determine the order in which client device settings apply when a device is subject to multiple conflicting device settings?

> **Answer:** You can use the Resultant Client Settings functionality in the Configuration Manager console to determine the resultant client settings when multiple client settings are applied.

Module 5

Managing inventory for PCs and applications

Contents:

Lesson 1

Overview of inventory collection

Contents:

Question and Answers

Question: Which of the following tasks could you use Configuration Manager Inventory for?

( ) Locate systems with particular file installed.

( ) Find all systems with specific hardware that you are planning on retiring.

( ) Assist an investigation by finding the dates, times, and systems that a user has signed in to.

( ) Deploy a software upgrade.

( ) Remote-control a device and assist a user with an issue.

Answer:

(√) Locate systems with particular file installed.

(√) Find all systems with specific hardware that you are planning on retiring.

( ) Assist an investigation by finding the dates, times, and systems that a user has signed in to.

(√) Deploy a software upgrade.

( ) Remote-control a device and assist a user with an issue.

Feedback:

Option 1 is a typical use of software inventory, option 2 is a typical use for hardware inventory, and option 4 can use either type of inventory, depending on how the application is installed. Option 3 includes information that is not fully collected by software or hardware inventory. Even though Asset Intelligence can provide information about which computer a user has signed in to, it will not record all the sign-ins. Option 5 is a separate feature of Configuration Manager.

Lesson 2

Configuring hardware and software inventory

Contents:

Question and Answers

Question: Which of the following types of information can be collected through a Hardware Inventory?

( ) Information about the operating system.

( ) Information about Unified Extensible Firmware Interface mode on a computer.

( ) Information about BitLocker status.

( ) A list of installed applications.

( ) Information about a user's desktop configuration.

Answer:

(√) Information about the operating system.

(√) Information about Unified Extensible Firmware Interface mode on a computer.

(√) Information about BitLocker status.

(√) A list of installed applications.

(√) Information about a user's desktop configuration.

Feedback:

All of these options include information that can be gathered from WMI. The purpose of the question is to illustrate the wide variety of information that can be included in a hardware inventory.

Resources

How is hardware inventory collected?

Additional Reading: For more information, refer to Open Management Infrastructure (OMI) "CIM/WBEM Manageability Services Broker": https://aka.ms/n6s6wy

Demonstration: Configuring client settings for hardware inventory

Demonstration Steps

1. On **LON-CFG**, on the taskbar, click the **Configuration Manager Console** icon.
2. In the **Configuration Manager** console, click the **Administration** workspace, and then click **Client Settings**.
3. In the results pane, double-click **Default Client Settings**.
4. In the **Default Settings** window, click **Hardware Inventory**.
5. Under **Device Settings**, next to **Enable hardware inventory on clients**, verify that the **Yes** option is selected.
6. Next to **Hardware inventory** schedule, click **Schedule**.
7. In the **Configure Client Setting** dialog box, select the **Custom schedule** option, and then click **Customize**.
8. Describe the **Time** and **Recurrence pattern** sections, and then click **Cancel**.
9. In the **Configure Client Setting** dialog box, click **Cancel**.

10. Under **Device Settings**, next to **Hardware inventory classes**, click **Set Classes**.
11. In the **Hardware Inventory Classes** dialog box, scroll down to view the various classes that are enabled or disabled.
12. Click **Filter by category**, and then review the various categories.
13. Click **Filter by type**, and then review the various types.
14. Click **Add**, review how you can connect to the WMI namespace of another computer, and then click **Cancel**.
15. Review the **Import** and **Export** buttons. To return to the **Default Settings** window, click **Cancel**.
16. Click the **Collect MIF files** drop-down list box. Review the options for configuring the collection of IDMIF and NOIDMIF files.
17. To close the **Default Settings** window, click **Cancel**.

Lesson 3

Managing inventory collection

Contents:

Question and Answers

Question: In your environment, how often will you schedule hardware inventory?

Answer: Answers will vary, but could include:

- Use the default schedule of once every seven days, because the hardware does not change that frequently.
- Schedule hardware inventory more frequently than the default schedule, if changes are expected or need to be detected sooner.

Also, discuss the implications of scheduling inventories too often (increased network traffic) or too infrequently (data going stale).

Demonstration: Initiating inventory collection on a client

Demonstration Steps

Initiate hardware inventory collection on a client

1. On **LON-CFG**, right-click **Start**, and then click **Control Panel**.
2. In **Control Panel**, click **System and Security**, and then click **Configuration Manager**.
3. In the **Configuration Manager Properties** dialog box, click the **Actions** tab. Take note of the available actions.
4. Click the **Machine Policy Retrieval & Evaluation Cycle** action, and then click **Run Now**. At the prompt, click **OK**.
5. Click the **Hardware Inventory Cycle** action, and then click **Run Now**. At the prompt, click **OK**.
6. To close the **Configuration Manager Properties** dialog box, click **OK**.
7. Close **Control Panel**.

Use Resource Explorer to view inventory results

1. On the taskbar, click the **Configuration Manager** console icon.
2. Click the **Assets and Compliance** workspace, and then click **Devices**.
3. In the results pane, right-click **LON-CFG**, point to **Start**, and then click **Resource Explorer**.
4. In the **System Center Configuration Manager - Resource Explorer** window, in the left pane, expand the **Hardware** node. Review the various hardware inventory nodes.
5. Click the different hardware inventory nodes, and then discuss the results.
6. In the **System Center Configuration Manager - Resource Explorer** window, in the left pane, expand the **Hardware History** node. Review and discuss any history data.
7. Close **System Center Configuration Manager - Resource Explorer**.

Use Configuration Manager inventory reports

1. In the **Configuration Manager** console, click the **Monitoring** workspace, expand the **Reporting** node, and then expand the **Reports** node. Review the various report categories.
2. In the left pane, click the **Hardware-Disk** folder. Notice the reports that pertain to disk information.
3. In the left pane, click the **Hardware-Memory** folder. Notice the reports that pertain to computer memory information.

Lesson 4
Configuring software metering

Contents:

Question and Answers

Question: In your environment, how do you plan to use Software Metering?

Answer: Answers will vary, but could include:

- To track actual application usage for licensing decisions.
- Used for Asset Intelligent data and recently used applications.

Demonstration: Configuring software-metering rules

Demonstration Steps

Configure the Software Metering Client Agent

1. On **LON-CFG**, on the taskbar, click the **Configuration Manager Console** icon.
2. Click the **Administration** workspace, and then click **Client Settings**.
3. Right-click **Default Client Settings**, and then click **Properties**.
4. In the **Default Settings** dialog box, in the left pane, click **Software Metering**.
5. Under Device Settings, verify that the **Enable software metering on clients** option is set to **Yes**.
6. Click **Schedule**. Describe the schedule options, and then click **Cancel**.
7. To close the **Default Settings** dialog box, click **Cancel**.

Configure a software metering rule

1. Click the **Assets and Compliance** workspace, and then click **Software Metering**.
2. In the navigation pane, right-click **Software Metering**, and then click **Create Software Metering Rule**.
3. In the **Name** text box, type **WordPadRule**.
4. Click **Browse**, and then navigate to **C:\Program Files\Windows NT\Accessories\**.
5. Click **Wordpad.exe**, and then click **Open**. Notice that the text boxes for **Original file name**, **Version**, and **Language** are populated automatically.
6. In the **Version** text box, delete the existing version text, and then type the asterisk wildcard character (*****).
7. In the **Language** drop-down list box, select **– Any –**, and then click **Next**.
8. Click **Next**, and then click **Close**.

Configure automatic software-metering rule generation

1. In the **Configuration Manager** console, right-click **Software Metering**, and then click **Software Metering Properties**.
2. In the **Software Metering Properties** dialog box, ensure that **Automatically create disabled metering rules from recent usage inventory data** is enabled.
3. In the **Specify the percentage of computers in the hierarchy that must use a program before a software metering rule is automatically created** box, type or select a setting of **5**.
4. In the **Specify the number of software metering rules that must be exceeded in the hierarchy before the automatic creation of rules is disabled** box, type or select a setting of **25**.
5. To close the **Software Metering Properties** dialog box, click **OK**.

View software metering reports

1. In the **Configuration Manager** console, click the **Monitoring** workspace, and then expand **Reporting**.
2. Expand **Reports**, and then click the **Software Metering** folder.
3. Describe the reports that display. Run reports as time allows.

Lesson 5

Configuring and managing Asset Intelligence

Contents:

Question and Answers

Question: Which of the following is not an Asset Intelligence component?

( ) Asset Intelligence Catalog

( ) Asset Intelligence Client Settings

( ) Asset Intelligence Synchronization point

( ) Asset Intelligence home page

( ) Asset Intelligence Reports

Answer:

( ) Asset Intelligence Catalog

(√) Asset Intelligence Client Settings

( ) Asset Intelligence Synchronization point

( ) Asset Intelligence home page

( ) Asset Intelligence Reports

Feedback:

Options 1, 3, 4, and 5 are all components of Asset Intelligence with interfaces in the Configuration Manager catalog. The "Asset Intelligence Client Settings" is a made-up term, because Asset Intelligence does not include any specific client settings.

Resources

Using the Product Lifecycle dashboard

Reference Links: To read about the Microsoft Life Cycle Policy, go to: https://aka.ms/AA42m4n.

Demonstration: Enabling Asset Intelligence data collection

Demonstration Steps

Enable Asset Intelligence reporting classes

1. On **LON-CFG**, on the taskbar, click the **Configuration Manager Console** icon.
2. Click the **Assets and Compliance** workspace, and then click **Asset Intelligence**.
3. Right-click **Asset Intelligence**, and then click **Edit Inventory Classes**.
4. In the **Edit Inventory Classes** dialog box, verify that **Enable only the selected Asset Intelligence reporting classes** is enabled.
5. Select the check boxes for all inventory classes, except **SMS_InstalledExecutable** and **SMS_SoftwareShortcut**.
6. Point to each reporting class, and then with the tooltip, discuss the reports that are associated with each class.
7. To close the **Edit Inventory Classes** dialog box, click **OK**, and then click **Yes**.

Import software license information

1. Right-click **Asset Intelligence**, and then click **Import Software Licenses**.
2. In the Import Software Licenses Wizard, click **Next**.
3. On the **Import** page, click the **General License Statement (.csv file)** option.
4. In the **Path** text box, type **\\LON-CFG\E$\Licenses\LicenseData.csv**, and then click **Next**.
5. On the **Summary** page, click **Next**.
6. On the **Completion** page, click **Close**.

Install an Asset Intelligence synchronization point

1. Click the **Administration** workspace, expand the **Site Configuration** node, and then click **Servers and Site System Roles**.
2. In the details pane, right-click **\\LON-CFG.Adatum.com**, and then click **Add Site System Roles**.
3. In the **Add Site System Roles Wizard**, click **Next**.
4. On the **Proxy** page, click **Next**.
5. On the **System Role Selection** page, select the **Asset Intelligence synchronization point** check box, and then click **Next**.
6. On the **Asset Intelligence Synchronization point Settings** page, click **Next**.
7. On the **Synchronization settings** page, ensure that **Enable synchronization on a schedule** is selected, that it is set to run every **7 days**, and then click **Next**.
8. On the **Summary** page, click **Next**.
9. On the **Completion** page, click **Close**.
10. Click the **Assets and Compliance** workspace, and then click **Asset Intelligence**. In the results pane, under **Catalog Synchronization**, review the status details. Refresh the page if required.
11. Right-click **Asset Intelligence**, and then point to **Synchronize**. Discuss the **Synchronize Asset Intelligence Catalog** and **Schedule Synchronization** options.

Note: If the options are not available, refresh the console, or click on another node, and then click the **Asset Intelligence** node again.

Module Review and Takeaways

Question: How can hardware and software inventory assist in software distribution?

> **Answer:** You can create collections of resources based on inventory data. For example, you can create a collection of computers that support the minimum hardware and software requirements for installing a particular software package, and then distribute the software to that collection.

Question: A user in your organization is having intermittent problems with their desktop computer. How can you use hardware and software inventory to troubleshoot the problem?

> **Answer:** You can use hardware inventory data to determine potential issues, such as a recent change in computer hardware. For example, you can find out if new hardware that has been installed has an improper configuration. You can use software inventory to determine if a user's computer has the latest service packs installed, or to collect log files from the client's computer.

Question: A department in your organization has deployed a user application with expensive per-user licenses. How can you use software inventory and software metering to help ensure that your organization is receiving the most value from this application?

> **Answer:** Use software inventory to determine which clients have the application installed. Use software metering to determine which users are running the application. Use the data to help determine if you need to install software on additional clients, and on which clients you need to remove software. Depending on the application, you also may use Asset Intelligence reports to obtain license reports from reported data.

Question: You have enabled software metering and have just deployed a new application throughout your network. By default, what will trigger the automatic creation of a disabled software-metering rule?

> **Answer:** The software-metering rule is created when the application is present in the inventory data and in use on 10 percent of computers of your network.

Lab Review Questions and Answers

Lab A: Configuring and managing inventory collection

Question and Answers

Question: How can you configure hardware and software inventory to minimize network impact?

> **Answer:** Consider configuring a simple schedule instead of a custom schedule. A simple schedule usually helps reduce network impact, because the client's install time determines the time at which that client's inventory data file is sent. When you configure a custom schedule, all clients run inventory at the time that you specify, which can cause network issues. Furthermore, consider minimizing the amount of information to collect during inventory.

Question: How can you determine whether hardware has changed on a managed computer?

> **Answer:** The hardware history displays any changes to inventory that a specific client has reported.

Lab B: Configuring software metering

Question and Answers

Question: You have created a new software-metering rule for a specific application that is installed on both Windows 7 and Windows 10 clients. You notice that only Windows 10 clients are reporting usage data. What might be the problem?

> **Answer:** There might be a specific version number entered that pertains only to the Windows 10 clients. Change the version value to the wildcard character (*) to cover all versions.

Question: What is the advantage of using the Browse button in a software-metering rule as opposed to entering the file name manually?

> **Answer:** Using the Browse button forces the wizard to read the file header and fills in the original file name, version, and language fields automatically. This is useful to ensure that an application is monitored, even if a user renames the executable file.

Lab C: Configuring and managing Asset Intelligence

Question and Answers

Question: You run an Asset Intelligence report to find computers that multiple users are using, but the report displays no records. How can you troubleshoot and correct the issue?

> **Answer:** You can troubleshoot and correct the issue by performing the following procedure:
>
> 1. Ensure that all computers are configured to audit logon events. Typically, you would do this by using Group Policy.
> 2. Apply the policy to a test machine, and then sign in to the test machine with several different users.
> 3. Verify that the audit events were written to the event log, and then perform a hardware inventory to collect the data. You should then be able to see the test machine in the report. Additional machines will be added to the report over time.

Module 6

Distributing and managing content used for deployments

Contents:

Lesson 1

Preparing the infrastructure for content management

Contents:

Question and Answers

Categorize each item into the appropriate category. Indicate your answer by writing the category number to the right of each item.

Items	
1	Can configure thresholds for the amount of storage used.
2	Cannot be configured on a distribution point on a site server.
3	Hosts content files.
4	Cannot host software update packages.
5	Prestaged content distribution settings override pull distribution.
6	Uses a single instance store for the files it hosts.
7	Supports downloading content from the cloud.
8	Retry settings do not apply.
9	Allows deduplication on store volumes.

Category 1		Category 2		Category 3
Cloud-based distribution points		Pull distribution points		Content Library

Answer:

Category 1		Category 2		Category 3
Cloud-based distribution points		Pull distribution points		Content Library

Category 1		Category 2		Category 3
Can configure thresholds for the amount of storage used. Cannot host software update packages. Supports downloading content from the cloud.		Cannot be configured on a distribution point on a site server. Prestaged content distribution settings override pull distribution. Retry settings do not apply.		Hosts content files. Uses a single instance store for the files it hosts. Allows deduplication on store volumes.

Creating and configuring distribution point groups

Question: If you do not add a boundary group to TOR-SVR2, when will clients in the London boundary group use TOR-SVR2?

> **Answer:** By default, the Create Site System Server Wizard or the Add Site System Roles Wizard configures a distribution point as a fallback source location. Therefore, clients from the London boundary group will use TOR-SVR2 only if the distribution point on LON-CFG does not contain the distributed content.

Demonstration: Creating and configuring distribution point groups

Demonstration Steps

1. On **TOR-SVR2**, open **Server Manager** if it is not already open.
2. In the **Server Manager** console, in the navigation pane, click **Local Server**, and then in the **Properties** for **TOR-SVR2** pane, click **Tasks**. Click **Computer Management**.
3. In the **Computer Management** console, expand **Local Users and Groups**, and then click **Groups**.
4. In the details pane, double-click **Administrators**.
5. In the **Administrators Properties** dialog box, click **Add**.
6. In the **Select Users, Computers, Service Accounts, or Groups** dialog box, click **Object Types**.
7. In the **Object Types** dialog box, select **Computers**, and then click **OK**.
8. In the **Select Users, Computers, Service Accounts, or Groups** dialog box, in the **Enter the object names to select** box, type **LON-CFG**. Click **Check Names**, and then click **OK**.
9. To close the **Administrators Properties** dialog box, click **OK**.
10. Close all open windows.
11. On **LON-CFG**, to open the **Configuration Manager** console, on the taskbar click the **Configuration Manager** icon.
12. In the **Configuration Manager** console, click the **Administration** workspace, expand **Site Configuration**, and then click **Servers and Site System Roles**.
13. Right-click **Servers and Site System Roles**, and then click **Create Site System Server**.
14. In the **Create Site System Server Wizard**, on the **General** page, describe the options, configure the following, and then click **Next**:
15. Name: **TOR-SVR2.Adatum.com**

16. Site code: **S01 – Adatum Site**
17. On the **Proxy** page, click **Next**.
    - On the **System Role Selection** page, select **Distribution point**, and then click **Next**.
    - On the **Distribution point** page, select both of the following options:
18. **Install and configure IIS if required by Configuration Manager**
19. **Enable this distribution point for prestaged content**
20. Discuss the other available options but do not configure any additional settings, and then click **Next**.
    - On the **Drive Settings** page, review the default settings, and then click **Next**.
    - On the **Pull Distribution Point** page, click **Next**.
21. On the **PXE Settings** page, click **Next**.
22. On the **Multicast** page, click **Next**.
23. On the **Content Validation** page, select **Validate content on a schedule**. Discuss the default schedule, and then click **Next**.
24. On the **Boundary Groups** page, discuss the options but do not change any settings, and then click **Next**.
25. On the **Summary** page, click **Next**.
26. On the **Completion** page, click **Close**.
27. Click the **Monitoring** workspace, expand **Distribution Status**, and then click **Distribution Point Configuration Status**.

Note: As the components install, the status might display an error state. This will not affect the rest of the tasks. In the **Microsoft.ConfigurationManagement** pop-up window, click the black **X** on the red background in the upper right to close without taking a specific action.

28. In the results pane, click **TOR-SVR2.Adatum.com**. In the preview pane, discuss the **Summary** and **Details** tabs.
29. In the **Administration** workspace, click the **Distribution Points** node.
30. In the results pane, click **TOR-SVR2.Adatum.com**, and then discuss the information in the preview pane.
31. In the results pane, right-click **TOR-SVR2.Adatum.com**, and then click **Properties**. Discuss the related settings for each tab, and then click **OK** to close the dialog box.
32. Click the **Distribution Point Groups** node.
33. Right-click **Distribution Point Groups**, and then click **Create Group**.
34. In the **Create New Distribution Point Group** dialog box, in the **Name** box, type **London DPs**, and then in the **Description** box, type **Distribution Points located in London**.
35. In the **Create New Distribution Point Group** dialog box, on the **Members** tab, click **Add**.
36. In the **Add Distribution Points** dialog box, select both **LON-CFG.ADATUM.COM** and **TOR-SVR2.ADATUM.COM**, and then click **OK**.
37. In the **Create New Distribution Point Group** dialog box, click the **Collections** tab, and then click **Add**.

38. In the **Select Collections** dialog box, click the drop-down menu, and then click **Device Collections**.
39. Select **All Windows 10 Workstations**, and then click **OK**.
40. To close the **Create New Distribution Point Group** dialog box, click **OK**.

Lesson 2

Distributing and managing content on distribution points

Contents:

Question and Answers

Question: You receive a report that certain software packages are not being installed correctly. You discover that some of the packages' content files have been corrupted. You repair the files on the main site server distribution point. How can you propagate the corrected files to all the other distribution points? Choose all that apply.

( ) From the Software Library workspace, select the content, and then open the Properties dialog box. Click the Content Locations tab, select the distribution point or distribution point group, and then click Redistribute.

( ) From the Monitoring workspace, open the Distribution Status node, and then select Content Status.

( ) From the Administration workspace, open the Distribution Points node. Right-click a distribution point, and then click Properties. On the Content tab, select the content, and then click Redistribute.

( ) On the General tab of the Distribution point properties dialog box, select the Enable this distribution point for prestaged content check box.

( ) From the Administration workspace, open the Distribution Point Groups node. Right-click a distribution point group, and then click Properties. On the Content tab, select the content, and then click Redistribute.

> **Answer:**
>
> (√) From the Software Library workspace, select the content, and then open the Properties dialog box. Click the Content Locations tab, select the distribution point or distribution point group, and then click Redistribute.
>
> ( ) From the Monitoring workspace, open the Distribution Status node, and then select Content Status.
>
> (√) From the Administration workspace, open the Distribution Points node. Right-click a distribution point, and then click Properties. On the Content tab, select the content, and then click Redistribute.
>
> ( ) On the General tab of the Distribution point properties dialog box, select the Enable this distribution point for prestaged content check box.
>
> (√) From the Administration workspace, open the Distribution Point Groups node. Right-click a distribution point group, and then click Properties. On the Content tab, select the content, and then click Redistribute.
>
> **Feedback:**
>
> Options 1, 3, and 5 are all correct and can all be used to redistribute content to distribution points. Option 2 is used to manage content while it is copying to a distribution point. Option 4 is used to prestage content on the distribution point.

Content management tasks and features for distribution points

Question: You plan to prestage a Microsoft Office package to a remote distribution point and then manually copy the initial file package. However, you want to ensure that any future updates to the source content automatically distribute to the distribution point. How do you do this?

> **Answer:** In the Microsoft Office package, for the **Prestaged distribution point settings** option, ensure that you select **Download only content changes to the distribution point**.

Managing content on distribution points

Question: You suspect that the content for a specific software application is corrupted on a distribution point. How can you fix the problem?

Answer: You can redistribute the content to the distribution point, from the properties of the software application or package or from the distribution point itself.

Demonstration: Distributing content to distribution points

Demonstration Steps

1. On **LON-CFG**, open the **Configuration Manager** console if it is not already open.
2. Click the **Software Library** workspace, expand **Application Management**, and then click **Packages**.
3. In the results pane, right-click **User State Migration Tool for Windows**, and then click **Distribute Content**.
4. In the **Distribute Content Wizard**, on the **General** page, click **Next**.
5. On the **Content Destination** page, click **Add**, and then click **Distribution Point Group**.
6. In the **Add Distribution Point Groups** dialog box, select **London DPs**, click **OK**, and then click **Next**.
7. On the **Summary** page, click **Next**.
8. On the **Completion** page, click **Close**.
9. Click the **Monitoring** workspace, expand **Distribution Status**, and then click **Content Status**.
10. In the results pane, click **Microsoft Corporation User State Migration Tool for Windows 10.0.17763.1** Discuss the information that displays in the details pane.
11. In the preview pane, click **View Status**. Discuss the information that displays on the **Success** tab.
12. Refresh the status until **LON-CFG.ADATUM.COM** displays on the **Success** tab, under **Asset Details**.

Demonstration: Managing content on distribution points

Demonstration Steps

1. On **LON-CFG**, in the **Administration** workspace, click the **Distribution Points** node.
2. In the results pane, right-click **LON-CFG.Adatum.com**, and then click **Properties**.
3. Click the **Content** tab. Discuss the **Validate**, **Redistribute**, and **Remove** buttons, and then click **OK**.
4. Click the **Software Library** workspace, expand **Application Management**, and then click **Packages**.
5. In the results pane, right-click **User State Migration Tool for Windows**, and then click **Properties**.
6. Click the **Content Locations** tab. Discuss the **Validate**, **Redistribute**, and **Remove** buttons, and then click **OK**.

Demonstration: Configuring content prestaging

Demonstration Steps

Create and distribute a package

1. On **LON-CFG**, in the **Configuration Manager** console, click the **Software Library** workspace.
2. In the navigation pane, expand **Application Management**, and then click the **Applications** node.
3. On the ribbon, click **Create**, and then click **Create Application**.
4. In the **Create Application Wizard**, on the **General** page, verify that in the **Type** box, **Windows Installer (*.msi file)** displays.

5. In the **Location** box, type **\\LON-CFG\E$\Software\MSI_Files\PPTViewer\ppviewer.msi**, and then click **Next**.
6. On the **Import Information** page, click **Next**.
7. On the **General Information** page, click **Next**.
8. On the **Summary** page, click **Next**.
9. On the **Completion** page, click **Close**.
10. In the Configuration Manager console, in the results pane, click the **Microsoft PowerPoint Viewer** application, and then on the ribbon, click **Deployment**. Click **Distribute Content**.
11. In the **Distribute Content Wizard**, on the **General** page, click **Next**.
12. On the **Content** page, click **Next**.
13. On the **Content Destination** page, click **Add**, and then click **Distribution Point**.
14. In the **Add Distribution Points** dialog box, select **LON-CFG.ADATUM.COM**, **TOR-SVR2.ADATUM.COM**, and then click **OK**.
15. On the **Content Destination** page, click **Next**.
16. On the **Summary** page, click **Next**.
17. On the **Completion** page, click **Close**.

Create a prestaged content file

1. On **LON-CFG**, in the **Configuration Manager** console, click the **Software Library** workspace, and then verify that you are in the **Applications** node.
2. In the results pane, click **Microsoft PowerPoint Viewer**, and then on the ribbon, in the Application area, click **Create Prestaged Content File**.
3. In the **Create Prestaged Content File Wizard**, on the **General** page, click **Browse**.
4. In the **Prestaged content file** dialog box, navigate to the **Allfiles (E:)** drive. In the **File name** box, type **PowerPointViewer**, and then click **Save**.
5. On the **General** page, click **Next**.
6. On the **Content** page, click **Next**.
7. On the **Content Locations** page, click **Add**.
8. In the **Add Distribution Points** dialog box, select **LON-CFG.Adatum.com**, and then click **OK**.
9. On the **Content Locations** page, click **Next**.
10. On the **Summary** page, click **Next**.
11. On the **Completion** page, click **Close**.
12. On the taskbar, click the **File Explorer** icon.
13. Browse to the **Allfiles (E:)** drive, right-click **PowerPointViewer.pkgx**, and then click **Copy**.
14. In the **File Explorer** address bar, type **\\TOR-SVR2\C$**, and then press Enter.
15. Right-click in the File Explorer window's results pane, and then click **Paste** on the context menu.

Extract a prestaged content file on a distribution point

1. On **TOR-SVR2**, click **Start**, type **CMD**, and then click **Command Prompt**.

2. At the command prompt, type the following commands, and then press Enter at the end of each command.

```
CD C:\SMS_DP$\sms\Tools
extractcontent.exe /P:C:\PowerPointViewer.pkgx /S
```

Monitor the prestaged content status

1. On **LON-CFG**, in the **Configuration Manager** console, click the **Monitoring** workspace.
2. In the navigation pane, expand **Distribution Status**, and then click the **Content Status** node.
3. In the results pane, click **Microsoft PowerPoint Viewer**.
4. Review the information in the preview pane. Notice that two distribution points were targeted and that **Success** is now listed as **2**. You might need to refresh the pane to view the updated results.

Module Review and Takeaways

Best Practices

- If the content on a distribution point includes sensitive data that you need to transmit over public networks, encrypt the transfer through HTTPS.
- A cloud-based distribution point can serve as an alternative to deploying a distribution point at a small branch site.
- Consider using prestaged content when you have limited network bandwidth between the site server and the distribution point.

Review Question

Question: In which scenarios would you prestage content?

> **Answer:** You would prestage content when you need to distribute large files to remote locations where the time or expense required to transfer the content across WAN links is prohibitive.

Tools

The following table lists the tools that this module references.

Tool	**Purpose**	**Where to find it**
Content Library Transfer Tool	Move the content library to a different location on a distribution point after the installation	CD.Latest\SMSSETUP\Tools\
Content Library Explorer	Assist in troubleshooting issues with the content library and viewing its contents	CD.Latest\SMSSETUP\Tools\

Lab Review Questions and Answers

Lab: Distributing and managing content for deployments

Question and Answers

Question: Where can you find the status of distributed software?

> **Answer:** You can review the status of distributed software in the Monitoring Workspace, under Distribution Status.

Question: How can you distribute content to multiple distribution points?

> **Answer:** One method of distributing content is to create a distribution point group. Additionally, you can select multiple distribution points in the Distribution Wizard.

Module 7

Deploying and managing applications

Contents:

Lesson 1

Overview of application management

Contents:

Question and Answers

Question: Which of the following components associate with deployments?

( ) The package's name with the location of source files.

( ) The command with the package files.

( ) A program with a target collection.

( ) The distribution points with the program.

( ) A program with the location of the source files.

Answer:

( ) The package's name with the location of source files.

( ) The command with the package files.

(√) A program with a target collection.

( ) The distribution points with the program.

( ) A program with the location of the source files.

Feedback:

From the text in the first topic above: Deployments, which are similar to advertisements in prior versions of Configuration Manager, associate a program with a target collection.

Lesson 2

Creating applications

Contents:

Question and Answers

Categorize each item into the appropriate category. Indicate your answer by writing the category number to the right of each item.

Items	
1	Application deployment types that are added as a prerequisite for another application's deployment type.
2	Defines attributes that Configuration Manager evaluates to determine if a deployment type applies to a particular user or device.
3	Application deployment evaluation cycle evaluates requirements for each deployment type for the target device or user.
4	Can be configured to install independently.
5	Builds requirements that will contain the checked values.
6	Uses value and existential rule types.
7	Ensures application requirements can be enforced or remediated.
8	Verifies that a specific .NET assembly is available.
9	Categories include user, device and custom.

Category 1		Category 2		Category 3
Dependencies		Global conditions		Requirements

Answer:

Category 1		Category 2		Category 3
Dependencies		Global conditions		Requirements

Category 1		Category 2		Category 3
Application deployment types that are added as a prerequisite for another application's deployment type. Can be configured to install independently. Ensures application requirements can be enforced or remediated.		Defines attributes that Configuration Manager evaluates to determine if a deployment type applies to a particular user or device. Builds requirements that will contain the checked values. Verifies that a specific .NET assembly is available.		Application deployment evaluation cycle evaluates requirements for each deployment type for the target device or user. Uses value and existential rule types. Categories include user, device and custom.

Demonstration: Creating an application from an MSI file

Demonstration Steps

Create an application from an .msi file

1. On **LON-CFG**, if not open already, open the Configuration Manager console.
2. Click the **Software Library** workspace, expand **Application Management**, and then click **Applications**.
3. Right-click **Applications**, and then click **Create Application**.
4. In the **Create Application Wizard**, on the **General** page, ensure that the **Automatically detect information about this application from installation files** option is selected and that the **Type** list displays **Windows Installer (*.msi file)**, and then click **Browse**.
5. Navigate to **\\LON-CFG\Software\MSI_Files\ExcelViewer**, click **xlview.msi**, and then click **Open**.
6. On the **General** page, click **Next**.
7. On the **Import Information** page, click **Next**.
8. On the **General Information** page, in the **Administrator comments** text box, type **Excel viewer program**. In the **Publisher** text box, type **Microsoft**, and then in the **Software version** text box, type **12.0.4518.1069**.
9. Next to **Administrative categories**, click **Select**.
10. In the **Manage Administrative Categories** dialog box, click **Create**.
11. In the **Create Administrative Category** text box, type **Viewer**, and then click **OK**.
12. In the **Manage Administrative Categories** dialog box, click **OK**.
13. On the **General Information** page, click **Next**.
14. On the **Summary** page, click **Next**.
15. On the **Completion** page, click **Close**.

Modify the application

1. In the results pane, click **Microsoft Office Excel Viewer**, and then on the ribbon, click **Properties**.
2. Review the settings on the **General Information** tab.
3. On the **Application Catalog** tab, next to **User categories**, click **Edit**.

4. In the **User Categories** dialog box, click **Create**.
5. In the **Create User Category** dialog box, in the **Specify the name of the new user category** text box, type **Viewers**, and then click **OK**.
6. In the **User Categories** dialog box, click **Create**.
7. In the **Create User Category** dialog box, in the **Specify the name of the new user category** text box, type **Excel**, and then click **OK**.
8. In the **User Categories** dialog box, click **OK**.
9. In the **Keywords** text box, type **Spreadsheet**, and then next to **Icon**, click **Browse**.
10. In the **Open** dialog box, navigate to **C:\Windows\System32\imageres.dll**, and then click **Open**.
11. Click any icon, and then click **OK**.
12. In the **Microsoft Office Excel Viewer Properties** dialog box, click **OK**.

Demonstration: Creating a global condition and deployment type requirement

Demonstration Steps

Create a global condition

1. On **LON-CFG**, if not open already, open the Configuration Manager console.
2. In the Configuration Manager console, click the **Software Library** workspace, expand the **Application Management** folder, and then click the **Global Conditions** node.
3. On the ribbon, click **Create Global Condition**.
4. In the **Create Global Condition** dialog box, click **Browse**.
5. In the **Browse Registry** dialog box, expand **HKEY_LOCAL_MACHINE**, expand **SOFTWARE**, expand **Microsoft**, click **Internet Explorer**. In the **Registry Value** box, click **Version**, and then click **OK**.
6. In the **Create Global Condition** dialog box, in the **Name** text box, type **Internet Explorer Version**.
7. In the **Create Global Condition** dialog box, click **OK**.

Use a global condition to create a requirement

1. In the **Software Library** workspace, in the **Application Management** folder, click the **Applications** node.
2. Right-click **Microsoft Office Excel Viewer**, and then click **Properties**.
3. Click the **Deployment Types** tab.
4. Click **Microsoft Office Excel Viewer – Windows Installer (*.msi file)**, and then click **Edit**.
5. Click the **Requirements** tab, and then click **Add**.
6. In the **Category** list, click **Custom**.
7. In the **Condition** list, click **Internet Explorer Version**.
8. In the **Value** box, type **9.11.14393.0**, and then click **Cancel**.
9. In the **Microsoft Office Excel Viewer - Windows Installer (*.msi file) Properties** dialog box, click **Cancel**.
10. In the **Microsoft Office Excel Viewer Properties** dialog box, click **Cancel**.

Lesson 3

Deploying applications

Contents:

Question and Answers

Question: You need to ensure that a deployed application only goes to users who request that application. When you are creating the application in Configuration Manager, what steps should you take to accomplish this?

( ) On the General page of the Deploy Software Wizard, select the specific user collection that applies to the users you want the application to go to.

( ) On the User Experience page of the Deploy Software Wizard, clear the Commit changes at deadline or during a maintenance window (requires restart) check box.

( ) On the Content page of the Deploy Software Wizard, specify the distribution point for the specific subset of users you want the application to go to.

( ) On the Deployment Settings page of the Deploy Software Wizard, select the Require administrator approval if users request this application check box.

( ) On the Deployment Settings page of the Deploy Software Wizard, in the Purpose dropdown box, click Required.

Answer:

( ) On the General page of the Deploy Software Wizard, select the specific user collection that applies to the users you want the application to go to.

( ) On the User Experience page of the Deploy Software Wizard, clear the Commit changes at deadline or during a maintenance window (requires restart) check box.

( ) On the Content page of the Deploy Software Wizard, specify the distribution point for the specific subset of users you want the application to go to.

(√) On the Deployment Settings page of the Deploy Software Wizard, select the Require administrator approval if users request this application check box.

( ) On the Deployment Settings page of the Deploy Software Wizard, in the Purpose dropdown box, click Required.

Feedback:

When you select the Require administrator approval if users request this application check box, the users see the application in the Application Catalog, but must have an administrator specifically provide it to them upon request.

Demonstration: Deploying an application

Demonstration Steps

1. On **LON-CFG**, if not open already, open the Configuration Manager console.
2. Click the **Software Library** workspace, and then under **Application Management**, click the **Applications** node.
3. Click **Microsoft Office Excel Viewer**.
4. On the ribbon, click **Deployment**, and then click **Deploy**.

Note: Depending on the screen resolution of your host system, the **Deployment** button may be expanded to be a **Deployment** section on the ribbon.

5. In the **Deploy Software Wizard**, on the **General** page, next to the **Collection** box, click **Browse**.

6. In the **Select Collection** dialog box, click **All Users**, click **OK**, and then click **Next**.
7. On the **Content** page, click **Add**, and then click **Distribution Point**.
8. In the **Add Distribution Points** dialog box, select the **LON-CFG.ADATUM.COM** check box, and then click **OK**.
9. On the **Content** page, click **Next**.
10. On the **Deployment Settings** page, in the **Purpose** list, click **Required**, and then click **Next**.
11. On the **Scheduling** page, select the **Schedule at** option, in the date list, select *tomorrow's date*, and then click **Next**.
12. On the **User Experience** page, click **Next**.
13. On the **Alerts** page, click **Next**.
14. On the **Summary** page, click **Next**.
15. On the **Completion** page, click **Close**.

Lesson 4

Managing applications

Contents:

Question and Answers

Question: An administrator needs to uninstall an application that is already deployed. To do so, the administrator must first remove the original deployment that installed the application, before creating a deployment package to uninstall the application.

( ) True

( ) False

Answer:

(√) True

( ) False

Feedback:

The uninstall deployment will fail if there is an existing install deployment for the software affecting the clients targeted with the uninstall action.

What is application revision history?

Question: When would you use revision history to revert to a previous version of the application?

Answer: Answers will vary based on the user's experience. One reason for reverting would be to undo a change to a deployment type that caused unexpected behavior.

Demonstration: Configuring application supersedence

Demonstration Steps

Configure a supersedence relationship

1. On LON-CFG, on the taskbar, click **Configuration Manager Console**.
2. Click the **Software Library** workspace, expand **Application Management**, and then click **Applications**.
3. Right-click **Applications**, and then click **Create Application**.
4. In the Create Application Wizard, on the **General** page, ensure that the **Automatically detect information about this application from installation files** option is selected, and that the **Type** list displays **Windows Installer (*.msi file)**, and then click **Browse**.
5. Navigate to **\\LON-CFG\Software\MSI_Files\VisioViewer**, click **vviewer.msi**, and then click **Open**.
6. On the **General** page, click **Next**.
7. On the **Import Information** page, click **Next**.
8. On the **General Information** page, click **Next**.
9. On the **Summary** page, click **Next**.
10. On the **Completion** page, click **Close**.
11. On LON-CFG, click the **Software Library** workspace, expand the **Application Management** folder, and then click the **Applications** node.
12. Click the **Microsoft Visio Viewer 2013** application, and on the ribbon, click **Properties**.
13. In the **Microsoft Visio Viewer 2013 Properties** dialog box, click the **Deployment Types** tab.
14. Click the **Microsoft Visio Viewer 2013 – Windows installer (*.msi file)** deployment type, and then click **Edit**.

15. In the **Microsoft Visio Viewer 2013 – Windows installer (*.msi file) Properties** dialog box, click the **Requirements** tab.
16. On the **Requirements** tab, click **Add**.
17. In the **Create Requirement** dialog box, click the **Category** drop-down list box, and then click **Device**.
18. Click the **Condition** drop-down list box, and then click **Operating system**.
19. In the **Operator** list, select the **Windows 10** check box.
20. In the **Create Requirement** dialog box, click **OK**.
21. In the **Microsoft Visio Viewer 2013 – Windows installer (*.msi file) Properties** dialog box, click **OK**.
22. Click the **Supersedence** tab.
23. Click the **Add** button.
24. In the **Specify Supersedence Relationship** dialog box, click **Browse**.
25. In the **Choose Application** dialog box, click **Microsoft Office Excel Viewer**, and then click **OK**.
26. In the **Specify Supersedence Relationship** dialog box, click the **New Deployment Type** drop-down list box, and then click **Microsoft Visio Viewer 2013 – Windows Installer (*.msi file)**.
27. Select the **Uninstall** check box for the **Microsoft Office Excel Viewer - Windows Installer (*.msi file)** deployment type, and then click **OK**.
28. In the **Microsoft Visio Viewer 2013 Properties** dialog box, click **OK**.

View the relationship

1. In the results pane, click **Microsoft Visio Viewer 2013**.
2. On the ribbon, click the **View Relationships** button, and then click **Supersedence**.
3. Discuss the Microsoft Visio Viewer 2013 Supersedence window, and then click **OK**.

Lesson 5

Deploying virtual applications by using System Center Configuration Manager (Optional)

Contents:

Question and Answers

Question: What are the two methods for virtualizing applications?

( ) Streaming and local delivery

( ) Remote and streaming

( ) Remote and local delivery

( ) App-V cache and streaming

( ) App-V cache and remote

Answer:

( ) Streaming and local delivery

(√) Remote and streaming

( ) Remote and local delivery

( ) App-V cache and streaming

( ) App-V cache and remote

Feedback:

Only option 2 is correct. All other options include various delivery and virtualization methods, but not the method to virtualize the application itself.

Lesson 6

Deploying and managing Windows Store apps

Contents:

Question and Answers

Deploying the System Center Configuration Manager Company Portal. Put the following steps in order by numbering each to indicate the correct order.

	Steps
	Create the CCM\PortalPackageFamily registry key. Ensure that the CCM\PortalPackageFamily registry key is set on every device that will have the company portal installed.
	Ensure an Application Catalog web service point site system role exists.
	Download and run the SCCMCompanyPortal.exe file, which extracts SCCMCompanyPortal.appx and license files.
	In Configuration Manager, create an application and deploy the SCCMCompanyPortal.appx file to all devices where you want the company portal installed.
	After all deployment conditions have been met, such as correct collection and scheduled time, check a Windows device and see if the System Center Configuration Manager Company Portal app is installed.

Answer:

	Steps
1	Create the CCM\PortalPackageFamily registry key. Ensure that the CCM\PortalPackageFamily registry key is set on every device that will have the company portal installed.
2	Ensure an Application Catalog web service point site system role exists.
3	Download and run the SCCMCompanyPortal.exe file, which extracts SCCMCompanyPortal.appx and license files.
4	In Configuration Manager, create an application and deploy the SCCMCompanyPortal.appx file to all devices where you want the company portal installed.
5	After all deployment conditions have been met, such as correct collection and scheduled time, check a Windows device and see if the System Center Configuration Manager Company Portal app is installed.

Resources

Requirements for deploying Windows Store apps

Additional Reading: For more information, refer to Using the Windows App Certification Kit: http://aka.ms/lkqcxq

Additional Reading: For more information, refer to Manage the certificates that Visual Studio uses to sign your app: http://aka.ms/g1cczy

Methods for accessing available Windows Store apps

Additional Reading: For more information, refer to About Client Settings in Configuration Manager: http://aka.ms/yhns46

Module Review and Takeaways

Best Practices

- Always remove an install application deployment before creating a deployment to uninstall that application.
- The phased deployment feature is a new evolving feature, but in Configuration Manager 1810 you currently can only perform a two-phased deployment.

Review Questions

Question: When deploying applications by using deployment types other than Windows Installer (*.msi files), such as Windows 8.1 apps and Microsoft Application Virtualization, how do you troubleshoot problems?

> **Answer:** You troubleshoot deployments by using the same method, regardless of the deployment type that you use. Methods include reviewing:
>
> - Any error messages generated.
> - The appropriate client log files.
> - The appropriate status messages.

Question: What are some of the differences between an application and a package?

> **Answer:** There are several differences between an application and a package, including, but not limited to:
>
> - An application uses deployment types instead of programs.
> - You can define supersedence relationships in an application.
> - You can add more user-searchable information to an application.

Question: For what do you use detection methods?

> **Answer:** Detection methods enable the deployment process to determine whether an application is present in a system. Detection methods can use file or folder properties, registry settings, or scripts for determining whether a particular application is installed.

Question: Can you add multiple instances of the same deployment types to a single application?

> **Answer:** Yes. In fact, in several situations you may need to create multiple instances of the same deployment types for a single application, such as when there are different dependencies based on the operating system target.

Tools

The following table lists the tools that this module references.

Tool	Used to	Where to find it
Windows App Certification Kit	Test your apps for the Windows Store (for Windows 10, Windows 8.1 and Windows 8), and for the Windows 10, Windows 8.1, Windows 8, and Windows 7 Windows Certification program for desktop applications.	The Windows SDK for Windows 10. You can download it from https://aka.ms/qnpijc

Tool	Used to	Where to find it
System Center Configuration Manager Company Portal app	Allows users of Windows 8, Windows 8.1 and Windows 10 machines to view and install applications made available to the user by their administrators.	The Windows Store and the Microsoft Download Center

Common Issues and Troubleshooting Tips

Common Issue	Troubleshooting Tip
After creating a deployment for the System Center Configuration Manager Company Portal, you notice some of the Windows devices have installed, but others do not.	Ensure that all Windows devices that you want to have the company portal on have the required registry key added.
You need to uninstall an older application from all users. You create an uninstall deployment for that application, but the uninstall fails.	Ensure that you first remove the original install deployment for that application.

Lab Review Questions and Answers

Lab A: Creating and deploying applications

Question and Answers

Question: Why do the statuses of the two deployed applications differ?

> **Answer:** You deployed Microsoft Office Word Viewer as Required. Therefore, the status is based on all users who have or have not installed the application, and the systems that have downloaded the content.
>
> You deployed Microsoft Office Excel Viewer as Available. Therefore, the status process does not have any information to use other than attempted installations.

Lab B: Managing application supersedence and removal

Question and Answers

Question: When you signed on as Pam during Exercise 1, why did you see information about only the Microsoft Excel application and the Microsoft Visio Viewer application?

> **Answer:** The Microsoft Visio Viewer application replaced the Microsoft Word Viewer application. Therefore, the Word Viewer application was no longer available.

Question: During Exercise 2, after you signed in as Pam, why did you see information for the Microsoft Visio Viewer application and the Excel Viewer application, but not the Word Viewer application?

> **Answer:** The Microsoft Visio Viewer application replaced the Word Viewer application. Therefore, information about the Word Viewer application no longer displays. The Excel Viewer application was uninstalled but not replaced, so the Excel Viewer application still exists on the server and could be made available in the future.

Lab C: Deploying virtual applications by using Configuration Manager (Optional)

Question and Answers

Question: In your environment, would you deploy App-V deployment types as the only deployment type in your applications, or would you include them as one of several deployment types?

> **Answer:** Answers may vary, but could include creating applications with both App-V and Windows Installer (*.msi file) deployment types, and then using requirements to determine the deployment type to use at runtime.

Question: Why would a large App-V application take a long time to start after the installation completes?

> **Answer:** The installation copied the package content into the Configuration Manager cache. The first time the application runs, the App-V client must copy the package content to the App-V cache.

Lab D: Using Configuration Manager to deploy Windows Store apps

Question and Answers

Question: How would you configure the sideloading GPO if your client computers used different versions of the Windows operating system?

Answer: Answers will vary depending on the students' experiences, but may include configuring a Windows Management Instrumentation (WMI) filter for the Group Policy Object (GPO) to limit applications to Windows 10–based computers. Another answer may include creating a Windows 10 device group, and configuring permissions to apply the policy only to that group.

Question: How can you troubleshoot Windows 10 app deployments?

Answer: Troubleshooting a Windows 10 app deployment is the same as troubleshooting any other application deployment. You use the related local log files on the client, and the status messages sent to the server.

Module 8

Maintaining software updates for managed PCs

Contents:

Lesson 1

The software updates process

Contents:

Question and Answers

Question: What are the prerequisites for the Software Updates feature in Configuration Manager?

> **Answer:** You must install WSUS either on the site server or on a remote server. You then add the software update point role to that server.

Question: Which version of WSUS should you use?

> **Answer:** You use Windows Server Update Services (WSUS) 4.0 included in Windows Server 2016 and later versions because Configuration Manager version 1702 does not support Windows Server 2008 or Windows Server 2008 R2, for site server installation or for most site system roles. Windows Server 2012 or Windows Server 2012 R2 could also be used but they require hotfixes installed to support feature upgrades on Windows 10. These hotfixes are not required on Windows Server 2016 or Windows Server 2019.

Resources

Prerequisites for the software updates feature

Reference Links: Download the **Update to enable WSUS support for Windows 10 feature upgrades** hotfix from: http://aka.ms/Rh2uzc

Additional Reading: Download the **Update enables ESD decryption provision in WSUS in Windows Server 2012 and Windows Server 2012 R2** hotfix from: https://aka.ms/ob283k

Lesson 2

Preparing a Configuration Manager site for software updates

Contents:

Question and Answers

Question: Why should you disable Automatic Updates on all your Configuration Manager client computers?

> **Answer:** This will ensure that the Windows Update agent does not detect pending restarts, displays an additional warning to the end user, or restarts the machine. This setting will also disable the Windows Update agent from updating itself from WSUS.

Question: You can use a maintenance window to control when a Configuration Manager client computer requests a policy update.

( ) True

( ) False

> **Answer:**
>
> ( ) True
>
> (√) False
>
> **Feedback:**
>
> No. You can use maintenance windows to control when:
>
> - Required software deployments can run
> - Software updates will deploy
> - Compliance setting deployments and evaluations can run
> - Operating system deployments can occur
> - Task sequence deployments can run

Demonstration: Installing and configuring the software update point

Demonstration Steps

1. On **LON-SVR1**, open **Server Manager**.
2. In the Server Manager console, click **Tools**, and then click **Computer Management**.
3. In Computer Management, expand **System Tools** (if needed), expand **Local Users and Groups**, and then click **Groups**.
4. In the details pane, double-click **Administrators**.
5. In the **Administrators Properties** dialog box, click **Add**.
6. In the **Select Users, Computers, Service Accounts, or Groups** dialog box, click **Object Types**.
7. In the **Object Types** dialog box, select the **Computers** check box, and then click **OK**.
8. In the **Select Users, Computers, Service Accounts, or Groups** text box, type **LON-CFG**, click **Check Names**, and then click **OK**.
9. To close the **Administrators Properties** dialog box, click **OK**. Close **Computer Management**.
10. In the **Server Manager** console, in the navigation pane, click **WSUS**. Verify that **LON-SVR1** is listed in the **SERVERS** section. This will indicate that **WSUS** is installed.
11. Close **Server Manager**.
12. On **LON-CFG**, open the **Configuration Manager console**.

13. Click the **Administration** workspace, expand **Site Configuration**, and then click **Servers and Site System Roles**.
14. Right-click **Servers and Site System Roles**, and then click **Create Site System Server**.
15. In the **Create Site System Server Wizard**, on the **General** page, describe the options, and then configure the following settings:
    - Name: **LON-SVR1.Adatum.com**
    - Site code: **S01 – Adatum Site**
16. Click **Next**.
17. On the **Proxy** page, click **Next**.
18. On the **System Role Selection** page, select the **Software update point** check box, and then click **Next**.
19. On the **Software Update Point** page, click the **WSUS is configured to use ports 8530 and 8531 for client communications (default settings for WSUS on Windows Server 2012)** option, and then click **Next**.
20. On the **Proxy and Account Settings** page, click **Next**.
21. On the **Synchronization Source** page, click **Do not synchronize from Microsoft Update or upstream data source**, and then click **Next**.
22. On the **Synchronization Schedule** page, click **Next**.
23. On the **Supersedence Rules** page, under **Supersedence behavior for NonFeature Update**, click **Immediately expire a superseded software update**.
24. Under **Supersedence behavior for Feature Update**, click **Immediately expire a superseded software update**. Discuss the other options, and then click **Next**.
25. On the **Updates Files** page, select **Download full files for all approved updates**, and then click **Next**.
26. On the **Classifications** page, select only the following (clear all other selections), and then click **Next**:
    - **Critical Updates**
    - **Definition Updates**
    - **Security Updates**
27. On the **Products** page, expand all the nodes and clear the check boxes next to all selected products, and then click **Next**.

Note: Point out that you do not select any products now, because Windows 10 and Microsoft Office 2016 will first be available after the initial synchronization. You will select them later in the demonstration.

28. On the **Languages** page, ensure that only **English** is selected. Clear any other selected languages, and then click **Next**.
29. On the **Summary** page, click **Next**.
30. On the **Completion** page, click **Close**.
31. Click the **Monitoring** workspace, expand **System Status**, and then click **Component Status**.

32. In the results pane, scroll down, and then click **SMS_WSUS_CONTROL_MANAGER**.
33. Right-click **SMS_WSUS_CONTROL_MANAGER**, point to **Show Messages**, and then click **All**.
34. In the **Status Messages: Set Viewing Period** dialog box, click **OK**.
35. In **Configuration Manager Status Message Viewer**, discuss the messages related to the component installation on **LON-SVR1**. Refresh the display until status message **1015** displays. This might take a few minutes.
36. Close **Configuration Manager Status Message Viewer**.
37. Click the **Software Library** workspace, expand **Software Updates**, and then click **All Software Updates**.
38. Right-click **All Software Updates**, click **Synchronize Software Updates**, and then click **Yes**.

Note: Wait for approximately five minutes. While you are waiting, explain that this initial synchronization will upload the latest product catalog.

39. Click the **Administration** workspace, expand **Site Configuration**, and then click **Sites**.
40. In the results pane, right-click **S01 – Adatum Site**, point to **Configure Site Components**, and then click **Software Update Point**.
41. Click the **Products** tab, and then select both **Office 2016** and **Windows 10**. If these products are not visible, repeat steps 36 through 39.
42. To close the **Software Update Point Component Properties** dialog box, click **OK**.
43. Click the **Software Library** workspace, expand **Software Updates**, and then click **All Software Updates**.
44. Right-click **All Software Updates**, and then click **Synchronize Software Updates**.
45. In the **Configuration Manager** dialog box, to initiate a site-wide synchronization of software updates, click **Yes**.
46. Click the **Monitoring** workspace, and then click **Software Update Point Synchronization Status**. Point out the information in the preview pane.
47. Refresh the view until the icon changes to a green circle with a white check mark.

Note: Depending on how quickly your virtual machines are performing, this step could take up to 15 minutes to complete.

48. Click the **Software Library** workspace, expand **Software Updates**, and then click **All Software Updates**.

Note: It may take a few minutes for the updates to display. If the updates do not display within a few minutes, repeat steps 42 and 44.

49. Click the **Administration** workspace, expand **Hierarchy Configuration** and then click **Boundary Groups**.
50. In the details pane, right-click **London** and then click **Properties**.
51. In the **London Properties** window, click the **References** tab and then click **Add**.

52. In the **Add Site Systems** window, click **\\LON-SVR1.Adatum.com** and then click **OK**.
53. In the **London Properties** window, click **OK**.
54. In the **Administration** workspace, and then click **Client Settings**.
55. In the results pane, right-click **Default Client Settings**, and then click **Properties**.
56. In the **Default Settings** dialog box, click **Software Updates**. Verify that software updates are enabled, and then discuss other options, as needed.
57. Click **State Messaging**. Verify that the **State Messaging** value has a reporting cycle of **5 minutes**.
58. To close the **Default Settings** dialog box, click **OK**.
59. On **LON-CL1**, click the **Start** button, type **control**, and then click **Control Panel**. Click **System and Security**.
60. In **System and Security**, scroll down to the bottom and click **Configuration Manager**.
61. In the **Configuration Manager Properties** dialog box, click the **Actions** tab, select **Machine Policy Retrieval & Evaluation Cycle**, and click **Run Now.** Then click **OK.**
62. Select **Software Updates Scan Cycle**, and click **Run Now.** Then click **OK.**
63. Click **OK** to close the **Configuration Manager** dialog box and then close the **Control Panel**.

Lesson 3
Managing software updates

Contents:

Question and Answers

Question: Even though you do not have to use software update groups when deploying software updates, why is it a recommended practice?

Answer: Using software update groups will let you:

- Ensure ease of management when you deploy multiple updates.
- Track the compliance status for multiple updates.
- Delegate the administration of software updates.

Question: How do you enable the WSUS cleanup task?

Answer:

1. In the Configuration Manager console, select the **Administration** workspace, expand **Site Configuration**, and then click the **Sites** node.
2. In the details pane, right-click the site object for your site (for example, **S01 - Adatum Site**), select **Configure Site Components**, and then select **Software Update point**.
3. In the **Software Update Point Component Properties** dialog box, click the **Supersedence Rules** tab.
4. On the **Supersedence Rules** tab, select **Run WSUS cleanup wizard**.

Resources

Managing WSUS cleanup tasks

Additional Reading: For more information, refer to The complete guide to Microsoft WSUS and Configuration Manager SUP maintenance: https://aka.ms/AA4n4xb

Demonstration: Creating software update groups and deployment packages

Demonstration Steps

1. On **LON-CFG**, open the **Configuration Manager console**.
2. Click the **Software Library** workspace, expand **Software Updates**, and then click **All Software Updates**.
3. In the results pane, select the update **2019-02 Cumulative Update for Windows 10 Version 1809 for x64-based Systems (KB4487044)**.
4. On the ribbon, click the **Home** tab, and then click **Create Software Update Group**.
5. In the **Create Software Update Group** dialog box, configure the following settings, and then click **Create**:
   - Name: **Security Updates – Windows 10**
   - Description: **Security Updates for Windows 10**
6. In the **Software Library** workspace, under **Software Updates**, click **Software Update Groups**. Verify that the **Security Updates – Windows 10** software update group displays in the results pane.
7. Select **Security Updates – Windows 10**, and then on the ribbon, click **Show Members**. Verify that the update that you added displays.

8. Under **Software Updates**, click **Software Update Groups**.
9. In the ribbon, click **Run Summarization**.
10. In the **Configuration Manager** dialog box, click **OK**.

Note: Wait for a few minutes for the preview pane to display the compliance statistics for the **Security Updates – Windows 10** software update group. Refresh the results pane, as necessary.

11. In the navigation pane, expand **Software Updates**, and then click **Software Update Groups**.
12. In the list pane, right-click **Security Updates – Windows 10**, and then click **Download**.
13. In the **Download Software Updates Wizard**, on the **Deployment Package** page, verify that **Create a new deployment package** is selected, configure the following settings, and then click **Next**:
    - Name: **Security Updates – Windows 10**
    - Package source: **\\LON-CFG\E$\Source\Updates**
14. On the **Distribution Points** page, click **Add**, and then click **Distribution Point**.
15. In the **Add Distribution Points** dialog box, select **LON-CFG.ADATUM.COM**, and then click **OK**.
16. On the **Distribution Points** page, click **Next**.
17. On the **Distribution Settings** page, click **Next**.
18. On the **Download Location** page, click **Download software updates from a location on my network**.
19. In the text box, type **\\LON-CFG\E$\Software\Updates**, and then click **Next**.
20. On the **Language Selection** page, verify that only **English** is selected, and then click **Next**.
21. On the **Summary** page, click **Next**.
22. On the **Completion** page, verify that the package and software updates show success as indicated by a green check mark icon, and then click **Close**.
23. In the navigation pane, under **Software Updates**, click **Deployment Packages**.
24. In the preview pane, verify that the **Distribution Point Status** shows **Success**, indicated by a full green circle.

Demonstration: Deploying software updates

Demonstration Steps

1. On **LON-CFG**, open the **Configuration Manager console**.
2. Click the **Software Library** workspace, expand **Software Updates**, and then click **Software Update Groups**.
3. In the results pane, click **Security Updates – Windows 10**. On the ribbon, click **Deploy**.
4. In the **Deploy Software Updates Wizard**, on the **General** page, configure the following settings, and then click **Next**:
    - Deployment Name: **Security Updates – Windows 10**
    - Collection: **All Windows 10 Workstations**

5. On the **Deployment Settings** page, next to **Type of deployment**, select **Required**, and then click **Next**.
6. On the **Scheduling** page, configure the following settings, and then click **Next**:
    - Schedule evaluation: **Client local time**
    - Software available time: **As soon as possible**
    - Installation deadline: **As soon as possible**
7. On the **User Experience** page, configure the following setting, and then click **Next**:
    - User notifications: **Display in Software Center and show all notifications**
8. On the **Alerts** page, select **Generate an alert when the following conditions are met**, and then click **Next**.
9. On the **Download Settings** page, click **Next**.
10. On the **Summary** page, verify that the settings are correct, and then click **Save As Template**. Be sure to point out this option so that students understand where to create a template.
11. In the **Save As Template** dialog box, in the **Name** text box, type **Security Updates – Windows 10**, and then click **Save**.
12. On the **Summary** page, click **Next**.
13. On the **Completion** page, click **Close**.
14. Switch to **LON-CL1**.
15. Open **Control Panel**, and then click **System and Security**.
16. In **System and Security**, click **Configuration Manager**.
17. In the **Configuration Manager Properties** dialog box, click the **Actions** tab.
18. On the **Actions** tab, click **Machine Policy Retrieval & Evaluation Cycle**, click **Run Now**, and then click **OK**.
19. On the **Actions** tab, click **Software Updates Deployment Evaluation Cycle**, click **Run Now**, and then click **OK**.
20. To close the **Configuration Manager Properties** dialog box, click **OK**. Close **Control Panel**.
21. After a few minutes, verify that the **Software changes are required** notification displays in the lower right corner.
22. When the notification displays, open **Software Center** by clicking the up-arrow in the taskbar next to then network icon. Click **Downloading and installing software** and then click **Open Software Center**.
23. In **Software Center**, on the **Installation Status** tab, take note of the installation status and the details for the software update.
24. When the software update installation is complete, click the **Requires restart**, and click **Restart** two times. Wait five minutes for **LON-CL1** to restart and report back status.
25. On **LON-CFG**, click the **Monitoring** workspace, and then click **Deployments**.
26. In the results pane, click **Security Updates – Windows 10**. On the ribbon, click **Run Summarization**, and then click **OK**. Describe the information in the preview pane. It may take several minutes for the details to appear.
27. On the **ribbon**, click **Refresh**.

28. If the **Completion Statistics** does not show **Compliant: 1**, repeat steps 27 and 28.
29. In the results pane, right-click **Security Updates – Windows 10**, and then click **View Status**. Review the information that displays on the **Deployment Status** page.

Lesson 4

Configuring automatic deployment rules

Contents:

Question and Answers

Question: Why would you use an automatic deployment rule for deploying Windows Defender or Endpoint Protection definition updates?

> **Answer:** Windows Defender and Microsoft System Center Endpoint Protection (Endpoint Protection) definition updates release approximately every eight hours, so it would require a lot of work to create these deployments manually. Furthermore, it is important that you always keep your antivirus solution updated.

Question: When you add a deployment to an existing automatic deployment rule, you need to specify a deployment package.

( ) True

( ) False

> **Answer:**
>
> ( ) True
>
> (√) False
>
> **Feedback:**
>
> False. The additional deployment will use the deployment package of the automatic deployment rule.

Demonstration: Creating automatic deployment rules

Demonstration Steps

1. On **LON-CFG**, open the **Configuration Manager console**.
2. Click the **Software Library** workspace, expand **Software Updates**, and then click **Automatic Deployment Rules**.
3. On the ribbon, click **Create Automatic Deployment Rule**.
4. In the **Create Automatic Deployment Rule Wizard**, on the **General** page, configure the following settings, and then click **Next**:
    - Name: **Required Critical Updates for Windows 10**
    - Template: **Patch Tuesday**
    - Collection: **All Windows 10 Workstations**
    - Select **Add to an existing Software Update Group**
5. On the **Deployment Settings** page, click **Next**.
6. On the **Software Updates** page, under **Property filters**, clear **Date Released or Revised**, click both **Product** and **Required**, verify that **Update Classification** is selected, configure the following settings, and then click **Next**:
    - Product: **Windows 10**
    - Required: **>=1**
    - Update Classification: **Critical Updates**
7. To show the updates, click **Preview**, and then click **Close**.
8. On the **Evaluation Schedule** page, verify that the **Run the rule on a schedule** option is selected. Click **Customize**, and then configure the schedule to recur every **2** days.

9. To close the **Custom Schedule** dialog box, click **OK**, and then click **Next**.
10. On the **Deployment Schedule** page, configure the following settings, and then click **Next**:
    - Time based on: **Client local time**
    - Software available time: **As soon as possible**
    - Installation deadline: **Specific time: 7 days**
11. On the **User Experience** page, configure the following setting, and then click **Next**:
    - User notifications: **Display in Software Center and show all notifications**
12. On the **Alerts** page, verify that **Generate an alert when the following conditions are met** is selected, and then click **Next**.
13. On the **Deployment Package** page, click **Create a new deployment package**, configure the following settings, and then click **Next**:
    - Name: **AutoDeployment**
    - Package source: **\\LON-CFG\E$\source\autoupdate**
14. On the **Distribution Points** page, click **Add**, and then click **Distribution Point**.
15. In the **Add Distribution Points** dialog box, select **LON-CFG.ADATUM.COM**, and then click **OK**.
16. On the **Distribution Points** page, click **Next**.
17. On the **Download Location** page, click **Download software updates from a location on my network**, in the text box, type **\\LON-CFG\E$\Software\Updates**, and then click **Next**.
18. On the **Language Selection** page, click **Next**.
19. On the **Download Settings** page, click **Next**.
20. On the **Summary** page, verify that the settings are correct, point out the **Save As Template** option to the students, and then click **Next**.
21. On the **Completion** page, click **Close**.
22. Click **Automatic Deployment Rules**, and then in the results pane, click **Required Critical Updates for Windows 10**.
23. On the ribbon, click **Run Now**, and then click **OK**.
24. In the navigation pane, click **Software Update Groups**.
25. Refresh the results pane, and then in the results pane, notice that a software update group named **Required Critical Updates for Windows 10** is listed. Additionally, notice that the **Created By** column displays **AutoUpdateRuleEngine**.
26. In the preview pane, click the **Deployment** tab. Notice that a deployment is created and enabled automatically.
27. In the results pane, right-click **Required Critical Updates for Windows 10**, and then click **Show Members**. Notice the list of software updates that have been added automatically to the software update group.
28. Click the **Software Library** workspace, expand **Software Updates**, and then click **Automatic Deployment Rules**.
29. In the details pane, right-click the **Required Critical Updates for Windows 10** automatic deployment rule, and then click **Add Deployment**.
30. In the **Add Deployment Wizard**, on the **Collection** page, click **Browse**.

31. In the **Select Collection** window, select the **London Clients** collection, click **OK**, and then click **Next**.
32. On the **Deployment Settings** page, click **Next**.
33. On the **Deployment Schedule** page, configure the following settings, and then click **Next**:
    - Time based on: **Client local time**
    - Software available time: **As soon as possible**
    - Installation deadline: **As soon as possible**
34. On the **User Experience** page, configure the following setting, and then click **Next**:
35. User notifications: **Hide in Software Center and all notifications**
36. On the **Alerts** page, select **Generate an alert when the following conditions are met**, and then click **Next**.
37. On the **Download Settings** page, click **Next**.
38. On the **Summary** page, verify that the settings are correct, and then click **Next**.
39. On the **Completion** page, click **Close**.
40. In the preview pane, click the **Deployment Settings** tab. Notice that a new deployment is created that targets **London Clients**.

Lesson 5

Monitoring and troubleshooting software updates

Contents:

Question and Answers

Question: What is the name of the log file in which you can find information about WSUS synchronization and site database synchronization with WSUS?

> **Answer:** The name of the log file is wsyncmgr.log and it is located in the INSTALL_PATH\Logs folder.

Question: Which tool can you use for viewing Configuration Manager log files?

> **Answer:** You can use the CMTrace tool to open Configuration Manager log files. The installation media in the SMSSETUP\TOOLS folder includes this tool.

Lesson 6
Enabling third-party updates

Contents:

Question and Answers

Question: Which type of catalogs can you use with third-party updates?

> **Answer:** There are two types of catalogs: partner catalogs and custom catalogs.
>
> Partner catalogs are catalogs supplied by partners and registered with Microsoft. You can subscribe to partner catalogs without providing any information. The **Third-Party Software Update Catalogs** node in the Configuration Manager console displays partner catalogs by default.
>
> Custom catalogs are usually a paid service, and you must add them by using the **Add Custom Catalog Wizard**.

Question: Currently, you are using SCUP to manage updates for third-party software. You would like to test third-party updates without causing any issues to the running configuration of SCUP. What must you do?

> **Answer:** You do not need to do anything because Configuration Manager can run both third-party updates and SCUP at the same time. You can even use the WSUS signing certificate that you are currently using with SCUP for third-party updates.

Resources

Configuration Manager support for third-party Updates

Additional Reading: For more information about SCUP, refer to Install Updates Publisher: https://aka.ms/AA42tr2

Prerequisites for configuring third-party updates

Additional Reading: For more information about configuring SSL for WSUS, refer to Step 2: Configure WSUS: https://aka.ms/AA42m4o
For more information about enabling SSL for a software update point, refer to Install and configure a software update point: https://aka.ms/AA42tr3

Additional Reading: For detailed information about creating the WSUS signing certificate, refer to System Center Updates Publisher Signing Certificate Requirements & Step-by-Step Guide: https://aka.ms/AA4n4xc
Even though this blog post is about SCUP, it is still applicable for third-party updates because the requirements for the WSUS signing certificate are the same. If you are already using SCUP, you can reuse the WSUS signing certificate for third-party updates.

Additional Reading: For more information about requirements for enabling third-party updates, refer to Enable third-party updates: https://aka.ms/AA42m4r

Module Review and Takeaways

Best Practices

Some of the best practices for installing and using WSUS and a software update point include:

- If installing more than one software update point in a single site, the additional software update points should use the same WSUS database for each instance of WSUS. This helps alleviate the network performance impact when clients change to a new software update point.
- When installing the Configuration Manager database and the WSUS database on the same computer running Microsoft SQL Server, use different instances for each database.
- Use the **Store updates locally** setting when installing WSUS.
- Create a new software update group each time the automatic deployment rules run. Each software update deployment is limited to a maximum of 1,000 updates.

Review Questions

Question: You have a specific group of computers that require a unique scan schedule for software updates. What can you do to accommodate this?

> **Answer:** You can create a custom client device setting that you configure with the update requirements. You then can assign the custom client device settings object to a collection that contains the group of computers.

Question: Which method would provide the most benefits for determining compliance with software updates?

> **Answer:** Answers will vary, but options include sorting, filtering, searching the All Software updates list, or using software updates compliance reports.

Question: You have a line-of-business application that you want to update. Which tool can you use to create a catalog for use with software updates?

> **Answer:** You can use SCUP to create a catalog for use with software updates.

Question: You need to provide information to the junior service desk staff to help them monitor update deployment. Without giving the junior service desk staff access to the Configuration Manager console, how can you give them the information?

> **Answer:** You can grant the junior service desk staff access to the Configuration Manager reporting website, where they can access the various reports that they require.

Question: You have created an automatic deployment rule for Office 2016 updates. You want to deploy the same updates automatically to another collection. What are your options?

> **Answer:** You could add a deployment to the existing automatic deployment rule and choose the other collection, and other settings as well.

Question: What are your options for managing the WSUS signing certificate when working with third-party updates in Configuration Manager?

> **Answer:** You can let Configuration Manager automatically manage the WSUS signing certificate for you, or you can manage it yourself.

Lab Review Questions and Answers

Lab A: Configuring the site for software updates

Question and Answers

Question: You plan to implement the software update point on a Windows Server 2016 server. Which version of WSUS should you install?

> **Answer:** For Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016, you need to install the WSUS server role, which is version 4.0.

Question: You need to add the service packs classification to synchronize for software updates. Where can you make this modification?

> **Answer:** You can modify this in the Software Update Point Component Properties dialog box.

Lab B: Deploying and managing software updates

Question and Answers

Question: What are some of the advantages of using a software update group?

> **Answer:** A software update group is an efficient way to organize, monitor, and deploy software updates.
>
> Some of the reports found in the Software Updates categories, such as the Overall Compliance report and the Deployments of an Update Group report require that you use a software update group name as a criterion.

Question: When is an automatic deployment rule useful?

> **Answer:** An automatic deployment rule is useful for automated deployments. However, it can be helpful for managing the deployment of Endpoint Protection definition files.

Module 9

Implementing Endpoint Protection for managed PCs

Contents:

Lesson 1

Overview of Endpoint Protection in Configuration Manager

Contents:

Question and Answers

Question: You plan to implement Endpoint Protection in your environment. You already have created an Automatic Deployment Rule for the definition updates and created an antimalware policy. You also created a Custom Device Settings object and chose Endpoint Protection. When you try to configure the **Manage Endpoint Protection client on client computers** setting, it is not available. What must you do in order to enable the setting?

> **Answer:** You must install an Endpoint Protection point before you can enable the setting.

Question: You have enabled the management of Windows Defender, which is running on your Windows 10 computers. You have created an Automatic Deployment Rule that creates a deployment of Endpoint Protection definition updates. However, you notice that Windows Defender is not being updated. What must you do to enable deployment of definition updates to your Windows 10 machines running Windows Defender?

> **Answer:** You must add Windows Defender as a product (found in the Windows category) on your software update point. Then, you must synchronize your software update point. Finally, you should include Windows Defender definition in your Automatic Deployment Rule.

Introducing the Endpoint Protection feature

Question: Do you currently use an antimalware solution in your organization? How will Configuration Manager integration benefit your current antimalware processes?

> **Answer:** Answers will vary based on student experiences.

Resources

Additional Reading: For more information, refer to Endpoint Protection in System Center Configuration Manager at: http://aka.ms/a2vg6k

Additional Reading: For more information about Windows Defender ATP, refer to Windows Defender Advanced Threat Protection at: https://aka.ms/jdyy2p

Endpoint Protection implementation workflow

Additional Reading: For information on Endpoint Protection workflow, refer to Endpoint Protection at: http://aka.ms/a2vg6k

Prerequisites for installing Endpoint Protection

Additional Reading: For more information, refer to Planning for Endpoint Protection in System Center Configuration Manager: http://aka.ms/rf042m

Demonstration: Configuring the Endpoint Protection point site system role and client settings

Demonstration Steps

1. On **LON-CFG**, on the taskbar, click **Configuration Manager Console**.
2. Click the **Administration** workspace. In the navigation pane, expand **Site Configuration**, and then click **Servers and Site System Roles**.

3. In the details pane, right-click **\\LON-CFG.Adatum.com**, and then click **Add Site System Roles**.
4. In the **Add Site System Roles Wizard**, on the **General** page, discuss the default settings, and then click **Next**.
5. On the **Proxy** page, click **Next**.
6. On the **System Role Selection** page, select the **Endpoint Protection point** check box, click **OK** in the message box, and then click **Next**.
7. On the **Endpoint Protection** page, select the **By checking this box, I acknowledge that I accept the License Terms and Privacy Statement** check box, and then click **Next**.
8. On the **Cloud Protection Service** page, click the **Do not join Cloud Protection Service** option, and then click **Next**.
9. On the **Summary** page, click **Next**.
10. On the **Completion** page, click **Close**.
11. Click the **Monitoring** workspace.
12. In the navigation pane, expand **System Status**, and then click **Component Status**.
13. In the results pane, scroll down, and then click **SMS_ENDPOINT_PROTECTION_MANAGER**.
14. On the ribbon, click **Show Messages**, and then click **All**.
15. In the **Status Messages: Set Viewing Period** dialog box, click **OK**.
16. In the **Configuration Manager Status Message Viewer**, discuss the messages related to the component installation.
17. Close the **Configuration Manager Status Message Viewer**.
18. Click the **Administration** workspace, and then click **Client Settings**.
19. Right-click **Client Settings**, and then click **Create Custom Client Device Settings**.
20. In the **Create Custom Client Device Settings** dialog box, in the **Name** text box, type **Endpoint Protection**, and then click **Endpoint Protection**.
21. Under **General**, click the **Endpoint Protection** item.
22. Configure the Endpoint Protection component as follows:
    - Manage Endpoint Protection client on client computers: **Yes**
    - Install Endpoint Protection client on client computers: **Yes**
    - Suppress any required computer restarts after the Endpoint Protection client is installed: **Yes**
    - Disable alternate sources (such as Microsoft Windows Update, Microsoft Windows Server Update Services, or UNC shares) for the initial definition update on client computers: **Yes**
23. To close the **Custom Device Settings** dialog box, click **OK**.
24. Right-click **Endpoint Protection**, and then click **Deploy**.
25. In the **Select Collection** dialog box, click **Endpoint Protection Pilot**, and then click **OK**.

Lesson 2

Configuring, deploying, and monitoring Endpoint Protection policies

Contents:

Question and Answers

Question: You want to scan incoming files on all of your running Endpoint Protection clients only. Where should you configure this?

> **Answer:** You can find this setting in the antimalware policy under **Real-time protection**. If you enable real-time protection, additional options are available to specify whether to scan incoming files, outgoing files, or both. The default setting is to scan both incoming files and outgoing files. You also can specify whether users can configure real-time protection settings on their computers.

Question: How many built-in reports exist for Endpoint Protection?

> **Answer:** There are six reports in the Endpoint Protection category on your reporting services point:
>
> - Antimalware Activity report
> - Antimalware overall status and history
> - Computer malware details
> - Infected computers
> - Top users by threads
> - User threat list

Configuring Endpoint Protection policies

Question: What additional tasks do you need to perform if you want to receive email notifications of Endpoint Protection alerts?

> **Answer:** You must add Windows Defender as a product (found in the Windows category) on your software update point. Then, you must synchronize your software update point. Finally, you should include Windows Defender definition in your Automatic Deployment Rule.
>
> **Feedback:**
>
> You must first configure email settings to specify an SMTP server. Then, you need to configure the properties of a device collection to specify alert settings. Finally, you need to create a subscription by specifying an email address to which to send the Endpoint Protection alerts.

Resources

Creating and deploying antimalware policies

Additional Reading: For more information, refer to How to create and deploy antimalware policies for Endpoint Protection in System Center Configuration Manager: http://aka.ms/ubdjsx
For information on how to manually download the latest antimalware definition updates for Microsoft Forefront Client Security, Microsoft Forefront Endpoint Protection 2010, and Microsoft System Center 2012 Endpoint Protection, refer to: http://aka.ms/ekdhf1
For a list of all the Microsoft Anti-Virus Exclusion that you can configure for Windows Server, refer to Microsoft Anti-Virus Exclusion List: http://aka.ms/p5jre7
For more information, refer to Definition updates for Windows Defender Antivirus and other Microsoft antimalware: https://aka.ms/AA42tr4

Creating and deploying Windows Defender Firewall policies

Additional Reading: For more information, refer to How to create and deploy Windows Firewall policies for Endpoint Protection in System Center Configuration Manager: http://aka.ms/tjons6

Managing Endpoint Protection policies

Additional Reading: For more information, refer to Manage antimalware policies and firewall settings: http://aka.ms/h0plns

Monitoring Endpoint Protection status

Additional Reading: For more information, refer to How to monitor Endpoint Protection status: http://aka.ms/ephlhn

Configuring antimalware alerts

Additional Reading: For more information, refer to Configure Alerts for Endpoint Protection in Configuration Manager: https://aka.ms/AA42tr7

Demonstration: Configuring Endpoint Protection policies

Demonstration Steps

1. On **LON-CFG**, on the taskbar, click **Configuration Manager Console**.
2. In the Configuration Manager console, click the **Assets and Compliance** workspace. In the navigation pane, expand **Endpoint Protection**, and then click **Antimalware Policies**.
3. On the ribbon, click **Create Antimalware Policy**.
4. In the **Create Antimalware Policy** dialog box, click **General**, and then configure the following settings:
   - Name: **All Workstations**
   - Scheduled scans: selected
   - Scan settings: selected
   - Real-time protection: selected
   - Advanced: selected
   - Definition updates: selected
5. Click **Scheduled scans**. Configure the following settings, and leave all other options as the default setting:
   - Run a scheduled scan on client computers: **Yes**
   - Scan day: **Thursday**
   - Scan time: **3 AM**

- Check for the latest definition updates before running a scan: **Yes**

6. Click **Scan settings**. Configure the following settings, and leave all other options as the default setting:
   - Scan email and email attachments: **Yes**
   - Scan removable storage devices such as USB drives: **Yes**
7. Click **Real-time protection**. Configure the following settings, and leave all other options as the default setting:
   - Enable real-time protection: **Yes**
   - Scan system files: **Scan incoming files only**
   - Enable behavior monitoring: **No**
8. Click **Advanced**. Configure the following setting, and leave all other options as the default setting:
   - Delete quarantined files after (days): **5**
9. Click **Definition updates**, and then click **Set Source**.
10. In the **Configure Definition Update Sources** dialog box, click to clear the check boxes for **Updates distributed from Microsoft Malware Protection Center** and **Updates distributed from WSUS**.
11. With **Updates distributed from Microsoft Update** selected, click the **Up** button until the selection is second in the list, and then click **OK**.
12. Configure the following settings, and leave all other options as the default setting:
   - Force a definition update if the client computer is offline for more than two consecutive scheduled updates: **Yes**
   - If Configuration Manager is used as a source for definition updates, clients will only update from alternative sources if definition is older than (hours): **16**
13. Click **OK** to close the **Create Antimalware Policy** dialog box.

Note: Notice that the policy now displays in the results pane.

14. Click the **Assets and Compliance** workspace. In the navigation pane, expand **Endpoint Protection**, and then click **Antimalware Policies**.
15. In the results pane, click **All Workstations** Policy, and then on the ribbon, click **Deploy**.
16. In the **Select Collection** dialog box, click **Endpoint Protection pilot**, and then click **OK**.
17. Click the **Assets and Compliance** workspace. In the navigation pane, expand **Endpoint Protection**, and then click **Windows Defender Firewall Policies**.
18. On the ribbon, click **Create Windows Defender Firewall Policy**.
19. In the **Create Windows Defender Firewall Policy Wizard**, on the **General** page, configure the following settings, and then click **Next**:
   - Name: **All Workstations Firewall Policy**
   - Description: **Windows 10 and Windows 7 Firewall Policy**
20. On the **Profile Settings** page, configure the following settings, and then click **Next**:
   - Enable Windows Defender Firewall – Domain profile: **Yes**

  - Notify the user when Windows Defender Firewall blocks a new program – Domain profile: **Yes**

21. On the **Summary** page, click **Next**.
22. On the **Completion** page, click **Close**.
23. Click the **Assets and Compliance** workspace. In the navigation pane, expand **Endpoint Protection**, and then click **Windows Defender Firewall Policies**.
24. In the results pane, click **All Workstations Firewall Policy**, and then on the ribbon, click **Deploy**.
25. In the **Deploy Windows Defender Firewall Policy** dialog box, click **Browse**.
26. In the **Select Collection** dialog box, click **Endpoint Protection pilot**, and then click **OK**.
27. In the **Deploy Windows Defender Firewall Policy** dialog box, verify that the **Simple schedule** is configured to run every **7 Days**, and then click **OK**.

Lesson 3

Configuring and deploying advanced threat policies

Contents:

Question and Answers

Question: You would like to block access to an untrusted website. Which kind of policy should you create in Configuration Manager?

> **Answer:** You should create a Windows Defender Application Guard policy.

Question: Which are the two features that Windows Defender Device Guard has been divided into?

> **Answer:** Windows Defender Device Guard has been divided into two separate features: Windows Defender Application Control and Windows Defender Exploit Guard.

Resources

Creating and deploying Application Guard policies

Additional Reading: For more information about Windows Defender Application Guard settings and configuration, refer to Windows Defender Application Guard overview: https://aka.ms/AA42m4v

Creating and deploying Windows Defender Exploit Guard policies

Additional Reading: For more information, refer to Import, export, and deploy exploit protection configurations: https://aka.ms/AA42tr8

Additional Reading: For more information about Windows Defender Exploit Guard, refer to Evaluate Windows Defender Exploit Guard: https://aka.ms/AA42m4x

Managing Windows Defender Application Control policies

Additional Reading: For more information, refer to Windows Defender Device Guard: https://aka.ms/AA42tr9

Additional Reading: For information about Intelligent Security Graph, refer to Use Windows Defender Application Control (WDAC) with the Microsoft Intelligent Security Graph: https://aka.ms/AA42tra

Module Review and Takeaways

Question: You have configured a software update point to deploy malware definitions to clients. Which definition update source should you use for the antimalware policy?

> **Answer:** If you intend to use software updates, use the **Updates distributed from Configuration Manager** antimalware policy.

Question: You have a client that is a member of two collections, and each collection has its own antimalware policy deployed separately. Which policy will affect the client?

> **Answer:** Multiple antimalware policies that are deployed to the same computer are merged. If two settings conflict, the highest priority setting affects the client.

Question: You need to determine the top malware that computers have reported. How can you find this information?

> **Answer:** You can find this information by viewing:
>
> 1. The Top Malware By Computers report.
> 2. The Top 5 malware by number of computers section of the System Center Endpoint Protection Status node.

Question: You want to test your Windows Defender Application Control policy before you implement it in production. You only want an entry in the Event Viewer on the machine when an application is blocked. How should you configure your policy?

> **Answer:** When you create the Windows Defender Application Control policy, you must set the **Enforcement Mode** to **Audit only**. Then the policy will not be enforced, and users will be able to execute all software, but the events will be recorded in the **Security** node of the Event Viewer on the local device.

Lab Review Questions and Answers

Lab A: Implementing Microsoft System Center Endpoint Protection

Question and Answers

Question: In the lab results, what does the Operational Status of Clients graph indicate?

> **Answer:** The Operational Status of Clients graph indicates that one of the clients needs to restart before the installation is complete.

Question: What is the status of the definitions according to the Definition Status on Computers graph?

> **Answer:** The definition status shows that the definitions are older than seven days for one client.

Question: You have received an alert that malware has been detected. How can you determine which computers the malware has affected?

> **Answer:** In the **Alerts** node, select the **Malware detection** alert, and then in the preview pane, click the **Machines** tab. This tab displays the computer names of the affected machines. You also can view Endpoint Protection reports for malware details.

Lab B: Implementing advanced threat policies

Question and Answers

Question: When you create a Windows Defender Exploit Guard policy, you can specify the location of the **configuration.xml** file that contains the configuration entries for Windows Defender Exploit Guard. How do you get the **configuration.xml** file?

> **Answer:** You can export this file by using the Windows Security app on the Windows 10 device that is representative of the devices used by your organization.

Question: What effect will the **Authorize software that is trusted by the Intelligent Security Graph** setting have on a device, when you enable it in a Windows Defender Application Control policy?

> **Answer:** It will allow software and processes that are trusted by the Microsoft Intelligent Security Graph to be executed on Windows 10 devices.

Module 10

Managing Compliance and Secure Data Access

Contents:

Lesson 1

Overview of Compliance Settings

Contents:

Question and Answers

Question: What types of settings would you want to monitor in your work environment?

> **Answer:** Answers will vary, but could include registry settings for specific applications or file versions.

Resources

Prerequisites for using compliance settings and supporting compliance policy

Reference Links: For more information about client device settings, refer to Module 4 of this course.

Reference Links: For more information about reporting in Configuration Manager, refer to Module 2 of this course.

Reference Links: For more information about role-based administration, refer to Module 12 of this course.

What are configuration items?

Additional Reading: For more information, refer to How to create configuration items for Windows 10 devices managed with the System Center Configuration Manager Client: https://aka.ms/AA42tqw

Common tasks for managing compliance

Additional Reading: For more information, refer to Common tasks for managing compliance on devices with the System Center Configuration Manager client: http://aka.ms/jv1agj

Lesson 2

Configuring compliance settings

Contents:

Question and Answers

Question: Why would you create a child configuration item?

> **Answer:** Answers will vary. A possible answer might be that you need a particular setting on all computers that run Windows operating systems, while also needing a related setting to be different on different groups of systems.

Question: When would you use a severity level of None?

> **Answer:** Answers will vary. One possible answer is if you want to report on all systems that do not have a particular version of a noncritical application.

Configuring remediation on a configuration item

Question: What kind of remediation will occur if you apply the evaluation rule that you created in the demonstration to a noncompliant system?

> **Answer:** The remediation action that will occur: Set the value if it exists but is not compliant.

Creating and deploying a configuration baseline

Question: How many configuration items should you include in a configuration baseline?

> **Answer:** Answers will vary. One possible answer is to include as many configuration items as necessary to define the system or application that you are monitoring, without adversely affecting system performance.

Demonstration: Creating a configuration item

Demonstration Steps

1. On **LON-CFG**, on the taskbar, click the **Configuration Manager console** icon.
2. Click the **Assets and Compliance** workspace, expand the **Compliance Settings** folder, and then click the **Configuration Items** node.
3. On the ribbon, click **Create Configuration Item**.
4. In the **Create Configuration Item Wizard**, on the **General** page, in the **Name** text box, type **Validate Remote Desktop is Enabled**.
5. Click **Categories**.
6. Select the **Client** check box, and then click **OK**.
7. On the **General** page, click **Next**.
8. On the **Supported Platforms** page, click **Next**.
9. On the **Settings** page, click **New**.
10. In the **Create Setting** dialog box, on the **General** tab, click **Browse**.
11. In the **Browse Registry** dialog box, in the **Computer name** text box, type **LON-DC1**, and then click **Connect**.
12. In the **Registry tree** area, expand the **LON-DC1** computer, and then navigate to **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server**.

Note: Some registry entries that you might want to monitor will not exist on the Configuration Manager server. In this case, you can connect to a remote registry to import any settings that you want to monitor.

13. In the **Browse Registry** dialog box, in the **Registry Value** area, click **fDenyTSConnections**.
14. Select the **This registry value must satisfy the following rule if present** check box. Explain to the students that because this value is already configured with the desired value, they do not need to change the setting.
15. In the **Browse Registry** dialog box, click **OK**.
16. In the **Create Setting** dialog box, click **OK**.
17. On the **Settings** page, click **Next**.
18. On the **Compliance Rules** page, under the **Name** heading, click the **fDenyTSConnections Equals 0** condition (expand the name column if necessary), and then click **Edit**.
19. In the **Noncompliance severity for reports** list, click **Critical**, and then click **OK**.
20. On the **Compliance Rules** page, click **Next**.
21. On the **Summary** page, click **Next**.
22. On the **Completion** page, click **Close**.

Demonstration: Configuring remediation on a configuration item

Demonstration Steps

1. On **LON-CFG**, in the Configuration Manager console, click the **Assets and Compliance** workspace, expand the **Compliance Settings** folder, and then click the **Configuration Items** node.
2. Click **Validate Remote Desktop is Enabled**.
3. On the ribbon, click **Properties**.
4. Click the **Compliance Rules** tab.
5. Under the **Condition** heading, click **Equals 0**, and then click **Edit**.
6. In the **Edit Rule** dialog box, select the **Remediate noncompliant rules when supported** check box. Explain that you do not specify how to remediate the problem. The remediation action depends on the type of rule that you select.
7. In the **Edit Rule** dialog box, click **OK**.
8. In the **Validate Remote Desktop is Enabled Properties** dialog box, click **OK**.

Demonstration: Creating and deploying a configuration baseline

Demonstration Steps

1. On **LON-CFG**, in the Configuration Manager console, click the **Assets and Compliance** workspace, expand the **Compliance Settings** folder, and then click the **Configuration Baselines** node.
2. On the ribbon, click **Create Configuration Baseline**.
3. In the **Create Configuration Baseline** dialog box, in the **Name** text box, type **IT Support Configuration Settings**.
4. Click **Add**, and then click **Configuration Items**.
5. Click **Validate Remote Desktop is Enabled**, and then click **Add**.
6. In the **Add Configuration Items** dialog box, click **OK**.
7. Click **Categories**, select the **IT Infrastructure** check box, and then click **OK**.
8. In the **Create Configuration Baseline** dialog box, click **OK**.

9. Click **IT Support Configuration Settings**.
10. On the ribbon, click **Deploy**.
11. In the **Deploy Configuration Baselines** dialog box, click **Browse**.
12. In the **Select Collection** dialog box, click the **User Collections** list, and then click **Device Collections**.
13. Click the **All Windows 10 Workstations** collection, and then click **OK**.
14. In the **Deploy Configuration Baselines** dialog box, click **OK**.

Lesson 3

Viewing compliance results

Contents:

Question and Answers

Question: When would you run an evaluation from the Configuration Manager client?

> **Answer:** Answers will vary. One possible answer is for troubleshooting purposes. You might want to run an evaluation off schedule to verify whether the client is in compliance.

Lesson 4

Managing resource settings and data access

Contents:

Question and Answers

Question: You can use VPN Profiles only to deploy VPN connections to Microsoft VPN.

( ) True

( ) False

> **Answer:**
>
> ( ) True
>
> (√) False

Question: You would like to clear the Microsoft Edge browser cache when you exit the application. How can you accomplish that with the least administrative effort?

> **Answer:** Create a Microsoft Edge profile and deploy it to a collection that contains the Windows 10 devices from which you want to clear the browser cache.

Question: You want to upgrade your Windows 10 Professional devices to Windows 10 Enterprise. You are using Key Management Service (KMS) to automatically activate your Windows 10 devices. What kind of product key must you use when you create the Windows 10 Edition Upgrade policy?

> **Answer:** You must use a Windows 10 Enterprise KMS key.

Resources

Overview of remote connection profiles

Best Practice: Manually specify user device affinity for devices affected by a Remote Connection Profile. Allowing users to identify their primary device or allowing device affinity to be set based on usage could allow unauthorized users to gain remote access to a system.

Additional Reading: For more information, refer to Remote connection profiles in System Center Configuration Manager: http://aka.ms/ugccsh

Configuring Microsoft Edge settings

Additional Reading: For information about the various settings you can configure for Microsoft Edge, refer to:
https://aka.ms/AA42m4i

Demonstration: Creating a user data and profiles configuration item

Demonstration Steps

1. Switch to the **LON-CFG** computer.
2. On the taskbar, click **Configuration Manager console**.
3. Click the **Assets and Compliance** workspace, expand the **Compliance Settings** folder, and then click the **User Data and Profiles** node.
4. On the ribbon, click **Create User Data and Profiles Configuration Item**.
5. On the **General** page of the Create User Data and Profiles Configuration Item Wizard, in the **Name** text box, type **Downloads Redirection**, select the **Folder redirection** check box, and then click **Next**.

6. On the **Folder Redirection** page, under the **Folder** heading, scroll down to **Downloads**, next to **Downloads**, click **Do not manage**, and then click **Redirect to remote**.
7. Click **Redirect to the users home folder**, click **Next** twice, and then click **Close**.
8. Explain that your next step would be to deploy the configuration item to a specific collection.

Module Review and Takeaways

Best Practices

Supplement or modify the following best practices for your own work situations:

- Create configuration items that combine multiple objects and settings to define a single unit of change.
- Provide meaningful display names and descriptions for configuration items and baselines so that other administrators can use them without needing to check and interpret their properties.
- Minimize the number of configuration items, dependent configuration baselines, and configuration baselines that deploy to computers when defining required compliance.
- Where possible, use child configuration items rather than duplicating configuration items.
- Schedule compliance evaluations according to business requirements and available computing resources.

Review Questions

Question: What are the components of compliance settings? Which component would you create first?

> **Answer:** Configuration items and configuration baselines are the components of compliance settings. You should first create configuration items and then configuration baselines.

Question: The default evaluation interval is seven days; under what circumstances would you modify this setting?

> **Answer:** Answers will vary, but can include regulatory compliance requirements or business requirements.

Question: How would you remediate noncompliant computers with a configuration item that requires the latest version of the Microsoft .NET Framework?

> **Answer:** You can use software distribution to deploy the latest version of the Microsoft .NET Framework to computers that do not have the appropriate version of the framework installed.

Question: You support a line-of-business (LOB) application that was developed in house. This application requires that Adobe Reader be the default application for opening .pdf files, regardless of the installed versions of Adobe. Some users have been changing their default program for the .pdf files. This generally results in calls to the help desk when the LOB application does not function properly. How can you use compliance settings to prevent this from happening?

> **Answer:** Answers will vary. One possible answer is to configure configuration items and configuration baselines representing the registry settings that control the default application settings for .pdf files, and then configure them for automatic remediation.

Question: You have apps that require specific versions of non-Microsoft add-ins. You can update these add-ins through the Internet. Certain users have administrative access to their computers and update the apps on their own. This occasionally causes problems. You would like to be able to quickly reference the version of the non-Microsoft apps they are running. How could you use compliance settings to help with this situation?

> **Answer:** Answers will vary. One possible answer is to create a file-based compliance rule for the run-time component so that user changes are reported quickly to the Configuration Manager database.

Question: Your audit department requires documentation showing that all client computers comply with the security updates for all apps. Your security department is responsible for producing this documentation. How can you use compliance settings to show compliance with security updates for all apps?

Answer: Answers will vary. One possible answer is to work with the security department to determine the apps that you can monitor through the registry and the file system. Then, develop configuration items for each application that you will monitor. Finally, create baselines for each department and the apps that they use.

Lab Review Questions and Answers

Lab: Managing compliance settings

Question and Answers

Question: In addition to Presence, what other values might you want to use with a file-based configuration item?

> **Answer:** Answers will vary, but might include Size, Date Created, Secure Hash Algorithm 1 (SHA-1), and Attributes and Permissions.

Question: What was the compliance state when you ran the evaluation for the first time?

> **Answer:** The evaluation showed noncompliant with a severity of Critical for the registry setting.

Question: What was the compliance state when you ran the evaluation for the last time?

> **Answer:** The evaluation showed compliant.

Question: Was the remediation successful?

> **Answer:** Yes.

Module 11

Managing operating system deployment

Contents:

Lesson 1

An overview of operating system deployment

Contents:

Question and Answers

Question: When creating a servicing plan for Windows 10, which kind of software update is included in the software update group created by the servicing plan rule?

> **Answer:** Only updates from the Upgrade classification are included in the created software update group.

Question: Which operating system deployment scenarios does Configuration Manager support?

> **Answer:** Configuration Manager supports the following four operating system deployment scenarios:
>
> - Operating system refresh
> - Bare-metal installation
> - In-place upgrade
> - Side-by-side migration

Resources

Deploying operating systems by using Configuration Manager

Additional Reading: For more information, refer to Customize operating system images with System Center Configuration Manager: http://aka.ms/vrzanf

Additional Reading: For more information, refer to Introduction to operating system deployment in System Center Configuration Manager: http://aka.ms/mhoe8o

Operating system deployment terminology

Additional Reading: For more information, refer to Introduction to operating system deployment in System Center Configuration Manager: http://aka.ms/jpu6xn

Overview of operating system deployment scenarios

Additional Reading: For more information, refer to Windows To Go: Feature Overview: http://aka.ms/vns2wj

Additional Reading: For more information, refer to Deploy Windows To Go with System Center Configuration Manager: http://aka.ms/d5hp3v

Additional Reading: For more information, refer to Methods to deploy enterprise operating systems using System Center Configuration Manager: http://aka.ms/mbxwm1

UEFI considerations for operating system deployment

Additional Reading: For more information, refer to Mitigate threats by using Windows 10 security features: http://aka.ms/bxmdcb

Additional Reading: For more information, refer to UEFI/GPT-based hard drive partitions: http://aka.ms/k6ckk0

Additional Reading: For more information, refer to MBR2GPT.EXE: https://aka.ms/rdb1wp

Additional Reading: For more information, refer to Task sequence steps to manage BIOS to UEFI conversion: https://aka.ms/s2vcch

Lesson 2
Preparing a site for operating system deployment

Contents:

Question and Answers

Question: What kind of drivers must you add to your boot images? With which operating system should they be used?

> **Answer:** You should only add network and mass storage drivers to your boot image, if they are needed. The drivers you add must be either 32-bit or 64-bit Windows 10 drivers, depending on the architecture of your boot image.

Question: How do you enable Windows PE Peer Cache in a task sequence?

> **Answer:** You must specify the task sequence variable **SMSTSPeerDownload** in your task sequence and set it to **TRUE**.

Question: You can only add one Network Access Account in Configuration Manager.

( ) True

( ) False

> **Answer:**
>
> ( ) True
>
> (√) False
>
> **Feedback:**
>
> You can add multiple Network Access Accounts in Configuration Manager.

Resources

Prerequisites for operating system deployment

Additional Reading: For more information, refer to Prepare site system roles for OS deployments with Configuration Manager: http://aka.ms/rg1b6s.

Additional Reading: For more information about supported ADK versions in Configuration Manager, refer to Support for Windows 10 in Configuration Manager: https://aka.ms/AA42tqx.

Additional Reading: To download the latest version of Windows ADK and the WinPE add-in, refer to Download and install the Windows ADK: https://aka.ms/AA42m4k

Additional Reading: For more information, refer to Supported operating systems for Configuration Manager site system servers: https://aka.ms/rph8v7.

Additional Reading: For more information, refer to What's new in version 1810 of Configuration Manager: https://aka.ms/AA42tqy.

Configuration Manager settings and component requirements

Additional Reading: For detailed information about Enhanced HTTP and how to configure it, refer to Enhanced HTTP: https://aka.ms/AA42tqz

Managing additional packages used by operating system deployment

Additional Reading: For more information, refer to Infrastructure requirements for OS deployment in Configuration Manager: https://aka.ms/fvpaw1

Demonstration: Enabling PXE and multicast on a Distribution Point

Demonstration Steps

1. On **LON-CFG**, on the taskbar, click **Configuration Manager Console**.
2. Click the **Administration** workspace, expand the **Site Configuration** node, and then click the **Servers and Site System Roles** node.
3. In the details pane, select **\\LON-CFG.Adatum.com** and in the preview pane, right-click the **Distribution point** role, and then click **Properties**.

1. In the **Distribution point Properties** dialog box, on the **PXE** tab, select the **Enable PXE support for clients** check box.
2. In the **Review Required ports for PXE** dialog box, click **Yes**.
3. Select the **Allow this distribution point to respond to incoming PXE requests** check box.
4. Select the **Enable unknown computer support** check box.
5. In the **Configuration Manager** message box, click **OK**.

Note: Explain that you can enable PXE without the need for Windows DS by selecting the **Enable a PXE responder without Windows Deployment Service** option.

6. In the **Password** and **Confirm password** field under **Require a password when computers use PXE**, type **Pa55w.rd**.
7. Click the **Multicast** tab, but do not configure anything.

Note: Tell the students that they enable multicast by selecting the **Enable multicast to simultaneously send data to multiple clients** check box. Also, tell them that they can configure additional settings for multicast on this page.

8. In the **Distribution point Properties** dialog box, click **OK**.
9. Click the **Monitoring** workspace, expand **Distribution Status**, and then click **Distribution Point Configuration Status**.
10. Right-click **\\LON-CFG.ADATUM.COM**, and click **Refresh**. Repeat periodically until the **PXE** column displays **Yes**.

Demonstration: Configuring the Network Access account

Demonstration Steps

1. In the Configuration Manager console, click the **Administration** workspace, expand **Site Configuration**, and then click the **Sites** node.
2. In the results pane, right-click **S01-Adatum Site**, select **Configure Site Components**, and then click **Software Distribution**.

3. In the **Software Distribution Component Properties** dialog box, on the **Network Access Account** tab, click the **Specify the account that accesses network locations** option.
4. Click **New** (the sun icon), and click **New Account**. Provide the following information as the credentials for the Network Access account:
   - User name: **Adatum\NetworkAccess**
   - Password: **Pa55w.rd**
   - Confirm password: **Pa55w.rd**

Note: Tell the students that they must create the Network Access account themselves. It should just be a normal domain user account and they should never use a Domain Administrator account. The account should have rights to create Computer Objects in Active Directory.

5. Click **Verify**.
6. In the **Network share** box, type **\\LON-CFG\SMS_S01**, and then click **Test connection**.
7. Ensure that you receive a message stating that the connection was verified successfully, and click **OK**.
8. To close the **Windows User Account** dialog box, click **OK**.
9. To close the **Software Distribution Component Properties** dialog box click **OK**.

Demonstration: Configuring and managing device drivers

Demonstration Steps

Import drivers into Configuration Manager

1. On **LON-CFG**, click the **Software Library** workspace, expand the **Operating Systems** folder, and then click the **Drivers** node.
2. Right-click the **Drivers** node, and then click **Import Driver**.
3. On the **Locate Driver** page, click **Browse**.
4. In the **Select Folder** dialog box, in the **Folder** box, type **\\LON-CFG\Software\Drivers\HypervX64**, and then click **Select Folder**.
5. On the **Locate Driver** page, click **Next**. Wait for the driver information to be validated.
6. On the **Driver Details** page, clear the **Hide drivers that are not digitally signed** option.
7. In the **Filter** box, type **display**, and then explain that you can use this functionality to filter drivers on their **File Name**, **Class**, **Architecture**, **Version**, and whether they are signed or not.

Note: Remember to clear the filter before you continue by clicking the red X.

8. Click **Categories**, and then in the **Manage Administrative Categories** dialog box, click **Create**.
9. In the **Create Administrative Category** box, type **64-bit Drivers**, and then click **OK**.
10. In the **Manage Administrative Categories** dialog box, click **Create**.
11. In the **Create Administrative Category** box, type **Hyper-V Drivers**, and then click **OK**.

12. In the **Manage Administrative Categories** dialog box, click **OK**, and then on the **Driver Details** page, click **Next**.
13. On the **Add Driver to Packages** page, click **New Package**.
14. In the **Create Driver Package** dialog box, in the **Name** box, type **Hyper-V Drivers**, and in the **Path** box, type **\\LON-CFG\E$\Source\Drivers**, and then click **OK**.
15. On the **Add Driver to Packages** page, click **Next**.
16. On the **Add Driver to Boot Images** page, click **Next**.
17. On the **Summary** page, click **Next**, and then on the **Completion** page, click **Close**.

Distribute a driver package

1. Click the **Driver Packages** node.
2. Right-click the **Hyper-V Drivers** package, and then click **Distribute Content**.
3. In the **Distribute Content Wizard**, on the **General** page, click **Next**.
4. On the **Content Destination** page, click **Add**, and then click **Distribution Point**.
5. In the **Add Distribution Points** dialog box, select the **LON-CFG.ADATUM.COM** check box, and then click **OK**.
6. On the **Content Destination** page, click **Next**.
7. On the **Summary** page, click **Next**, and then on the **Completion** page, click **Close**.
8. Right-click the **Hyper-V Drivers** package, and then click **Refresh**. Repeat this step until the **Content Status** shows **Success: 1**. This will be indicated by a full green circle. This should take about one minute.

Demonstration: Managing the default boot images

Demonstration Steps

Modify the default boot images

1. On **LON-CFG**, in the Configuration Manager console, click the **Software Library** workspace.
2. Expand **Operating Systems**, and then click the **Boot Images** node.
3. In the results pane, right-click **Boot Image (x64)**, and then click **Properties**.
4. Click the **Drivers** tab, and then click **New** (the sun icon).
5. In the **Select a driver** dialog box, clear the **Hide drivers that are not digitally signed** option. Select **Microsoft Hyper-V Network Adapter**, and then click **OK**.

> **Note:** Remove the driver again by selecting it and clicking the red X. Tell the students that Hyper-V drivers are not needed to do the demonstrations and labs in this module.

6. Click the **Customization** tab, and select the **Enable command support (testing only)** check box.
7. Click the **Data Source** tab, and then verify that the **Deploy this boot image from the PXE-enabled distribution point** check box is selected.
8. Click the **Optional Components** tab and in the **Components** section, click **new** (the sun symbol).
9. In the **Select optional components** window, select **Windows PowerShell (WinPE-PowerShell)**, and when prompted, click **OK**. Then click **OK** to close the **Select optional Components** dialog box.

10. In the **Boot Image (x64) Properties** dialog box, click **OK**.
11. In the **Configuration Manager** dialog box, click **Yes**.
12. In the **Update Distribution Points Wizard**, on the **General** page, click **Next**.
13. In the **Update Distribution Points Wizard**, on the **Summary** page, click **Next**. Wait for the wizard to complete.
14. In the **Update Distribution Points Wizard**, on the **Completion** page, click **Close**.
15. Right-click **Boot Image (x86)**, and then click **Properties**.
16. Click the **Customization** tab, and then select the **Enable command support (testing only)** check box.
17. Click the **Data Source** tab, and then verify that the **Deploy this boot image from the PXE-enabled Distribution Point** check box is selected.
18. Click the **Optional Components** tab, and in the **Components** section, click **new** (the sun symbol).
19. In the **Select optional components** window, select **Windows PowerShell (WinPE-PowerShell)**, and when prompted, click **OK**. Then click **OK** to close the **Select optional Components** dialog box.
20. In the **Boot Image (x86) Properties** dialog box, click **OK**.
21. In the **Configuration Manager** dialog box, click **Yes**.
22. In the **Update Distribution Points Wizard**, on the **General** page, click **Next**.
23. In the **Update Distribution Points Wizard**, on the **Summary** page, click **Next**.
24. In the **Update Distribution Points Wizard**, on the **Completion** page, click **Close**.

Distribute the default boot images

1. Click **Boot Image (x64)**, hold down the Ctrl key, click **Boot Image (x86)**, right-click **Boot Image (x64)**, and then click **Distribute Content**.
2. In the **Distribute Content Wizard**, on the **General** page, click **Next**.
3. On the **Content Destination** page, click **Add**, and then click **Distribution Point**.
4. In the **Add Distribution Points** dialog box, select **LON-CFG.ADATUM.COM**, and then click **OK**.
5. On the **Content Destination** page, click **Next**.
6. On the **Summary** page, click **Next**.
7. On the **Completion** page, click **Close**.
8. Right-click one of the packages, and then click **Refresh**. Repeat this step for the other package to check its status. Repeat periodically until both show a **Content Status** of **Success: 1**. This will be indicated by full green circle and should take about one minute.

Lesson 3

Deploying an operating system

Contents:

Question and Answers

Question: You have enabled Unknown Computer support on your PXE-enabled Distribution Point. You have a task sequence that deploys Windows 10 Enterprise X64, and you want to deploy it to a newly purchased machine that is not known by Configuration Manager. What should you do next?

> **Answer:** You must deploy the Windows 10 task sequence to the All Unknown Computers collection.

Question: You have created a task sequence that will install Windows 10 Enterprise and you want to deploy it on a few computers while minimizing the impact on your network. Which deployment method would be best suited to accomplish that task?

> **Answer:** You should create a standalone media on a USB drive that includes the boot image, operating system image, applications, packages, and potentially scripts. You do not need to use a network connection during the deployment.

Resources

Process for deploying an operating system image

Additional Reading: For more information, refer to Introduction to operating system deployment in System Center Configuration Manager: https://aka.ms/dwv0s1

Adding an operating system image to Configuration Manager

Additional Reading: For more information, refer to Customize operating system images with System Center Configuration Manager: http://aka.ms/vrzanf

Methods for running an installation task sequence

Additional Reading: For more information, refer to What's new in System Center Configuration Manager incremental versions: https://aka.ms/nler8v

Demonstration: Import a single computer object into Configuration Manager

Demonstration Steps

1. In the **Hyper-V Manager** on your host computer, right-click the **20703-1B-LON-IMG** virtual machine and select **Start**.

2. Wait 5 seconds, right-click the **20703-1B-LON-IMG** virtual machine again and select **Turn Off**. If prompted by the **Turn Off Machine** dialog box, click **Turn Off**.

   Note: You need to start the **LON-IMG** virtual machine in order to assign a MAC address to it.

3. In the details pane for the **20703-1B-LON-IMG** virtual machine, click the **Networking** tab, and in the **Adapter** column find the **MAC** address. You may need to expand the **Adapter** Column to see the **MAC address** fully. Write down the MAC address.

4. On **LON-CFG**, open the **Configuration Manager console**.
5. Click the **Assets and Compliance** workspace, right-click the **Devices** node, and then select **Import Computer Information**.
6. On the **Select Source** page of the **Import Computer Information Wizard**, select **Import single computer**, and then click **Next**.
7. On the **Single Computer** page, enter the following information, and then click **Next**:
8. Computer Name: **LON-IMG**
9. MAC address: **<The MAC address you wrote down>**
10. On the **Data Preview** page, verify the name and MAC address, and then click **Next**.
    - On the **Collections** page, click **Add**.
    - In the **Select Collections** window, select the **Adatum production image** collection, and then click **OK**.
11. On the **Collections** page, click **Next**.
12. On the **Summary** page, verify your selections, and then click **Next**.
13. On the **Confirmation** page, click **Close**.
14. Click the **Device Collections** node, right-click the **All Systems** collection, and then select **Update Membership**. When prompted, click **Yes**.
15. Right-click the **Adatum production image** collection, and then select **Update Membership**. When prompted, click **Yes**.
16. Click the **Adatum production image** collection, and then after 10 seconds press F5.
17. When the **Member Count** column changes to **1**, right-click the **Adatum production image** collection, and then select **Show Members**. You should now see the computer you added.

Demonstration: Importing and distributing an operating system image

Demonstration Steps

Import an operating system image

1. On **LON-CFG**, in the Configuration Manager console, click the **Software Library** workspace, expand **Operating Systems**, and click **Operating System Images**.
2. On the ribbon, in the **Create** group, click **Add Operating System Image**.
3. In the **Add Operating System Image Wizard**, on the **Data Source** page, in the **Path** box, type **\\LON-CFG\e$\Capture\Win10EntX64Eval.wim**, and then click **Next**.
4. On the **General** page, in the **Name** field, type **Windows 10 Enterprise X64 Eval**, and then click **Next**.
5. On the **Summary** page, click **Next**, and then on the **Completion** page, click **Close**.

Distribute an operating system image

1. Right-click the **Windows 10 Enterprise X64 Eval** image, and select **Distribute Content**.
2. In the **Distribute Content Wizard**, on the **General** page, click **Next**.
3. On the **Content Destination** page, click **Add**, and then select **Distribution Point**.

4. In the **Add Distribution Points** dialog box, select the **LON-CFG.ADATUM.COM** check box, and then click **OK**.
5. On the **Content Destination** page, click **Next**.
6. On the **Summary** page, click **Next**, and then on the **Completion** page, click **Close**.
7. Right-click the **Windows 10 Enterprise X64 Eval** image, and then click **Refresh**. Repeat periodically until the **Content Status** shows **Success: 1**. This will be indicated by a full green circle and should take around 5 minutes.

Demonstration: Creating and modifying a task sequence to deploy an existing image

Demonstration Steps

Create a task sequence to deploy an existing image

1. On **LON-CFG**, in the Configuration Manager console, click the **Software Library** workspace, and then expand **Operating Systems**.
2. Right-click **Task Sequences**, and select **Create Task Sequence**.
3. In the **Create Task Sequence Wizard**, on the **Create New Task Sequence** page, select the **Install an existing image package** option, and then click **Next**.
4. On the **Task Sequence Information** page, in the **Task sequence name** box, type **Deploy Windows 10 Enterprise X64 Eval**, and then click **Browse**.
5. In the **Select a Boot Image** dialog box, click **Boot image (x64) en-US**, and then click **OK**.
6. On the **Task Sequence Information** page, click **Next**.
7. On the **Install Windows** page, click **Browse**.
8. In the **Select an Operating System Image** dialog box, click **Windows 10 Enterprise X64 Eval en-US**, and then click **OK**.
9. Clear the check mark next to **Configure task sequence for use with BitLocker**.
10. Select the **Enable the account and specify the local administrator password** option, in the **Password** box, type **Pa55w.rd**, in the **Confirm password** box, type **Pa55w.rd**, and then click **Next**.
11. On the **Configure Network** page, select the **Join a domain** option.
12. In the area next to **Domain**, select **Browse**, click **Adatum.com**, and then click **OK**.
13. In the area next to **Domain OU**, click **Browse**, select **London Clients**, and then click **OK**.
14. Click **Set**.
15. In the **Windows User Account** dialog box, in the **User name** box, type **Adatum\DomainJoin**, in the **Password** box, type **Pa55w.rd**, in the **Confirm password** box, type **Pa55w.rd**, and then click **OK**.
16. On the **Configure Network** page, click **Next**.
17. On the **Install Configuration Manager** page, click **Next**.
18. On the **State Migration** page, clear all selected options, and then click **Next**.
19. On the **Include Updates** page, click **Next**.
20. On the **Install Applications** page, click **Next**.
21. On the **Summary** page, click **Next**.

22. On the **Completion** page, click **Close**.

Edit a task sequence

1. Right-click the **Deploy Windows 10 Enterprise X64 Eval** task sequence, and then click **Edit**.
2. Select the **Apply Windows Settings** option.
3. In the **User name** field type **A. Datum IT Services**, and in the **Organization name** field, type **A. Datum**.
4. In the **Deploy Windows 10 Enterprise X64 Eval Task Sequence Editor** window, click **OK**.

Demonstration: Deploying and running a task sequence

Demonstration Steps

Deploy a task sequence

1. Right-click the **Deploy Windows 10 Enterprise X64 Eval** task sequence, and then click **Deploy**.
2. In the **Deploy Software Wizard**, on the **General** page, in the area next to **Collection**, click **Browse**. When prompted, click **OK**.
3. In the **Select Collection** dialog box, select **Adatum production image**, and then click **OK**.
4. On the **General** page, click **Next**.
5. On the **Deployment Settings** page, next to **Purpose**, verify **Available** is selected, and under **Make Available to the following**, select **Only media and PXE**, and then click **Next**.
6. On the **Scheduling** page, click **Next**.
7. On the **User Experience** page, click **Next**.
8. On the **Alerts** page, click **Next**.
9. On the **Distribution Points** page, click **Next**.
10. On the **Summary** page, click **Next**.
11. On the **Completion** page, click **Close**.

Run a task sequence to deploy an operating system

1. On the host computer, in **Hyper-V Manager**, click **20703-1B-LON-IMG**, and in the **Actions** pane, click **Connect**.
2. In the Virtual Machine Connection window, select **Action**, and then click **Start**.
3. When **LON-IMG** boots, click inside the **Virtual Machine Connection** window. Wait until the message **Press F12 for network service boot** appears and then press F12. It will take approximately 10 seconds before you see the message.

   Note: Wait for the boot image to be staged and for the machine to boot up into Windows PE.

4. In the **Welcome to the Task Sequence Wizard** window, in the password field, type **Pa55w.rd**, and then click **Next**.
5. In the **Select a task sequence to run** window, verify that the task sequence you created earlier is displayed and selected, and then click **Next**.

6. Monitor the deployment. The task sequence will take between 15-25 minutes to complete depending on the performance of the Hyper-V host.
7. After the deployment is complete, click **Skip for now** on the **Let's connect you to a network** page.
8. On the **Connect now to save time later** page, click **No**.
9. Sign in to **LON-IMG** as **Adatum\Administrator** with the password **Pa55w.rd**, and then verify that the machine is name **LON-IMG**.

Note: It will take approximately 30 seconds before the desktop appears because a profile must be created for the user.

Lesson 4
Managing Windows as a service

Contents:

Question and Answers

Question: What are the requirements for implementing Windows 10 servicing in Configuration Manager?

Answer: Windows 10 servicing in Configuration Manager has the following requirements:

Question: What are the four servicing channels used to control the delivery of feature updates and quality updates to devices?

Answer: The four servicing channels are:

Resources

Overview of Windows 10 servicing

Additional Reading: For more information, refer to More on Windows 7 and Windows 8.1 servicing changes: http://aka.ms/AA2koby

Additional Reading: The older designations such as CB, CBB, and LTSB might still be visible in some Microsoft products, but they will be removed eventually.

Additional Reading: For more information, refer to Windows lifecycle fact sheet: http://aka.ms/AA2kvht and Helping customers shift to a modern desktop: http://aka.ms/AA2p3f9

Additional Reading: For more information, refer to Overview of Windows as a service: https://aka.ms/cfqi9t

Prerequisites for Windows 10 service management

Additional Reading: For more information, refer to Update Windows 10 in enterprise deployments: http://aka.ms/ttoygg

Demonstration: Creating a Windows 10 servicing plan

Demonstration Steps

1. On **LON-CFG**, open the Configuration Manager console, click the **Software Library** workspace, and then expand the **Windows 10 Servicing** node.
2. Right-click **Servicing Plans**, and then select **Create Servicing Plan**.
3. On the **General** page of the **Create Servicing Plan** Wizard, in the **Name** field, type **Windows 10 – Ring 1 – IT Pilot**, and then click **Next**.
4. On the **Servicing Plan** page, click **Browse**, select the **W10 servicing – Ring 1 – IT Pilot** collection, and then click **OK** and **Next**.
5. On the **Deployment Ring** page, verify that **Semi-Annual Channel (Targeted)** is selected. Move the slider to 10 days, and then click **Next**.
6. On the **Upgrades** page, click **Next**.
7. On the **Deployment Schedule** page, click **Next**.
8. On the **User Experience** page, click **Next**.
9. On the **Deployment Package** page, select **Create a new Deployment package**. Fill in the following details, and then click **Next**:

- Name: **W10 Upgrades**
- Package source: **\\LON-CFG\e$\Source\W10Upgrades**

10. On the **Distribution Points** page, click **Add**, and select **Distribution Point**. In the **Add Distribution Point** dialog box, select **LON-CFG.ADATUM.COM**, click **OK**, and then click **Next**.
11. On the **Download Location** page, click **Next**.
12. On the **Language Selection** page, clear all check boxes so only **English** is selected, and then click **Next**.
13. On the **Summary** page, click **Next**.
14. On the **Completion** page, click **Close**.

Module Review and Takeaways

Best Practices

Supplement or modify the following best practices for your own work situations:

- Implement access controls to protect bootable media. When you create bootable media, you should always assign a password and control physical access to the media.
- Always install the most recent security updates on a reference computer. Starting with an up-to-date reference computer helps decrease the window of vulnerability for newly deployed computers.
- Implement access controls to prevent unauthorized computers from connecting to the network if you are deploying operating systems to unknown computers. Although deploying to unknown computers can be a convenient way to deploy multiple computers on demand, it can also allow a hacker to add a trusted computer on your network. It also can mistakenly deploy an operating system image to computers that have not yet been discovered by Configuration Manager.

Review Questions

Question: How can operating system deployment assist in managing your organization's systems?

Answer: Answers will vary, but can include standardization and ease of deployment.

Question: What packages could you use for operating system deployment?

Answer: The packages for operating system deployment include: operating system installer package, device driver packages, Configuration Manager client upgrade package, application packages, and the USMT package.

Question: Why would you use task sequences outside of operating system deployment?

Answer: You use task sequences to run any series of commands on multiple client computers, such as installing a set of related applications on multiple computers.

Question: Why should you import computer information into the Configuration Manager database before deployment?

Answer: To prevent accidently sending a task sequence to unknown computers, you should use the Import Computer Information Wizard to import computer information into the Configuration Manager database before deployment. In the wizard, add the new computers to an appropriate target collection and target the task sequences accordingly.

Real-world Issues and Scenarios

Question: You are creating a new image for a new corporate standard laptop. You have discovered that the accelerometer driver is not installed automatically during operating system deployment. What can you do to install the accelerometer driver without user intervention?

Answer: Answers will vary. One possible solution is to create a package for the driver and add a task sequence step to install the driver after the operating system installs.

Tools

The following section includes the tools needed for this module.

1. Tool	2. Use for	3. Where to find it
Microsoft Deployment Toolkit	Managing deployment images	

1. Tool	2. Use for	3. Where to find it
		Additional Reading: For more information, refer to Microsoft Deployment Toolkit (MDT): https://aka.ms/adaz86

Lab Review Questions and Answers

Lab A: Preparing the site for operating system deployment

Question and Answers

Question: In your work environment, would you enable unknown computer support for PXE boot?

> **Answer:** Answers will vary. Discuss the advantages, such as ease of deployment, and the disadvantages, such as accidental deployment of enabling unknown computer support for PXE boot. Also, discuss the use of a password for PXE boot support.

Question: Apart from the packages deployed in the lab, what packages would you include as part of the operating system deployment process?

> **Answer:** Answers will vary.

Lab B: Deploying operating system images for bare-metal installations

Question and Answers

Question: When would you include an application in the Install an existing image task sequence rather than the build and capture task sequence?

> **Answer:** You include applications in the build and capture task sequence in situations where all computers should have the same applications, such as Microsoft Office. In the Install an existing image task sequence, you add additional applications that should only be installed on certain systems.

Question: In your work environment, will you use the USMT for state migration?

> **Answer:** Answers will vary. If you are using roaming profiles, state migration might not be necessary.

Module 12

Managing and maintaining a Configuration Manager site

Contents:

Lesson 1

Configuring role-based administration

Contents:

Question and Answers

Question: You need to verify all actions that Configuration Manager administrators perform. What can you do?

> **Answer:** You can view role-based access reports, including the Administration activity log.

Demonstration: Implementing role-based administration

Demonstration Steps

View security roles

1. On LON-CFG, on the taskbar, click the **Configuration Manager** icon.
2. In the Configuration Manager console, click the **Administration** workspace, expand the **Security** node, and then click **Security Roles**.
3. In the results pane, notice the 15 default security roles that display.
4. In the results pane, double-click **Operations Administrator**.
5. In the **Operations Administrator Properties** dialog box, click and then view the **General** tab, the **Administrative Users** tab, and the **Permissions** tab.
6. In the **Operations Administrator Properties** dialog box, click **OK**.

Create security scopes

1. In the Administration workspace, expand the **Security** node, and then click **Security Scopes**. Notice the built-in security scopes on this page.
2. Right-click **Security Scopes**, and then click **Create Security Scope**.
3. In the **Create Security Scope** dialog box, use the following settings, and then click **OK**:
   - Security scope name: **Desktop Administration**
   - Description: **Scope for Desktop related objects**
4. Right-click **Security Scopes**, and then click **Create Security Scope**.
5. In the **Create Security Scope** dialog box, use the following settings, and then click **OK**:
   - Security scope name: **Server Administration**
   - Description: **Scope for Server related objects**

Assign securable objects to security scopes

1. In the Configuration Manager console, click the **Software Library** workspace, expand the **Application Management** node, and then click **Applications**. Notice the XML Notepad 2007 application in the results pane. You will assign this application to the **Server Administration Scope** security scope.
2. In the results pane, right-click **XML Notepad 2007**, and then click **Set Security Scopes**.
3. In the **Set Security Scopes** dialog box, clear the **Default** check box, select the **Server Administration Scope** check box, and then click **OK**.
4. Under the Application Management node, click **Packages**. Notice the application package named Configuration Manager Client Package. You will assign this package to the Desktop Administration Scope security scope.
5. Right-click **Configuration Manager Client Package**, and then click **Set Security Scopes**.

6. In the **Set Security Scopes** dialog box, clear the **Default** check box, select the **Desktop Administration Scope** check box, and then click **OK**.

Add an administrative user

1. In the Configuration Manager console, click the **Administration** workspace, expand the **Security** node, and then click **Administrative Users**. Notice that the initial administrative user is the user who installed the Configuration Manager site.
2. Right-click **Administrative Users**, and then click **Add User or Group**.
3. In the **Add User or Group** dialog box, use the following settings, and then click **OK**:
    - User or group name: Browse to **Desktop Admins**
    - Assigned security roles: **Operations Administrator**
    - Assigned security scopes and collections: **Desktop Administration** scope and **London Clients**. Remove all other collections and the default scope.

Note: If the **London Clients** collection does not exist, create a **London Clients** collection with LON-CL1 as a direct member.

4. Close the **Configuration Manager console**.
5. Open the Configuration Manager console as a different user. To do this, press and hold the Shift key, right-click **Configuration Manager Console**, and then click **Run as different user**.
6. In the **Windows Security** dialog box, in the **User name** text box, type **Lara**. In the **Password** text box, type **Pa55w.rd**, and then click **OK**.
7. Browse to the Configuration Manager console, and then verify permissions.

Note: Lara is a member of the Desktop Admins group, and she should only see objects that are assigned to the Desktop Administration scope. This means that in the Device Collections node of the Assets and Compliance workspace, she should see the London Clients collection only. In the Software Library workspace, Lara should only see the Configuration Manager Client Package when the Packages node is selected.

8. Close the Configuration Manager console.

Lesson 2

Configuring Remote Tools

Contents:

Question and Answers

Question: What is the purpose of the Remote Control Permitted viewers list?

> **Answer:** The Remote Control Permitted viewers list is a list of users who are allowed to use Configuration Manager Remote Tools functionality on clients. The Remote Control Permitted viewers list does not validate until the Remote Tools Agent attempts to add the specified users to the ConfigMgr Remote Control Users group.

Question: What would happen if you tried to control the Remote Assistance settings through both Group Policy and Configuration Manager?

> **Answer:** When you refresh Group Policy on the client, by default, it processes all changes made to the applied Group Policy Objects (GPOs). However, Configuration Manager changes the settings in the local security policy, which by default overwrites any GPO setting. Administrators can force a GPO setting to override a local policy. Therefore, be aware that setting the policy in both places could lead to inconsistent results. Choose one of these methods to configure Remote Assistance settings.

Lesson 3

Overview of Configuration Manager site maintenance and Management Insights

Contents:

Question and Answers

Question: What tools can you use to monitor the health of Configuration Manager site systems?

> **Answer:** You can use the monitoring features in the Configuration Manager console to view the status of the site systems, to monitor replication, and to configure alerts. Additionally, you can use Operations Manager to monitor your Configuration Manager environment.

Question: Why should you delete aged inventory history data?

> **Answer:** Most database data is inventory data, which becomes obsolete when clients become inactive in your infrastructure. You should configure removal of aged inventory history data after it becomes obsolete in your environment.

Question: What happens when you click on the Take action button in a Management Insights rule?

> **Answer:** If you click the Take action button in the Rule Details dialog box, the following will happen depending on the rule:
>
> - You will automatically be taken to the place in the console where you can make the configuration or changes that the rule recommends; for example, the Client Settings node where you could change the client settings.
> - You will see a filtered view of objects; for example, a list of applications without any deployments or a list of Collections without any members.

Resources

Maintaining a Configuration Manager site

Additional Reading: For more information, refer to Connect Configuration Manager to Log Analytics: https://aka.ms/obdldp.

Lesson 4

Backing up and recovering a Configuration Manager site

Contents:

Question and Answers

Question: How do you recover your entire site if your site server fails?

> **Answer:** If your site server fails, perform the recovery by running the **System Center Configuration Manager Setup Wizard**, and then select the Recover a site option.

Question: What tool can you use to configure the archive of backup files that begins automatically after the site backup completes?

> **Answer:** You can configure the AfterBackup.bat file to initiate automatic archiving of files after the site backup completes.

Resources

Overview of backup and recovery

Additional Reading: For more information, refer to Use the Maintenance Plan Wizard: https://aka.ms/AA46r41.

Demonstration: Backing up a primary site

Demonstration Steps

Configure the Backup Site Server task

1. If necessary, sign in to LON-CFG as **Adatum\Administrator** with the password **Pa55w.rd**.
2. Open the Configuration Manager console, and then click the **Administration** workspace.
3. In the navigation pane, expand **Site Configuration**, and then click **Sites**.
4. In the results pane, click **S01 – Adatum Site**.
5. On the ribbon, click **Settings**, and then click **Site Maintenance**.
6. In the **Site Maintenance** dialog box, click **Backup Site Server**, and then click **Edit**.
7. In the **Backup Site Server Properties** dialog box, click **Enable this task**, and then click **Set Paths**.
8. In the **Set Backup Paths** dialog box, verify that the **Local drive on site server for site data and database** option is selected, and then click **Browse**.
9. In the **Select Folder** dialog box, browse to drive E, create a new folder named **Backup**, and then click **Select Folder**.
10. In the **Set Backup Paths** dialog box, verify that **E:\Backup** displays in the text box, and then click **OK**.
11. In the **Backup Site Server Properties** dialog box, in the **Start after** text box, set the time to start three minutes from now, verify that **Latest start time** is at least one hour from now, and then click **OK**.
12. In the **Site Maintenance** dialog box, verify that the word "Yes" displays in the **Enabled** column next to the Backup Site Server task, and then click **OK**.

Trigger and monitor a backup

1. Click **Start**, click **Windows Administrative Tools**, and then double-click **Services**.
2. In the Services console, in the details pane, click the **SMS_SITE_BACKUP** service, and then on the toolbar, click **Start Service**.

3. Browse to **C:\Program Files\Microsoft Configuration Manager\Logs**, and double-click the **Smsbkup.log** file. It will open in the Configuration Manager Trace Log Tool.
4. Wait until the **Smsbkup.log** displays that the **SMS_SITE_BACKUP** service stopped.
5. To verify that the backup occurred successfully, find the log entry that begins with "STATMSG: ID=5035".
6. Browse to the **E:\Backup\S01Backup\CD.Latest** folder, and then verify that the installation files backed up to the folder.
7. Browse to the **E:\Backup\S01Backup\SiteDBServer** folder, and then verify that the database files backed up to the folder.
8. Browse to the **E:\Backup\S01Backup\SiteServer\SMSServer** folder, and then observe the content. You should see **data**, **inboxes**, **logs**, and **srvacct** folders.
9. Close the File Explorer window.
10. In the Configuration Manager console, click the **Monitoring** workspace.
11. In the navigation pane, expand **System Status**, and then click the **Component Status** node.
12. In the results pane, click the **SMS_SITE_BACKUP** component.
13. On the ribbon, click **Show Messages**, and then click **All**.
14. In the **Status Messages: Set Viewing Period** dialog box, accept the default of **1 day ago**, and then click **OK**.
15. In **Configuration Manager Status Message Viewer**, look for a message with a message ID of "5035."
16. Close all open windows on LON-CFG.

Demonstration: Recovering a primary site

Demonstration Steps

1. Sign in to LON-CFG as **Adatum\Administrator** with the password **Pa55w.rd**.
2. Start the **System Center Configuration Manager Setup Wizard** by running **E:\Backup\S01Backup\CD.Latest\SMSSETUP\BIN\X64\setup.exe**.

Note: To perform a site recovery, you need to start the setup program from your site's most recent updated installation media. If you want to perform a site reset only, you need to start the setup from the installation path.

3. When the **System Center Configuration Manager Setup Wizard** starts, on the **Before You Begin** page, click **Next**.
4. On the **Getting Started** page, under **Available Setup Options**, verify that **Recover a site** is selected, and then click **Next**.
5. On the **Site Server and Database Recovery Options** page, click **Recover the site database using the backup set at the following location**, and then click **Browse**.
6. In the **Browse For Folder** dialog box, click the **E:\Backup\S01Backup** folder, and then click **OK**.
7. On the **Site Server and Database Recovery Options** page, click **Next**.

8. On the **Site Recovery Information** page, verify that the **Recover primary site** option is selected, and then click **Next**.
9. On the **Product Key** page, click **Install the evaluation edition of this product**, and then click **Next**.
10. On the **Product License Terms** page, select all check boxes, and then click **Next**.
11. On the **Prerequisite Downloads** page, click **Use previously downloaded files**. In the **Path** text box, type **E:\Backup\S01Backup\CD.Latest\Redist**, and then click **Next**.
12. In the **Configuration Manager Setup Downloader** dialog box, wait for the prerequisite validation to finish.
13. On the **Site and Installation Settings** page, click **Next**.
14. On the **Database Information** page, click **Next** twice.
15. On the **Diagnostic and Usage Data** page, click **Next**.
16. On the **Settings Summary** page, click **Next**.
17. On the **Prerequisite Check** page, click **Cancel**, and then click **Yes**.

Note: For an actual system recovery, you would click **Begin Install**. However, for demonstration purposes, you cancel the wizard. If you have time, you may test this lab to completion by adding a text comment to your S01 site, after a successful backup. Delete the CM_S01 database in SQL Server Management Studio, and proceed with the recovery lab without the original database. Your recovery could take approximately 30 minutes. You can follow the processing by viewing the log (C:\ConfigmgrSetup.log) interactively, or examine it after the recovery is complete. You should find your site intact, without the test comment that you added after your backup operation and before the recovery.

Lesson 5

Updating the Configuration Manager infrastructure

Contents:

Question and Answers

Question: In your environment, what factors would you consider when deciding between online mode or offline mode for receiving updates?

> **Answer:** Answers will vary. Security restrictions and the need for strict version control indicate a choice of offline mode, whereas a need for ease of administration would favor online mode.

Question: What security role would you grant to permit an assistant to view any new updates and features, but without the capability to install servicing updates or enable new features?

> **Answer:** For separation of duties and to observe the principle of least privilege, you would assign your assistant the Read-only Analyst role and the Default security scope.

Resources

Configuration Manager baseline versions and update versions

Additional Reading: For more information, refer to Updates and servicing for Configuration Manager: https://aka.ms/dh74j7.

Additional Reading: For more information, refer to Checklist for installing update 1810 for Configuration Manager: https://aka.ms/AA474qk.

Managing in-console updates

Additional Reading: For more information, refer to Use the Service Connection Tool for System Center Configuration Manager: https://aka.ms/jelwok.

Additional Reading: For more information, refer to About the service connection point in Configuration Manager: https://aka.ms/b5ie2v.

Upgrading clients after a servicing update

Additional Reading: For more information, refer to How to test client upgrades in a pre-production collection in System Center Configuration Manager: https://aka.ms/jtgdy0.

Additional Reading: For more information, refer to System Center Configuration Manager Feedback: https://aka.ms/fk79i7.

Module Review and Takeaways

Review Questions

Question: For what purposes do you use the AfterBackup.bat file?

> **Answer:** You use the AfterBackup.bat file to copy additional files from your Configuration Manager implementation, to archive a backup to a different location, and to perform validation tests.

Question: What factors determine how frequently you should perform a backup?

> **Answer:** The frequency with which you perform backups depends on several factors, including the number of configuration changes that you made to the environment since the last backup, and whether you are backing up a stand-alone primary site or a hierarchy. If you want to back up a hierarchy, you can use an older backup to perform recovery because the latest configuration changes transfer from other sites through replication.

Question: Under what circumstances should you perform unscheduled backups?

> **Answer:** You should perform unscheduled backups whenever you make a significant change to your Configuration Manager hierarchy, such as adding a new site.

Question: How can you minimize data loss when you do not perform backups?

> **Answer:** When you do not perform backups, you can minimize data loss by ensuring that you have a Configuration Manager hierarchy that contains at least two sites.

Question: Where can you get an overview of the Management Insights rules that you have already implemented in your environment?

> **Answer:** You can see that information in the Management Insights dashboard by selecting the **Show Completed** filtering option. It displays the rules with a status of **Completed** in the All Insights tile.

Lab Review Questions and Answers

Lab A: Configuring role-based administration

Question and Answers

Question: In the Configuration Manager console, what are some of the object types that you can associate with a specific security scope?

> **Answer:** The object types that you can associate with a specific security scope are:
>
> - Applications
> - Packages
> - Boot images
> - Sites
> - Custom client settings
> - Distribution points and distribution point groups
> - Software update groups

Question: You want to provide an administrative user with permissions to create and deploy apps. Which security role provides these capabilities?

> **Answer:** The Application Administrator role provides these capabilities because it includes the permissions for the Application Author and Application Deployment Manager roles.

Question: You want an administrative user to administer a specific collection only. How can you configure this?

> **Answer:** You need to configure the user or group so that its access is for a specific collection only. You need to remove all other default collections.

Lab B: Configuring Remote Tools

Question and Answers

Question: You have two groups of desktop devices that different service desk groups manage. You need to ensure that each service desk group can remotely connect only to the desktops that their group manages. How should you configure the Remote Control settings for each desktop group?

> **Answer:** You need to create a separate client settings object for each group.

Question: You need to allow service desk professionals to guide users remotely through procedures during service desk calls. Users should see what the service desk professional is doing while connecting remotely to the user's computer. What remote administration tool should the service desk professional use?

> **Answer:** The service desk professional should use Remote Assistance.

Lab C: Maintaining a Configuration Manager site

Question and Answers

Question: How do you configure a site backup?

> **Answer:** You configure a site backup by configuring the Backup Site Server task in the Site Maintenance tasks list.

Question: How do you perform site recovery?

> **Answer:** You perform site recovery by running the System Center Configuration Manager Setup Wizard and then selecting the Recover a site option.

Question: What can you do to keep your Configuration Manager database as small as possible?

> **Answer:** You configure maintenance tasks to delete aged data.