Microsoft

OFFICIAL MICROSOFT LEARNING PRODUCT

20345-2A

Designing and Deploying Microsoft Exchange Server 2016

Companion Content

Product Number: 20345-2A

Released: 05/2016

MICROSOFT LICENSE TERMS
MICROSOFT INSTRUCTOR-LED COURSEWARE

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

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

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

1. DEFINITIONS.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

provided you comply with the following:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

This limitation applies to

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

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

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

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

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

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

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

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

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

Revised July 2013

Module 1

Planning Exchange Server deployments

Contents:

Lesson 1: New features in Exchange Server 2016 2

Lesson 2: Gathering business requirements for an Exchange Server 2016 deployment 4

Lesson 3: Planning for an Exchange Server 2016 deployment 7

Lesson 4: Designing a UM deployment 9

Module Review and Takeaways 11

Lesson 1

New features in Exchange Server 2016

Contents:

Question and Answers 3
Resources 3

Question and Answers

Question: Which service on Exchange Server 2016 accepts client connections?

Answer: The front-end client access service accepts client connections.

Question: What is the most important architectural change in Exchange Server 2016 and what benefits does this change provide?

Answer: The most important architectural change is that all key functionalities including the Mailbox server role, Client Access server role, Hub Transport server role, and UM server role are now located on the Mailbox server. This architectural change provides the following benefits:

- Fewer physical or virtual servers
- Simplified management
- Better scalability and reliability

Resources

What is new in Exchange Server 2016 for Exchange 2013 administrators

 **Additional Reading:** For more information, refer to What's new in Exchange 2016: http://aka.ms/E2xouf

Discontinued and de-emphasized features in Exchange Server 2016

 **Additional Reading:** For more information, refer to What's discontinued in Exchange 2016: http://aka.ms/Upk34z

Lesson 2

Gathering business requirements for an Exchange Server 2016 deployment

Contents:

Question and Answers 5

Question and Answers

Question: What is an SLA, and why is it important?

Answer: Service level agreements (SLAs) are understandings reached between an organization and its information technology (IT) department, or between a service provider and a client, that define expected infrastructure performance levels. Defining an SLA is important, because it documents the service expectations and requirements that an organization expects the IT department to deliver.

Question: Why is it important to include end-user requirements when gathering requirements for a deployment plan?

Answer: User requirements might differ from business requirements. They can be useful, because users typically are interested in the system's ease of use, and how it enables them to perform tasks more efficiently.

Discussion: Identifying regulatory and organizational compliance requirements

Question: In what type of business does your organization participate? What are the legislated compliance requirements for your organization?

Answer: Answers will vary depending on the type of business in which your organization participates. Examples of legislation restricting how organizations manage information include:

- United States:
  - Sarbanes-Oxley Act of 2002
  - Gramm-Leach-Bliley Act (Financial Services Modernization Act of 1999)
  - Health Insurance Portability and Accountability Act of 1996
  - Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA Patriot Act)
- Canada: The Personal Information Protection and Electronic Documents Act
- Australia: Privacy Act 1988
- Europe: European Union Data Protection Directive
- Japan: Act on the Protection of Personal Information

Question: What additional compliance requirements does your organization have?

Answer: Answers will vary. For example, organizations might impose strict requirements for managing email. Some might add legal disclaimers to outgoing communications, or require that certain messages include an intellectual property disclosure disclaimer. Additionally, the organization might have requirements for message retention that require certain messages be retained, while others can be deleted after a specific amount of time.

Question: What issues do regulatory and organizational compliance requirements raise for your organization? How are you addressing these issues? What are the gaps between the requirements and the solutions?

Answer: Answers will vary. Traditionally, it is difficult to address regulatory and organizational compliance requirements. Answers might include:

- Archiving all messages by using a non-Microsoft tool.
- Specifying policies to regulate the types of information sent via email.

- Enforcing policies through auditing.
- Scanning messages for content and applying necessary disclaimers.

Question: Are the compliance solutions based on a policy or a technology? In other words, does your organization only have written policies that define what users can do, or is there a technological solution in place to enforce some or all of the requirements? If you are using a policy-based solution, how do you enforce policies?

Answer: Answers will vary. Typically, organizations have policy-based solutions for cases where a technology-based solution does not exist. Additionally, policy-based solutions are difficult to enforce, and policy violators often are detected only through difficult investigations.

Lesson 3

Planning for an Exchange Server 2016 deployment

Contents:

Question and Answers 8
Resources 8

Question and Answers

Question: What are the key aspects of AD DS that you should consider when planning Exchange Server 2016 deployment?

> **Answer:** You should consider schema and related changes, current Active Directory site configuration, and the placement of domain controllers and global catalog servers.

Question: What are the key factors that can influence your decision about deploying the Mailbox server role in a specific site?

> **Answer:** These factors include (but are not limited to) the number of users in the site, link bandwidth between that site and main site, and high availability requirements.

Resources

Preparing AD DS for an Exchange Server 2016 deployment

 **Additional Reading:** For more information, refer to Exchange 2016 Active Directory schema changes: http://aka.ms/Gzjm43

 **Additional Reading:** For more information, refer to Prepare Active Directory and domains: http://aka.ms/O8gk68

Lesson 4

Designing a UM deployment

Contents:

Question and Answers 10
Resources 10

Question and Answers

Question: What is the purpose of the UM Call Router Service?

Answer: This service manages signaling of traffic, and forwards processing of the client requests to the responsible Mailbox server.

Question: Do you need to configure the Edge Transport Server role when you deploy UM?

Answer: No, the Edge Transport server role does not work with the UM service.

Resources

Requirements to implement UM

 **Additional Reading:** For more information, refer to Telephony advisor for Exchange 2013: http://aka.ms/Cpadnv

Configuring UM

 **Additional Reading:** For more information, refer to Configuration notes for supported VoIP gateways, IP PBXs, and PBXs: http://aka.ms/B3838w

Module Review and Takeaways

Best Practices

- Understand the new features and architectural changes in Exchange Server 2016 before planning for deployment.
- Be sure to provide alternatives for discontinued features.
- Be as detailed as possible when gathering requirements.
- Provide clear mapping between business and technical requirements.

Module 2

Planning and deploying Exchange Server 2016 Mailbox services

Contents:

Lesson 1: Planning Exchange Server hardware requirements 2

Lesson 2: Planning Exchange Server for virtualization and Azure integration 6

Lesson 3: Planning and implementing public folders 8

Module Review and Takeaways 10

Lab Review Questions and Answers 11

Lesson 1

Planning Exchange Server hardware requirements

Contents:

Question and Answers 3
Resources 3
Demonstration: Using the Exchange Server 2016 Role Requirements Calculator to plan for mailbox databases 3

Question and Answers

Question: Besides using the Exchange Server Role Requirements Calculator, what other methods can you use to size your Exchange 2016 environment?

> **Answer:** You can use the current Exchange environment's sizing or you can gather information by using Performance Monitor.
>
> **Feedback:** Exchange Server 2013 and Exchange Server 2016 have similar sizing profiles. While using the Exchange Server Role Requirements Calculator is the best way to size your Exchange Server 2016 environment, you can use the current size of your Exchange Server 2013 environment as an alternative. You also can use Performance Monitor against your existing environment to gain some insight into the CPU, memory, storage, and IOPS in use.

Question: When designing a DAG, how can you ensure that database-seeding operations do not take a long time per database?

> **Answer:** Use small database sizes.
>
> **Feedback:** Exchange Server 2016 supports very large volume sizes, but there are some practical limitations. When you create a DAG, your databases needed to be copied over the WAN. If you have very large databases, that process can take a long time. By using small databases sizes, the copy process can be reduced.

Resources

Planning file system requirements

 **Additional Reading:** For more detail about the preferred architecture, refer to: Ther Exchange 2016 Preferred Architecture at: http://aka.ms/Dqcvdd

Demonstration: Using the Exchange Server 2016 Role Requirements Calculator to plan for mailbox databases

Demonstration Steps

1. Sign into **LON-CL1** as **ADATUM\Administrator** with the password **Pa$$w0rd**.
2. If a network notification is displayed asking if you want the PC to be discoverable to other devices on the network, click **No**.
3. Open File Explorer and navigate to **C:\Labfiles**.
4. Double-click **ExchangeCalcv7.8.xlsm** to open the Exchange Server Role Requirements Calculator. If an error dialog box is displayed, click **OK** and double-click **ExchangeCalcv7.8.xlsm** again.
5. In the PROTECTED VIEW ribbon notification, click **Enable Editing**.
6. In the SECURITY WARNING ribbon notification, click **Enable Content**.
7. In the Exchange Environment Configuration section, update the following values in the calculator:
   - Server Role Virtualization: **Yes**
   - Number of Mailbox Servers Hosting Active Mailboxes / DAG (Primary Datacenter): **2**
   - Number of Database Availability Groups: **1**
8. In the Mailbox Database Copy Configuration section, update the following values in the calculator:
   - Total Number of Lagged Database Copy Instances within DAG: **0**

9. In the Site Resilience Configuration section, update the Site Resilience User Distribution Model to **Active/Passive.**
10. In the Exchange Data Configuration section, update the following values in the calculator:
    - Data Overhead Factor: **25%**
    - Volume Free Space Percentage: **10%**
11. Scroll down to the Role Requirements Input Factors – Mailbox Configuration area of the calculator. In the Tier-1 User Mailbox Configuration section, update the following values in the calculator:
    - Total Number of Tier-1 User Mailboxes / Environment: **400**
    - Projected Mailbox Number Growth Percentage: **10%**
    - Total Send/Receive Capability / Mailbox / Day: **300 messages**
    - Average Message Size (KB): **100**
    - Initial Mailbox Size (MB): **10240**
    - Mailbox Size Limit (MB): **25625**
    - Deleted Item Retention Window (Days): **30**
12. In the Tier-2 User Mailbox Configuration section, update the following values in the calculator:
    - Total Number of Tier-2 User Mailboxes / Environment: **2400**
    - Projected Mailbox Number Growth Percentage: **10%**
    - Initial Mailbox Size (MB): **2048**
    - Mailbox Size Limit (MB): **5120**
13. In the Tier-3 User Mailbox Configuration section, update the following values in the calculator:
    - Total Number of Tier-3 Mailboxes / Environment: **400**
    - Projected Mailbox Number Growth Percentage: **10%**
    - Total Send/Receive Capability / Mailbox / Day: **150 messages**
    - Average Message Size (KB): **50**
    - Mailbox Size Limit (MB): **2048**
14. Scroll to the bottom of the worksheet, and you should see three servers listed in the **Server** section.
    - For Server 1 Primary Site Failure Domain 1 (1-Franklin), type **LON-EX1.**
    - For Server 2 Primary Site Failure Domain 1 (2-Washington), type **LON-EX2.**
    - For Server 3 Primary Site Failure Domain 1 (3-Jackson), type **BER-EX1.**
15. Click the **Role Requirements** tab. In the User Mailbox Configurations section, verify that the number of user mailboxes / environment is 440 under Tier-1, 2640 under Tier-2, and 440 under Tier-3. Verify that the user mailbox size within the database is 27610 MB for Tier-1, 5555 MB for Tier-2, and 2244 MB for Tier-3.
16. Scroll down to the **Disk Space Requirements** section. In the database space required row, verify that it shows **808 GB** per database, **33937 GB** per server, **101810 GB** per DAG and environment.
17. Click the **Distribution** tab.
18. At the top of the page, click **Export DAG List**.

19. In the Role Calculator – Export DAG List window, change the Export Path to **C:\Users\Administrator\Desktop**, and then click **OK**.
20. In the Role Calculator – Export DAG List window, click **OK**. Wait briefly until the information changes.
21. Verify that all three Exchange servers are assigned forty-two mailbox copies with the two servers in London (LON-EX1 and LON-EX2) hosting twenty-one active mailbox databases each.
22. On the left side of the worksheet, just above the column for LON-EX1, click **Fail Server.** You should see that LON-EX2 is now hosting all active mailbox databases.
23. Click **Refresh Database Layout** in the upper-left corner to reset the Distribution worksheet.
24. Click **Fail WAN** and **Fail Server** on the left side. With only one server of the three online and reachable, you should see DAG quorum has failed, and that all mailbox databases are offline.
25. Click **Refresh Database Layout** in the upper-left corner to reset the Distribution worksheet.
26. Click the **Volume Requirements** tab and verify that each storage volume contains two Exchange mailbox databases by reviewing the value of the **Number of Databases / Volume** item in the Volume Configuration section. Verify that the database size with overhead is **808 GB** by reviewing the **DB Size + Overhead** column in the Database and Log Configuration / Server section.
27. Click the **Mailbox Space Modeling** tab, verify that the Tier-1 mailbox space modeling is 26.96 for maximum mailbox size, and 18.55 for the number of months to reach maximum mailbox size.

Lesson 2

Planning Exchange Server for virtualization and Azure integration

Contents:

Question and Answers 7

Question and Answers

Question: When you deploy Exchange Server 2016 to virtual machines in Microsoft Azure, how do you refer to the deployment?

( ) A hybrid deployment

( ) Platform as a Service (PaaS)

( ) Infrastructure as a Service (IaaS)

( ) Software as a Service (SaaS)

( ) Exchange Online

Answer:

( ) A hybrid deployment

( ) Platform as a Service (PaaS)

(√) Infrastructure as a Service (IaaS)

( ) Software as a Service (SaaS)

( ) Exchange Online

Feedback: Deploying Exchange Server 2016 to virtual machines in Microsoft Azure is referred to as IaaS because Azure is used as the infrastructure.

Question: You are planning to run Exchange Server 2016 on Hyper-V virtual machines. You already sized the resources for physical servers. How should you change the resource allocation for VMs?

( ) Keep everything the same.

( ) Increase only the CPU.

( ) Increase only the RAM.

( ) Increase only the storage.

( ) Increase the CPU and the RAM.

Answer:

(√) Keep everything the same.

( ) Increase only the CPU.

( ) Increase only the RAM.

( ) Increase only the storage.

( ) Increase the CPU and the RAM.

Feedback: The hardware requirements for Exchange Server 2016 are the same whether the servers will be physical or virtual. Thus, no changes are required.

Lesson 3

Planning and implementing public folders

Contents:

Question and Answers 9
Resources 9

Question and Answers

Question: You can place a public folder mailbox in a DAG to increase redundancy.

( ) True

( ) False

Answer:

(√) True

( ) False

Feedback: You can place public folder mailboxes, which are stored in standard mailbox databases, in a DAG to increase redundancy.

Question: What are the pros and cons of delegating public folder permissions to employees?

Answer: The advantages are that it offloads some of the day-to-day administration from the IT department. Additionally, users feel empowered and are often closer to the day-to-day delegation requirements, which helps to ensure that permissions are assigned appropriately. The disadvantages are that non-IT users might not be familiar with the company security policies and might not manage folder permissions to meet the standards. Users also might create too many public folders. Finally, users might not understand how public folder permissions work, which might enable individuals to access to data that they should not access.

Resources

Planning the Public Folder hierarchy

 **Additional Reading:** For the most up to date limitations, refer to Limits for public folders at http://aka.ms/W6dy7p

Module Review and Takeaways

Question: The management team has asked you to develop a solution for collaboration between teams at the company. The management team needs to have people share contact information for vendors, share a calendar, have discussions, and share documents. Management also wants to enable document versioning. Which solution should you recommend?

Answer: SharePoint Server

Feedback: In this scenario, you should recommend SharePoint Server. While Exchange public folders can handle most of the requirements, they do not offer document versioning. SharePoint Server meets all of the requirements.

Common Issues and Troubleshooting Tips

Common Issue	Troubleshooting Tip
You are unable to use a file server as a witness server in your DAG.	Check the Windows firewall to ensure that it is not blocking the communication. You can log dropped packets (preferred) or you can temporarily shut off the firewall to validate.
You are unable to move a mailbox database from one server to another.	Check the status of the mailbox database copy. If it is not healthy, it might not move.
You are unable to see public folders in Outlook on the web.	In Outlook on the web, in the left pane, right-click **Favorites,** and then click **Add public folder to Favorites**. Then, add one or more folders to the favorites by clicking a folder, and then clicking **Add to Favorites**. Thereafter, you will see the folder in your email folder list.

Lab Review Questions and Answers

Lab: Plan and implement Exchange virtualization, mailbox databases, and public folders

Question and Answers

Question: When you size your Exchange environment, what is the primary role of email data growth?

Answer: Email data growth helps you calculate how much storage you will need for your Exchange environment, based on the number of years you plan to operate it. By planning your storage with email data growth in the equation, you can minimize the chances of running out of disk space or having to add disk space routinely.

Question: Which cmdlet do you use to move a database from one server to another?

Answer: You use the **Move-ActiveMailboxDatabase** cmdlet to move a database.

Feedback: You use the **Move-ActiveMailboxDatabase** cmdlet to move a database. You can also perform the action from the Exchange admin center.

Module 3

Planning and deploying message transport

Contents:

Lesson 1: Designing message routing 2

Lesson 2: Designing transport services 4

Lesson 3: Designing the message-routing perimeter 6

Lesson 4: Designing and implementing transport compliance 8

Module Review and Takeaways 11

Lab Review Questions and Answers 12

Lesson 1

Designing message routing

Contents:

Question and Answers 3
Resources 3

Question and Answers

Question: Although no manual actions are required from you to resubmit messages from the Safety Net, what are the two scenarios in which the Safety Net will resubmit messages?

( ) After the automatic or manual failover of a mailbox database in an Exchange Server Database Availability Group (DAG)

( ) After you add a Mailbox server to the Exchange Server DAG

( ) After you activate a lagged copy of a mailbox database

( ) After you deactivate a lagged copy of a mailbox database

( ) After you replay logs from a lagged copy of a mailbox database

Answer:

(√) After the automatic or manual failover of a mailbox database in an Exchange Server Database Availability Group (DAG)

( ) After you add a Mailbox server to the Exchange Server DAG

(√) After you activate a lagged copy of a mailbox database

( ) After you deactivate a lagged copy of a mailbox database

( ) After you replay logs from a lagged copy of a mailbox database

Feedback: The only significant difference between these two scenarios is how far back in time you need to go to resubmit messages from the Safety Net. Typically, for failover in an Exchange Server DAG, the new active copy of the mailbox database is several minutes to several hours behind the old active copy. A lagged copy of a mailbox database typically is several days behind the old active copy.

There is one main requirement for a lagged copy's successful resubmission from the Safety Net. The amount of time that messages are stored in the Safety Net must be greater than or equal to the replay lag time of the mailbox database's lagged copy. In other words, the value of the **SafetyNetHoldTime** parameter on the **Set-TransportConfig** Windows PowerShell cmdlet must be greater than or equal to the value of the **ReplayLagTime** parameter on the **Set-MailboxDatabaseCopy** Windows PowerShell cmdlet for the lagged copy.

Resources

Designing message routing to mitigate the effects of message-routing failure

Additional Reading: For more information on the Active Directory subnets recommendations, refer to the published guidance on creating an Active Directory site: http://aka.ms/Lxc72d

Additional Reading: For more information on the recommendations from the Exchange Engineering Team, refer to The Preferred Architecture: http://aka.ms/Jx6r6y

Lesson 2

Designing transport services

Contents:

Question and Answers 5
Demonstration: Reviewing mail flow settings 5

Question and Answers

Question: When enabling an Exchange Server hybrid deployment, which Exchange Server domain settings are enabled and why?

> **Answer:** Because Exchange Online is a separate domain name, the Hybrid Configuration wizard will create an additional remote domain configured with the domain name of TenantName.mail.onmicrosoft.com on the Exchange Server. The remote domain settings will configure out-of-office and message-formatting settings.
>
> Additionally, the Hybrid Configuration wizard will create an additional accepted domain name, which will have the TenantName.onmicrosoft.com domain name on the Exchange Server. The accepted domain settings will configure the TenantName.onmicrosoft.com domain name as an internal relay. As users migrate to Exchange Online, Exchange Server will forward to Exchange Online any new emails to users with the domain name of TenantName.onmicrosoft.com.

Demonstration: Reviewing mail flow settings

Demonstration Steps

1. On LON-EX1, open Internet Explorer.
2. In the address bar, type **https://LON-EX1.adatum.com/ecp**, and then press Enter.
3. Sign in as **Adatum\Administrator** with the password **Pa$$w0rd**.
4. On the **Choose your preferred display language and home time zone below** page, on the **Time Zone** menu, select your time zone, and then click **Save**.
5. In the Exchange admin center, in the feature pane, click **mail flow**.
6. Click the **rules** tab. Explain to the students that on this tab, you can create transport rules that are applied on messages during transport between senders and recipients.
7. Click the **delivery reports** tab. Explain that on this tab, you can perform message tracking by searching a specific mailbox, or by searching by sender, recipient, or keyword. Also, explain that a similar interface is available to Microsoft Outlook on the Web users.
8. Click the **accepted domains** tab.
9. Click **Adatum.com**, and then click **Edit**.
10. In the Adatum.com window, show that this domain is added by default as an authoritative email domain. Click **cancel**.
11. Click the **email address policies** tab. Click **Default Policy**, and then click **Edit**.
12. In the Email Address Policy window, click **email address format**.
13. In the list, double-click **@adatum.com**, and then show how the email address is constructed for users in Adatum.com.
14. Click **cancel** two times.
15. Click the **receive connectors** tab. Explain that here you can configure Receive connectors for incoming SMTP traffic. Also, show the connectors that are created by default.
16. Click the **send connectors** tab. Explain that this is where you create SMTP connectors for outgoing SMTP traffic.
17. Leave the Exchange admin center open.

Lesson 3

Designing the message-routing perimeter

Contents:

Question and Answers 7

Question and Answers

Question: You have deployed Exchange Server 2016 to your organization, and you have enabled an Edge Transport server for accepting email from the Internet and for sending email from your organization to the Internet.

Users in your organization have recently started receiving unusual threats, such as *spear-phishing attacks*, which are emails that include malicious URLs, and *zero-day malware* in attachments from senders at multiple sites. However, management at your company would like you to minimize the effect of any changes to your users.

Zero-day malware is a first generation, previously unknown variant of malware, which has not been captured or analyzed. With zero-day malware, most antimalware engines do not have any definitions available for detecting it. The malware is not considered "zero-day" after a sample is captured and analyzed by antimalware engines, and a definition is created to detect it based on the unique signature of the malware.

You need to deploy a solution that meets the following requirements, including that it:

- Increases protection from inbound spear-phishing attacks.
- Increases protection from malware in attachments in inbound and outbound emails.
- Ensures users can manage their safe and blocked sender's lists from Outlook.
- Ensures minimal delays in outbound email.

How will you deploy?

> **Answer:** Based on the requirements, you will need to deploy Exchange Online Protection (EOP) and configure your MX records to route email through EOP. You will need to enable the Advanced Threat Protection add-on in EOP to combat spear-phishing attacks, and you must enable the anti-malware protection feature in EOP to protect inbound emails from malware. You will need to enable content filtering on your Exchange Edge servers, to protect your users from malware in attachments in inbound and outbound emails. You also must use directory synchronization to synchronize user's junk email filtering in Outlook to Exchange Online. Finally, you will need to configure the Exchange Edge servers to send outbound email to the Internet, based on MX record lookups, so you ensure minimal delays in outbound email.

Planning hardware and placements for your Edge Transport servers

Question: Is high availability for Edge Transport servers important for your organization?

> **Answer:** In most cases, yes. Modern businesses rely on email communication with external vendors and customers. Any significant outage is a problem.

Lesson 4

Designing and implementing transport compliance

Contents:

Question and Answers 9
Demonstration: Configuring message moderation and journaling 9

Question and Answers

Planning for message journaling

Question: The Legal department of your company has requested that you record all future inbound and outbound email communications for your company's employees. Your company has several vendors and contractors who can sign in to your network. While your users can see the email addresses of your vendors and contractors in Outlook, your vendors and contractors have mailboxes outside of your Exchange Server organization. The Legal department has requested that you not record any email communications to your vendors or contractors from outside the company. Your solution should use the least amount of administrative effort.

> **Answer:** You need to configure standard journaling in the properties of the mailbox database. This will record all future inbound and outbound email communications of the employee's in your company, and exclude email communications from outside the company to your vendors and contractors.

Demonstration: Configuring message moderation and journaling

Demonstration Steps

Configure moderation settings for the Managers distribution group

1. On LON-EX1, open Internet Explorer.
2. If the Exchange admin center is not open, in the address bar, type **https://LON-EX1.adatum.com/ecp**, and then press **Enter** to open the Exchange admin center.
3. Sign in as **Adatum\Administrator** with the password **Pa$$w0rd**.
4. In the Exchange admin center, navigate to **recipients – groups**.
5. In the result pane, click the **Managers** distribution group, and then click **Edit**.
6. On the **properties** page, click **message approval**, and then complete the following:
   - Select the **Messages sent to this group have to be approved by a moderator** check box.
   - In the **group moderators** list, click **Add**.
   - In the Select group moderators window, find and select **Ed**, click **add**, and then click **ok**.
   - In the **Senders who don't require message approval** list, click **Add**.
   - In the Select senders window, find and select user **Erwin** from the list, click **add**, and then click **ok**.
   - In Select moderation notifications window, select the **Notify senders in your organization when their messages aren't approved** option.
7. Click **save**.
8. Sign out of Exchange admin center.
9. Open a new Internet Explorer tab, in the address bar, type **https://lon-EX1.adatum.com/owa**, and then press Enter to open Outlook on the Web.
10. Sign in as **Adatum\Ankur** with the password **Pa$$w0rd**.
11. On the **Choose your preferred display language and home time zone below** page, on the **Time Zone** menu, select your time zone, and then click **Save**.
12. Near the top of the page, click **New** to compose a new email.

13. In the **To** field, type **Managers**, and then press Enter. A Mail Tip window appears, to inform you that this group is moderated.
14. In the **Subject** text box, type **Message to Managers group**. Observe the mail tip when composing the email.
15. Click **Send**.

Note: If you receive an alert when trying to send the message, verify that all Exchange services are started and then try sending the message again.

16. Sign in to LON-CL1 as user **Adatum\Ed** with the password **Pa$$w0rd**.
17. Double-click Outlook 2016 from the **All Apps** screen. Click **Next** three times, and then click **Finish** to create the Outlook profile for Ed.
18. If you receive a warning that the connection to Exchange is unavailable, click **OK**, and then in the Add Account window, click **Retry**.
19. If you receive a warning that Microsoft Office is not activated, in the Microsoft Office Activation Wizard window, click **Close**.
20. In the **First things first** dialog box, click **Ask me later**, and then click **Accept**.
21. Check that the message from Ankur is in Ed's Inbox for approval.
22. Click **Reject**, and then click **OK** to reject the message. Close Outlook. Sign out Ed from LON-CL1.
23. Switch to the LON-EX1 virtual machine, open Internet Explorer for Outlook on the Web and sign in as Adatum/Ankur with the password **Pa$$w0rd**.
24. Check the Inbox in Outlook on the Web for the rejected message to the Managers group.
25. Read the information in the rejected message.
26. Sign out as Ankur from Outlook on the Web.

Configure a journal rule to journal all messages that all of your organization's users send and receive

1. Open Internet Explorer, and in the address bar, type **https://lon-EX1.adatum.com/ecp**, and then press Enter to open the Exchange admin center.
2. Sign in as **Adatum\administrator** with the password **Pa$$w0rd**.
3. Navigate to **compliance management**, click **journal rules**, and then click **New**.
4. In the field **Send journal reports to**, type **Journal**.
5. In the **Name** field, type **Adatum Journal Rule** as the name for the journal rule.
6. In the **If the message is sent to or received from** field, click **Apply to all messages**.
7. In the **Journal the following messages** field, select **All messages**.
8. Click **save**, and then in the warning window, click **yes**.

Module Review and Takeaways

Best Practices

- Use transport rules to check messages for specific conditions and take defined actions on the messages before they reach the recipients.
- Use message moderation to avoid cases when messages with unimportant content are sent to large distribution lists.

Review Question(s)

Question: What happens if a message to a moderated recipient is not answered within five days?

Answer: If a message to a moderated recipient is not answered within five days, the message expires and is sent back to the sender.

Question: The network security policy at your company requires that you retain the mailboxes of employees who are no longer with the company for 30 days. The policy also requires that you reject emails sent to these mailboxes, and that the **Address blocked for delivery – Recipient is no longer active** reply is sent to the sender. How would you configure a transport rule to meet the requirements?

Answer: Create a distribution group named **Adatum All Disabled**. Then, create a transport rule with the following settings:

- Apply this rule if:
  - The recipient is a member of: **Adatum All Disabled**
- Do the following:
  - Reject the message with the explanation: **Address blocked for delivery – Recipient is no longer active**

Question: The network security team for your company wants to receive copies of specific delivery status notifications (DSN) messages that your users receive. How would you configure this in your Exchange Server organization?

Answer: You need to use the **Set-OrganizationConfig** Exchange Management Shell cmdlet, with the *MicrosoftExchangeRecipientReplyRecipient* property, to send copies of delivery status notifications (DSN) messages to the network security team. You need to use the **Set-TransportConfig** Exchange Management Shell cmdlet, with the *GenerateCopyOfDSNFor* property, to configure the specific DSN messages to send to the network security team.

Lab Review Questions and Answers

Lab: Planning and deploying message transport

Question and Answers

Question: If your Exchange Server 2016 deployment did not include the Edge Transport server, how could your message plan meet the requirements for the Contoso partner?

Answer: You can apply the same configuration settings of your Edge Transport server, which you identified in your message transport plan, to the Mailbox server in your Exchange Server 2016 deployment.

Question: The network security policy at your company requires that users not forward voicemail in Exchange Server 2016 to recipients outside the company. Based on your understanding of transport rules, how would you configure this?

Hint: All voicemails in Exchange Server 2016 include the words "Voice Mail" in the subject and include an attachment with a file type of wma or mp3.

Answer: You should configure a transport rule with the following settings:

- Apply this rule if:
  - The recipient is located: **Outside the organization**
  - The subject includes: **Voice Mail**
  - Any attachment's file extension matches: **wma or mp3**
- Do the following:
  - Block the message

If the message is blocked, you could also add a custom system message in Exchange Server 2016 that will remind users of the company policy. This additional **Reject the message with the enhanced status code** option is available when you create the transport rule in Exchange Server 2016.

Module 4

Planning and deploying client access

Contents:

Lesson 1: Planning Exchange Server 2016 clients 2

Lesson 2: Planning for client access 4

Lesson 3: Planning and implementing Microsoft Office Online Server 6

Lesson 4: Planning and implementing coexistence of SharePoint 2016 with Exchange 11

Lesson 5: Designing external client access 13

Module Review and Takeaways 18

Lab Review Questions and Answers 19

Lesson 1

Planning Exchange Server 2016 clients

Contents:

Question and Answers 3

Question and Answers

Question: Which client types use Autodiscover to identify configuration information? Choose all that apply.

( ) Outlook

( ) Outlook on the web

( ) POP3

( ) IMAP4

( ) Exchange ActiveSync

Answer:

(√) Outlook

( ) Outlook on the web

( ) POP3

( ) IMAP4

(√) Exchange ActiveSync

Question: If an Outlook client cannot contact an Autodiscover URL specified by an in-site SCP object, then it will attempt to connect by using DNS lookup methods.

( ) True

( ) False

Answer:

(√) True

( ) False

Feedback: When an Outlook client cannot contact an Autodiscover URL specified by an in-site SCP object, it does not attempt to connect to Autodiscover URLs specified by out-of-site SCP objects. If in-site URLs fail, DNS lookup methods are used to locate Autodiscover.

Lesson 2

Planning for client access

Contents:

Question and Answers 5
Resources 5

Question and Answers

Question: Describe some of the considerations when creating an SSL certificate for Exchange Server.

Answer: Some of the considerations for an SSL certificate are:

- Trust. The certificate source needs to be trusted. This generally means that the certificate should be from a public CA.
- Names. All namespaces need to be included on the certificate. Typically you use a SAN or UC certificate.
- Same certificate on all servers sharing the namespace. When you implement load balancing for high availability, all servers need to use the same certificate to ensure that encryption does not need to be renegotiated.

Resources

What is the client access functionality?

 **Additional Reading:** For more information, see "Outlook Connectivity with MAPI over HTTP": http://aka.ms/F9b28t

Lesson 3

Planning and implementing Microsoft Office Online Server

Contents:

Question and Answers 7
Demonstration: Deploying and testing Office Online Server for Exchange 2016 7

Question and Answers

Question: Which cmdlet should you use to configure Outlook on the web integration with Office Online Server when Exchange Server 2016 and Exchange Server 2013 coexist?

( ) Set-ClientAccessService

( ) Set-OrganizationConfig

( ) Set-MailboxServer

( ) Set-OutlookWebAppPolicy

( ) Set-WacDiscoveryEndpoint

Answer:

( ) Set-ClientAccessService

( ) Set-OrganizationConfig

(√) Set-MailboxServer

( ) Set-OutlookWebAppPolicy

( ) Set-WacDiscoveryEndpoint

Feedback: Both **Set-MailboxServer** and **Set-OrganizationConfig** have the **WacDiscoveryEndpoint** parameter. However, Exchange Server 2013 cannot use Office Online Server. For this reason, during coexistence, you should use **Set-MailboxServer** to configure only the Exchange 2016 servers to use Office Online Server.

Question: If you have three datacenters with Exchange Server, how many Office Online Server farms should you have?

Answer: You should have one Office Online Server farm for each datacenter with Exchange Server. Configure the Exchange servers in each datacenter to use the local Office Online Server farm.

Demonstration: Deploying and testing Office Online Server for Exchange 2016

Demonstration Steps

Configure a certificate on LON-EX1

1. On LON-EX1, click Start, type **mmc**, and press Enter.
2. In the Console1 window, click **File** and click **Add/Remove Snap-in**.
3. In the Add or Remove Snap-ins window, double-click **Certificates**.
4. In the Certificates snap-in window, click **Computer account** and click **Next**.
5. Click **Local computer** and click **Finish**.
6. In the Add or Remove Snap-ins window, click **OK**.
7. In the Console1 window, expand **Certificates (Local Computers)**, expand **Personal**, and click **Certificates**.
8. Right-click **Certificates**, point to **All Tasks**, and click **Request New Certificate**.
9. In the Certificate Enrollment Wizard, click Next.

10. On the **Select Certificate Enrollment Policy** page, click **Active Directory Enrollment Policy**, and click **Next**.
11. On the **Request Certificates** page, select the **Computer** check box, and click **Enroll**.
12. On the **Certificate Installation Results** page, click **Finish**.
13. In the Console1 window, right-click **LON-EX1.Adatum.com**, and click **Properties**.
14. In the LON-EX1.Adatum.com Properties window, in the **Friendly name** box, type **ExchangeCert**, and click **OK**.
15. Close the Console1 window, and do not save the console settings.
16. On the desktop, double-click **Exchange Administrative Center**.
17. Sign in as **Adatum\Administrator** with the password **Pa$$w0rd**.
18. In Exchange admin center, click **servers**, and click **certificates**.
19. Double-click **ExchangeCert**.
20. In the **ExchangeCert** window, on the **services** tab, select the **IIS** check box, and click **Save**.
21. Close Internet Explorer.

Request a certificate for Office Online Server

1. On LON-OOS, click **Start**, type **mmc**, and press Enter.
2. In the Console1 window, click **File**, and click **Add/Remove Snap-in**.
3. In the Add or Remove Snap-ins window, double-click **Certificates**.
4. In the Certificates snap-in window, click **Computer account**, and click **Next**.
5. Click **Local computer**, and click **Finish**.
6. In the Add or Remove Snap-ins window, click **OK**.
7. In the Console1 window, expand **Certificates (Local Computers)**, expand **Personal**, and click **Certificates**.
8. Right-click **Certificates**, point to **All Tasks**, and click **Request New Certificate**.
9. In the Certificate Enrollment Wizard, click **Next**.
10. On the **Select Certificate Enrollment Policy** page, click **Active Directory Enrollment Policy**, and click **Next**.
11. On the **Request Certificates** page, select the **Computer** check box, and click **Enroll**.
12. On the **Certificate Installation Results** page, click **Finish**.
13. In the Console1 window, right-click **LON-OOS.Adatum.com**, and click **Properties**.
14. In the LON-OOS.Adatum.com Properties window, in the **Friendly name** box, type **OOSCertificate**, and click **OK**.
15. Close the Console1 window, and do not save the console settings.

Install prerequisites

1. On LON-OOS, open Server Manager, click **Manage**, and click **Add Roles and Features**.
2. In the Add Roles and Features Wizard, click **Next**.
3. On the **Select installation type** page, click **Role-based or feature-based installation**, and click **Next**.

4. On the **Select destination server** page, click **LON-OOS.Adatum.com**, and click **Next**.
5. On the **Select server roles** page, expand **Web Server (IIS)**, expand **Web Server**, and expand **Application Development**.
6. Select the **Server Side Includes** check box, and click **Next**.
7. On the **Select features** page, click **Next**.
8. On the **Confirm installation selections** page, click **Install**.
9. When the installation is complete, click **Close**.

Install and configure Office Online Server

1. On LON-OOS, in the taskbar, click **File Explorer**.
2. In File Explorer, browse to **D:**, and double-click **setup.exe**.
3. In the Microsoft Office Online Server 2013 window, select the **I accept the terms of this agreement** check box, and click **Continue**.
4. On the **Choose a file location** page, click **Install Now** to accept the default location.
5. When installation is complete, click **Close**.
6. Close File Explorer.
7. On the taskbar, click **Windows PowerShell**.
8. At the Windows PowerShell prompt, type **New-OfficeWebAppsFarm -InternalURL https://LON-OOS.Adatum.com –ExternalURL https://LON-OOS.adatum.com –CertificateName OOSCertificate**, and press Enter.

Configure Exchange Server 2016 for Office Online Server

1. On LON-EX1, click Start, and click **Internet Explorer**.
2. In Internet Explorer, in the address bar, type **https://lon-oos.adatum.com/hosting/discovery**, and press Enter.
3. Close Internet Explorer.
4. On the taskbar, click **Exchange Management Shell**.
5. In EMS, type **Set-OrganizationConfig –WacDiscoveryEndpoint https://LON-OOS.adatum.com/hosting/discovery**, and press Enter.
6. Type **iisreset**, and press Enter.
7. Close EMS.

Verify Office Online Server functionality in Outlook on the web

1. On LON-CL1, sign in as **Adatum\Don** with the password **Pa$$w0rd**.
2. On the taskbar, click **File Explorer**.
3. In File Explorer, double-click **Documents**.
4. Right-click and empty area, point to **New**, and click **Microsoft Word Document**.
5. Type **TestFile**, and press Enter to rename the document.
6. Double-click **TestFile**.
7. In the First things first window, click **Ask me later**, and click **Accept**.
8. In the document, type **This is my document content**.

9. Close Word, and click **Save** to save the changes.
10. Close File Explorer.
11. On the taskbar, click **Microsoft Edge**.
12. In Microsoft Edge, type **https://lon-ex1.adatum.com/owa**, and press Enter.
13. Sign in as **Adatum\Don** with the password **Pa$$w0rd**.
14. Select the **(UTC-8:00) Pacific Time (US & Canada)** time zone, and click **Save.**
15. In Outlook on the web, click **New**.
16. In the new message, in the **To** field, type **Administrator**.
17. In the **Subject** field, type **Test document for viewing**.
18. Click **Attach**, click **TestFile**, and click **Open**.
19. Click **Send**, and close **Microsoft Edge**.
20. On the taskbar, click **Microsoft Edge**.
21. In Microsoft Edge, type **https://lon-ex1.adatum.com/owa**, and press Enter.
22. Sign in as **Adatum\Administrator** with the password **Pa$$w0rd**.
23. Select the **(UTC-8:00) Pacific Time (US & Canada)** time zone, and click **Save.**
24. In the **Inbox**, click the message from **Don Funk**.
25. In the viewing pane, click the down arrow on **TestFile.docx**, and click **View**.
26. Click **Edit and Reply**.
27. Click **Discard**, and click **Discard**.
28. Close Microsoft Edge.

Lesson 4

Planning and implementing coexistence of SharePoint 2016 with Exchange

Contents:

Question and Answers 12
Resources 12

Question and Answers

Question: Which functions are provided by integrating SharePoint and Exchange Server?

Answer: When you integrate Exchange Server and SharePoint, you can implement the following functions:

- Perform integrated search in eDiscovery Center.
- Create site mailboxes for projects.
- Use modern attachments.
- Display user photos from Exchange in SharePoint.

Question: By implementing modern attachments, you reduce average mailbox size.

( ) True

( ) False

Answer:

(√) True

( ) False

Feedback: When a message includes a traditional attachment, the mailbox increases by the size of the attachment, which is typically much larger than the other message content. A modern attachment is just a link to the document. Consequently, the mailbox size will be smaller.

Resources

What is SharePoint Online?

Additional Reading: For a detailed list of SharePoint Online features supported with various subscription plans, see "SharePoint Online Server Description": http://aka.ms/Wv10n1

Process to implement online modern attachments

Additional Reading: For detailed steps on how to configure OAuth authentication between Exchange Server 2016 and Office 365, see “Configure OAuth authentication between Exchange and Exchange Online organizations”: http://aka.ms/N8li2e

Lesson 5

Designing external client access

Contents:

Question and Answers 14
Resources 14
Demonstration: Configuring Web Application Proxy 14

Question and Answers

Question: What is TCP port 587 used for when implementing Exchange Server?

( ) Outlook on the web

( ) Exchange ActiveSync

( ) Outlook Anywhere

( ) MAPI over HTTP

( ) Mail delivery for POP3 clients

Answer:

( ) Outlook on the web

( ) Exchange ActiveSync

( ) Outlook Anywhere

( ) MAPI over HTTP

(√) Mail delivery for POP3 clients

Feedback: POP3 and IMAP4 clients use TCP port 587 to send SMTP messages.

Question: What risk is associated with enabling account lockout for accounts with Exchange mailboxes? How can this risk be reduced?

Answer: Many times, when users update their passwords in AD DS, they do not immediately update the password on all of their devices. As a result, the mobile device can attempt many connections by using the old password, and trigger an account lockout. To minimize this risk, raise the number of incorrect authentication attempts to a relatively high value, such as 50.

Resources

Planning reverse proxy configuration

Additional Reading: For more information about logging X-Forwarded-For headers in IIS 8.5, see “Enhanced Logging for IIS 8.5”: http://aka.ms/Iamusy

Additional Reading: For detailed information about planning WAP deployment, see "Plan to Publish Applications through Web Application Proxy": http://aka.ms/Qzuezg

Additional Reading: For more information about Exchange Server 2013 and claims-aware authentication, see "Using AD FS claims-based authentication with Outlook Web App and EAC": http://aka.ms/S1fhlb

Additional Reading: For more information about the value of reverse proxies and preauthentication, see "Life in a Post TMG World – Is It as Scary As You Think?": http://aka.ms/jfh7em

Demonstration: Configuring Web Application Proxy

Demonstration Steps

Install AD FS

1. On LON-DC1, in Server Manager, click **Manage**, and click **Add Roles and Features**.
2. In the Add Roles and Features Wizard, click **Next**.

3. On the **Select installation type** page, click **Role-based or feature-based installation**, and click **Next**.
4. On the Select destination server page, click **LON-DC1.Adatum.com**, and click **Next**.
5. On the Select server roles page, select the **Active Directory Federations Services** check box, and click **Next**.
6. On the **Select features** page, click **Next**.
7. On the **Active Directory Federation Services (AD FS)** page, click **Next**.
8. On the **Confirm installation selections** page, click **Install**.
9. When installation is complete, click **Close**.
10. In Server Manager, click **Notifications**, and click **Configure the federation service on this server**.
11. In the Active Directory Federation Services Configuration Wizard, on the **Welcome** page, click **Create the first federation server in a federation server farm**, and click **Next**.
12. On the **Connect to Active Directory Domain Services** page, click **Next** to use the Adatum\Administrator account.
13. On the **Specify Service Properties** page, in the **SSL Certificate** box, select the second **LON-DC1.adatum.com**.
14. In the **Federation Service Display Name** box, type **A. Datum Corporation**, and click **Next**.
15. On the **Specify Service Account** page, click **Use an existing domain user account or group Managed Service Account**, and then click **Select**.
16. In the Select User or Service Account window, type **Administrator**, and click **OK**.
17. In the **Account Password** box, type **Pa$$w0rd**, and click **Next**.
18. On the **Specify Configuration Database** page, click **Create a database on this server using Windows Internal Database**, and click **Next**.
19. On the **Review Options** page, click **Next**.
20. On the **Pre-requisite Checks** page, click **Configure**.
21. When configuration is complete, click **Close**.

 **Note:** You can ignore the error about a duplicate SPN. This is caused by using the server name as the federation service name. This will not occur in a production environment, where a separate federation service name will be configured.

Configure a certificate on the WAP server

1. On LON-SVR1, click **Start**, type **mmc**, and press Enter.
2. In the Console1 window, click **File**, and click **Add/Remove Snap-in**.
3. In the Add or Remove Snap-ins window, double-click **Certificates**.
4. In the Certificates snap-in window, click **Computer account**, and click **Next**.
5. Click **Local computer**, and click **Finish**.
6. In the Add or Remove Snap-ins window, click **OK**.
7. In the Console1 window, expand **Certificates (Local Computers)**, and click **Personal**.

8. Right-click **Personal**, point to **All Tasks**, and click **Request New Certificate**.
9. In the Certificate Enrollment Wizard, click **Next**.
10. On the **Select Certificate Enrollment Policy** page, click **Active Directory Enrollment Policy**, and click **Next**.
11. On the **Request Certificates** page, select the **Adatum Web** check box, and click **More information is required to enroll for this certificate. Click here to configure settings**.
12. In the Certificate Properties window, on the **Subject** tab, in the **Subject name** area, in the **Type** box, select **Full DN**.
13. In the Value box, type **cn=lon-dc1.adatum.com**, and click **Add**.
14. In the **Alternative name** area, in the **Type** box, select **DNS**.
15. In the **Value** box, type **mail.adatum.com**, and click **Add**.
16. Click **OK**.
17. On the **Request Certificates** page, click **Enroll**.
18. On the **Certificate Installation Results** page, click **Finish**.
19. In the Console1 window, click **Certificates**, right-click **LON-DC1.Adatum.com**, and click **Properties**.
20. In the LON-DC1.Adatum.com Properties window, in the **Friendly name** box, type **WAPCertificate**, and click **OK**.
21. Close the Console1 window and do not save the console settings.

Install WAP

1. On LON-SVR1, on the taskbar, click **Server Manager**.
2. In Server Manager, click **Manage**, and click **Add Roles and Features**.
3. In the Add Roles and Features Wizard, click **Next**.
4. On the **Select installation type** page, click **Role-based or feature-based installation**, and click **Next**.
5. On the Select destination server page, click **LON-SVR1.Adatum.com**, and click **Next**.
6. On the **Select server roles** page, select the **Remote Access** check box, and click **Next**.
7. On the Select features page, click **Next**.
8. On the **Remote Access** page, click **Next**.
9. On the **Select role services** page, select the **Web Application Proxy** check box, click **Add Features**, and click **Next**.
10. On the **Confirm installation selections** page, click **Install**.
11. When the installation is complete, click **Close**.
12. In Server Manager, click **Notifications**, and click **Open the Web Application Proxy Wizard**.
13. In the Web Application Proxy Wizard, click **Next**.
14. On the **Federation Server** page, in the **Federation service name** box, type **LON-DC1.adatum.com**.
15. In the User name box, type **Adatum\Administrator**.
16. In the **Password** box, type **Pa$$w0rd** and click **Next**.

17. On the AD FS Proxy Certificate page, in the **Select a certificate to be used by the AD FS proxy** box, select **lon-dc1.adatum.com** and click **Next**.
18. On the **Confirmation** page, click **Configure**.
19. On the **Results** page, click **Close**.
20. The Remote Access Management Console opens automatically.

Create an application for Outlook on the web

1. In the Remote Access Management Console, in **Tasks** pan, click **Publish**.
2. In the **Publish New Application Wizard**, click **Next**.
3. On the **Preauthentication** page, click **Pass-through**, and click **Next**.
4. On the **Publishing Settings** page, in the **Name** box, type **Outlook on the web**.
5. In the **External URL** box, type **https://mail.adatum.com/owa/**.
6. In the External certificate box, select **lon-dc1.adatum.com**.
7. In the **Backend server URL** box, type **https://lon-ex1.adatum.com/owa/**, and click **Next**.
8. On the **Confirmation** page, click **Publish**.
9. On the **Results** page, click **Close**.

Note: The URLs specified when publishing the application must end with a trailing slash (/).

Verify connectivity through WAP

1. On LON-DC1, in Server Manager, click **Tools**, and click **DNS**.
2. In DNS Manager, expand **Forward Lookup Zones**, and click **Adatum.com**.
3. Right-click **Adatum.com**, and click **New Host (A or AAAA)**.
4. In the New Host window, in the **Name** box, type **mail**.
5. In the **IP address** box, type **172.16.0.12**, and click **Add Host**.
6. Click **OK**, and click **Done**.
7. On LON-CL1, on the taskbar, click **Microsoft Edge**.
8. In Microsoft Edge, type **https://mail.adatum.com/owa**, and press Enter.
9. Sign in as **Adatum\Don** with a password of **Pa$$w0rd**.
10. Close Internet Explorer.

Module Review and Takeaways

Review Question(s)

Question: How would you investigate Outlook clients that display a warning about an untrusted certificate?

Answer: This warning could be caused by any web service that has an incorrectly configured internal or external URL that is not included in the certificate installed on Exchange servers. However, URLs are most commonly misconfigured for services that are not configurable in Exchange admin center. For this reason, the MAPI over HTTP and Autodiscover URLs should be verified. When the error is displayed, you can view the certificate and verify the names that are included in the certificate.

Question: How does implementing modern attachments avoid multiple copies of the same document?

Answer: When you use a modern attachment, you are sending others a link to a document stored centrally in SharePoint or One Drive for Business. Then, as each user edits the document, changes are made on the original document, where the changes are available to everyone.

Lab Review Questions and Answers

Lab: Planning and deploying client access solutions

Question and Answers

Question: Why do you create a separate DNS record for an Office Online Server farm that is different from the server name?

Answer: If you implement only one Office Online Server, you can use the name of the server for the Office Online Server farm. However, this is not a best practice because this limits you to a single server in the farm. If you ever want multiple servers in the Office Online Server farm, you need a separate name that is load balanced across the members of the farm.

Question: Which internal and external URLs can you configure only in the Exchange Management Shell and not in the Exchange admin center?

Answer: URLs for the following services cannot be configured in Exchange admin center:

- MAPI over HTTP. The virtual directory for MAPI over HTTP is not listed in the virtual directories in Exchange admin center. Use the cmdlet **Set-MapiVirtualDirectory**.
- Autodiscover. The internal URL for Autodiscover is configured for each server with the cmdlet **Set-ClientAccessService.**

Module 5

Designing and implementing high availability

Contents:

Lesson 1: Planning high availability for Exchange Server 2016 2

Lesson 2: Planning for load balancing 4

Lesson 3: Planning for site resilience 6

Module Review and Takeaways 8

Lab Review Questions and Answers 9

Lesson 1

Planning high availability for Exchange Server 2016

Contents:

Question and Answers 3

Question and Answers

Question: Which infrastructure is highly available in your organization?

Answer: Answers might vary and might include:

- Datacenter infrastructure
- Server hardware
- Storage
- Network infrastructure
- Internet connectivity
- Network services

Question: What are the Exchange Server 2016 components that you need to configure for high availability?

Answer: The Exchange Server 2016 components that you need to configure for high availability include:

- Mailbox databases
- Client Access services
- Transport services

Question: What are the scenarios in which you should use lagged database copies?

Answer: Scenarios will include:

- Organizations that have more than three copies of each database.
- Organizations that deploy Exchange native data protection and that do not perform backup.

Question: What is the benefit of configuring AutoReseed in Exchange Server 2016?

Answer: The AutoReseed feature automatically reseeds a database copy by using spare disks that an administrator previously provisioned.

Lesson 2

Planning for load balancing

Contents:

Question and Answers 5

Question and Answers

Question: What options do organizations have to provide high availability for Client Access services?

Answer: Organizations have the following options to provide high availability:

- DNS round robin
- Layer 4 NLB with a single namespace
- Layer 7 NLB with a single namespace
- Layer 4 NLB with multiple namespaces

Lesson 3

Planning for site resilience

Contents:

Question and Answers 7

Question and Answers

Question: Does your organization plan for site resilience as part of its disaster recovery planning?

Answer: Answers might vary. Each student might describe his or her organization's plan for site resilience.

Module Review and Takeaways

Best Practices

- Carefully plan a site resilience design by testing and validating the final design.
- Never rely solely on the high availability features in Windows Server or Exchange Server. You must be familiar with the proper way to manage the software, and you must properly maintain the environment by installing updates and performing maintenance.

Review Question(s)

Question: You are planning a two-site, active/active site resilience deployment. How can you determine how many database copies you need?

Answer: Answer the following questions to determine the number of copies that you need:

- Do you want to activate the copy in the secondary site when you maintain DAG members in the primary site?
- Do you need redundancy in the secondary site for maintenance or to help provide protection during a primary site failure?
- Will you be using Exchange native protection?
- Will you be using just a bunch of disks (JBOD) storage?

Tools

The Exchange Server Role Requirements Calculator helps you identify storage and network requirements for a multisite DAG deployment.

 **Additional Reading:** To download the Exchange Server Role Requirements Calculator, go to: http://aka.ms/Mw4ove

Lab Review Questions and Answers

Lab: Designing and implementing site resiliency

Question and Answers

Question: Why does Outlook no longer connect to the mailbox after LON-EX1 and LON-EX1 shut down?

Answer: The cluster no longer has a quorum, which causes the mailbox databases to dismount. You need to recover the DAG to mount the databases before they can be accessed again.

Question: In the lab, how is failover for Outlook Anywhere provided?

Answer: Round robin DNS provides Outlook Anywhere with the IP addresses for both Mailbox servers. When one Mailbox server goes offline, Outlook can fail over to the other IP address and reconnect.

Module 6

Maintaining Exchange Server 2016

Contents:

Lesson 1: Using Managed Availability to improve high availability 2

Lesson 2: Implementing DSC 5

Module Review and Takeaways 8

Lab Review Questions and Answers 9

Lesson 1

Using Managed Availability to improve high availability

Contents:

Question and Answers 3
Demonstration: Viewing Managed Availability configuration in Event Log 4

Question and Answers

Question: Which of the following MonitorDefinition properties does a monitor evaluate to determine if a threshold has been exceeded?

( ) MonitoringThreshold

( ) RecurrenceIntervalSeconds

( ) MonitoringIntervalSeconds

( ) SecondaryMonitoringThreshold

( ) SampleMask

Answer:

(√) MonitoringThreshold

( ) RecurrenceIntervalSeconds

(√) MonitoringIntervalSeconds

(√) SecondaryMonitoringThreshold

(√) SampleMask

Feedback: All options are correct except for RecurrenceIntervalSeconds. RecurrenceIntervalSeconds only specifies how often a monitor runs, and you cannot use it to determine if a threshold has been exceeded.

A monitor uses SampleMask to determine the probe results that need to be evaluated.

MonitoringThreshold is the number of probe failures or aggregate percentage of probe failures that must be exceeded for a monitor to be unhealthy. In performance-based monitors, this is the number of performance counters that must be exceeded.

MonitoringIntervalSeconds is the duration over which probe results are evaluated.

SecondaryMonitoringThreshold is used with performance-based monitors to determine the number of performance counter results that must be exceeded.

Question: In which of the following locations does Managed Availability store data?

( ) Windows Registry

( ) AD DS

( ) Local XML configuration files

( ) Health Mailboxes

( ) Windows Event Log

Answer:

(√) Windows Registry

(√) AD DS

(√) Local XML configuration files

(√) Health Mailboxes

(√) Windows Event Log

Feedback: All of the options are correct. Managed Availability stores local overrides in the Windows registry and global overrides in AD DS. It also stores configuration settings for probe

and monitor items within XML files in the C:\Program Files\Microsoft\Exchange Server\v15\bin\Monitoring\config folder. The results of probe activity are stored in the Health Mailboxes created for each database. Finally, Managed Availability stores the definitions and results of all probes, monitors, and responders in the Windows Event log, along with recovery action data and escalations requiring manual intervention.

Demonstration: Viewing Managed Availability configuration in Event Log

Demonstration Steps

1. On LON-EX1, click **Start**, and then click **Administrative Tools**.
2. In the Administrative Tools window, double-click **Event Viewer**.
3. In Event Viewer, navigate to **Applications and Services Logs\Microsoft\Exchange\ActiveMonitoring**. Select the **ProbeDefinition** crimson channel.
4. In the Action pane, click **Find**. In the **Find What:** field, type **EWSCtpProbe.**
5. Click **Find Next**. After the event log entry has been found, click **Cancel** to close the **Find** dialog box.
6. On the **General** tab, verify that you have selected the probe definition for **Identity=EWS/EWSCtpProbe/LON-EX1.Adatum.com**.
7. Click the **Details** tab, and ensure **Friendly View** is selected. Expand **UserData, EventXML**. Scroll through the attributes, and take note of the different names and values.
8. Close **Event Viewer**.
9. Open **Exchange Management Shell**.
10. Type the following command, and then press Enter:

```
(Get-WinEvent -LogName Microsoft-Exchange-ActiveMonitoring/ProbeDefinition | %
{[XML]$_.toXml()}).event.userData.eventXml | ? {$_.Name -like "EWSCtpProbe"} | fl
```

11. Note how the names and values returned are the same values seen in Step 7.
12. Close **Exchange Management Shell**.

Lesson 2

Implementing DSC

Contents:

Question and Answers 6

Question and Answers

Question: Which of the following statements can be attributed to the declarative approach used by Windows PowerShell DSC, as opposed to imperative approach used by Exchange Management Shell scripts?

( ) Defines how a task should be performed.

( ) Defines what should be configured.

( ) Uses built-in logic to detect and correct configuration drift.

( ) Requires custom logic to detect and correct configuration drift.

( ) Syntax is typically easier to understand.

Answer:

( ) Defines how a task should be performed.

(√) Defines what should be configured.

(√) Uses built-in logic to detect and correct configuration drift.

( ) Requires custom logic to detect and correct configuration drift.

(√) Syntax is typically easier to understand.

Feedback:

Correct answers:

Declarative approaches define what should be configured.

Declarative approaches use built-in logic to detect and correct configuration drift.

Declarative approaches use syntax that is typically easier to understand.

Incorrect answers:

Imperative approaches define how a task should be performed.

Imperative approaches require custom logic to detect and correct configuration drift.

Question: Which of the following components do you require to author and deploy DSC configurations for Exchange Server 2016?

( ) The PowerShellGet module

( ) Windows PowerShell version 4.0 or higher

( ) The xExchange module

( ) Windows Remote Management (WinRM) listener enabled on target system

( ) The LCM agent on target system configured for pull mode

Answer:

( ) The PowerShellGet module

(√) Windows PowerShell version 4.0 or higher

(√) The xExchange module

(√) Windows Remote Management (WinRM) listener enabled on target system

( ) The LCM agent on target system configured for pull mode

Feedback:

Correct answers:

Windows PowerShell version 4.0 or newer is required to author and deploy DSC configurations.

The xExchange module from the PowerShell Gallery contains all the required DSC resources for configuring Exchange Server 2016.

A WinRM listener must be enabled on the target system to receive and process configurations.

Incorrect answers:

The PowerShellGet module can be used to download modules from the PowerShell Gallery, but it is not required directly to author and deploy configurations. This is because the xExchange module can be copied manually to the Modules directory on a target system or deployed from a pull server.

The LCM agent can be configured in pull mode if you have configured a pull server, but it is not required because you can still push configurations to a target node.

Module Review and Takeaways

Best Practices

- Ensure that you understand the configuration of the different Managed Availability Health Sets and components, but avoid creating overrides unless you are certain it is necessary or you have been advised to do so by a Microsoft support professional.
- While Managed Availability configuration can be viewed through the Event Viewer, you will find that it is more efficient to use the **Get-WinEvent** cmdlet in Windows PowerShell.
- DSC is declarative, which means that it defines what should be done. Exchange Management Shell scripts are imperative, which means that they define how something should be done.
- DSC configurations do not run directly in Windows PowerShell. Windows PowerShell is the mechanism by which you compile DSC configurations into .mof files that are either pushed to or pulled by the Local Configuration Manager (LCM) agent on a target system.
- DSC configurations using Exchange Server 2016 resources typically will require passing a credential with Organization Management rights. To prevent these credentials from being stored in clear text in the compiled .mof file, you must take necessary steps to ensure that the credentials are encrypted.

Tools

Tool name	Description
Event Viewer (eventvwr.msc)	Use this MMC snap-in to view logged events in the Microsoft-Exchange-ActiveMonitoring and Microsoft-Exchange-ManagedAvailability crimson channel logs.
Windows PowerShell ISE	Use Windows PowerShell IDE to author Windows PowerShell scripts, including configurations for DSC.
PowerShellGet	Windows PowerShell module that allows you to download and install Windows PowerShell modules from the PowerShell Gallery by using the **Find-Module** and **Install-Module** cmdlets.
xExchange	Windows PowerShell module that contains all of the DSC resources that you need to author configurations for Exchange Server 2016.

Common Issues and Troubleshooting Tips

Common Issue	Troubleshooting Tip
One or more Managed Availability components are unhealthy.	Use the **Get-HealthReport** and **Get-ServerHealth** cmdlets to find the specific component(s) contributing to the unhealthy state. Look through the RecoveryActions crimson channel to determine if any recovery actions have been executed. Work your way backward by finding the associated responder, monitors, and probes. Then, find failed probe results to help determine the root cause.

Lab Review Questions and Answers

Lab: Maintaining Exchange Server 2016

Question and Answers

Question: In the Managed Availability lab exercise, why did it take approximately four minutes for the responder to restart the AppPool that you stopped manually, even though you configured the MonitoringIntervalSeconds of the monitor to 120 (two minutes)?

Answer: In this scenario, the associated probe only runs every 60 seconds. So it could take up to 60 seconds before a failed probe result is even logged. The monitor only polls for probe results every 120 seconds (two minutes). So depending on the timing, an additional two minutes could elapse before the monitor detects the failed probe. The monitor is not configured to invoke the responder until 60 seconds after the state change to Degraded1 (TargetHealthState=5), which is defined by the StateTransitionsXml property of the monitor and the TargetHealthState property of the ActiveSyncProxyTestRecycleAppPool responder.

Question: Besides managing virtual directory settings in your Exchange Server 2016 organization, what other settings might you manage using DSC?

Answer: In addition to managing virtual directory configuration settings, you can also use the xExchange module for DSC to manage certificates, databases, database mount points, DAGs, transport services, receive connectors, and mailbox servers. DSC also can be utilized to test JetStress and to install Exchange Server 2016.

Module 7

Designing messaging security

Contents:

Lesson 1: Planning messaging security 2

Lesson 2: Designing and implementing AD RMS and Azure RMS integration 4

Module Review and Takeaways 6

Lab Review Questions and Answers 7

Lesson 1

Planning messaging security

Contents:

Question and Answers 3

Question and Answers

Question: What are some reasons that S/MIME is not widely deployed to most organizations?

> **Answer:** S/MIME is complex for users. There are several steps to take before users can communicate back and forth by using S/MIME. Also, administrative overhead is high for IT administrators.

Question: What are the advantages to having an SMTP gateway solution in your perimeter network instead of in your LAN?

> **Answer:** An SMTP gateway solution handles all inbound email and is often also responsible for scanning incoming and outgoing email for malicious content and spam. An SMTP gateway solution in the perimeter network can reject malicious content and spam before it gets to your LAN or Exchange servers on the LAN. This can reduce network congestion, increase security, and reduce the amount of resources the Exchange servers on the LAN require.

Lesson 2

Designing and implementing AD RMS and Azure RMS integration

Contents:

Question and Answers 5
Resources 5

Question and Answers

Question: How does Azure RMS reduce administrative overhead for IT departments compared to AD RMS?

Answer: With Azure RMS, the IT department does not have to manage AD RMS servers and any related components, such as reverse proxy servers and AD FS servers that are deployed to support AD RMS.

Question: Why is digital rights management, by itself, not a failsafe way to protect data?

Answer: While digital rights management can protect data and minimize data misuse, users can opt to bypass the protection in a variety of ways. For example, a user can use her smartphone to take a picture of her monitor while the protected data is displayed. Then, the user can send the picture to anybody. Or, a user can give his password to an unauthorized user to allow the unauthorized user to read protected content. As you implement digital rights management, it is important to know the limitations so that you can use digital rights management as one layer of your data protection solution.

Discussion: Which message encryption options would you use?

Question: Which message encryption options would you use? Why?

Answer: Answers will vary, but may include:

- For general message encryption, the use of Azure RMS is preferable, because it works seamlessly with users outside an organization. It is also beneficial not to have to manage additional servers in the data center.
- For some use cases, the use of S/MIME is beneficial. For example, in the United States, the Internal Revenue Service only supports secure communication by using S/MIME.

Question: If you were to implement RMS, would you use AD RMS or Azure RMS? Why?

Answer: Answers will vary, but may include:

- Some organizations only plan to secure communications internally and do not send sensitive information outside the organization. Such organizations would prefer the use of AD RMS. There is also the added benefit of having full control over the organization's infrastructure technologies.

Resources

Planning to use Azure RMS for an on-premises environment

 **Additional Reading:** For more information, refer to Rights Management sharing application user guide: http://aka.ms/H13jp9

How to configure Azure RMS for on-premises

 **Additional Reading:** For more information, refer to Microsoft Rights Management: http://aka.ms/Wk0zak

Module Review and Takeaways

Review Question(s)

Question: What are the ramifications of not configuring transport decryption when you integrate AD RMS and Exchange Server?

Answer: If you do not configure transport decryption when you integrate AD RMS and Exchange Server, some Exchange functionality will not work. For example, transport rules will not be able to decrypt a message to see if an action needs to be taken. Journaling rules will not be able to decrypt a message to see if journaling is required.

Lab Review Questions and Answers

Lab: Designing message security

Question and Answers

Question: Why is it important to choose a unique word or text to use in a message transport rule?

Answer: You should use a unique word, phrase, or text when creating a message transport rule. If you do not do so, you may inadvertently apply a transport rule to an email message that should not have the rule. For example, if you protect every email message with the word *secure* in the message body, you might protect more email messages than you intend to. It is a good practice to use a phrase such as "***Secure***" instead, because it is very unlikely to be used inadvertently.

Question: What are some of the user considerations that you must consider when implementing message transport rules?

Answer: You need to consider training users about the message transport rules so that they can take specific steps to use them when they need to, and so they know what rules they may encounter in the day-to-day communication. You can reduce calls to the IT department, reduce recipient confusion, and provide a better user experience by providing your users with an overview of your message transport rules before you implement them.

Module 8

Designing and implementing message retention

Contents:

Lesson 2: Designing In-Place Archiving 2

Lesson 3: Designing and implementing message retention 4

Module Review and Takeaways 6

Lab Review Questions and Answers 7

Lesson 2

Designing In-Place Archiving

Contents:

Question and Answers 3
Demonstration: Managing In-Place Archiving 3

Question and Answers

Question: What current mailbox archiving technologies are in use in your organization, and how do they compare with In-Place Archiving?

Answer: Answers will vary.

Demonstration: Managing In-Place Archiving

Demonstration Steps

1. Sign in to LON-EX1 with the user name **Adatum\Administrator** and the password **Pa$$w0rd**.
2. On LON-EX1, on the desktop, double-click the Exchange Administrative Center icon.
3. Sign in as **Adatum\Administrator** with the password **Pa$$w0rd**.
4. In the left navigation pane, select **recipients**.
5. In the tabs pane, select **mailboxes**.
6. On the toolbar, click **More**. Select **Add / Remove columns**.
7. Scroll down through the list, and then select **Archive Database** and **Department**. Click **OK**.
8. Set **Items per page** to **500**.
9. Click **Department** to sort the users.
10. In the list view, select all the users in the **IT** department.
11. In the Bulk Edit pane, scroll down, click **More options**, and then click **Archive – Enable**.
12. In the Bulk Enable Archive window, click **browse**, and then select the mailbox database **Research** as the destination for the archive mailboxes. Click **OK**, click **Save**, and then click **Close**.
13. On the toolbar, click **Refresh**.
14. In the list view, verify that each user of the information technology (IT) department now has an archive mailbox enabled.
15. Sign out the administrator from the Exchange Administration Center.
16. In Internet Explorer, type **https://LON-EX1.adatum.com/owa**, and then press Enter.
17. Type the user name **Adatum\Michael** and the password **Pa$$w0rd** to sign in to Michael's mailbox with Microsoft Outlook on the web. When prompted, select Pacific Time, and then click **Save**.
18. In the navigation pane, check that **In-Place Archive – Michael Allen** is visible. Expand the folder structure.
19. Sign out the user Michael from Outlook on the web, and then close Internet Explorer.

Lesson 3

Designing and implementing message retention

Contents:

Question and Answers 5
Demonstration: Using MRM in Outlook on the web 5

Question and Answers

Question: Do you currently use MRM in your own environments?

Answer: Answers will vary.

Demonstration: Using MRM in Outlook on the web

Demonstration Steps

1. Sign in to LON-EX1 as **adatum\Administrator** with the password **Pa$$w0rd**.
2. To create a new default policy tag, from the Start screen, open the Exchange Management Shell, type the following cmdlet, and then press Enter.

```
New-RetentionPolicyTag DefaultTag –Type:All –MessageClass AllMailboxContent –
RetentionEnabled $True –AgeLimitForRetention 365 –RetentionAction
PermanentlyDelete
```

3. To create a new retention policy tag for the Inbox folder, type the following cmdlet, and then press Enter.

```
New-RetentionPolicyTag InboxTag –Type:Inbox –MessageClass:* –
AgeLimitForRetention:30 –RetentionEnabled:$True –
RetentionAction:MovetoDeletedItems
```

4. To create a new personal tag that moves messages to the user's archive mailbox, type the following cmdlet, and then press Enter.

```
New-RetentionPolicyTag BusinessCritical –Type:Personal –MessageClass:* –
AgeLimitForRetention:1095 –RetentionEnabled:$True –RetentionAction:MoveToArchive
```

5. To create a new retention policy and to link it with the retention tags you just created, type the following cmdlet, and then press Enter.

```
New-RetentionPolicy AllTagsPolicy –
RetentionPolicyTagLinks:DefaultTag,InboxTag,BusinessCritical
```

6. To assign the retention policy to user Kim, type the following cmdlet, and then press Enter.

```
Set-Mailbox Kim –RetentionPolicy AllTagsPolicy
```

7. To immediately start the Managed Folder Assistant to force showing the new tags, type the following cmdlet, and then press Enter.

```
Start-ManagedFolderAssistant –id Kim
```

8. Open Internet Explorer. In the address bar, type **https://LON-EX1.adatum.com/owa**, and then sign in as user **adatum\Kim** with the password **Pa$$w0rd**. Select Pacific Time and then click **Save** when prompted.
9. Send a message to Kim, right-click the message, and then check that the retention policy is applied to the user's mailbox by verifying that the **assign policy** option is available.
10. If the **assign policy** option is not available, close Internet Explorer. Open it again, connect to **https://LON-EX1.adatum.com/owa**, and then sign in as user **adatum\Kim** with the password **Pa$$w0rd**. Right-click the message, and then check that the retention policy is applied to the user's mailbox by verifying that the **assign policy** option is available.

Module Review and Takeaways

Review Question(s)

Question: What happens when a user's mailbox is enabled for In-Place Archiving?

Answer: When a user's mailbox is enabled for In-Place Archiving, the Default MRM Policy is applied to the user's mailbox and an archive mailbox is created.

Question: What happens if the quota for a user's In-Place Archive mailbox is reached?

Answer: Quota information is written to the application event log, and if the available archive mailbox space is reached, a message is sent to the user's mailbox.

Lab Review Questions and Answers

Lab: Designing and implementing message retention

Question and Answers

Question: Which retention tags can users use to stamp items in their mailboxes themselves?

Answer: Users can use personal tags to stamp objects themselves.

Question: Where can you store the In-Place Archive mailbox, if you enable this feature on a user's mailbox?

Answer: You can store the In-Place Archive mailbox on any Mailbox server in the user's AD DS site. You can also store the In-Place Archive mailbox as a cloud-based archive.

Module 9

Designing messaging compliance

Contents:

Lesson 1: Designing and implementing data loss prevention 2

Lesson 2: Designing and Implementing In-Place Hold 6

Lesson 3: Designing and implementing In-Place eDiscovery 9

Module Review and Takeaways 12

Lab Review Questions and Answers 13

Lesson 1

Designing and implementing data loss prevention

Contents:

Question and Answers 3
Demonstration: Creating a data loss prevention policy from a template 3
Demonstration: Configuring Document Fingerprinting 4

Question and Answers

Question: To apply DLP policies you need to have:

( ) Enterprise CAL

( ) Standard CAL

( ) Azure Premium license

( ) RMS license

( ) Windows Server CAL

Answer:

(√) Enterprise CAL

( ) Standard CAL

( ) Azure Premium license

( ) RMS license

( ) Windows Server CAL

Overview of data loss prevention

Question: What type of business does your organization conduct?

Answer: Answers may vary.

Question: Does your organization have any technology for DLP in place? Does your organization have defined requirements for DLP?

Answer: Answers may vary. Some students may say that they already have DLP policies in their Exchange Server 2013 environment.

Demonstration: Creating a data loss prevention policy from a template

Demonstration Steps

1. On LON-EX1, open the Internet Explorer browser, and then to open the Exchange admin center type **https://LON-EX1.adatum.com/ecp**.
2. Sign in as **adatum\administrator** with the password **Pa$$w0rd**. On the page with language and time zone settings, select **(UTC-08:00) Pacific Time (US & Canada)** from the Time zone drop down list and click **Save**.
3. In the Exchange admin center, in the feature pane, click **compliance management**.
4. Click the **data loss prevention** tab.
5. Click **New** (+), and then click **New DLP policy from template**.
6. In the DLP Policy from Template window, in **Name**, type **Prevent financial information**.
7. In **Choose a template**, scroll down, and then select **U.S. Financial Data**.
8. Click **Save**.
9. In the Exchange admin center, click **Prevent financial information**, and then click **Edit**.
10. In the edit DLP policy window, on the **general** tab, click **Test DLP Policy with Policy Tips**.
11. Click **Save**.

12. In the Exchange admin center, click **Customize Policy Tips (fourth icon from the left on the toolbar)**.
13. In the **Policy Tips** window, click **New**.
14. In the New Policy Tip setting window, under **Policy Tip**, click **Notify the sender**.
15. In **Locale**, click **English**.
16. In **Text**, type: **This message contains information that you are not allowed to send**.
17. Click **Save**, and then click **Close**.
18. In the Exchange admin center, in the **feature** pane, click **mail flow**.
19. Click the **rules** tab.
20. Notice that several transport rules are created as a result of creating the DLP policy.
21. Leave the Exchange admin center open.

Demonstration: Configuring Document Fingerprinting

Demonstration Steps

1. On LON-EX1, in the Exchange admin center, in the feature pane, click **compliance management**.
2. Click the **data loss prevention** tab.
3. Click the **Manage document fingerprints** link.
4. In the document fingerprints window click **New**.
5. In the new document fingerprint window, in the **Name** textbox, type **Employee form**, in the **Description** field, type **test**, and then, in **Document list** section, click **Add**.
6. In the Choose File to Upload window, browse to **C:\LabFiles\Mod09**, click **Adatum-EmployeeForm.docx**, and then click **Open**.
7. In the new document fingerprint window, click **Save**.
8. In the document fingerprints window, click **Close**.
9. In the Exchange admin center, on the data loss prevention tab, click **New** (+).
10. Click **New custom DLP Policy**.
11. In the new custom DLP policy window, in the **Name** box, type **Employee form block**.
12. Click **Enforce**, and then click **Save**.
13. Click **Employee form block**, and then click **Edit**.
14. In the Employee form block window, click **rules**.
15. Click **New** (+), and then click **Block messages with sensitive information**.
16. In the new rule window, click **Outside the organization**. In the select recipient location window, click **Inside the organization**, and then click **OK**.
17. Click **Select sensitive information types**.
18. In the Sensitive information types window, click **Add**.
19. Scroll down the list and select **Employee form**, click **add**, and then click **OK** twice.
20. In **Do the following**, click **Generate incident report and send it to**, and then click the first **Select one** link. In the Select Members list, select **Administrator**, and then click **OK**.

21. Click the **Custom content** link, ensure that **original mail is selected**, and then click **OK**.
22. Click the **Block the message** link.
23. In **notify the sender with a Policy Tip**, in the **Enter the message for the NDR that users will receive** text box, type **Your message is blocked**, and then click **OK**.
24. Select the **Activate this rule on the following date** check box, and then in the drop-down box click **today.**
25. Under Choose a mode for this rule, select **Enforce**, and then click **Save**. If warning window appears, click **OK**.
26. In Employee form block window, click **Save**.
27. Leave Exchange admin center opened on LON-EX1.
28. Switch to LON-CL1 and sign in as **Adatum\Aidan** with the password **Pa$$w0rd**.
29. Open File Explorer and navigate to \\LON-EX1\C$**. When prompted for credentials, type Administrator for User name and Pa$$w0rd for password, and click OK.**
30. **Open LabFiles folder and then open Mod09 folder.**
31. Copy the file **Adatum-EmployeeForm.docx** to the desktop of LON-CL1 computer.
32. On the LON-CL1 desktop, double-click the file **Adatum-EmployeeForm.docx**. If the Microsoft Office Activation Wizard appears click **Close**. If the First thing first window appears, select **Ask me later** and click **Accept**.
33. When the file opens in Word 2016, type some data in to the form. You can choose to fill in any field in the document. Save the document on the Desktop, with the name **Adatum1.docx**.
34. Open Microsoft Edge browser and navigate to **https://lon-ex1.adatum.com/owa**. Sign in as **Adatum\Aidan** with the password **Pa$$w0rd**. On the page with language and time zone settings, select **(UTC-08:00) Pacific Time (US & Canada)** from the Time zone drop down list and click **Save**.
35. In the Mail window, click **New**.
36. In the **To:** field type **Allie**, click **Search Directory**, and then click **Allie Bellew**.
37. In the **Subject:** field type **my document**.
38. In the message body, type any text, and then click **Attach**.
39. In the Choose File to Upload window navigate to **Desktop**, click **Adatum1.docx**, and then click **Open**.
40. Ensure that Policy tip is displayed at the top of your message. Click **Show details**, and then click **Learn more**.
41. Ensure that **Employee form** is detected as sensitive information type.
42. Close Microsoft Edge window, and then sign out from LON-CL1.

Lesson 2

Designing and Implementing In-Place Hold

Contents:

Question and Answers 7
Demonstration: Configuring In-Place Hold 7

Question and Answers

Question: What should you do to delegate permission to use the In-Place Hold feature?

Answer: You need to put the delegated user account to Discovery Management security group.

Demonstration: Configuring In-Place Hold

Demonstration Steps

1. On LON-DC1, open the Server Manager console, click **Tools**, and then click **Active Directory Users and Computers**.
2. In the Active Directory Users and Computers console, expand **Adatum.com**, and then click **Microsoft Exchange Security Groups**.
3. In the **details** pane on the right, double-click **Discovery Management**.
4. In the Discovery Management Properties window, click the **Members** tab.
5. Click **Add**.
6. In the Select Users, Contacts, Computers, Service Accounts, or Groups window, type **April**, and then click **OK** twice.
7. On LON-DC1, open Internet Explorer, and then go to **https://LON-EX1.adatum.com/ecp**.
8. Sign in as **Adatum\April** with the password **Pa$$w0rd**. On the page with language and time zone settings, select **(UTC-08:00) Pacific Time (US & Canada)** from the Time zone drop down list and click **Save**.
9. Verify that the **compliance management** option is available in the feature pane.
10. Click **compliance management**.
11. Click **New**.
12. In the new in-place eDiscovery & hold window, in the **Name** box, type **hold for Amr Zaki**, and then click **Next**.
13. On the **Mailboxes** page, make sure that **Specify mailboxes to search** is selected, and then click **Add**.
14. In the **Select Mailbox** window, select **Amr Zaki**, click **add**, and then click **OK**.
15. Click **Next**.
16. On the Search query page, click **Filter based on criteria**.
17. In **From**, click **add users**.
18. In the Select Mailbox window, select **Administrator**, click **add**, and then click **OK**.
19. Click **select message types**. In the message types to search window, click **Select the message types to search**, and then click **Email**. Click **OK**, and then click **Next**.
20. On the In-Place Hold settings page, click **Place content matching the search query in selected mailboxes on hold**.
21. Click **Specify number of days to hold items relative to their received date**, and then type **365**.
22. Click **Finish**.
23. Click **Close**. Leave the Exchange Admin Center open.
24. Switch to LON-EX1. From task bar, click Exchange Management Shell.

25. Type **Get-Mailbox –Identity Amr | FL**, and then press Enter.
26. When the mailbox details appear, verify that the **LitigationHoldEnabled** parameter is set to False and that the **InPlaceHolds** parameter has a value.
27. Type **Get-MailboxSearch**, and then press Enter.
28. Ensure that **hold for Amr Zaki** is listed and that the value of the **InPlaceHoldEnabled** parameter is **True**.
29. Close the Exchange Management Shell.

Lesson 3

Designing and implementing In-Place eDiscovery

Contents:

Question and Answers 10
Demonstration: Configuring In-Place eDiscovery 10

Question and Answers

Question: Which technology does eDiscovery use to perform a fast search on mailboxes?

Answer: eDiscovery uses the content indexes that the Exchange Search service creates.

Demonstration: Configuring In-Place eDiscovery

Demonstration Steps

1. On LON-CL1, sign in as **Adatum\Allie** with the password of **Pa$$w0rd**.
2. Click the **Start** icon, click **All apps**, and then click **Outlook 2016**.
3. To configure Allie's Outlook profile, click **Next** three times, and then click **Finish**. If Microsoft Office Activation Wizard window appears, click **Close**. In the **First things first** window, click **Ask me later**, and then click **Accept**.
4. Click **New Email**.
5. In the new email window, in the **To** box, type **Aidan**.
6. In the **Subject** box, type **just for you**.
7. In the message body box, type **This is my password : Pa$$w0rd**.
8. Click **Send**.
9. Switch to the LON-EX1 computer and restore the Exchange admin center.
10. In the Exchange admin center, on the **feature** pane, click **permissions**.
11. Click the **admin roles** tab.
12. Double-click **Discovery Management**.
13. In the Role Group window, ensure that April Reagan is in the Members list.
14. Restore the Exchange admin center on LON-DC1, where you signed in as Adatum\April.
15. In the Exchange admin center, on the feature pane, click **compliance management**.
16. On the toolbar, click **New**.
17. In the new in-place eDiscovery & hold window, in the **Name** box, type **password search**, and then click **Next**.
18. Click **Search all mailboxes**, and then click **Next**.
19. Click **Filter based on criteria**, and then, in **Keywords**, type **password**.
20. Click **select message types**.
21. In the message types to search window, click **Select the message types to search**, and then click **Email**.
22. Click **OK**, and then click **Next**.
23. On the In-Place Hold settings page, click **Finish**.
24. Click **Close**.
25. In the Exchange admin center, on the toolbar, click **Refresh**.
26. Look at the details pane on the right and ensure that the status is **Estimate Succeeded**. If it is not, wait one or two minutes, and then click **Refresh** again.
27. Click **password search**. Click **Preview search results** in password search pane.

28. Ensure that you can see email messages between Allie and Aidan that contain words you were searching for.

Module Review and Takeaways

Best Practices

- Always define business and legal requirements before implementing DLP strategies.
- Review the rules that a DLP policy template contains before you apply a DLP policy template.
- Always test DLP policies with Policy Tips before you enforce them.
- Avoid applying an In-Place Hold on all mailbox items.

Review Question(s)

Question: What is data loss prevention?

Answer: Data loss prevention is a set of technologies that work together to help minimize the possibility of losing business critical data by sending it in an email, or some other way, either purposefully or inadvertently.

Question: What is the main purpose of In-Place Hold?

Answer: The main purpose of In-Place Hold is to preserve data from one or more mailboxes, while preventing users from changing or deleting data that relates to a specific issue.

Question: How do you give someone permission to perform an eDiscovery search?

Answer: To give someone permission to perform an eDiscovery search, add that person to the Discovery Management role group.

Common Issues and Troubleshooting Tips

Common Issue	Troubleshooting Tip
DLP policy does not block email messages that contain sensitive information	• Check the rules in the policy. • Check whether the policy is enforced. • Check whether the policy contains the correct definition of sensitive information.
No compliance management in the feature pane	• The user is not a member of the Discovery Management role.

Lab Review Questions and Answers

Lab: Designing and implementing messaging compliance

Question and Answers

Question: When should you use custom DLP policies instead of policies based on templates?

Answer: You should create custom DLP policies only if DLP policy templates cannot meet your requirements.

Question: How can you notify users that they are about to violate DLP policy before they actually send an email message?

Answer: You can use Policy Tips to notify users that they are about to violate DLP policy.

Module 10

Designing and implementing messaging coexistence

Contents:

Lesson 1: Designing and implementing federation 2

Lesson 2: Designing coexistence between Exchange Server organizations 4

Lesson 3: Designing and implementing cross-forest mailbox moves 6

Module Review and Takeaways 9

Lab Review Questions and Answers 10

Lesson 1

Designing and implementing federation

Contents:

Question and Answers 3
Resources 3

Question and Answers

Question: What component is mandatory if you want to establish federation between two Exchange organizations?

Answer: When you configure federation, you must configure a federated trust with the Azure AD authentication system.

Question: What functionalities can you configure when you implement integration between multiple Exchange organizations?

( ) Sharing calendar information and GALs.

( ) Using a single database store.

( ) Sending secure email between organizations.

( ) Sending digitally signed messages.

( ) Rights Management protection.

Answer:

(√) Sharing calendar information and GALs.

( ) Using a single database store.

(√) Sending secure email between organizations.

( ) Sending digitally signed messages.

( ) Rights Management protection.

Resources

Configuring organization relationships

Additional Reading: For more information, refer to Sharing: http://aka.ms/Xh71wb

Lesson 2

Designing coexistence between Exchange Server organizations

Contents:

Question and Answers 5

Question and Answers

Question: When you integrate two Exchange organizations, what are three important decisions you should make?

( ) Which namespace to use

( ) What DNS servers to use

( ) Whether to synchronize free/busy information

( ) Which Edge Server to use

( ) Whether to synchronize the GAL

Answer:

(√) Which namespace to use

( ) What DNS servers to use

(√) Whether to synchronize free/busy information

( ) Which Edge Server to use

(√) Whether to synchronize the GAL

Lesson 3

Designing and implementing cross-forest mailbox moves

Contents:

Question and Answers 7
Demonstration: Moving mailboxes between forests 7

Question and Answers

Question: What is the alternative to moving mailboxes from one Exchange organization to another?

> **Answer:** The alternative is to export each mailbox from the source Exchange Server organization to a .PST file, and then to import the .PST files to an appropriate user's mailbox in the destination forest.

Demonstration: Moving mailboxes between forests

Demonstration Steps

1. On LON-EX1, restore the Exchange Management Shell.
2. Type **cd** "**C:\Program Files\Microsoft\Exchange Server\v15\scripts"**, and then press Enter.
3. Type the following at a command prompt, and then press Enter:

```
$Local = Get-Credential
```

4. In the Windows PowerShell Credential window, for **User name**, type **Adatum\Administrator**, and for **Password**, type **Pa$$w0rd**, and then click **OK**.
5. Type the following at a command prompt, and then press Enter:

```
$Remote= Get-Credential
```

6. In the Windows PowerShell Credential window, for **User name**, type **Treyresearch\Administrator**, and for **Password**, type **Pa$$w0rd**, and then click **OK**.
7. Type the following at a command prompt, and then press Enter:

```
 .\Prepare-MoveRequest.Ps1 -Identity Cindy@treyresearch.net -
RemoteForestDomainController trey-dc1.treyresearch.net -RemoteForestCredential
$Remote -LocalForestDomainController lon-dc1.adatum.com -LocalForestCredential $Local
-TargetMailUserOU "OU=IT,dc=adatum,dc=com"
```

8. Ensure that you receive the message **1 mailbox(s) ready to move**.
9. Switch to LON-DC1. Open Active Directory Users and Computers.
10. Double-click the **IT** organizational unit (OU).
11. Ensure that there is an object called **Cindy White** and that it is disabled.
12. Close Active Directory Users and Computers.
13. On LON-EX1, in the Internet Explorer, open the Exchange admin center by browsing to https://lon-ex1.adatum.com/ecp and signing in as **Adatum\Administrator**.
14. In the feature pane, click **recipients**.
15. Click the **migration** tab.
16. Click the arrow next to the **New** icon (plus sign (+)).
17. Click **Move to this forest**.
18. In the new cross-forest mailbox move window, click **Add**.
19. In the Select Mail User window, select **Cindy White**, click **add**, and then click **OK**.
20. Click **Next**.
21. On the **Enter the Windows user account credential** page, type **Treyresearch\administrator** for the Domain\user name, and type **Pa$$w0rd** for the password, and then click **Next**.

22. On the **Confirm the migration endpoint** page, type **trey-ex1.treyresearch.net** in the **Remote MRS Proxy Server** text box, and then click **Next**.

Note: If you get an error that connection to trey-ex1.treyresearch.net cannot be made, restart the TREY-EX1 machine, wait for 5 to 6 minutes, and then try this step again

23. On the **Move configuration** page, in **New migration batch name**, type **Cindy**.
24. In the **Target delivery domain** drop-down list box, select **Adatum.com.**
25. In the **Target database** section, click **Browse**.
26. In the Select Mailbox Database window, click **Mailbox Database 1**, click **add->**, and then click **OK**.
27. In both text boxes for **Bad item limit** and **Large item limit**, type **10**.
28. Click **Next**.
29. On the **Start the batch** page, click **Browse**, and then click **Administrator**.
30. Ensure that **Automatically start the batch** is selected. Click **new**.
31. Wait until the **Status of Cindy object** becomes **Synced**. You can click **Refresh** a few times. It might take a few minutes to finish.
32. When the status switches to **Synced**, select the object **Cindy**, and in the tasks pane, click **Complete this migration batch**.
33. In the warning window, click **Yes**.
34. Wait until the status of the **Cindy** object becomes **Completed**. It might take a few minutes to finish.

Module Review and Takeaways

Best Practices

- Always design coexistence carefully before you implement it.
- Use Sharing policies to precisely define the level of information sharing between organizations.
- Always implement secure message routing between partner Exchange organizations.
- Use public trusted certificates to establish federation.
- Use tools such as ADMT or MIM to synchronize user objects between organizations.
- Use organization relationships for a large number of users to share calendar information with an external organization, such as a partner or subsidiary.
- Specify a security distribution group in an organization relationship to limit the sharing of calendar data to specific users.

Review Question(s)

Question: How can MIM help synchronize GALs between two Exchange Server organizations?

> **Answer:** Unlike other solutions, which you must schedule, MIM can recognize directory changes as they happen, and it then can replicate those changes to the other Exchange Server organization. This capability means that contacts in each Exchange Server organization are always up-to-date.

Question: Which option for sharing calendar information can you use for both Exchange Server 2016 and Exchange Server 2010?

> **Answer:** Both Exchange Server 2010 and Exchange Server 2016 have the Availability Web Service for sharing free/busy information between organizations.

Common Issues and Troubleshooting Tips

Common Issue	Troubleshooting Tip
Cannot establish a connection to the Azure AD authentication system.	• Check Internet connection and firewall rules. • Check if certificate installed on Exchange server is globally trusted.
Secure SMTP messaging between organizations is not working.	• Check certificates on Exchange servers. • Check revocation locations for certificates being used. • Check connector configuration. • Monitor network traffic between Exchange servers.
Mailbox move between organizations does not work.	• Check if source server has MRSProxy service up and running. • Check Handle Mappings in IIS. • Check if mail enabled user object exists in destination domain.

Lab Review Questions and Answers

Lab: Implementing messaging coexistence

Question and Answers

Question: If you are using the internal public key infrastructure (PKI) to issue certificates in both Exchange organizations, why do you need to set up a CA cross-forest trust before you establish a relationship between the organizations?

Answer: Certificates are for domain security technology that helps secure the SMTP transport between organizations. Each Exchange server must trust the certificate issuer that provides the certificate for the Exchange server in another organization.

Question: Why is the user object that is copied from the source domain in a disabled state?

Answer: The user object that is copied from the source domain is in a disabled state because the password is not set on this object during the migration preparation. To synchronize the password, use a solution such as MIM 2016 or the ADMT.

Module 11

Upgrading to Exchange Server 2016

Contents:

Lesson 1: Planning an upgrade from previous Exchange Server versions 2

Lesson 2: Implementing the upgrade from previous Exchange versions 4

Module Review and Takeaways 6

Lab Review Questions and Answers 7

Lesson 1

Planning an upgrade from previous Exchange Server versions

Contents:

Question and Answers 3

Question and Answers

Question: What are the supported migration paths to Exchange Server 2016 from previous versions of Exchange Server?

> **Answer:** You can migrate from Exchange Server 2010 or Exchange Server 2013 to Exchange Server 2016 by installing Exchange Server 2016 in a coexistence scenario. You can migrate from Exchange Server 2007 or older to Exchange Server 2016 by setting up a new Active Directory forest and performing a cross-forest migration.

Question: Which Active Directory forest-functional and domain-functional levels do you require to install Exchange Server 2016?

> **Answer:** The Active Directory forest needs to be at least at the Windows Server 2008 forest-functional level or higher. The domain functional level needs to be 2008 or higher.

Lesson 2

Implementing the upgrade from previous Exchange versions

Contents:

Question and Answers 5

Question and Answers

Question: Which Exchange functionality migrates first to Exchange Server 2016?

Answer: Client connectivity is the first functionality that migrates to Exchange Server 2016. When you migrate client connectivity to Exchange Server 2016, you guarantee that Exchange Server 2016 handles all client connections. Exchange Server 2016 provides all the required logic and functionality to redirect or proxy client connections to the Exchange Servers hosting user mailboxes.

Module Review and Takeaways

Best Practice

Before attempting an Exchange Server upgrade in a production environment, verify the migration path in a test lab. This is particularly important in a complex Exchange environment that contains multiple sites and domains.

Best Practice

Ensure that all email clients have been upgraded in your organization before moving users' mailboxes to Exchange Server 2016. Only Outlook 2010 SP3 with the Outlook 2010 April 2015 update or newer clients are supported. Apple Macintosh clients must be upgraded to Outlook for Mac 2011 or Outlook for Mac for Office 365.

Best Practice

Always upgrade the Exchange Servers in Internet-facing sites before upgrading internal sites. This will enable the Exchange 2016 Mailbox servers in the Internet-facing sites to proxy client requests to previous versions of Exchange Server in the internal sites.

Review Question(s)

Question: Your organization includes two locations and Active Directory sites. You have deployed Exchange Server 2010 servers in both sites. You now are deploying Exchange Server 2016 servers in one of the sites and removing the Exchange Server 2010 servers. When can you remove the last Exchange 2010 Hub Transport server in the site?

> **Answer:** You can remove the last Hub Transport server when you move all of the mailboxes, public folders, and connectors from the Exchange Server 2010 servers in the site. As long as there is an Exchange 2010 Mailbox server with mailboxes in the site, you must maintain an Exchange 2010 Hub Transport server.

Common Issues and Troubleshooting Tips

Common Issue	Troubleshooting Tip
When you try to remove the public folder database in Exchange Server 2010, you are prevented from doing so. The error states that the database still contains public folders.	First, verify that the public folder migration to Exchange Server 2016 has completed and that it has been finalized. If you are confident that you will not need to revert to using the public folders on the previous version of Exchange again, you can remove the database by using Active Directory Services Interfaces Editor.

Lab Review Questions and Answers

Lab: Upgrading from Exchange Server 2013 to Exchange Server 2016

Question and Answers

Question: When you changed the Domain DNS settings for Mail.TreyResearch.net to point to TREY-EX16, how could users access their mailboxes on TREY-EX1 while using Outlook on the web?

Answer: When users connected and authenticated to the Exchange 2016 Mailbox server, the Exchange 2016 Mailbox server proxies the Outlook on the web request to the Exchange 2013 Client Access server role.

Question: What is the primary difference between a modern public folder migration and legacy public folder migrations?

Answer: The modern public folder migration has no impact to the public folder client access. The users whose mailboxes were on Exchange 2010 servers would not be able to access the modern public folders until their mailboxes were moved.

Module 12

Planning a hybrid Exchange deployment

Contents:

Lesson 1: Basics of a hybrid deployment 2

Lesson 2: Planning and implementing a hybrid deployment 4

Lesson 3: Implementing advanced functionality for hybrid deployments 6

Module Review and Takeaways 8

Lab Review Questions and Answers 10

Lesson 1

Basics of a hybrid deployment

Contents:

Resources 3
Demonstration: How to install and configure Azure AD Connect 3
Demonstration: How to configure and test SSO by using AD FS 3

Resources

What is Active Directory Federation Services?

Additional Reading: For more information about using devices for MFA and SSO, see Overview: Join to Workplace from Any Device for SSO and Seamless Second Factor Authentication Across Company Applications, refer to: http://aka.ms/Urch26

Demonstration: How to install and configure Azure AD Connect

Demonstration Steps

1. Point out that the demonstration uses custom settings for the Azure AD Connect tool. We recommend express installation for a single domain where you want to synchronize all user accounts in a single domain, to configure password synchronization, and to synchronize all attributes. This demonstration shows how to synchronize specific users to simulate a pilot deployment.
2. Mention that in this demonstration, the option to configure password synchronization is selected, and AD FS will be enabled in the next demonstration.
3. Point out that when the user signs in to Office 365, Azure AD authenticates the user. Compare this to the user experience after enabling SSO.

Demonstration: How to configure and test SSO by using AD FS

Demonstration Steps

1. Point out that you can configure AD FS and Web Application Proxy by using built-in Windows Server 2012 R2 tools. The Azure AD Connect tool just makes it easier to configure these components when you configure SSO for Azure.
2. Point out the credentials and certificates that are necessary to configure the two components. The Web Application Proxy server requires administrator credentials on the AD FS server so that it can retrieve the correct certificate from the AD FS server.
3. Mention that in the demonstration environment, the Web Application Proxy server is already configured to communicate with the AD FS server, so this step is not included when you configure SSO.
4. Point out that when you select the Azure AD domain, the domain automatically switches to a federated domain, which means that all users who are using the domain name must use AD FS to authenticate.
5. Point out the difference in the user experience when you sign in to Azure AD after enabling SSO. Now the user account authenticates by using the on-premises AD DS domain through AD FS.
6. Review the information provided by the Remote Connectivity Analyzer.

Lesson 2

Planning and implementing a hybrid deployment

Contents:

Resources 5
Demonstration: Run the Hybrid Configuration Wizard 5

Resources

Best Practices for implementing a hybrid deployment

 **Additional Reading:** For more information about Hybrid deployment best practices are available on the Exchange Team Blog, refer to: http://aka.ms/Ub6sfj

Demonstration: Run the Hybrid Configuration Wizard

Demonstration Steps

1. Point out that the recommended approach for downloading the HCW is to get it from Office 365. This ensures that you will always get the latest version of the wizard.
2. The demonstration doesn't show the process for validating the Office 365 domain. To validate the domain, create a TXT record in the external DNS zone and paste the value provided by the wizard into the TXT record.
3. The demonstration shows the configuration if you are using an Edge server as an SMTP gateway between on-premises and Office 365.
4. The demonstration shows just a few of the changes made to the on-premises environment after the wizard runs successfully.

Lesson 3

Implementing advanced functionality for hybrid deployments

Contents:

Resources 7

Resources

Configuring OAuth in a mixed Exchange Server deployment

Additional Reading: For more information about how to configure OAuth authentication between Exchange and Exchange Online organization, refer to: http://aka.ms/Jeilpx

Configuring Public Folder coexistence with Office 365

Additional Reading: The Mail-enabled Public Folders directory sync script is available here: http://aka.ms/Hdixzj

Using OneDrive for Business to store on-premises mailbox attachments

Additional Reading: For more information about how to configure document collaboration with OneDrive for Business and Exchange Server 2016 on-premises, refer to: http://aka.ms/D8nqz4

Using eDiscovery in a hybrid environment

Additional Reading: For more information about OAuth authentication to support eDiscovery in an Exchange hybrid deployment, refer to: http://aka.ms/Qrymiv

Module Review and Takeaways

Review Question(s)

Question: What deployment options do you have when you deploy Exchange Online?

Answer: You can use Exchange Online only, Exchange Server on-premises only, or a hybrid deployment that connects Exchange Server on-premises and Exchange Online.

Question: What additional functionality does Exchange Online Protection provide?

Answer: Exchange Online Protection provides a cloud-based antivirus and anti-spam service that scans email messages and cleans them if it finds malicious software.

Question: What functionality does Federated Sharing provide?

Answer: Exchange Server Federated Sharing provides the ability to exchange information between two Exchange Server organizations, such as Exchange Server on-premises and Exchange Online. For example, you can share free/busy information, share MailTips, and track messages by using delivery reports.

Question: When planning a hybrid deployment for your organization, what components do you need to consider implementing, and what is their purpose?

Answer: You need to use Azure AD Connect to synchronize your on-premises Active Directory with Office 365. You have the option of implementing Active Directory Federation Services (AD FS) for single sign-on (SSO). You need to configure Federated Sharing in order to exchange information such as free/busy information and MailTips. To configure Federated Sharing, you can use the HCW.

Question: You created a new mailbox in Exchange Online, and now the on-premises users complain that they cannot see the new mailbox. What can you do?

Answer: You cannot make the new mailbox visible to viewers, because there is no way to synchronize Exchange Online mailboxes or accounts to the on-premises environment. To correct this problem, you need to delete and then re-create the mailboxes in the on-premises Active Directory Domain Services (AD DS) by using the Exchange Admin Center or Exchange Management Shell. Then you need to wait for the Azure AD Connect to synchronize the mailbox to Exchange Online.

Tools

You can use the tools listed in the following table to monitor and test a hybrid deployment.

Tool	Use for	Where to find it
Microsoft Remote Connectivity Analyzer	Troubleshooting your on-premises SSO, Exchange ActiveSync, or Exchange Web Service.	http://aka.ms/RCA
Test-FederationTrust cmdlet	Ensure the federation trust is working correctly.	Exchange Management Shell

Review Question(s)

Question: You implemented a hybrid deployment in your Exchange Server 2016 organization. Currently your domain's MX record points to your on-premises Exchange environment. You started to migrate half of your mailboxes to Office 365.

When should you consider switching the DNS MX record to Office 365?

Answer: You can switch it any time, in a fully operational hybrid deployment. However, most companies consider switching the DNS MX record once more mailboxes are in the cloud than are on-premises.

There might be reasons for your company to never switch the DNS MX record to Office 365, for example, if you have governmental or compliance-related requirements such as archiving.

Common Issues and Troubleshooting Tips

Common Issue	Troubleshooting Tip
Free/busy information is not available for mailboxes in Exchange Online when accessing the information about mailboxes that are stored on-premises.	Ensure the certificates are working and that AutoDiscover works from the Internet. Use the Microsoft Remote Connectivity Analyzer to verify that Office 365 can contact your on-premises AutoDiscover record correctly.
Moving mailboxes between Exchange Online and on-premises fails.	Ensure the on-premises database has all copies mounted and that they are healthy. If one of them is not healthy, the Mailbox Replication Service proxy does not allow mailboxes to move to this database.

Lab Review Questions and Answers

Lab: Designing Integration with Exchange Online

Question and Answers

Question: Before you can run the HCW in the Exchange Admin Center, what do you need to do?

Answer: Before you can run the HCW in the Exchange Admin Center, you need to sign in to your Office 365 tenant using a Global Administrator account in the Exchange Admin Center.

Question: Does Exchange Server 2010 support Open Authentication (OAuth)?

Answer: No, Exchange Server 2010 does not support OAuth. Only Exchange Server 2016 and Exchange Server 2013 support OAuth.