Microsoft

OFFICIAL MICROSOFT LEARNING PRODUCT

10993A

Integrating On-Premises Identity Infrastructure with Microsoft Azure

Companion Content

Product Number: 10993A

Released: 01/2017

MICROSOFT LICENSE TERMS
MICROSOFT INSTRUCTOR-LED COURSEWARE

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

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

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

1. DEFINITIONS.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

provided you comply with the following:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

This limitation applies to

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

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

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

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

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

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

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

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

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

Revised July 2013

Module 1

Introducing Azure AD

Contents:

Lesson 1

Overview of Azure AD

Contents:

Question and Answers

Question: Which of the following are characteristics of Azure AD?

( ) Is multi-tenant by design

( ) Contains organizational units

( ) Uses LDAP for directory lookups

( ) Supports Group Policy

( ) Offers native support for multi-factor authentication

Answer:

(√) Is multi-tenant by design

( ) Contains organizational units

( ) Uses LDAP for directory lookups

( ) Supports Group Policy

(√) Offers native support for multi-factor authentication

Feedback:

Unlike AD DS, Azure AD is multi-tenant by design. It does not support organizational units (OUs). It relies on Internet-friendly protocols for directory lookups (Graph API over HTTPS) rather than Lightweight Directory Access Protocol (LDAP). It does not support Group Policy for management of its domain-joined devices; you can use a mobile device management solution, such as Microsoft Intune, instead. It offers native support for multi-factor authentication.

Resources

Azure AD as a directory service for cloud apps

 **Additional Reading:** For more information, refer to How to configure your App Service application to use Azure Active Directory login: http://aka.ms/L27lid

Lesson 2

Implementing and configuring Azure AD

Contents:

Question and Answers

Question: How will your organization use Azure AD?

Answer: Answers will vary, but might include:

- To secure access to Azure-based services.
- To delegate management of Azure-based services.
- To enhance authentication security by using multi-factor authentication.
- To provide SSO functionality for access to SaaS applications.

As an identity and access management solution, Azure AD provides a range of features that integrate with other cloud and on-premises services. It is easy to take advantage of Azure AD to authenticate Azure web apps, Azure PaaS cloud services, and web applications running in Azure virtual machines.

Similarly, you can delegate management of Azure AD resources that are accessible via the Azure Portal by using Role-Based Access Control (RBAC). You can also use Azure AD accounts when designating co-administrators of a subscription.

Azure AD offers additional authentication enhancements, including multi-factor authentication and SSO for access to SaaS applications or cloud-based Web applications, including both Azure portals. In addition, directory synchronization with AD DS makes it possible to sign in to cloud-based applications by using on-premises credentials.

For example, an organization that deploys a web app for sales personnel to Azure can use Azure AD to authenticate user requests to the app and can choose to implement multi-factor authentication when sales personnel access the app via a browser or a mobile device.

Demonstration: Creating an Azure AD tenant

Demonstration Steps

1. On LON-CL1, open Microsoft Edge, and then browse to https://manage.windowsazure.com.
2. If prompted, sign in with your Microsoft account that is associated with your Azure trial subscription.
3. If the **WINDOWS AZURE TOUR** window appears, close it.
4. Click **NEW** and in the window that opens, click **APP SERVICES**, click **ACTIVE DIRECTORY** click **DIRECTORY**, and then click **CUSTOM CREATE**.
5. In **the Add directory** window, in the **DIRECTORY** drop-down list, choose **Use existing directory**, and then select **I am ready to be signed out now**.
6. Click the check mark icon. If you get an error message, just click the link to go back to **manage.windowsazure.com**.
7. On the Microsoft Azure page, click your account from **adatumyyxxxxx.onmicrosoft.com** domain. It should be listed below your Microsoft account on outlook.com domain.
8. If prompted, enter your password, which is **Pa55w.rd1**, and then click **Sign in**.
9. If prompted, click **continue** in the prompt window to use the **Adatum** directory with Microsoft Azure.
10. Click **Sign out now**.
11. Sign in with your Microsoft account on the outlook.com domain that is associated with your Azure subscription.

12. Ensure that you see **Adatum** directory instance in the Azure classic portal. Click the **Adatum** text. If the **Let's talk about Azure AD** page appears, close it.
13. In the left navigation pane, click the **SETTINGS** icon. It is the last icon in the list.
14. Click the Azure Pass subscription. Click the **EDIT DIRECTORY** icon.
15. In the **EDIT DIRECTORY** window, ensure that the **Adatumyyxxxxx.onmicrosoft.com** directory is selected, and then click the arrow icon.
16. On the **Confirm directory mapping** page, click the check mark icon.
17. Click **OK** to reload the page.
18. In the navigation panel on the left, click **ACTIVE DIRECTORY**.
19. Click the **Adatum** directory. If the **Let's talk about Azure AD** page appears, close it.
20. Click **LICENSES**.
21. Click **TRY AZURE ACTIVE DIRECTORY PREMIUM NOW**.
22. In the **Activate Azure AD Premium trial** pop-up window, click the check mark to confirm the selection.
23. Click the **Click here to refresh** link, and then verify that Azure AD Premium is activated. You should see 100 in the **ACTIVE UNITS** column.
24. In the Microsoft Edge browser window, in the Azure classic portal, click **DOMAINS**.
25. Click **ADD A CUSTOM DOMAIN**.
26. On the **Specify a domain name** page, in the **DOMAIN NAME** box, type **yourdomain.hostdomain.com**.

 **Note: yourdomain** is the domain name assigned to you by the lab hosting provider. If you are not sure about your domain name, ask your instructor.

27. Click **add**. Wait until the message about successfully added domain appears at the top of the window.
28. Click the right arrow.
29. On the **Verify yourdomain.hostdomain.com** page, in the **RECORD TYPE** box, note the options: **TXT record** and **MX record**. Click the check mark icon.

Lesson 3

Managing Azure AD

Contents:

Question and Answers

Question: You can use a single account to manage multiple Azure AD tenants.

( ) True

( ) False

Answer:

(√) True

( ) False

Feedback:

You can manage all existing Azure AD directories, such as Azure, Office 365, and Intune, by using the same account—as long as the same account is a Global Administrator for all the directories.

Resources

User roles in Azure AD

Additional Reading: For more information, refer to Assigning administrator roles in Azure Active Directory: https://aka.ms/wxqeod

Demonstration: Creating users and groups in Azure AD

Demonstration Steps

1. On the **active directory** page, click **Adatum**.
2. If the **Let's talk about Azure AD** page appears, close it.
3. On the **Adatum** page, click **USERS**.
4. Click the **ADD USER** button at the bottom of the page.
5. In the **Tell us about this user** dialog box, enter the following settings, and then click **Next**:
   - TYPE OF USER: **New user in your organization**
   - USER NAME: **ereeve**
6. In the **user profile** dialog box, enter the following settings, and then click **Next**:
   - FIRST NAME: **Edmund**
   - LAST NAME: **Reeve**
   - DISPLAY NAME: **Edmund Reeve**
   - ROLE: **User**
   - ALTERNATE EMAIL ADDRESS: Provide your email address
   - Enable Multi-Factor Authentication: Not selected
7. Click **Create**.
8. On the **Get temporary password** page, note the value for **NEW PASSWORD**.
9. Click **Complete** (check mark).
10. At the upper right of the page, click your Microsoft account name, and then click **Sign out**.

11. On the **You have been signed out** page, click **SIGN IN**.
12. On the **Microsoft Azure** page, click **Use another account**, type **ereeve@adatumyyxxxx.onmicrosoft.com** in the text box, and then click **Continue**.
13. Sign in to Azure by using the following credentials, where your domain name is your unique Adatum number:
    - Select: **Work or school, or personal Microsoft account**
    - Username: **ereeve@adatumyyxxxx.onmicrosoft.com**
    - Password: The temporary password that you noted above
14. On the **Update your password** page, in the **Current password** box, type the temporary password, in the **New password** and **Confirm password** text boxes, type **Pa55w.rd!**, and then click **Update password and sign in**.

 **Note:** By design, the attempt to sign in to the portal fails with a "We were unable to find any Azure subscriptions where you are a service administrator or co-administrator" message.

Module Review and Takeaways

Review Question

Question: What are some benefits of hosting part or all of an organization's Active Directory infrastructure in Azure?

Answer: Benefits include:

- Centralized identity management.
- SSO across applications, including those that are hosted outside of the organization.
- Scalability and availability without additional infrastructure.
- Built-in disaster recovery.
- The integration of non-Microsoft identity providers, if required.
- Easily integrated with any existing Office 365, Intune, and Microsoft Dynamics CRM Online accounts.
- Hybrid scenarios also enable some resources to be secured on-premises, with others in the cloud.

Lab Review Questions and Answers

Lab: Creating and managing an Azure AD tenant

Question and Answers

Question: What role should you assign to a user account in the Azure AD directory instance to enable the user to fully manage all of its objects?

Answer: You should assign the Global Administrator role to the user account. The Global Administrator role grants full control of the Azure AD tenant where this role exists. Note that this role does not grant any access rights to Azure subscription resources.

Question: What account should you have before you create your first Azure subscription?

Answer: You should have a Microsoft account.

Module 2

Integrating on-premises Active Directory with Azure

Contents:

Lesson 1

Extending an on-premises Active Directory domain to Azure

Contents:

Question and Answers

Question: When you deploy a domain controller from your local AD DS in the Azure, do you use Azure AD?

Answer: In this scenario, Azure AD is not used. The local AD DS database is replicated to the domain controller deployed in Azure.

Lesson 2

Directory synchronization overview

Contents:

Question and Answers

Question: When you implement directory synchronization with password sync, what method is used to synchronize the user's password?

Answer: Directory synchronization with password synchronization copies password hashes, instead of actual passwords, to Azure AD.

Question: When you implement directory synchronization, user accounts and groups are moved from your local AD DS to the Azure AD.

( ) True

( ) False

Answer:

( ) True

(√) False

Feedback:

Directory synchronization does not move objects. It copies objects from local AD DS with a subset of their attributes, and it creates new objects in Azure AD.

Lesson 3

Implementing and configuring directory synchronization

Contents:

Question and Answers

Question: If you want to have SSO for both cloud-based and on-premises services, what do you need to deploy?

( ) Azure monitoring tools

( ) AD FS

( ) Azure AD Connect

( ) Office 365

Answer:

( ) Azure monitoring tools

(√) AD FS

(√) Azure AD Connect

( ) Office 365

Feedback:

Deploy both AD FS and Azure AD Connect

Resources

Preparing on-premises Active Directory for directory synchronization

Additional Reading: For more information, refer to Azure AD Connect sync: Attributes synchronized to Azure Active Directory: http://aka.ms/aoe050

Additional Reading: For more information, refer to: http://aka.ms/xp2jdy

Additional Reading: The CodePlex download link for Active DirectoryModify.NET is: http://aka.ms/j6168k

Installing and configuring directory synchronization by using Azure AD Connect

Additional Reading: For more information, refer to "Prerequisites for Azure AD Connect" at: http://aka.ms/s4a991

Demonstration: Implementing directory synchronization by using the Azure AD Connect custom wizard

Demonstration Steps

1. On LON-DS1, sign in as **Adatum\Administrator** with the password **Pa55w.rd**. If the **Network** pane appears, click **Yes**.
2. Open Internet Explorer, and then go to **http://www.microsoft.com/en-us/download/details.aspx?id=47594**.
3. On the **Microsoft Azure Active Directory Connect** page, click **Download**, and then click **Run**.

Note: If you experience any problems while launching the download, add the **https://download.microsoft.com** website to your Trusted sites.

4. In the **Microsoft Azure Active Directory Connect Wizard**, on the **Welcome to Azure AD Connect** page, select the **I agree to the license terms and privacy notice** check box, and then click **Continue**.
5. On the **Express Settings** page, click **Customize**.
6. On the **Install required components** page, click **Install**.
7. On the **User sign-in** page, ensure that **Password Synchronization** is selected, and then click **Next**.
8. On the **Connect to Azure AD** page, in the **USERNAME** and **PASSWORD** boxes, enter the SYNC account user name and the password **Pa55w.rd!**, and then click **Next**.
9. On the Connect your directories page, in the **USERNAME** box, type ***Adatum*\administrator**. In the **PASSWORD** box, type **Pa55w.rd**, click **Add Directory**, and then click **Next**.
10. On the **Azure AD sign-in configuration** page, ensure that your custom domain is listed as verified. Ensure that in the **USER PRINCIPAL NAME** drop-down list, **userPrincipalName** value is selected, and then click **Next**.
11. On the **Domain and OU filtering** page, click **Sync selected domains and OUs**.
12. Expand **Adatum.com**, and ensure that the check boxes are selected only for the following items: **Computers**, **IT**, **Managers**, **Marketing**, **Research**, and **Sales**. Remove the selections on other items, and then click **Next**.
13. On the **Uniquely identifying your users** page, click **Next**.
14. On the **Filter users and devices** page, click **Next**.
15. On the **Optional features** page, review available options, but do not make any changes. Ensure that **Password synchronization** is selected, and then click **Next**.
16. On the **Ready to configure** page, ensure that **Start the synchronization process when configuration completes** is selected, and then click **Install**.
17. When the installation is complete, click **Exit**.
18. At this time, synchronization of objects from your local AD DS and Azure AD begins. You must wait approximately 10 minutes for this process to complete. Close the Internet Explorer window on LON-DS1.
19. On the **LON-DS1** computer, click the **Start** button, and then type **Synchronization**.
20. In the search pane, click **Synchronization Service**.
21. In the **Synchronization Service Manager** on the LON-DS1 window, click the **Operations** tab.
22. Ensure that you see the **Export**, **Delta Synchronization**, and **Delta Import** tasks. Ensure that all tasks have the current time and date in the **Start Time** and **End Time** columns.
23. Close the Synchronization Service Manager.

Lesson 4

Managing synchronized directories

Contents:

Question and Answers

Question: What feature do you need to configure so that objects are synchronized from Azure AD to your local AD DS?

> **Answer:** You need to deploy writeback functionalities. Currently, you can use password writeback, groups writeback, and devices writeback.

Resources

Modifying directory synchronization scope

Additional Reading: For more information, refer to "Azure AD Connect sync: Configure Filtering" at: http://aka.ms/au8smo

Demonstration: Modifying options for directory synchronization

Demonstration Steps

1. On LON-DS1, click **Start**, open the all apps list (arrow icon), and then click **Synchronization Service**.
2. In **Synchronization Service Manager**, click the **Connectors** tab.
3. In the **Connectors** tab, double-click **Adatum.com**.
4. In the **Properties** dialog box, click **Configure Directory Partitions**.
5. Click **Containers**.
6. In the **Credentials** dialog box, enter the following credentials, and then click **OK**:
   - User name: **Administrator**
   - Password: **Pa55w.rd**
   - Domain: **Adatum.com**

Note: While this account is not the one used for directory synchronization, you use the account credentials temporarily to access AD DS for configuring filtering.

7. In the **Select Containers** dialog box, select the **Development** check box, and then click **OK**.
8. To close the **Properties** dialog box, click **OK**.
9. On LON-DS1, open the Start screen, and then click **Synchronization Rules Editor**.
10. In **Synchronization Rules Editor**, in **Direction**, click **Inbound**, and then click **Add new rule**.
11. In the **Create inbound synchronization rule** dialog box, in the **Name** text box, type **In from AD – User DoNotSyncFilter**
12. In the **Connected System** drop-down list, select **Adatum.com**.
13. In the **Connected System Object Type** drop-down list, select **user**.
14. In the **Metaverse Object Type** drop-down list, select **person**.
15. In the **Link Type** drop-down list, select **Join**.
16. In the **Precedence** text box, type **50**.
17. Click **Next**.

18. In the **Create inbound synchronization rule** dialog box, on the **Scoping filter** tab, click **Add Group**, and then click **Add Clause**.
19. In **Add scoping filters**:
    - For **Attribute**, select **msDS-cloudExtensionAttribute15**.
    - For **Operator**, select **EQUAL**.
    - For **Value**, type **NoSync**,
20. Click **Next**.
21. On the **Add join rules** page, click **Next**.
22. On the **Add transformations** page, click **Add transformation**.
23. In the **FlowType** drop-down list, select **Constant**.
24. In the **Target Attribute** drop-down list, select **cloudFiltered**.
25. In the **Source** text box, type **True**.
26. To save the rule, click **Add**, and then close the **Synchronization Rules Editor** window.
27. Open Windows PowerShell from the taskbar. In Windows PowerShell, type the following command, and then press Enter. The initial synchronization can take several minutes to complete. Leave the Windows PowerShell window open.

```
Start-ADSyncSyncCycle –PolicyType Initial
```

Module Review and Takeaways

Best Practices

- Always plan on how you want to extend your Active Directory functionality.
- Avoid using separate credentials for cloud resources.
- For simple deployments, use the Express installation option in Azure AD Connect.
- To establish two-way sync, use writeback functionalities.
- Keep credentials for the sync account in a secure place.

Review Question

Question: What tools should you use to resolve potential attribute issues in AD DS before implementing directory synchronization?

Answer: You can use the IdFix and ADModify.NET tools.

Tools

- Azure AD Connect
- IdFix
- ADModify.NET
- Azure Management portal

Lab Review Questions and Answers

Lab: Implementing directory synchronization

Question and Answers

Question: What was the purpose of adding new UPN to users locally?

Answer: You added another UPN in your local AD DS so that you can use same UPN format when signing in locally and to cloud resources.

Question: What are some benefits of using filtering options in Azure AD Connect?

Answer: Filtering makes synchronization more secure, with no forgotten accounts in online services, therefore providing a smaller attack surface. Filtering can also help you limit the number of objects, which in turn can help you minimize the size of your Azure AD Connect database.

Module 3

Using Azure AD as a directory service in hybrid environments

Contents:

Lesson 1

Azure AD as a directory service for on-premises environments

Contents:

Question and Answers

Question: What service should you consider if you want to have the same features in Azure AD that you have in your on-premises AD DS?

Answer: You should consider Azure AD Domain Services.

Question: Which operating systems can join Azure AD?

( ) Windows 8

( ) Windows 8.1

( ) Windows 10

( ) Windows 7

( ) Windows 10 Mobile

Answer:

( ) Windows 8

( ) Windows 8.1

(√) Windows 10

( ) Windows 7

(√) Windows 10 Mobile

Feedback:

Windows 10 and Windows 10 Mobile

Demonstration: Joining Windows 10 clients to Azure AD

Demonstration Steps

1. On **LON-CL2**, ensure that you are signed in as the local administrator.
2. Click the **Start** menu, click **Settings**, and then click **System**.
3. In the **SYSTEM** window, in the **navigation** pane, click **About**, and then click **Connect to work or school**.
4. On the **Connect to work or school** page, click **Connect**.
5. On the **Set up a work or school account** page, click **Join this device to Azure Active Directory**.
6. On the **Let's get you signed in** page, type **Bruno@*yourdomain*.hostdomain.com** for username and **Pa55w.rd** for password and click **Sign in**.
7. At the **Make sure this is your organization** prompt, click **Join**, click **Done**, and then close the **Settings** window.
8. Restart **LON-CL2**.
9. When computer restarts, click **Other user** on the sign-in screen.
10. Sign in as **Bruno@*yourdomain*.hostdomain**.com with password **Pa55w.rd**.
11. On the **Set up a PIN** page, click **Set up PIN**.
12. On the **Help us protect your account** page, close the window and then click **Skip for now**.
13. Ensure that you are signed in.

Lesson 2

Configuring SSO with Azure AD

Contents:

Question and Answers

Question: How can you verify if your local federation service on **fs.adatum.com** is working?

> **Answer:** You can browse to **https://fs.adatum.com/federationmetadata/2007-06/federationmetadata.xml**.

Resources

What is claims-based authentication?

 **Additional Reading:** For more information, refer to Claims-based identity term definitions: http://aka.ms/wnc2ys

Integrating applications with Azure AD

 **Reference Links:** You can access the Azure AD application gallery from: https://aka.ms/mbm8ad

Demonstration: Enabling SSO for claims-aware applications in the Azure gallery

Demonstration Steps

1. On **LON-CL2**, open Microsoft Edge, and then browse to **https://manage.windowsazure.com**.
2. On the **Microsoft Azure** page, click **SIGN OUT**, and then click **SIGN IN**.
3. On the **Microsoft Azure** page, click **Use another account**, type the Microsoft account that is associated with your Azure subscription, and then click **Continue**.
4. On the **Sign-in** page, sign in with the Microsoft account that is associated with your Azure subscription.
5. On the Azure portal, click **Adatum**. On the **Adatum** directory page, click **APPLICATIONS**, and then click **ADD**.
6. In the **What do you want to do?** dialog box, click **Add an application from the gallery**.
7. In the **Add an application for my organization to use** dialog box, in the **search** box, type **Microsoft**, and then press Enter.
8. Click **Microsoft Account (Windows Live)**, type **Microsoft Account (Windows Live)** in the **DISPLAY NAME** text box, and then click the check mark.
9. Verify that **Configure single sign-on** has been enabled by default, and then click **Assign accounts**.
10. In the **SHOW** drop-down list box, select **All Users** and click the **checkmark** icon. In the user list, click **Abbi Skinner**.
11. At the bottom of the screen, click **ASSIGN**.
12. In the **Assign Users** dialog box, select the **I want to enter Microsoft Account (Windows Live) credentials on behalf of the user** check box.
13. In the **Email Address** text box, type the email address of the Microsoft account that you used for the Azure subscription. In the **Password** text box, type your Azure subscription password, and then click the check mark.

14. Above the Microsoft account, click the back arrow.
15. At the bottom of the screen, click **ADD**.
16. In the **What do you want to do?** dialog box, click **Add an application from the gallery**.
17. In the **Add an application for my organization to use** dialog box, in the **search** box, type **Skype**, and then press Enter. Click **Skype**, type **Skype** in the **DISPLAY NAME** text box, and then click the check mark.
18. Verify that **Configure single sign-on** has been enabled by default, and then click **Assign accounts**.
19. In the **SHOW** drop-down list box, select **All Users** and click the **checkmark** icon. In the user list, click **Abbi Skinner**.
20. At the bottom of the screen, click **ASSIGN**.
21. In the **Assign Users** dialog box, do not select the **I want to enter Skype credentials on behalf of the user** check box, and then click the check mark.
22. At the top right of the **Azure portal** page, click your Azure account name, and then click **Sign out**.
23. Close the Microsoft Edge browser.

Lesson 3

Implementing Azure AD PIM

Contents:

Question and Answers

Question: You can use Azure AD PIM to manage privileges for both local and cloud-based resources.

( ) True

( ) False

Answer:

( ) True

(√) False

Feedback:

Currently, Azure AD PIM can manage privileges for cloud-based resources only. You can use PAM to manage privileges for local resources.

Demonstration: Enabling and configuring Azure AD PIM

Demonstration Steps

1. On your local computer, open the Microsoft Edge browser, and then browse to **https://portal.azure.com**.
2. Sign in as **msnider@adatumyyxxxx.onmicrosoft.com** with password **Pa55w.rd!**.
3. On the Azure portal, click **More services**, navigate through the list, and then click **Azure AD Privileged Identity Management**.
4. In the **Privileged Identity Management** window, click the **Azure AD Privileged Identity Management** link.
5. On the next page, click **Azure AD Privileged Identity Management**.
6. On the next page, click **Create**.
7. On the next page, click the **Verify my identity** link.
8. On the **Microsoft Azure** page, click **Set it up now**.
9. On the **Additional security verification** page, ensure that **Authentication phone** is selected in first drop-down list, select your country or region, and then type your mobile phone number. Select the **Send me a code by text message** option, and then click **Contact me**.
10. On the **Additional security verification** page, type the code that you received in SMS, and then click **Verify**.
11. When you receive the "Verification successful!" message, click **Done**; you will redirect back to the Azure portal.
12. On the Azure portal, click **Create**.
13. In the Azure portal, click **Discover privileged roles**. On the **Discover privileged roles** page, click **Global Administrator**. Review the users who have a global administrator role assigned. Click **User Administrator** and review users with this privilege and then click **Next**.
14. On the **Convert users to eligible** page, select **Edmund Reeve**, and then click **Next**.
15. On the **Review changes** page, click **OK**.
16. On the **Privileged Identity Management** page, click **Manage privileged roles**.
17. In the right pane, click **Settings**.
18. On the **Settings** page, click **Privileged Roles**, and then click **User Administrator**.

19. In the **User Administrator** pane, click **Enable** in the **Notifications** section, and then click **Enable** in the **Incident/Request Ticket** section.
20. Change the **Maximum Activation duration (hours)** value to **2**, and then click **Save**.
21. In the **Settings** pane, click **Alerts**.
22. In the **Alerts** pane, click **Roles are being activated too frequently**.
23. In the **Security alert** settings pane, in the **Number of renewals** section, change the value to **7**, and then click **Save**.
24. In the **Alerts** pane, click **Administrators aren't using their privileged roles**.
25. On the **Security alert settings** page, change the value to **21 days**, and then click **Save**.
26. Go back to the **Manage privileged roles** pane, and then in **Roles summary** section, click **User Administrator**.
27. In the **User Administrator** pane, ensure that Edmund Reeve account have a **Eligible** value in the **PERMISSION** column.

Module Review and Takeaways

Best Practices

- Join Azure AD computers that are frequently out of your local network and that access most resources in cloud.
- If you configure SSO with AD FS, always provide a high availability infrastructure for AD FS.
- Be aware that in a SSO with AD FS scenario, your local Internet link becomes even more critical.
- Avoid configuring too many permanent administrators in Azure AD PIM.

Common Issues and Troubleshooting Tips

Common Issue	Troubleshooting Tip
You cannot join a computer to Azure AD.	• Check if Azure AD is configured to allow devices to join. • Check if you have permissions to join a computer to Azure AD.
Users cannot access your local AD FS sign-in page in an SSO scenario.	• Check if you have configured certificates properly. • Check if you configured your firewall to accept authentication requests from Azure AD. • Check if you configured Web Application Proxy properly.

Lab Review Questions and Answers

Lab: Using Azure AD in hybrid environments

Question and Answers

Question: What was the purpose of the **Convert-MsolDomainToFederated** cmdlet that you executed in the lab?

Answer: This cmdlet converts the domain that was configured in Azure AD to a federated domain. By doing this, you configure Azure AD to redirect authentication requests to your local AD FS and AD DS.

Question: What is the purpose of the Web Application Proxy component when configuring SSO?

Answer: Authentication requests from Azure AD that come to your local AD DS proxy through Web Application Proxy to AD FS.

Module 4

Configuring and protecting authentication in hybrid environments

Contents:

Lesson 1

Authenticating users in hybrid environments

Contents:

Question and Answers

Question: If you implement directory synchronization with password synchronization between AD DS and Azure AD, which system authenticates users when they access services such as Office365?

> **Answer:** In this case, Azure AD authenticates the users because this scenario does not support SSO.

Question: When you join a computer to the AD DS domain, you establish a trust relationship.

( ) True

( ) False

> **Answer:**
>
> (√) True
>
> ( ) False
>
> **Feedback:**
>
> When you join a computer to the AD DS domain, your computer starts to trust tokens that Kerberos, the authentication service in AD DS, issues. Because of this, you are able to access local resources on your laptop or desktop computer, when you sign in with the domain account from AD DS.

Demonstration: Configuring self-service password reset

Demonstration Steps

1. On **LON-DS1**, on the desktop, double-click **Azure AD Connect**.
2. On the **Additional tasks** page, click **Customize synchronization options**, and then click **Next**.
3. On the **Connect to Azure AD** page, type **SYNC@adatumyyxxxx.onmicrosoft.com** in the **USERNAME** text box, type **Pa55w.rd!** in the **PASSWORD** text box, and then click **Next**.
4. On the **Connect to your directories** page, click **Next**.
5. On the **Domain and OU filtering** page, click **Next**.
6. On the **Optional features** page, select **Password writeback**, and then click **Next**.
7. On the **Ready to configure** page, click **Configure**.
8. On the **Configuration complete** page, click **Exit**.
9. Open Microsoft Internet Explorer browser on LON-DS1, and go to **https://manage.windowsazure.com**.
10. Sign in with the Microsoft account associated with your Azure trial subscription.
11. In the Azure portal, click the **Adatum** directory item.
12. Click the **CONFIGURE** tab.
13. In the **user password reset policy** section, select **YES** for **USERS ENABLED FOR PASSWORD RESET**.
14. For the **AUTHENTICATION METHODS AVAILABLE TO USERS** option, ensure that **Mobile Phone** and **Alternate Email Address** are selected, and then select **Security Questions**.
15. In the **SECURITY QUESTIONS** section, in the **Knowledge base** dropdown list, select three questions of your choice.
16. For the **NUMBER OF QUESTIONS REQUIRED TO REGISTER**, select **3**.

17. For the **NUMBER OF QUESTIONS REQUIRED TO RESET**, select **3**.
18. Scroll to **PASSWORD WRITE BACK SERVICE STATUS**, and then verify that it is set to **Configured** and that the option **WRITE BACK PASSWORDS TO ON-PREMISES ACTIVE DIRECTORY** is set to **YES**.
19. Click **SAVE**.
20. Close the **Microsoft Internet Explorer** browser window, and then reopen it.

Lesson 2

Implementing multi-factor authentication

Contents:

Question and Answers

Question: A. Datum requires that their applications use multi-factor authentication. The organization has implemented this technology in its on-premises infrastructure and wants to extend it for apps and resources that reside in Azure. A. Datum wants to use authentication methods that are similar to what they are currently using in the on-premises infrastructure. Can they use Multi-Factor Authentication for this, and if so, why?

Answer: Yes, they can use Multi-Factor Authentication because Azure Multi-Factor Authentication Server supports the following authentication methods to complement usernames and passwords:

- A phone call
- A two-way SMS
- A two-way SMS with PIN
- A one-way SMS
- A one-way SMS with PIN
- An OAuth token
- Mobile app

Question: Do you have any resources in your organization that you need to protect with multi-factor authentication?

Answer: Answers may vary.

Demonstration: Configuring and enabling Multi-Factor Authentication

Demonstration Steps

1. On the taskbar on LON-CL1, click **Microsoft Edge**.
2. In the **Microsoft Edge** window, in the address box, type **https://manage.windowsazure.com**, and then press **Enter**.
3. On the **Microsoft Azure** page, type the credentials for the Microsoft account associated with your Azure subscription, click **Continue**, and then sign in with your password for the Microsoft account.
4. Click the **Adatum** directory item.
5. Click **CONFIGURE**.
6. Under **multi-factor authentication**, click **Manage service settings**.
7. If you get a **Sign in** page, type the credentials for the Microsoft account associated with your Azure subscription, and then click **Sign in**.
8. On the **multi-factor authentication** page, click **users**.
9. In the **users** list, select the check box for **Abbi Skinner**, and then in the quick steps section, click **Enable**.
10. On the **About enabling multi-factor auth** page, click **enable multi-factor auth**.
11. On the **Updates successful** page, click **close**.
12. Click **service settings**.
13. Review the available options for trusted IP addresses and the verification options. Do not make any changes.

14. Click the **Go to the portal** link.
15. In the **Azure Multi-Factor Authentication** portal, click **CONFIGURE**.
16. Explain the available options.
17. Click **Voice Messages** in the left navigation pane.
18. Explain the available options.

Demonstration: Configuring Multi-Factor Authentication Server on premises

Demonstration Steps

1. Switch to **LON-SVR2** computer. Open **Server Manager**, click **Tools** and then click **Routing and Remote Access**.
2. Right-click **LON-SVR2 (local)**, and then click **Configure and Enable Routing and Remote Access**.
3. On the **Welcome to the Routing and Remote Access Server Setup Wizard** page, click **Next**.
4. On the **Configuration** page, select **Remote access (dial-up or VPN)**, and then click **Next**.
5. On the **Remote Access** page, select **VPN**, and then click **Next**.
6. On the **VPN Connection** page, select the adapter with the address **131.107.0.1**, and then click **Next**.
7. On the **IP Address Assignment** page, select **Automatically**, and then click **Next**.
8. On the **Managing Multiple Remote Access Server** page, select **Yes**, **setup this server to work with a RADIUS server** and then click **Next**.
9. On the **RADIUS Server Selection** page, type **lon-svr1.adatum.com** in the **Primary RADIUS server** text box, type **Pa55w.rd** in the **Shared secret** text box, click **Next**, click **Finish**, and then click **OK**.
10. Right click **LON-SVR2 (local)**, and then select **Properties**.
11. Click the **Security** tab, ensure that **RADIUS Authentication** is selected as **Authentication provider**, and then click **Configure**.
12. In the **RADIUS Authentication** window, select **lon-svr1.adatum.com**, and then click **Edit**.
13. In the **Edit RADIUS Server** window, type **60** in the **Time-out (seconds)** text box.
14. Click **OK**, click **OK**, and then click **OK** again.
15. Switch back to **LON-SVR1**.
16. On the **VPN with RADIUS** page, type IP address of the **lon-svr2** server (10.0.0.14), type **Pa55w.rd** in the **Shared secret** and **Confirm shared secret** text boxes, and then click **Next**.
17. On the **VPN Target** page, select **Windows domain**, and then click **Next**.
18. On the **VPN Configuration Complete** page, and then click **Next**.
19. On the **Finish** page, if you see the option **Reboot now**, select it, and then click **Finish**. Wait until the server reboots. If option to reboot server is not available skip to step 23.
20. Sign in to **LON-SVR1** as **Adatum\Administrator** with the password **Pa55w.rd**.
21. Click **Start**, and then click the arrow to show all applications.
22. Click **Multi-Factor Authentication Server** from the list.
23. In the **Multi-Factor Authentication Server** window, in the left pane, click **Users**.
24. Click **Import from Active Directory**...

25. In the **Import from Active Directory** window, click **Import**, click **OK**, and then click **Close**.
26. In the list of users, double click **Administrator@yourdomain.hostdomain.com**.
27. In the **Edit User** window, click the **Administrator** tab, select **User is a User Portal Administrator**, click **Apply**, and then click **Close**.
28. In the list of users, double-click **Abbi@yourdomain.hostdomain.com**.
29. In the **Edit User** window, on the **General** tab, select the **Enabled** check box, select your country from the **Country code** drop-down list. and then type your mobile phone number in the **Phone** text box.
30. Ensure that **Phone call** is selected with **Standard** option.
31. On the **Advanced** tab, in the **Phone call language** drop-down list, find and select your language, click **Apply**, and then click **Close**.

Note: If you can't find your language, select **en:English**.

32. In the **Multi-Factor Authentication Server** window, click **RADIUS Authentication** in the left pane.
33. In the right pane, click **10.0.0.14**, and then click **Edit**.
34. In the **Edit RADIUS Client** window, select **Require Multi-Factor Authentication user match**, and then click **OK**.

Module Review and Takeaways

Best Practices

- Implement the password writeback functionality to keep passwords consistent between Azure AD and AD DS.
- Suggest that users use the mobile app as a multi-factor authentication method.
- Use Multi-Factor Authentication Server to protect VPN connections.
- Protect privileged role activation with Multi-Factor Authentication.
- Configure multi-factor authentication messages in local language to make this service easier to use for your users.

Review Question

Question: If you don't want to use self-service password reset from Azure AD, what is the alternative to provide this functionality for AD DS?

Answer: You can deploy Microsoft Identity Manager on premises.

Common Issues and Troubleshooting Tips

Common Issue	Troubleshooting Tip
Multi-factor authentication does not work for VPN connections	Ensure that you configured your VPN server or VPN appliance as the RADIUS client for Multi-Factor Authentication Server

Lab Review Questions and Answers

Lab: Configuring authentication in hybrid environments

Question and Answers

Question: When a user resets the password by using the Azure AD profile page, what should you enable to maintain password consistency in Azure AD and AD DS?

Answer: You should implement the password writeback functionality.

Question: You want to enforce multi-factor authentication for your business critical website. What should you use?

Answer: You should use Multi-Factor Authentication Server.

Module 5

Deploying Azure RMS with on-premises services

Contents:

Lesson 1

RMS overview

Contents:

Question and Answers

Question: How does Azure RMS fit into a company-wide data protection initiative?

Answer: Answers will vary, but might include:

- Azure RMS protects specific files that users have opted to protect. However, you should still protect data that users have not specifically protected with the help of Azure RMS. You can use BitLocker Drive Encryption to protect entire volumes while still using Azure RMS to further protect documents, especially those that will be shared.
- Azure RMS protects email messages, but only when users opt to do so. However, to automate protection, you can use server-based Exchange transport rules to protect email messages after a user sends them, but before they leave the organization.
- Beyond just protecting data with Azure RMS, you need the ability to audit data access. You can track documents protected with Azure RMS. You also can use the advanced auditing features of Group Policy to audit access to files and folders.

Question: You can protect picture files with Azure RMS.

( ) True

( ) False

Answer:

(√) True

( ) False

Feedback:

Azure RMS with the RMS sharing application allows you to protect picture files.

Question: What are some of the key differences between Azure RMS and AD RMS?

Answer: Azure RMS integrates with on-premises servers, and with Microsoft Office 365, Exchange Online, and SharePoint Online. AD RMS only integrates with on-premises servers. In addition, Azure RMS lets you share protected content seamlessly with users outside of your organization. While AD RMS offers this functionality, it requires a large amount of setup time and federation with each outside organization with which you will share protected content. Finally, Azure RMS supports Azure Multi-Factor Authentication (Azure MFA), but AD RMS does not.

Resources

What is Azure RMS and how does it work?

Additional Reading: For more information, refer to "Protecting and Tracking Sensitive Data with RMS: Today and What's Next" at: http://aka.ms/w4bald

Azure RMS vs. RMS for Office 365 vs. AD RMS

Additional Reading: For more information, refer to "Comparing Azure Rights Management and AD RMS" at: http://aka.ms/sndlw0

Lesson 2

Implementing Azure RMS

Contents:

Question and Answers

Question: What is the disadvantage of configuring a protected document to be immediately revocable?

> **Answer:** When you configure a protected document to be immediately revocable, the recipient of the document must authenticate to Azure RMS every time they open the document.

Resources

Activating Azure RMS

Additional Reading: For more information, see "Comparison of Rights Management Services (RMS) Offerings" at: http://aka.ms/wqy43u

Azure RMS document tracking

Additional Reading: For more information on tracking and revoking your documents when you use the RMS sharing application, refer to: http://aka.ms/u3ugcp

Demonstration: Configuring Azure RMS templates

Demonstration Steps

1. In the Azure portal on LON-DC1, on active directory page, click **Adatum**.
2. On the **adatum** page, click **TEMPLATES**.
3. On the **TEMPLATES** page, review the available templates. You should see **Adatum – Confidential** and **Adatum – Confidential View Only** templates. You cannot modify these templates. Minimize Internet Explorer window.
4. Open Server Manager from Start Menu. Click **Tools** and then click **Active Directory Users and Computers**.
5. Click on **Managers** OU.
6. In the right pane, double click **Managers** group.
7. In the Managers Properties window, type **managers@yourdomain.hostdomain.com** in **E-mail** textbox. Click **OK**.
8. Switch to LON-DS1. Double click **Windows Azure Active Directory Module for Windows PowerShell** on the desktop.
9. In the PowerShell window type: **Start-ADSyncSyncCycle -PolicyType Delta** and press Enter. Wait for 2-3 minutes. Leave PowerShell window open.
10. Switch back to LON-DC1, restore Internet Explorer window, with Azure portal.
11. Click **ADD**.
12. In the **Add a new rights policy template** window, in the **Language** drop-down list box, click **English – United States**.
13. In the **Name** text box, type **Managers Only**.
14. In the **Description** text box, type **Accessible only by managers**.
15. Click the check mark icon. Wait until the new template is added.

16. In the **Azure portal**, click the **Managers Only** template icon.
17. On the **managers only** page, click **RIGHTS**, and then click **ADD**.
18. In the **CONFIGURE RIGHTS FOR USERS** window, click the **Managers** group, and then click the right arrow.
19. On the **USER AND GROUP RIGHTS** page, click **Co-Author**, and then click the check mark icon.
20. Click **SCOPE**, and then click **ADD**.
21. On the **TEMPLATE VISIBILITY** page, click **Managers**, and then click the check mark icon.
22. Click **CONFIGURE**.
23. In the **general** section, click **PUBLISH**.
24. In the **content expiration** section, ensure that **Content never expires** is selected.
25. In the **offline access** section, ensure that **Number of days the content is available without an Internet connection** is selected, and then in the text box, type **5**.
26. Click **SAVE**.

Demonstration: Installing and using the RMS sharing application

Demonstration Steps

1. On the **LON-CL2** computer, open Microsoft Edge, and browse to https://www.microsoft.com/en-us/download/details.aspx?id=40857
2. On the **Microsoft Rights Management sharing application for Windows** page, click **Download**.
3. On the **Choose the download you want** page, select all files, and then click **Next**.
4. On the **Thank you for downloading** page, at the prompt that appears at the bottom of the page, click **Save as**.
5. From the right-side menu, click the **Downloads** folder, and then click **Save**.
6. Repeat steps 4 and 5 for all download prompts.
7. From the desktop taskbar, open **File Explorer**, and then navigate to the **Downloads** folder.
8. Double-click the **setup.exe** file.
9. At the **User Account Control** prompt, click **Yes**.
10. In the **Setup Microsoft RMS** window, click **Next**.
11. Wait until the required files are downloaded.
12. Ensure that all items listed have the status **Success** at the end of installation.
13. If prompted to do so, restart the computer by clicking **Restart**. If not, in the **Setting up Microsoft RMS** window, click **Close**.
14. Open File Explorer, and in the **C:\temp** folder, right-click the empty space, click **New**, and then click **Text Document**.
15. Name the new document **Doc1**. Open it, and type some text inside. Save the document, and then close it.
16. Right-click the document, click **Protect with RMS**, click **Protect in-place**, and then click **Company-defined Protection**.

17. In the **Microsoft Rights Management** prompt window, sign in with your Azure AD tenant administrative account that you created on your custom domain.
18. After you are signed in, in the **add protection** window, in the **Select permission** drop-down list box, click the **Managers** template.
19. Click **Apply**.
20. After the window closes, ensure that the file has changed the extension to **.ptxt**.
21. Double-click the file. Ensure that it now opens in the Microsoft Rights Management application and not in Notepad.
22. Close the file.

Lesson 3

Integrating Azure RMS with on-premises services

Contents:

Question and Answers

Question: What kind of Azure RMS protection would you implement in your organization?

> **Answer:** Answers may vary, but students will most probably mention that Azure RMS integration with Windows Server FCI or with SharePoint library would be the appropriate option.

Resources

What is the RMS connector?

 **Additional Reading:** For more information on deploying the RMS connector, refer to: http://aka.ms/ylfrax

Demonstration: Installing and configuring an RMS connector

Demonstration Steps

1. If needed, sign in to **LON-SVR2** as **ADATUM\Administrator** with the password **Pa55w.rd**.
2. Open **Internet Explorer** from the task bar and navigate to: https://www.microsoft.com/en-us/download/details.aspx?id=40839
3. On the **Microsoft Rights Management connector** page, click **Download**.
4. On the **Choose the download you want** page, select all items and click **Next**.
5. Click **Allow once** to allow popup window for download.
6. Save all three files to **Downloads** folder.
7. Open File Explorer, navigate to **Downloads** and double-click **RMSConnectorSetup.exe**.
8. In the **Open File – Security Warning** window, click **Run**.
9. In the **Microsoft Rights Management connector setup** window, on the **Welcome to Microsoft Rights Management connector setup** page, click **Next**.
10. On the **End-User License Agreement** page, select the **I accept the terms in the License Agreement** check box, and then click **Next**.
11. On the **Microsoft RMS administrator credentials** page, type msnider@adatumyyxxxx.onmicrosoft.com *for User name* and type **Pa55w.rd!** for password, and then click **Next**.
12. On the **Ready to install Microsoft Rights Management connector** page, click **Install**.
13. On the **Installation of Microsoft Rights Management connector completed** page, clear the **Launch connector administration console to authorize servers** check box, and then click **Finish**.
14. In the **File Explorer** window, in the **Downloads** folder, right-click **GenConnectorConfig.ps1**, and then select **Copy**.
15. In the address bar of File Explorer, type **\\LON-SVR1\C$** and then press Enter.
16. Right-click the empty space in the window and select **Paste**.
17. Close the **Internet Explorer** window on **LON-SVR2**.

Demonstration: Configuring Azure RMS with FCI

Demonstration Steps

1. On **LON-SVR2**, on the desktop, double-click the **Microsoft RMS connector administration tool** shortcut on the desktop.
2. In the **Microsoft Rights Management connector administration tool** window, in the **Username** text box, type **msnider@adatumyyxxxx.onmicrosoft.com**. In the **Password** text box, type **Pa55w.rd!**, and then click **Sign In**.
3. On the **Servers allowed to utilize the connector** page, click **Add**.
4. In the **Allow a server to utilize the connector** window, click the **Role** drop-down list box, and then click **FCI Server**.
5. Next to the **Account or group** designation, click **Browse**.
6. In the **Select User, Computer, Service Account, or Group** window, type **LON-SVR1**, and then click **Check Names**.
7. After the server name resolves, (it will be underlined), click **OK**.
8. In the **Allow a server to utilize the connector** window, click **OK**.
9. In the **Microsoft Rights Management connector administration tool** window, click **Close.**
10. If needed, sign in to **LON-SVR1** as **ADATUM\Administrator** with the password **Pa55w.rd**.
11. Click **Start**, and then click the **Windows PowerShell** icon.
12. At the Windows PowerShell command-line prompt, navigate to **C:**. Run the **.\GenConnectorConfig.ps1 –ConnectorUri http://lon-svr2.adatum.com -SetFCI2012** command.
13. Type **R** when prompted and then press Enter.

Module Review and Takeaways

Best Practices

- When protecting content, configure documents to have immediate revocation if the files are sensitive or if your organization has a high-security environment.
- Run at least two RMS connector servers to provide for high availability and to ensure that users can always gain access to protected content.
- If you have Exchange, SharePoint, and Windows Server FCI, you should integrate all three with Azure RMS to expand the availability of data protection.
- Use Group Policy to configure servers for Azure RMS. You can use a GPO to populate the registry with your Azure RMS information automatically.
- Use an application delivery solution such as Microsoft System Center Configuration Manager, to distribute the RMS sharing application to all employees. This helps to maximize the use of data protection.

Review Question

Question: What changes must you make on an Exchange Server, a SharePoint Server, or an FCI server in order to integrate it with Azure RMS?

Answer: You must update the registry to point to Azure RMS.

Common Issues and Troubleshooting Tips

Common Issue	Troubleshooting Tip
You cannot view a protected document that you used to be able to view.	The sender might have revoked your access. Contact the sender to inquire.
You cannot import the Active Directory Rights Management (AADRM) module for Windows PowerShell.	By default, the AADRM module is not available for import. You need to download the Azure Rights Management Administration Tool, install it, and then you can import the AADRM module. You can download the tool from http://aka.ms/h45lwq
You cannot activate Azure RMS.	A standard Azure subscription does not include use rights for Azure RMS, and thus you will not be able to activate Azure RMS. To activate Azure RMS, you must have either an Office 365 subscription, an Azure Rights Management Premium subscription, an Enterprise Mobility Suite subscription, or an RMS for individual subscription.

Lab Review Questions and Answers

Lab: Implementing Azure RMS

Question and Answers

Question: When configuring Azure RMS integration for Windows Server FCI, Exchange, or SharePoint, why do you need to use Windows PowerShell as part of the process?

Answer: You need to obtain your RMS connector Uniform Resource Indicator (URI), which you use to configure the registry on integrated servers.

Question: What application should you use to protect JPEG files with RMS?

Answer: You should use the RMS sharing application for Windows.

Module 6

Monitoring Azure AD

Contents:

Lesson 1

Azure AD reporting

Contents:

Question and Answers

Question: What should you use to provide alert and notification capabilities for locally deployed AD DS?

> **Answer:** Because AD DS does not have built-in capabilities for alerts or notifications, you should use additional software solutions such as Operations Manager.

Demonstration: Using Azure AD reports and configuring notifications

Demonstration Steps

1. On your host machine, open the Microsoft Edge or Internet Explorer browser, and then go to https://manage.windowsazure.com.
2. Sign in with administrative credentials for your Azure AD tenant.
3. On the Azure classic portal, click the **Adatum** directory item.
4. On the **adatum** directory page, click **REPORTS**.
5. Review the available reports. Discuss with the class which reports you consider most important for your organization.
6. Click **Audit report**, and then review the content of the audit report.
7. Click the **Password reset registration activity** report, and then ensure that you can see all the users who are registered for password reset functionality.
8. Click the **Application usage** report, click the checkmark icon and then review the report content. There might some application or none listed here.
9. Click the back icon.
10. On the Azure portal, on the **adatum** directory page, click **CONFIGURE**.
11. On the directory properties page, scroll down to the **notifications** section.
12. Ensure that the **EMAIL NOTIFICATION OF ANOMALOUS SIGN INS** option has a status of **ENABLED**.
13. For the **NOTIFY ADMINS WHEN OTHER ADMINS RESET THEIR OWN PASSWORDS** option, click **YES**.
14. Ensure that the **NOTIFY USERS AND ADMINS WHEN THEIR OWN PASSWORD HAS BEEN RESET** option has a status of **YES**, and then click **SAVE**.

Lesson 2

Monitoring Azure AD

Contents:

Question and Answers

Question: Do you need to deploy agent software to monitor Azure AD with OMS?

Answer: No. You need agent software only for AD DS monitoring.

Question: Which of the following resources can you monitor and manage by using OMS?

( ) An infrastructure as a service (IaaS) VM that is running Linux

( ) A platform as a service (PaaS) Cloud Service worker role

( ) A PaaS web app

( ) An Azure Storage account

( ) An on-premises computer that is running the 32-bit Enterprise edition of Windows 8

Answer:

(√) An infrastructure as a service (IaaS) VM that is running Linux

(√) A platform as a service (PaaS) Cloud Service worker role

( ) A PaaS web app

( ) An Azure Storage account

(√) An on-premises computer that is running the 32-bit Enterprise edition of Windows 8

Feedback:

By using OMS, you can monitor Windows and Linux operating systems, both in Azure and on-premises, but not Azure PaaS services.

Demonstration: Configuring Azure AD Connect Health

Demonstration Steps

1. On **LON-DC1**, open Internet Explorer, and then go to https://portal.azure.com.
2. Sign in as msnider@adatumyyxxxx.onmicrosoft.com, and then click **More Services**.
3. In the list of services, click **Azure AD Connect Health**.
4. In the right pane, click **Create**.
5. In the **Azure AD Connect Health** pane, select **Pin blade to dashboard**.
6. In the **Azure AD Connect Health** pane, in the **Azure Active Directory Connect (Sync)** section, click your tenant name.
7. In the right pane, review the report.
8. Click the **Quick Start** icon, click **Download Azure AD Connect Health Agent for AD DS**, and then click **Run** when prompted.
9. In the **Microsoft Azure AD Connect Health agent for AD DS** window, click **Install**.
10. When installation completes, click **Configure Now**.
11. When prompted, sign in as **msnider@adatumyyxxxx.onmicrosoft.com** with password **Pa55w.rd!**. A Windows PowerShell command-line interface window will open.
12. Wait until the configuration completes; you will receive an "Agent registration completed successfully" message. Close the Windows PowerShell window.

13. Switch to Microsoft Internet Explorer, where you have the Azure portal open, click the **Microsoft Azure** link in the top-left corner, and then click the **Azure Active Directory Connect Health** tile.
14. In the **Azure Active Directory Connect Health** pane, scroll down and notice that you now have the **Active Directory Domain Services** tile.
15. Click **Adatum.com** on that tile, and then review the report. Leave the Azure portal open.

Demonstration: Configuring OMS

Demonstration Steps

1. In Microsoft Internet Explorer window on LON-DS1, open a new tab.
2. On the new tab, browse to https://mms.microsoft.com. Sign in with your Microsoft account that is associated with your Azure trial subscription.
3. In the **Microsoft Operations Management Suite** window, click **OK** to create a new OMS workspace.
4. In the **Microsoft Operations Management Suite** window, type **Adatum*XXX***, where *XXX* is the number of your choice, for the **Workspace Name**, and then fill out the rest of the fields with your data.
5. Select the **I agree to the subscription agreement, offer details and privacy statement** check box, and then click **CREATE**. Wait for a minute or two until the workspace is created.
6. On the Link Azure Subscription page, in the Select Azure directory dropdown box, select **Adatum** and then click **LINK**.
7. In the **Microsoft Operations Management Suite** window, click the **Solutions Gallery** tile.
8. In the Solutions Gallery windows, click **Security & Compliance** tile.
9. In the Security & Compliance click **Add**.
10. Click **Settings.**
11. Click the **Connected Sources** tab, click **Windows Servers** and then click **Download Windows Agent (64-bit)**.
12. When prompted, click **Save as**.
13. Create the **C:\temp** folder, and then save the **MMASetup-AMD64.exe** file to the **C:\temp** folder.
14. Open Notepad, click the copy icon next to the **WORKSPACE ID** text box. If prompted, click **Allow access** and then paste the value in Notepad.
15. Click the copy icon next to the **PRIMARY KEY** text box, and then paste the value in Notepad.
16. Save the text file with the workspace ID and Primary key in **C:\temp**.
17. Open File Explorer, browse to **C:\temp**, and then double-click the **MMASetup-AMD64.exe** file. If the Open File – Security Warning window appears, click **Run**.
18. On the **Welcome to the Microsoft Monitoring Agent Setup Wizard** page, click **Next**.
19. On the **Microsoft Software License Terms** page, click **I Agree**.
20. On the **Destination Folder** page, click **Next**.
21. On the **Agent Setup Options** page, select **Connect the agent to Azure Log Analytics (OMS)**, and then click **Next**.
22. On the **Azure Log Analytics** page, paste the values for workspace ID and Workspace Key from Notepad in the appropriate text boxes, and then click **Next**.

23. On the **Microsoft Update** page, if it appears, click **Next**.
24. On the **Ready to install** page, click **Install**.
25. When installation completes, click **Finish**.
26. Restore the Internet Explorer window, where you have the Microsoft Operations Management Suite (OMS) portal open, click the **Data** tab, and then click **Windows Event logs** in the left pane.
27. In the **Collect events from the following event logs** text box, type **System**, and then click the plus sign (**+**) to add.
28. In the **Collect events from the following event logs** text box, type **Application**, and then click the plus sign (**+**) sign to add.
29. Click **Windows Performance counters**. Review performance counters that are selected in the right pane, and then click **Add the selected performance counters**.
30. In the toolbar, click **Save**.
31. In the left toolbar, click the **Home** icon. Wait for a minute or two until the assessment is completed. Refresh the page.
32. Click the **Security and Audit** tile, and then review results. Click **Enable alerts** when prompted and then click **OK**.
33. On the left toolbar, click the **Home** icon.
34. Click the **Log Search** tile. If Search quick tips window appears, close it.
35. In the **Log Search** window, in the **few more queries to try** section, click **Count of all data collected grouped by Type**.
36. In the **Log Search** window, review the results of the query.

Module Review and Takeaways

Best Practices

- If you are not able to use cloud services for AD DS monitoring, we recommend that you use Operations Manager with the AD DS management pack.
- Review Azure AD reports frequently.
- Ensure that at least one Azure AD administrator reviews the notifications that Azure AD provides.
- Use Azure AD Connect Health for directory synchronization monitoring.

Review Question

Question: If you want to check the status of antivirus and antimalware scans on multiple servers, which tool or service should you use?

> **Answer:** You should use OMS with the Malware Assessment solution that is available in the OMS Solutions Gallery.

Common Issues and Troubleshooting Tips

Common Issue	Troubleshooting Tip
The OMS agent that is installed on a locally deployed server cannot communicate with OMS.	Check the firewall on the local computer.

Lab Review Questions and Answers

Lab: Configuring reporting and monitoring

Question and Answers

Question: What should you configure to monitor Azure AD in OMS?

Answer: You should deploy the Office 365 solution from the OMS Solutions Gallery.

Question: What can you monitor with Azure AD Connect Health?

Answer: The primary functionality of Azure AD Connect Health is to monitor syncing between AD DS and Azure AD. However, you can also use it to monitor Active Directory Federation Services (AD FS) and AD DS.