Microsoft

Microsoft Official Course

AZ-900T00

Microsoft Azure Fundamentals

AZ-900T00
Microsoft Azure Fundamentals

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

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

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

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

© 2019 Microsoft Corporation. All rights reserved.

Microsoft and the trademarks listed at **http://www.microsoft.com/trademarks** [1]are trademarks of the Microsoft group of companies. All other trademarks are property of their respective owners.

1 http://www.microsoft.com/trademarks

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

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.**

   1. "Authorized Learning Center" means a Microsoft Imagine Academy (MSIA) Program Member, Microsoft Learning Competency Member, or such other entity as Microsoft may designate from time to time.
   2. "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.
   3. "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.
   4. "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 an MPN Member (defined below), or (iii) a Microsoft full-time employee, a Microsoft Imagine Academy (MSIA) Program Member, or a Microsoft Learn for Educators – Validated Educator.
   5. "Licensed Content" means the content accompanying this agreement which may include the Microsoft Instructor-Led Courseware or Trainer Content.
   6. "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.
   7. "Microsoft Instructor-Led Courseware" means the Microsoft-branded instructor-led training course that educates IT professionals, developers, students at an academic institution, and other learners on Microsoft technologies. A Microsoft Instructor-Led Courseware title may be branded as MOC, Microsoft Dynamics, or Microsoft Business Group courseware.
   8. "Microsoft Imagine Academy (MSIA) Program Member" means an active member of the Microsoft Imagine Academy Program.
   9. "Microsoft Learn for Educators – Validated Educator" means an educator who has been validated through the Microsoft Learn for Educators program as an active educator at a college, university, community college, polytechnic or K-12 institution.
   10. "Microsoft Learning Competency Member" means an active member of the Microsoft Partner Network program in good standing that currently holds the Learning Competency status.
   11. "MOC" means the "Official Microsoft Learning Product" instructor-led courseware known as Microsoft Official Course that educates IT professionals, developers, students at an academic institution, and other learners on Microsoft technologies.
   12. "MPN Member" means an active Microsoft Partner Network program member in good standing.

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

13. "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.
14. "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.
15. "Trainer" means (i) an academically accredited educator engaged by a Microsoft Imagine Academy Program Member to teach an Authorized Training Session, (ii) an academically accredited educator validated as a Microsoft Learn for Educators – Validated Educator, and/or (iii) a MCT.
16. "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.

  1. **If you are a Microsoft Imagine Academy (MSIA) Program Member:**

     1. 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.
     2. 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.
     3. For each license you acquire, you must comply with the following:

        1. you will only provide access to the Licensed Content to those individuals who have acquired a valid license to the Licensed Content,
        2. 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,
        3. 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,

4. 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,
5. 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,
6. you will only deliver a maximum of 15 hours of training per week for each Authorized Training Session that uses a MOC title, and
7. you acknowledge that Trainers that are not MCTs will not have access to all of the trainer resources for the Microsoft Instructor-Led Courseware.

2. **If you are a Microsoft Learning Competency Member:**
   1. Each license acquire 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.
   2. For each license you acquire on behalf of an End User or MCT, 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) MCT with the unique redemption code and instructions on how they can access one (1) Trainer Content.
   3. For each license you acquire, you must comply with the following:
      1. you will only provide access to the Licensed Content to those individuals who have acquired a valid license to the Licensed Content,
      2. 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,
      3. 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,

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

4. you will ensure that each MCT teaching an Authorized Training Session has their own valid licensed copy of the Trainer Content that is the subject of the Authorized Training Session,
5. 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,
6. you will only provide access to the Microsoft Instructor-Led Courseware to End Users, and
7. you will only provide access to the Trainer Content to MCTs.

3. **If you are a MPN Member:**
   1. 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.
   2. 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.
   3. For each license you acquire, you must comply with the following:
      1. you will only provide access to the Licensed Content to those individuals who have acquired a valid license to the Licensed Content,
      2. 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,
      3. 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,
      4. 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,

5. 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,
6. 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,
7. you will only provide access to the Microsoft Instructor-Led Courseware to End Users, and
8. you will only provide access to the Trainer Content to Trainers.

4. **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.

5. **If you are a Trainer.**

1. 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.
2. If you are an MCT, 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.
3. If you elect to exercise the foregoing rights, you agree to comply with the following: (i) customizations may only be used for teaching Authorized Training Sessions and Private Training Sessions, and (ii) all customizations will comply with this agreement. For clarity, any use of "customize" refers only to changing the order of slides and content, and/or not using all the slides or content, it does not mean changing or modifying any slide or content.

- 2.2 **Separation of Components.** The Licensed Content is licensed as a single unit and you may not separate their components and install them on different devices.
- 2.3 **Redistribution of Licensed Content.** Except as expressly provided in the use rights above, you may not distribute any Licensed Content or any portion thereof (including any permitted modifications) to any third parties without the express written permission of Microsoft.
- 2.4 **Third Party Notices.** The Licensed Content may include third party code that Microsoft, not the third party, licenses to you under this agreement. Notices, if any, for the third party code are included for your information only.
- 2.5 **Additional Terms.** Some Licensed Content may contain components with additional terms, conditions, and licenses regarding its use. Any non-conflicting terms in those conditions and licenses also apply to your use of that respective component and supplements the terms described in this agreement.

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

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:

   1. **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.

   2. **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.

   3. **Pre-release Term.** If you are an Microsoft Imagine Academy Program Member, Microsoft Learning Competency Member, MPN Member, Microsoft Learn for Educators – Validated Educator, 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 provided "as is", we are not obligated to 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.**

    1. 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.

    2. 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.**

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

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 contre-façon 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 April 2019

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

Contents

Module 0 Course Introduction 1
About This Course 1

Module 1 Describe core Azure concepts 5
Learning Objectives 5
Introduction to Azure fundamentals 6
Discuss Azure fundamental concepts 23
Describe core Azure architectural components 31
Module 1 Review Questions 41
Module 1 Summary 43

Module 2 Describe core Azure services 47
Learning Objectives 47
Explore Azure database and analytics services 48
Explore Azure compute services 57
Explore Azure Storage services 71
Explore Azure networking services 77
Module 2 Review Questions 91
Module 2 Summary 94

Module 3 Describe core solutions and management tools on Azure 99
Learning Objectives 99
Choose the best AI service for your needs 100
Choose the best tools to help organizations build better solutions 106
Choose the best monitoring service for visibility, insight, and outage mitigation 112
Choose the best tools for managing and configuring your Azure environment 119
Choose the best Azure serverless technology for your business scenario 125
Choose the best Azure IoT service for your application 130
Module 3 Review Questions 137
Module 3 Summary 141

Module 4 Describe general security and network security features 149
Learning Objectives 149
Protect against security threats on Azure 150
Secure network connectivity on Azure 158
Module 4 Review Questions 165
Module 4 Summary 167

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

Module 5 Describe identity, governance, privacy, and compliance features 171
Learning Objectives 171
Secure access to your applications by using Azure identity services 172
Build a cloud governance strategy on Azure 180
Examine privacy, compliance, and data protection standards on Azure 216
Module 5 Review Questions 228
Module 5 Summary 230

Module 6 Describe Azure cost management and service level agreements 235
Learning Objectives 235
Plan and manage your Azure costs 236
Choose the right Azure services by examining SLAs and service lifecycle 257
Module 6 Review Questions 267
Module 6 Summary 269

Module 7 Course Conclusion 273
Summary 273

Module 0 Course Introduction

About This Course

About This Course

Course Description

This course provides foundational level knowledge on cloud concepts; core Azure services; security, privacy, compliance, and trust; and Azure pricing and support.

Level:

Beginner

Audience

The audience for this course is just beginning to learn about cloud computing and how Microsoft Azure provides that service. There are two versions of this course a one day version and a two day version. The content for both courses aligns to the AZ-900 exam objective domain.

- **AZ-900T00**. This two day course provides an Azure pass and time for students to participate in hands-on labs during the course.
- **AZ-900T01**. This one day course does not provide an Azure pass or time for students to participate in hands-on labs during the course.

Prerequisites

There are no prerequisites for this course, however students with some IT knowledge or experience will find the concepts easier to understand.

Expected learning

- The basics of cloud computing and Azure, and how to get started with Azure's subscriptions and accounts.
- The advantages of using cloud computing services, learning to differentiate between the categories and types of cloud computing, and how to examine the various concepts, resources, and terminology that are necessary to work with Azure architecture.
- The core services available with Microsoft Azure.

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

- The core solutions that encompass a wide array of tools and services from Microsoft Azure.
- The general security and network security features, and how you can use the various Azure services to help ensure that your cloud resources are safe, secure, and trusted.
- The identity, governance, privacy, and compliance features, and how Azure can help you secure access to cloud resources, what it means to build a cloud governance strategy, and how Azure adheres to common regulatory and compliance standards.
- The factors that influence cost, tools you can use to help estimate and manage your cloud spend, and how Azure's service-level agreements (SLAs) can impact your application design decisions.

Course Syllabus

Module 1 - Describe core Azure concepts

This module introduces you to the basics of cloud computing and Azure, and how to get started with Azure's subscriptions and accounts. You'll learn about the advantages of using cloud computing services, learn to differentiate between the categories and types of cloud computing, and examine the various concepts, resources, and terminology that are necessary to work with Azure architecture.

- Lesson 1 - Learning Objectives
- Lesson 2 - Introduction to Azure fundamentals
- Lesson 3 - Discuss Azure fundamental concepts
- Lesson 4 - Describe core Azure architectural components
- Lesson 5 - Module 1 Review Questions
- Lesson 6 - Module 1 Summary

Module 2 - Describe core Azure services

In this module, learn about core services available with Microsoft Azure.

- Lesson 1 - Learning Objectives
- Lesson 2 - Explore Azure database and analytics services
- Lesson 3 - Explore Azure compute services
- Lesson 4 - Explore Azure Storage services
- Lesson 5 - Explore Azure networking services
- Lesson 6 - Module 2 Review Questions
- Lesson 7 - Module 2 Summary

Module 3 - Describe core solutions and management tools on Azure

Core solutions encompass a wide array of tools and services from Microsoft Azure. In this module, you'll be introduced to many of these tools and services, and will be asked to help choose the best one for a given business scenario.

- Lesson 1 - Learning Objectives
- Lesson 2 - Choose the best AI service for your needs
- Lesson 3 - Choose the best tools to help organizations build better solutions
- Lesson 4 - Choose the best monitoring service for visibility, insight, and outage mitigation
- Lesson 5 - Choose the best tools for managing and configuring your Azure environment

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

- Lesson 6 - Choose the best Azure serverless technology for your business scenario
- Lesson 7 - Choose the best Azure IoT service for your application
- Lesson 8 - Module 3 Review Questions
- Lesson 9 - Module 3 Summary

Module 4 - Describe general security and network security features

In this module you'll learn about general security and network security features, and learn about how you can use the various Azure services to help ensure that your cloud resources are safe, secure, and trusted.

- Lesson 1 - Learning Objectives
- Lesson 2 - Protect against security threats on Azure
- Lesson 3 - Secure network connectivity on Azure
- Lesson 4 - Module 4 Review Questions
- Lesson 5 - Module 4 Summary

Module 5 - Describe identity, governance, privacy, and compliance features

In this module you'll about identity, governance, privacy, and compliance features. You'll learn how Azure can help you secure access to cloud resources, what it means to build a cloud governance strategy, and how Azure adheres to common regulatory and compliance standards.

- Lesson 1 - Learning Objectives
- Lesson 2 - Secure access to your applications by using Azure identity services
- Lesson 3 - Build a cloud governance strategy on Azure
- Lesson 4 - Examine privacy, compliance, and data protection standards on Azure
- Lesson 5 - Module 5 Review Questions
- Lesson 6 - Module 5 Summary

Module 6 - Describe general security and network security features

Learn about the factors that influence cost, tools you can use to help estimate and manage your cloud spend, and how Azure's service-level agreements (SLAs) can impact your application design decisions.

- Lesson 1 - Learning Objectives
- Lesson 2 - Plan and manage your Azure costs
- Lesson 3 - Choose the right Azure services by examining SLAs and service lifecycle
- Lesson 4 - Module 6 Review Questions
- Lesson 5 - Module 6 Summary

AZ-900 Certification Exam

The **AZ-900, Microsoft Azure Fundamentals,**[1] certification exam is designed for candidates looking to demonstrate foundational level knowledge of cloud services and how those services are provided with Microsoft Azure. The exam is intended for candidates with non-technical backgrounds, such as those involved in selling or purchasing cloud based solutions and services or who have some involvement with cloud based solutions and services, as well as those with a technical background who have a need to

1 https://www.microsoft.com/en-us/learning/exam-AZ-900.aspx

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

validate their foundational level knowledge around cloud services. Technical IT experience is not required however some general IT knowledge or experience would be beneficial.

This exam can be taken as an optional first step in learning about cloud services and how those concepts are exemplified by Microsoft Azure. It can be taken as a precursor to Microsoft Azure or Microsoft cloud services exams. While it would be a beneficial first step, validating foundational level knowledge, taking this exam is not a pre-requisite before taking any other Azure-based certifications.

The exam includes four study areas. The percentages indicate the relative weight of each area on the exam. The higher the percentage, the more questions the exam will contain. Be sure to read the exam page for specifics about what skills are covered in each area.

AZ-900 Study Areas	Weights
Describe cloud concepts	20-25%
Describe Core Azure Services	15-20%
Describe core solutions and management tools on Azure	10-15%
Describe general security and network security features	10-15%
Describe identity, governance, privacy, and compliance features	20-25%
Describe Azure cost management and Service Level Agreements	10-15%

✓ This exam does not include a hands-on testing component.

Accessing Labs

To access the labs for this course, please visit GitHub at https://github.com/MicrosoftLearning/AZ-900T0x-MicrosoftAzureFundamentals/tree/master/Instructions/Walkthroughs.

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

Module 1 Describe core Azure concepts

Learning Objectives

Learning Objectives

After completing this module, you'll be able to:

- Understand the benefits of cloud computing in Azure and how it can save you time and money
- Explain cloud concepts such as high availability, scalability, elasticity, agility, and disaster recovery
- Describe core Azure architecture components such as subscriptions, management groups, resources and resource groups
- Summarize geographic distribution concepts such as Azure regions, region pairs, and availability zones

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

Introduction to Azure fundamentals

Introduction

Microsoft Azure is a cloud computing platform with an ever expanding set of services to help you build solutions to meet your business goals. Azure services range from simple web services for hosting your business presence in the cloud, to running fully virtualized computers for you to run your custom software solutions. Azure provides a wealth of cloud-based services like remote storage, database hosting, centralized account management, and new capabilities like artificial intelligence and Internet of Things (IoT).

In this module, you'll take an entry level end-to-end look at Azure and its capabilities, which will provide you with a solid foundation for completing the available modules for Azure Fundamentals.

Learning objectives

After completing this module, you'll be able to:

- Describe the basic concepts of cloud computing
- Determine whether Azure is the right solution for your business needs
- Differentiate between the different methods of creating an Azure subscription

Prerequisites

- You should be familiar with basic computing concepts and terminology
- Familiarity with cloud computing is helpful, but isn't necessary

What is cloud computing?

If you've ever wondered, “What is cloud computing?” It's the delivery of computing services - including servers, storage, databases, networking, software, analytics, and intelligence over the Internet ("the cloud"). Cloud computing offers faster innovation, flexible resources, and economies of scale.

https://sec.ch9.ms/ch9/875d/c14bd0e3-198e-449b-9303-86829f14875d/CloudComputing_high.mp4

Why is cloud computing typically cheaper to use?

Cloud computing is the delivery of computing services over the Internet using a *pay-as-you-go pricing* model. You typically pay only for cloud services you use, which helps you lower your operating costs, run your infrastructure more efficiently, and scale as your business needs change. To put that another way, cloud computing is a way to rent compute power and storage from someone else's datacenter. You can

treat cloud resources like you would your resources in your own datacenter. When you're done using them, you give them back. You're billed only for what you use.

Instead of maintaining CPUs and storage in your datacenter, you rent them for the time that you need them. The cloud provider takes care of maintaining the underlying infrastructure for you. While this approach is great, the real value of the cloud is that it enables you to quickly solve your toughest business challenges and bring cutting edge solutions to your users.

Why should I move to the cloud?

The cloud helps you move faster and innovate in ways that were once nearly impossible.

In our ever-changing digital world, two trends emerge:

- Teams are delivering new features to their users at record speeds.
- End users expect an increasingly rich and immersive experience with their devices and with software.

Software releases were once scheduled in terms of months or even years. Today, teams are releasing features in smaller batches. Releases are now often scheduled in terms of days or weeks. Some teams even deliver software updates continuously - sometimes with multiple releases within the same day.

Think of all the ways you interact with devices that you couldn't do just a few years ago. Many devices can recognize your face and respond to voice commands. Augmented reality changes the way you interact with the physical world. Household appliances are even beginning to act intelligently. These technologies are just a few examples, many of which are powered by the cloud.

To power your services and deliver innovative and novel user experiences more quickly, the cloud provides on-demand access to:

- A nearly limitless pool of raw compute, storage, and networking components.
- Speech recognition and other cognitive services that help make your application stand out from the crowd.
- Analytics services that enable you to make sense of telemetry data coming back from your software and devices.

What are some cloud computing advantages?

There are several benefits that a cloud environment has over a physical environment. For example, cloud-based applications employ a myriad of related strategies:

- **High availability** - depending on the service-level agreement (SLA) that you choose, your cloud-based applications can provide a continuous user experience with no apparent downtime even when things go wrong
- **Scalability** - applications in the cloud can be scaled two ways:
  - *Vertically* - computing capacity can be increased by adding additional RAM or CPUs to a virtual machine
  - *Horizontally* - computing capacity can be increased by adding instances of a resource, such as adding additional virtual machines to your configuration
- **Elasticity** - cloud-based applications can be configured to take advantage of autoscaling, so your applications will always have the resources they need
- **Agility** - cloud-based resources can be deployed and configured quickly as your application requirements change

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

- **Geo-distribution** - applications and data can be deployed to regional datacenters around the globe, thereby ensuring that your customers always have the best performance in their region
- **Disaster recovery** - by taking advantage of cloud-based backup services, data replication, and geo-distribution, you can deploy your applications with the confidence that comes from knowing that your data is safe in the event that disaster should occur

What are cloud service models?

Clouding computing falls into one of the following computing models. If you've been around cloud computing for a while, you've probably seen the *PaaS*, *IaaS*, and *SaaS* acronyms for the different *cloud service models*, which define the different level of shared responsibility that a cloud provider and cloud tenent are responsible for.

Service Models	Definition	Description
IaaS	*Infrastructure-as-a-Service*	This cloud service model is the closest to managing physical servers; a cloud provider will keep the hardware up-to-date, but operating system maintenance and network configuration is left to the cloud tenent. For example: Azure Virtual Machines are fully operational virtual compute devices running in Microsoft's datacenters. An advantage of this cloud service model is rapid deployment of new compute devices; setting up a new virtual machine is considerably faster than procuring, installing, and configuring a physical server.
PaaS	*Platform-as-a-Service*	This cloud service model is a managed hosting environment, where the cloud provider manages the virtual machines and networking resources, and the cloud tenent deploys their applications into the managed hosting environment. For example: Azure App Services provides a managed hosting environment where developers can upload their web applications, without having to worry about dealing with the physical hardware and software requirements.

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

Service Models	Definition	Description
SaaS	*Software-as-a-Service*	In this cloud service model, the cloud provider manages all aspects of the application environment - virtual machines, networking resources, data storage, applications, and so on - and the cloud tenent only needs to provide their data to the application managed by the cloud provider. For example: Microsoft Office 365 provides a fully working version of Microsoft Office that runs in the cloud; all that you need to do is create your content, and Office 365 takes care of everything else.

The following illustration demonstrates the services that might run in each of the cloud service models.

The following chart illustrates the various levels of responsibility between a cloud provider and a cloud tenent.

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

What is serverless computing?

Overlapping with PaaS, serverless computing enables developers to build applications faster by eliminating the need for them to manage infrastructure. With serverless applications, the cloud service provider automatically provisions, scales, and manages the infrastructure required to run the code. Serverless architectures are highly scalable and event-driven, only using resources when a specific function or trigger occurs.

In understanding the definition of serverless computing, it's important to note that servers are still running the code. The serverless name comes from the fact that the tasks associated with infrastructure provisioning and management are invisible to the developer. This approach enables developers to increase their focus on the business logic and deliver more value to the core of the business. Serverless computing helps teams increase their productivity and bring products to market faster, and it allows organizations to better optimize resources and stay focused on innovation.

What are public, private, and hybrid clouds?

There are three deployment models for cloud computing: *public cloud*, *private cloud*, and *hybrid cloud*. Each deployment model has different aspects that you should consider as you migrate to the cloud.

Deployment model	Description
Public cloud	Services are offered over the public internet and available to anyone who wants to purchase them. Cloud resources - such as servers and storage - are owned and operated by a third-party cloud service provider, and delivered over the internet.
Private cloud	A private cloud consists of computing resources used exclusively by users from one business or organization. A private cloud can be physically located at your organization's on-site datacenter, or it can be hosted by a third-party service provider.
Hybrid cloud	A hybrid cloud is a computing environment that combines a public cloud and a private cloud by allowing data and applications to be shared between them.

The following image illustrates several of the cloud computing concepts that are presented in this unit. In this example, several factors are demonstrated when you are considering where to deploy a database server in a Hybrid cloud environment: as your resources move from on-premises to off-premises, your costs are reduced, and your administration requirements decrease.

What is Azure?

Azure is a continually expanding set of cloud services that help your organization meet your current and future business challenges. Azure gives you the freedom to build, manage, and deploy applications on a massive global network using your favorite tools and frameworks.

What does Azure offer?

With help from Azure, you have everything you need to build your next great solution. The following table lists several of the benefits that Azure provides, so you can easily **Invent with purpose**.

	Be future ready -Continuous innovation from Microsoft supports your development today, and your product visions for tomorrow.
	Build on your terms - You have choices. With a commitment to open source, and support for all languages and frameworks, build how you want, and deploy where you want to.

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

	Operate hybrid seamlessly - On-premises, in the cloud, and at the edge - we'll meet you where you are. Integrate and manage your environments with tools and services designed for hybrid cloud.
	Trust your cloud - Get security from the ground up, backed by a team of experts, and proactive compliance trusted by enterprises, governments, and startups.

What can I do with Azure?

Azure provides over 100 services that enable you to do everything from running your existing applications on virtual machines to exploring new software paradigms such as intelligent bots and mixed reality.

Many teams start exploring the cloud by moving their existing applications to virtual machines that run in Azure. While migrating your existing apps to virtual machines is a good start, the cloud is more than just "a different place to run your virtual machines".

For example, Azure provides AI and machine-learning services that can naturally communicate with your users through vision, hearing, and speech. It also provides storage solutions that dynamically grow to accommodate massive amounts of data. Azure services enable solutions that are not feasible without the power of the cloud.

What is the Azure portal?

The Azure portal is a web-based, unified console that provides an alternative to command-line tools. With the Azure portal, you can manage your Azure subscription using a graphical user interface. You can build, manage, and monitor everything from simple web apps to complex cloud deployments. Create custom dashboards for an organized view of resources. Configure accessibility options for an optimal experience.

The Azure portal is designed for resiliency and continuous availability, and maintains a presence in every Azure datacenter. This configuration makes the Azure portal resilient to individual datacenter failures, and avoids network slow-downs by being close to users. The Azure portal updates continuously and requires no downtime for maintenance activities.

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

What is Azure Marketplace?

Azure Marketplace[1] is a service on Azure that helps connect end users with Microsoft partners, independent software vendors (ISVs), and start-ups that are offering their solutions and services, which are optimized to run on Azure. Azure Marketplace allows customers - mostly IT professionals and cloud developers - to find, try, purchase, and provision applications and services from hundreds of leading service providers, all certified to run on Azure.

1 https://azuremarketplace.microsoft.com?azure-portal=true

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

The solution catalog spans several industry categories, including but not limited to: open-source container platforms, virtual machine images, databases, application build and deployment software, developer tools, threat detection, and blockchain. Using Azure Marketplace, you can provision end-to-end solutions quickly and reliably, hosted in your own Azure environment. At the time of writing, this includes over 8,000 listings.

While Azure Marketplace is designed for IT professionals and cloud developers interested in commercial and IT software, Microsoft Partners also use it as a launch point for all joint Go-To-Market activities.

Tour of Azure services

Azure can help you tackle tough business challenges. You bring your requirements, creativity, and favorite software development tools. Azure brings a massive global infrastructure that's always available for you to build your applications on.

Let's take a quick tour of the high-level services Azure offers.

Azure services

Here's a big-picture view of the available services and features in Azure.

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

Let's take a closer look at the most commonly used categories:

• Compute • Networking • Storage • Mobile • Databases	• Web • Internet of Things • Big data • Artificial intelligence • DevOps

Compute

Compute services are often one of the primary reasons why companies move to the Azure platform. Azure provides a range of options for hosting applications and services. Here are some examples of compute services in Azure:

Service name	Service function
Azure Virtual Machines	Windows or Linux virtual machines (VMs) hosted in Azure
Azure Virtual Machine Scale Sets	Scaling for Windows or Linux VMs hosted in Azure
Azure Kubernetes Service	Enables management of a cluster of VMs that run containerized services
Azure Service Fabric	Distributed systems platform. Runs in Azure or on-premises
Azure Batch	Managed service for parallel and high-performance computing applications
Azure Container Instances	Run containerized apps on Azure without provisioning servers or VMs

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

Service name	Service function
Azure Functions	An event-driven, serverless compute service

Networking

Linking compute resources and providing access to applications is the key function of Azure networking. Networking functionality in Azure includes a range of options to connect the outside world to services and features in the global Microsoft Azure datacenters.

Here are some examples of networking services in Azure:

Service name	Service function
Azure Virtual Network	Connects VMs to incoming Virtual Private Network (VPN) connections
Azure Load Balancer	Balances inbound and outbound connections to applications or service endpoints
Azure Application Gateway	Optimizes app server farm delivery while increasing application security
Azure VPN Gateway	Accesses Azure Virtual Networks through high-performance VPN gateways
Azure DNS	Provides ultra-fast DNS responses and ultra-high domain availability
Azure Content Delivery Network	Delivers high-bandwidth content to customers globally
Azure DDoS Protection	Protects Azure-hosted applications from distributed denial of service (DDOS) attacks
Azure Traffic Manager	Distributes network traffic across Azure regions worldwide
Azure ExpressRoute	Connects to Azure over high-bandwidth dedicated secure connections
Azure Network Watcher	Monitors and diagnoses network issues using scenario-based analysis
Azure Firewall	Implements high-security, high-availability firewall with unlimited scalability
Azure Virtual WAN	Creates a unified wide area network (WAN), connecting local and remote sites

Storage

Azure provides four main types of storage services. These services are:

Service name	Service function
Azure Blob storage	Storage service for very large objects, such as video files or bitmaps
Azure File storage	File shares that you can access and manage like a file server
Azure Queue storage	A data store for queuing and reliably delivering messages between applications

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

Service name	Service function
Azure Table storage	A NoSQL store that hosts unstructured data independent of any schema

These services all share several common characteristics:

- **Durable** and highly available with redundancy and replication.
- **Secure** through automatic encryption and role-based access control.
- **Scalable** with virtually unlimited storage.
- **Managed**, handling maintenance and any critical problems for you.
- **Accessible** from anywhere in the world over HTTP or HTTPS.

Mobile

Azure enables developers to create mobile backend services for iOS, Android, and Windows apps quickly and easily. Features that used to take time and increase project risks, such as adding corporate sign-in and then connecting to on-premises resources such as SAP, Oracle, SQL Server, and SharePoint, are now simple to include.

Other features of this service include:

- Offline data synchronization.
- Connectivity to on-premises data.
- Broadcasting push notifications.
- Autoscaling to match business needs.

Databases

Azure provides multiple database services to store a wide variety of data types and volumes. And with global connectivity, this data is available to users instantly.

Service name	Service function
Azure Cosmos DB	Globally distributed database that supports NoSQL options
Azure SQL Database	Fully managed relational database with auto-scale, integral intelligence, and robust security
Azure Database for MySQL	Fully managed and scalable MySQL relational database with high availability and security
Azure Database for PostgreSQL	Fully managed and scalable PostgreSQL relational database with high availability and security
SQL Server on VMs	Host enterprise SQL Server apps in the cloud
Azure Synapse Analytics	Fully managed data warehouse with integral security at every level of scale at no extra cost
Azure Database Migration Service	Migrates your databases to the cloud with no application code changes
Azure Cache for Redis	Caches frequently used and static data to reduce data and application latency

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

Service name	Service function
Azure Database for MariaDB	Fully managed and scalable MariaDB relational database with high availability and security

Web

Having a great web experience is critical in today's business world. Azure includes first-class support to build and host web apps and HTTP-based web services. The Azure services focused on web hosting include:

Service Name	Description
Azure App Service	Quickly create powerful cloud web-based apps
Azure Notification Hubs	Send push notifications to any platform from any back end.
Azure API Management	Publish APIs to developers, partners, and employees securely and at scale.
Azure Cognitive Search	Fully managed search as a service.
Web Apps feature of Azure App Service	Create and deploy mission-critical web apps at scale.
Azure SignalR Service	Add real-time web functionalities easily.

Internet of Things (IoT)

People are able to access more information than ever before. It began with personal digital assistants (PDAs), then morphed into smartphones. Now there are smart watches, smart thermostats, even smart refrigerators. Personal computers used to be the norm. Now the internet allows any item that's online-capable to access valuable information. This ability for devices to garner and then relay information for data analysis is referred to as the Internet of Things (IoT).

There are a number of services that can assist and drive end-to-end solutions for IoT on Azure.

Service Name	Description
IoT Central	Fully-managed global IoT software as a service (SaaS) solution that makes it easy to connect, monitor, and manage your IoT assets at scale
Azure IoT Hub	Messaging hub that provides secure communications between and monitoring of millions of IoT devices
IoT Edge	Push your data analysis models directly onto your IoT devices, allowing them to react quickly to state changes without needing to consult cloud-based AI models.

Big data

Data comes in all formats and sizes. When we talk about big data, we're referring to *large* volumes of data. Data from weather systems, communications systems, genomic research, imaging platforms, and many other scenarios generate hundreds of gigabytes of data. This amount of data makes it hard to analyze and make decisions. It's often so large that traditional forms of processing and analysis are no longer appropriate.

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

Open source cluster technologies have been developed to deal with these large data sets. Microsoft Azure supports a broad range of technologies and services to provide big data and analytic solutions.

Service Name	Description
Azure Synapse Analytics	Run analytics at a massive scale using a cloud-based Enterprise Data Warehouse (EDW) that leverages massive parallel processing (MPP) to run complex queries quickly across petabytes of data
Azure HDInsight	Process massive amounts of data with managed clusters of Hadoop clusters in the cloud
Azure Databricks	Collaborative Apache Spark-based analytics service that can be integrated with other big data services in Azure.

Artificial intelligence

Artificial intelligence, in the context of cloud computing, is based around a broad range of services, the core of which is machine learning. Machine learning is a data science technique that allows computers to use existing data to forecast future behaviors, outcomes, and trends. Using machine learning, computers learn without being explicitly programmed.

Forecasts or predictions from machine learning can make apps and devices smarter. For example, when you shop online, machine learning helps recommend other products you might like based on what you've purchased. Or when your credit card is swiped, machine learning compares the transaction to a database of transactions and helps detect fraud. And when your robot vacuum cleaner vacuums a room, machine learning helps it decide whether the job is done.

Some of the most common artificial intelligence and machine learning service types in Azure are:

Service Name	Description
Azure Machine Learning Service	Cloud-based environment you can use to develop, train, test, deploy, manage, and track machine learning models. It can auto-generate a model and auto-tune it for you. It will let you start training on your local machine, and then scale out to the cloud
Azure Machine Learning Studio	Collaborative, drag-and-drop visual workspace where you can build, test, and deploy machine learning solutions using pre-built machine learning algorithms and data-handling modules

A closely related set of products are the *cognitive services*. These are pre-built APIs you can leverage in your applications to solve complex problems.

Service Name	Description
Vision	Image-processing algorithms to smartly identify, caption, index, and moderate your pictures and videos.
Speech	Convert spoken audio into text, use voice for verification, or add speaker recognition to your app.

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

Service Name	Description
Knowledge mapping	Map complex information and data in order to solve tasks such as intelligent recommendations and semantic search.
Bing Search	Add Bing Search APIs to your apps and harness the ability to comb billions of webpages, images, videos, and news with a single API call.
Natural Language processing	Allow your apps to process natural language with pre-built scripts, evaluate sentiment and learn how to recognize what users want.

DevOps

DevOps (Development and Operations) brings together people, processes, and technology, automating software delivery to provide continuous value to your users. Azure DevOps Services allows you to create *build* and *release* pipelines that provide continuous integration, delivery, and deployment for your applications. You can integrate repositories and application tests, perform application monitoring, and work with build artifacts. You can also work with and backlog items for tracking, automate infrastructure deployment and integrate a range of third-party tools and services such as Jenkins and Chef. All of these functions and many more are closely integrated with Azure to allow for consistent, repeatable deployments for your applications to provide streamlined build and release processes.

Some of the main DevOps services available with Azure are Azure DevOps Services and Azure DevTest Labs.

Service Name	Description
Azure DevOps	Azure DevOps Services (formerly known as Visual Studio Team Services, or VSTS), provides development collaboration tools including high-performance pipelines, free private Git repositories, configurable Kanban boards, and extensive automated and cloud-based load testing
Azure DevTest Labs	Quickly create on-demand Windows and Linux environments you can use to test or demo your applications directly from your deployment pipelines

Get started with Azure accounts

To create and use Azure services, you need an Azure subscription. When you are completing modules on Microsoft Learn, most of the time a temporary subscription is created for you, which runs in an environment called the *Microsoft Learn Sandbox*. However, when you are working with your own applications and business needs, you need to create an Azure account, and a subscription will be created for you. Once you've created an Azure account, you are free to create additional subscriptions; for example: your company might use a single Azure account for your business, and separate subscriptions for development, marketing, and sales departments. Once you have created an Azure subscription, you can start creating Azure resources within each subscription.

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

If you're new to Azure, you can sign up for a free account on the Azure website to start exploring at no cost to you. Once you're ready, you can choose to upgrade your free account and create a new subscription that enables you to start paying for Azure services you need to use that are beyond the limits of a free account.

How to create an Azure account

You can purchase Azure access directly from Microsoft by signing up on the **Azure website**[2], or through a Microsoft representative. You can also purchase Azure access through a Microsoft partner. Cloud Solution Provider partners offer a range of complete managed-cloud solutions for Azure.

What is the Azure free account?

The Azure free account includes free access to popular Azure products for 12 months, a credit to spend for the first 30 days, and access to more than 25 products that are always free. The Azure free account is an excellent way for new users to get started and explore. To sign up, you need a phone number, a credit card, and a Microsoft or GitHub account. The credit card information is used for identity verification only; you won't be charged for any services until you upgrade to a paid subscription.

Case study introduction

Throughout the Azure Fundamentals, we'll be working with a fictional company named **Tailwind Traders**[3], a fictitious home improvement retailer. They operate retail hardware stores across the globe and online.

2 https://azure.microsoft.com/?azure-portal=true
3 https://www.tailwindtraders.com/?azure-portal=true

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

Tailwind Traders currently manages an on-premises datacenter that hosts the company's retail website, and stores all of the data and streaming video for its applications. The IT department is currently responsible for all of management tasks for their computing hardware and software. For example, let's suppose that you work as an Information Technology (IT) specialist for the company's IT department. Your IT team handles the procurement process to buy new hardware, installs and configures software, and deploys everything throughout the datacenter.

However, these management responsibilities create numerous obstacles for delivering your applications to your users in a timely fashion. As a technology professional, you realize that it would be advantageous to have servers, storage, databases, and other services immediately available when developing and deploying applications. You should be able to click a button to start up a new server or add services to your solutions.

You've learned about some of the cloud-based services that Tailwind Traders can use to address each of their technology challenges. With that in mind, the services that are available through Microsoft Azure can help Tailwind Traders conduct its business more efficiently.

As you complete the various modules in the Azure Fundamentals, we'll analyze the challenges that Tailwind Traders is facing, and how you can Microsoft Azure services to address each of those issues as they arise. When you've completed each of the modules, the knowledge that you will have gained from resolving the hypothetical challenges that the fictional Tailwind Traders company was encountering should benefit you in your real world environments.

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

Discuss Azure fundamental concepts

Introduction

You work in the IT department for Tailwind Traders, which has decided to migrate their applications and data to Microsoft Azure. You're aware that cloud computing will save your company time and money by migrating from your existing on-premises physical hardware to a cloud solution, where you will only need to pay for the resources and computing time that you use.

However, some of the cloud computing concepts are new to many of your IT staff members, and they've been asking some specific questions about what cloud computing can do for them. For example, the team that manages Tailwind Traders' website would like to know how Azure will improve their availability and scalability, whereas the team that handles the deployment of new hardware is curious to see how cloud computing can make their deployment processes faster. In addition, your developer team would like to learn about the different options that will be available to them as they are designing new applications. For example, is there a way to run their applications in a hybrid configuration, where part of their application runs on-premises and the rest of the application runs in the cloud?

In this module, you'll learn about the fundamental concepts of cloud computing, how Azure implements these concepts, and how Tailwind Traders might benefit from migrating to a cloud computing environment.

Learning objectives

Upon completion of this module, you'll be able to:

- Identify the benefits and considerations of using cloud services
- Describe the differences between categories of cloud services
- Describe the differences between types of cloud computing

Prerequisites

- You should be familiar with basic computing concepts and terminology
- Familiarity with cloud computing is helpful, but isn't necessary

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

Describe the benefits of cloud computing

What are some cloud computing advantages?

There are several advantages that a cloud environment has over a physical environment that Tailwind Traders can utilize following its migration to Azure.

- **High Availability** - depending on the service-level agreement (SLA) that you choose, your cloud-based applications can provide a continuous user experience with no apparent downtime even when things go wrong
- **Scalability** - applications in the cloud can be scaled two ways:
  - *Vertically* - computing capacity can be increased by adding additional RAM or CPUs to a virtual machine
  - *Horizontally* - computing capacity can be increased by adding instances of a resource, such as adding additional virtual machines to your configuration
- **Elasticity** - cloud-based applications can be configured to take advantage of autoscaling, so your applications will always have the resources they need
- **Agility** - cloud-based resources can be deployed and configured quickly as your application requirements change
- **Geo-distribution** - applications and data can be deployed to regional datacenters around the globe, thereby ensuring that your customers always have the best performance in their region
- **Disaster Recovery** - by taking advantage of cloud-based backup services, data replication, and geo-distribution, you can deploy your applications with the confidence that comes from knowing that your data is safe in the event that disaster should occur

Cloud computing is a consumption-based model

Cloud service providers operate on a **consumption-based model**, which means that end users only pay for the resources that they use. Whatever they use is what they pay for.

A consumption-based model has many benefits, including:

- No upfront costs.
- No need to purchase and manage costly infrastructure that they may or may not use to its fullest.
- The ability to pay for additional resources when they are needed.
- The ability to stop paying for resources that are no longer needed.

Capital expenses versus operating expenses

There are two different types of expenses that you should consider:

- **Capital Expenditure (CapEx)** is the up front spending of money on physical infrastructure, and then deducting that up front expense over time. The up front cost from CapEx has a value that reduces over time.
- **Operational Expenditure (OpEx)** is spending money on services or products now and being billed for them now. You can deduct this expense in the same year you spend it. There is no up front cost, as you pay for a service or product as you use it.

In other words, when Tailwind Traders owns its infrastructure, it buys equipment that goes onto its balance sheets as assets. Because a capital investment was made, accountants categorize this transaction as a *Capital Expense* (CapEx). Over time, to account for the assets' limited useful lifespan, assets are depreciated or amortized.

Cloud services, on the other hand, are categorized as an *Operating Expense* (OpEx), because of their consumption model. Under this scheme, there is no asset for Tailwind Traders to amortize, and its cloud service provider (Azure) manages the costs that are associated with the purchase and lifespan of the physical equipment. As a result, OpEx has a direct impact on net profit, taxable income, and the associated expenses on the balance sheet.

To summarize, CapEx requires significant up-front financial costs, as well ongoing maintainence and support expenditures. Whereas OpEx is a consumption-based model, so Tailwind Traders is only responsible for the cost of the computing resources that it uses.

Describe the different categories of cloud services

What are cloud service models?

Clouding computing falls into one of the following computing models. If you've been around cloud computing for a while, you've probably seen the *PaaS*, *IaaS*, and *SaaS* acronyms for the different *cloud service models*, which define the different level of shared responsibility that a cloud provider and cloud tenent are responsible for.

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

Service Model	Definition	Description
IaaS	*Infrastructure-as-a-Service*	This cloud service model is the closest to managing physical servers; a cloud provider will keep the hardware up-to-date, but operating system maintenance and network configuration is left to the cloud tenent. For example: Azure Virtual Machines are fully operational virtual compute devices running in Microsoft's datacenters. An advantage of this cloud service model is rapid deployment of new compute devices; setting up a new virtual machine is considerably faster than procuring, installing, and configuring a physical server.
PaaS	*Platform-as-a-Service*	This cloud service model is a managed hosting environment, where the cloud provider manages the virtual machines and networking resources, and the cloud tenent deploys their applications into the managed hosting environment. For example: Azure App Services provides a managed hosting environment where developers can upload their web applications, without having to worry about dealing with the physical hardware and software requirements.

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

Service Model	Definition	Description
SaaS	*Software-as-a-Service*	In this cloud service model, the cloud provider manages all aspects of the application environment - virtual machines, networking resources, data storage, applications, and so on - and the cloud tenent only needs to provide their data to the application managed by the cloud provider. For example: Microsoft Office 365 provides a fully working version of Microsoft Office that runs in the cloud; all that you need to do is create your content, and Office 365 takes care of everything else.

The following illustration demonstrates the services that might run in each of the cloud service models.

Each of these three models will be compared in the following sections.

Infrastructure-as-a-Service (IaaS)

IaaS is the most flexible category of cloud services. It aims to give you complete control over the hardware that runs your application. Instead of buying hardware, with IaaS, you rent it.

Advantages

No CapEx. Users have no upfront costs.

Agility. Applications can be made accessible quickly, and deprovisioned whenever needed.

Management. The shared responsibility model applies; the user manages and maintains the services they have provisioned, and the cloud provider manages and maintains the cloud infrastructure.

Consumption-based model. Organizations pay only for what they use and operate under an OpEx model.

Skills. No deep technical skills are required to deploy, use, and gain the benefits of a public cloud. Organizations can leverage the skills and expertise of the cloud provider to ensure workloads are secure, safe, and highly available.

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

Cloud benefits. Organizations can leverage the skills and expertise of the cloud provider to ensure workloads are made secure and highly available.

Flexibility. IaaS is the most flexible cloud service as you have control to configure and manage the hardware running your application.

Platform-as-a-Service (PaaS)

PaaS provides the same benefits and considerations as IaaS, but there are some additional benefits to be aware of.

Advantages

No CapEx. Users have no upfront costs.

Agility. PaaS is more agile than IaaS, and users do not need to configure servers for running applications.

Platform limitations. There may be some limitations to a cloud platform that could affect how an application runs. Any limitations should be taken into consideration when considering which PaaS platform is best suited for a workload.

Consumption-based model. Users pay only for what they use, and operate on an OpEx model.

Skills. No deep technical skills are required to deploy, use, and gain the benefits of PaaS.

Cloud benefits. Users can leverage the skills and expertise of the cloud provider to ensure their workloads are made secure and highly available. In addition, users can gain access to more cutting-edge development tools and toolsets. They then can apply these tools and toolsets across an application's lifecycle.

Productivity. Users can focus on application development only, as all platform management is handled by the cloud provider. Working with distributed teams as services is easier, as the platform is accessed over the internet and can be made globally available more easily.

Disadvantage

Platform limitations. There can be some limitations to a cloud platform that might affect how an application runs. When you're evaluating which PaaS platform is best suited for a workload, be sure to consider any limitations in this area.

Software-as-a-Service (SaaS)

SaaS is software that's centrally hosted and managed for you and your users or customers. Usually one version of the application is used for all customers, and it's licensed through a monthly or annual subscription.

SaaS provides the same benefits as IaaS, but again there are some additional benefits to be aware of too.

Advantages

No CapEx. Users have no upfront costs.

Agility. Users can provide staff with access to the latest software quickly and easily.

Software limitations. There may be some limitations to a software application that might affect how users work. Since you are using as-is software you don't have direct control of features. Any business

needs and software limitations should be taken into consideration when considering which SaaS platform is best suited for a workload.

Pay-as-you-go pricing model. Users pay for the software they use on a subscription model, typically monthly or yearly, regardless of how much they use the software.

Skills. No deep technical skills are required to deploy, use, and gain the benefits of PaaS.

Flexibility. Users can access the same application data from anywhere.

Disadvantage

Software limitations. There can be some limitations to a software application that might affect how users work. Because you're using as-is software, you don't have direct control of features. When you're evaluating which SaaS platform is best suited for a workload, be sure to consider any business needs and software limitations.

What is serverless computing?

Overlapping with PaaS, serverless computing enables developers to build applications faster by eliminating the need for them to manage infrastructure. With serverless applications, the cloud service provider automatically provisions, scales, and manages the infrastructure required to run the code. Serverless architectures are highly scalable and event-driven, only using resources when a specific function or trigger occurs.

In understanding the definition of serverless computing, it's important to note that servers are still running the code. The serverless name comes from the fact that the tasks associated with infrastructure provisioning and management are invisible to the developer. This approach enables developers to increase their focus on the business logic and deliver more value to the core of the business. Serverless computing helps teams increase their productivity and bring products to market faster, and it allows organizations to better optimize resources and stay focused on innovation.

Describe the different types of cloud computing

What are Public, Private, and Hybrid clouds?

There are three deployment models for cloud computing: *public cloud*, *private cloud*, and *hybrid cloud*. Each deployment model has different aspects that you should consider as you migrate to the cloud.

Deployment Model	Description
Public cloud	Services are offered over the public internet and available to anyone who wants to purchase them. Cloud resources - such as servers and storage - are owned and operated by a third-party cloud service provider, and delivered over the internet.
Private cloud	A private cloud consists of computing resources used exclusively by users from one business or organization. A private cloud can be physically located at your organization's on-site (on-premises) datacenter, or it can be hosted by a third-party service provider.

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

Deployment Model	Description
Hybrid cloud	A hybrid cloud is a computing environment that combines a public cloud and a private cloud by allowing data and applications to be shared between them.

The following image illustrates several of the cloud computing concepts that are presented in this unit. In this example, several factors are demonstrated when you are considering where to deploy a database server in a Hybrid cloud environment: as your resources move from on-premises to off-premises, your costs are reduced, and your administration requirements decrease.

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

Describe core Azure architectural components

Introduction

Let's say that you work as a developer for a successful hardware manufacturing company, Tailwind Traders. Your company's Chief Technology Officer (CTO) recently decided to adopt Microsoft Azure as the cloud computing platform, and you are currently in the planning stages for the migration. Before you begin the migration process, you decide to study the various Azure concepts, resources, and terminology in order to ensure that your migration is a success.

In this module, you'll learn about several of the components that are necessary to successfully deploy resources on Microsoft Azure.

Learning objectives

After completing this module, you'll be able to describe the benefits and usage of:

- Azure Subscriptions and Management Groups
- Azure Resources, Resource Groups, and the Azure Resource Manager
- Azure Regions, Region Pairs, and Availability zones

Prerequisites

- You should be familiar with basic computing concepts and terminology
- Familiarity with cloud computing is helpful, but isn't necessary

Overview of Azure subscriptions, management groups, resources, and regions

As part of your research for Tailwind Traders, you need to learn the organizing structure for resources in Azure, which has four levels: **management groups**, **subscriptions**, **resource groups**, and **resources**.

The following image shows the top-down hierarchy of organization for these levels.

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

Having seen the top-down hierarchy of organization, let's describe each of those levels from the bottom up:

- **Resources**: Resources are instances of services that you create, like virtual machines, storage, or SQL databases.
- **Resource groups**: Resources are combined into resource groups, which act as a logical container into which Azure resources like web apps, databases, and storage accounts are deployed and managed.
- **Subscriptions**: A subscription groups together user accounts and the resources that have been created by those user accounts. For each subscription, there are limits or quotas on the amount of resources that you can create and use. Organizations can use subscriptions to manage costs and the resources that are created by users, teams, or projects.
- **Management groups**: These groups help you manage access, policy, and compliance for multiple subscriptions. All subscriptions in a management group automatically inherit the conditions applied to the management group.

You'll examine each of these four organizational levels next.

Azure subscriptions and management groups

As Tailwind Traders gets started with Azure, one of your first steps will be to create at least one **Azure Subscription**, which you will use to create your cloud-based resources in Azure.

Note: An Azure *resource* is a manageable item that is available through Azure. Virtual machines, storage accounts, web apps, databases, and virtual networks are all examples of resources.

Azure subscriptions

Using Azure requires an Azure subscription which provides you with authenticated and authorized access to Azure products and services and allows you to provision resources. An Azure subscription is a logical unit of Azure services that links to an Azure account, which is an identity in Azure Active Directory (Azure AD) or in a directory that an Azure AD trusts.

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

An account can have one subscription or multiple subscriptions that have different billing models and to which you apply different access-management policies. You can use Azure subscriptions to define boundaries around Azure products, services, and resources. There are two types of subscription boundaries that you can use, including:

- **Billing boundary**. This subscription type determines how an Azure account is billed for using Azure. You can create multiple subscriptions for different types of billing requirements, and Azure will generate separate billing reports and invoices for each subscription so that you can organize and manage costs.
- **Access control boundary**. Azure will apply access-management policies at the subscription level, and you can create separate subscriptions to reflect different organizational structures. An example is that within a business, you have different departments to which you apply distinct Azure subscription policies. This allows you to manage and control access to the resources that users provision with specific subscriptions.

Create additional Azure subscriptions

You might want to create additional subscriptions for resource or billing management purposes. For example, you might choose to create additional subscriptions to separate:

- **Environments:** When managing your resources, you can choose to create subscriptions to set up separate environments for development and testing, security, or to isolate data for compliance reasons. This is particularly useful because resource access control occurs at the subscription level.
- **Organizational structures:** You can create subscriptions to reflect different organizational structures. For example, you could limit a team to lower-cost resources, while allowing the IT department a full range. This design allows you to manage and control access to the resources that users provision within each subscription.
- **Billing:** You might want to also create additional subscriptions for billing purposes. Because costs are first aggregated at the subscription level, you might want to create subscriptions to manage and track costs based on your needs. For instance, you might want to create a subscription for your production workloads and another subscription for your development and testing workloads.

You might also need additional subscriptions due to:

- **Subscription limits:** Subscriptions are bound to some hard limitations. For example, the maximum number of Express Route circuits per subscription is 10. Those limits should be considered as you create subscriptions on your account. If there is a need to go over those limits in particular scenarios, then you might need additional subscriptions.

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

Customize billing to meet your needs

If you have multiple subscriptions, you can organize them into invoice sections. Each invoice section is a line item on the invoice that shows the charges incurred that month. For example, you might need a single invoice for your organization but want to organize charges by department, team, or project.

Depending on your needs, you can set up multiple invoices within the same billing account. To do this, create additional billing profiles. Each billing profile has its own monthly invoice and payment method.

The following diagram shows an overview of how billing is structured. If you've previously signed up for Azure or if your organization has an Enterprise Agreement, your billing might be set up differently.

Azure management groups

If your organization has many subscriptions, you may need a way to efficiently manage access, policies, and compliance for those subscriptions. Azure management groups provide a level of scope above subscriptions. You organize subscriptions into containers called “management groups” and apply your governance conditions to the management groups. All subscriptions within a management group automatically inherit the conditions applied to the management group. Management groups give you enterprise-grade management at a large scale no matter what type of subscriptions you might have. All subscriptions within a single management group must trust the same Azure Active Directory tenant.

For example, you can apply policies to a management group that limits the regions available for virtual machine (VM) creation. This policy would be applied to all management groups, subscriptions, and resources under that management group by only allowing VMs to be created in that region.

Hierarchy of management groups and subscriptions

You can build a flexible structure of management groups and subscriptions to organize your resources into a hierarchy for unified policy and access management. The following diagram shows an example of creating a hierarchy for governance using management groups.

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

You can create a hierarchy that applies a policy, for example, which limits VM locations to the US West Region in the group called "Production". This policy will inherit onto all the Enterprise Agreement (EA) subscriptions that are descendants of that management group and will apply to all VMs under those subscriptions. This security policy cannot be altered by the resource or subscription owner allowing for improved governance.

Another scenario where you would use management groups is to provide user access to multiple subscriptions. By moving multiple subscriptions under that management group, you can create one role-based access control (RBAC) assignment on the management group, which will inherit that access to all the subscriptions. One assignment on the management group can enable users to have access to everything they need instead of scripting RBAC over different subscriptions.

Important facts about management groups

- 10,000 management groups can be supported in a single directory.
- A management group tree can support up to six levels of depth. (This limit doesn't include the Root level or the subscription level.)
- Each management group and subscription can only support one parent.
- Each management group can have many children.
- All subscriptions and management groups are within a single hierarchy in each directory.

Azure resources and Azure Resource Manager

After you have created a subscription for Tailwind Traders, you're ready to start creating resources and storing those in resource groups. With that in mind, it's important to define those terms:

- **Resource** - A manageable item that is available through Azure. Virtual machines, storage accounts, web apps, databases, and virtual networks are examples of resources.
- **Resource group** - A container that holds related resources for an Azure solution. The resource group includes those resources that you want to manage as a group. You decide which resources belong in a resource group based on what makes the most sense for your organization.

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

Azure resource groups

Resource groups are a fundamental element of the Azure platform. A resource group is a logical container for resources deployed on Azure. These resources are anything you create in an Azure subscription like virtual machines, Application Gateways, and CosmosDB instances. All resources must be in a resource group and a resource can only be a member of a single resource group. Many resources can be moved between resource groups with some services having specific limitations or requirements to move. Resource groups can't be nested. Before any resource can be provisioned, you need a resource group for it to be placed in.

Logical grouping

Resource groups exist to help manage and organize your Azure resources. By placing resources of similar usage, type, or location, you can provide some order and organization to resources you create in Azure. Logical grouping is the aspect that you're most interested in here, since there's a lot of disorder among our resources.

Life cycle

If you delete a resource group, all resources contained within are also deleted. Organizing resources by life cycle can be useful in non-production environments, where you might try an experiment, but then dispose of it when done. Resource groups make it easy to remove a set of resources at once.

Authorization

Resource groups are also a scope for applying role-based access control (RBAC) permissions. By applying RBAC permissions to a resource group, you can ease administration and limit access to allow only what is needed.

Azure Resource Manager

Azure Resource Manager is the deployment and management service for Azure. It provides a management layer that enables you to create, update, and delete resources in your Azure account. You use management features, like access control, locks, and tags, to secure and organize your resources after deployment.

When a user sends a request from any of the Azure tools, APIs, or SDKs, Resource Manager receives the request. It authenticates and authorizes the request. Resource Manager sends the request to the Azure service, which takes the requested action. Because all requests are handled through the same API, you see consistent results and capabilities in all the different tools.

The following image shows the role Azure Resource Manager plays in handling Azure requests.

All capabilities that are available in the portal are also available through PowerShell, Azure CLI, REST APIs, and client SDKs. Functionality initially released through APIs will be represented in the portal within 180 days of initial release.

The benefits of using Azure Resource Manager

With Azure Resource Manager, you can:

- Manage your infrastructure through declarative templates rather than scripts. An Azure Resource Manager template is a JSON file that define what you want to deploy to Azure.
- Deploy, manage, and monitor all the resources for your solution as a group, rather than handling these resources individually.
- Redeploy your solution throughout the development lifecycle and have confidence your resources are deployed in a consistent state.
- Define the dependencies between resources so they're deployed in the correct order.
- Apply access control to all services because Role-Based Access Control (RBAC) is natively integrated into the management platform.
- Apply tags to resources to logically organize all the resources in your subscription.
- Clarify your organization's billing by viewing costs for a group of resources sharing the same tag.

Azure regions and availability zones

In the previous unit, you learned about Azure resources and resource groups. Resources are created in **Regions**, which are different geographical locations around the globe that contain Azure datacenters. Microsoft Azure is made up of datacenters located around the globe. When you leverage a service or create a resource such as a SQL database or virtual machine, you are using physical equipment in one or more of these locations. These specific datacenters aren't exposed to end users directly; instead, Azure organizes them into *regions*. As you will see later in this unit, some of these regions offer **Availability Zones**, which are different Azure datacenters within that region.

Azure regions

A **region** is a geographical area on the planet containing at least one, but potentially multiple data-centers that are nearby and networked together with a low-latency network. Azure intelligently assigns and controls the resources within each region to ensure workloads are appropriately balanced.

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

When you deploy a resource in Azure, you will often need to choose the region where you want your resource deployed.

Important: *Some services or virtual machine features are only available in certain regions, such as specific virtual machine sizes or storage types. There are also some global Azure services that do not require you to select a particular region, such as Microsoft Azure Active Directory, Microsoft Azure Traffic Manager, and Azure DNS.*

A few examples of regions are *West US*, *Canada Central*, *West Europe*, *Australia East*, and *Japan West*. Here's a view of all the available regions as of February 2020:

Why are regions important?

Azure has more global regions than any other cloud provider. These regions give you the flexibility to bring applications closer to your users no matter where they are. It also provides better scalability, redundancy, and preserves data residency for your services.

Special Azure regions

Azure has specialized regions that you might want to use when building out your applications for compliance or legal purposes. A few examples include:

- *US DoD Central*, *US Gov Virginia*, *US Gov Iowa* and more: These regions are physical and logical network-isolated instances of Azure for US government agencies and partners. These datacenters are operated by screened US persons and include additional compliance certifications.
- *China East*, *China North* and more: These regions are available through a unique partnership between Microsoft and 21Vianet, whereby Microsoft does not directly maintain the datacenters.

Regions are what you use to identify the location for your resources, but there are two other terms you should also be aware of: *geographies* and *availability zones*.

Azure availability zones

You want to ensure your services and data are redundant so you can protect your information in case of failure. When you are hosting your infrastructure, setting up your own redundancy requires creating duplicate hardware environments. Azure can help make your app highly available through *Availability Zones*.

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

What is an availability zone?

Availability Zones are physically separate datacenters within an Azure region. Each Availability Zone is made up of one or more datacenters equipped with independent power, cooling, and networking. It is set up to be an *isolation boundary*. If one zone goes down, the other continues working. Availability Zones are connected through high-speed, private fiber-optic networks.

Supported regions

Not every region has support for Availability Zones. For an updated list, see **Regions that support Availability Zones in Azure**[4].

Using availability zones in your apps

You can use Availability Zones to run mission-critical applications and build high-availability into your application architecture by co-locating your compute, storage, networking, and data resources within a zone and replicating in other zones. Keep in mind that there could be a cost to duplicating your services and transferring data between zones.

Availability Zones are primarily for VMs, managed disks, load balancers, and SQL databases. Azure services that support Availability Zones fall into two categories:

- **Zonal services** - you pin the resource to a specific zone (for example, virtual machines, managed disks, IP addresses)
- **Zone-redundant services** - platform replicates automatically across zones (for example, zone-redundant storage, SQL Database).

Check the documentation to determine which elements of your architecture you can associate with an Availability Zone.

4 https://docs.microsoft.com/azure/availability-zones/az-region?azure-portal=true

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

Azure region pairs

Availability zones are created using one or more datacenters, and there is a minimum of three zones within a single region. However, it's possible that a large enough disaster could cause an outage large enough to affect even two datacenters. That's why Azure also creates *region pairs*.

What is a region pair?

Each Azure region is always paired with another region within the same geography (such as US, Europe, or Asia) at least **300 miles away**. This approach allows for the replication of resources (such as virtual machine storage) across a geography that helps reduce the likelihood of interruptions due to events such as natural disasters, civil unrest, power outages, or physical network outages affecting both regions at once. If a region in a pair was affected by a natural disaster, for instance, services would automatically fail over to the other region in its region pair.

Examples of region pairs in Azure are West US paired with East US, and SouthEast Asia paired with East Asia.

Since the pair of regions is directly connected and far enough apart to be isolated from regional disasters, you can use them to provide reliable services and data redundancy. Some services offer automatic geo-redundant storage using region pairs.

Additional advantages of region pairs include:

- If there's an extensive Azure outage, one region out of every pair is prioritized to make sure at least one is restored as quick as possible for applications hosted in that region pair.
- Planned Azure updates are rolled out to paired regions one region at a time to minimize downtime and risk of application outage.
- Data continues to reside within the same geography as its pair (except for Brazil South) for tax and law enforcement jurisdiction purposes.

Having a broadly distributed set of datacenters allows Azure to provide a high guarantee of availability.

Module 1 Review Questions

Module 01 Review Questions

Review Question 1

Which of the following statements is not true about cloud computing?

- ☐ Cloud computing resources are usually limited to specific geographic regions.
- ☐ IaaS, PaaS, and SaaS are examples of cloud computing service models.
- ☐ IaaS, PaaS, and SaaS are common cloud computing service models and are respectively infrastructure as a service, platform as a service, and software as a service.

Review Question 2

True or false: You need to purchase an Azure account before you can use any Azure resources.

- ☐ False
- ☐ True

Review Question 4

True or false: In an IaaS environment, the cloud tenant is responsible for routine hardware maintenance.

- ☐ True
- ☐ False

Review Question 5

Which of the following choices isn't a cloud computing category?

- ☐ Platform-as-a-Service (PaaS)
- ☐ Networking-as-a-Service (NaaS)
- ☐ Infrastructure-as-a-Service (IaaS)
- ☐ Software-as-a-Service (SaaS)

Review Question 6

Which of the following options isn't a type of cloud computing?

- ☐ Hybrid cloud
- ☐ Private cloud
- ☐ Public cloud
- ☐ Distributed cloud

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

Review Question 7

Which of the following choices isn't a benefit of using cloud services?

- ☐ Scalability
- ☐ Disaster recovery
- ☐ Geographic isolation
- ☐ High availability

Review Question 8

Which of the following can be used to manage governance across multiple Azure subscriptions?

- ☐ Management groups
- ☐ Azure initiatives
- ☐ Resource groups

Review Question 9

Which of the following is a logical unit of Azure services that links to an Azure account?

- ☐ Management group
- ☐ Resource group
- ☐ Azure subscription

Review Question 10

Which of the following features doesn't apply to resource groups?

- ☐ Using Azure doesn't require a subscription.
- ☐ An Azure subscription is a logical unit of Azure services.
- ☐ You can't have more than one subscription.

Review Question 11

Which of the following statements is true?

- ☐ With Operating Expenses (OpEx), you are only responsible for the computing resources that you use.
- ☐ With Operating Expenses (OpEx), you are responsible for purchasing and maintaining your computing resources.
- ☐ With Capital Expenses (CapEx), you are only responsible for the computing resources that you use.

Module 1 Summary

Module 01 Summary

Introduction to Azure fundamentals

In this lesson, you were introduced to the basics of cloud computing and Azure, and how to get started with Azure's subscriptions and accounts.

You learned how to:

- Describe the basic concepts of cloud computing
- Determine whether Azure is the right solution for their business needs
- Differentiate between the different methods of creating an Azure subscription

Discuss Azure fundamental concepts

In this lesson, you learned how Tailwind Traders can take advantage of several cloud computing features, which will help them reduce their overall computing costs. You examined several of the benefits that clouding computing provides - such as high availability, scalability, and geographic distribution - and you compared the differences between capital expenses and operating expenses in a cloud computing scenario. Lastly, you learned about the different categories (IaaS, PaaS, SaaS) and types (public, private, and hybrid) of cloud computing. Armed with this new knowledge, you can help Tailwind Traders migrate successfully to Azure.

Describe core Azure architectural components

In this lesson, you learned the concepts and terminology for several of the core Azure architecture components. Armed with this new knowledge, you have the basic level of understanding for Azure architecture that you will need to make Tailwind Traders successful as they migrate to the cloud.

You learned how to describe the benefits and usage of:

- Azure Subscriptions and Management Groups
- Azure Resources, Resource Groups, and the Azure Resource Manager
- Azure Regions, Region Pairs, and Availability zones

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

Answers

Review Question 1

Which of the following statements is *not* true about cloud computing?

- ■ Cloud computing resources are usually limited to specific geographic regions.
- ☐ IaaS, PaaS, and SaaS are examples of cloud computing service models.
- ☐ IaaS, PaaS, and SaaS are common cloud computing service models and are respectively infrastructure as a service, platform as a service, and software as a service.

Explanation
Most cloud computing resources can be distributed to global datacenters.

Review Question 2

True or false: You need to purchase an Azure account before you can use any Azure resources.

- ■ False
- ☐ True

Explanation
You can use a free Azure account or a Microsoft Learn sandbox to create resources.

Review Question 4

True or false: In an IaaS environment, the cloud tenant is responsible for routine hardware maintenance.

- ■ True
- ☐ False

Explanation
In an IaaS environment, the cloud provider is responsible for any hardware maintenance.

Review Question 5

Which of the following choices isn't a cloud computing category?

- ☐ Platform-as-a-Service (PaaS)
- ■ Networking-as-a-Service (NaaS)
- ☐ Infrastructure-as-a-Service (IaaS)
- ☐ Software-as-a-Service (SaaS)

Explanation
NaaS isn't a cloud computing category.

Review Question 6

Which of the following options isn't a type of cloud computing?

- ☐ Hybrid cloud
- ☐ Private cloud
- ☐ Public cloud
- ■ Distributed cloud

Explanation
A distributed cloud isn't a valid type of cloud computing.

Review Question 7

Which of the following choices isn't a benefit of using cloud services?

- ☐ Scalability
- ☐ Disaster recovery
- ■ Geographic isolation
- ☐ High availability

Explanation
You can choose to create resources in a single region; however, one of the primary advantages to cloud computing is geographic distribution.

Review Question 8

Which of the following can be used to manage governance across multiple Azure subscriptions?

- ■ Management groups
- ☐ Azure initiatives
- ☐ Resource groups

Explanation
Management groups facilitate the hierarchical ordering of Azure resources into collections, at a level of scope above subscriptions. Distinct governance conditions can be applied to each management group, with Azure Policy and Azure role-based access controls, to manage Azure subscriptions effectively. The resources and subscriptions assigned to a management group automatically inherit the conditions applied to the management group.

Review Question 9

Which of the following is a logical unit of Azure services that links to an Azure account?

- ☐ Management group
- ☐ Resource group
- ■ Azure subscription

Explanation
An Azure subscription is a logical unit of Azure services that links to an Azure account.

Review Question 10

Which of the following features doesn't apply to resource groups?

- ☐ Using Azure doesn't require a subscription.
- ■ An Azure subscription is a logical unit of Azure services.
- ☐ You can't have more than one subscription.

Explanation
A subscription is a set of Azure services bundled together for tracking and billing purposes.

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

Review Question 11

Which of the following statements is true?

- ■ With Operating Expenses (OpEx), you are only responsible for the computing resources that you use.
- ☐ With Operating Expenses (OpEx), you are responsible for purchasing and maintaining your computing resources.
- ☐ With Capital Expenses (CapEx), you are only responsible for the computing resources that you use.

Explanation
With Operating Expenses (OpEx), you are only responsible for the computing resources that you use.

Module 2 Describe core Azure services

Learning Objectives

Learning Objectives

After completing this module, you'll be able to:

- Understand the breadth of services available in Azure including compute, network, storage, and database
- Identify virtualization services such as Azure Virtual Machines, Azure Container Instances, Azure Kubernetes Service, and Windows Virtual Desktop
- Compare Azure's database services such as Azure Cosmos DB, Azure SQL, Azure Database for MySQL, Azure Database for PostgreSQL, and Azure's big data and analysis services
- Examine Azure networking resources such as Virtual Networks, VPN Gateways, and Azure Express-Route
- Summarize Azure storage services such Azure Blob Storage, Azure Disk Storage, and Azure File Storage

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

Explore Azure database and analytics services

Introduction

Due to a growing number of acquisitions over the last decade, Tailwind Traders uses a variety of database and analytics technologies. As they begin to migrate existing data workloads and deploy new data workloads to Azure, they need to understand which Azure technology will be appropriate for each workload. As a database administrator for Tailwind Traders, you have been tasked by your company's Chief Technology Officer (CTO) to research the different database options that are available, and help your company choose the right options for each of your data scenarios.

Today's applications are required to be highly responsive and always online. To achieve low latency and high availability, instances of these applications need to be deployed in datacenters that are close to their users. Applications need to respond in real time to large changes in usage at peak hours, store ever increasing volumes of data, and make this data available to users in milliseconds. To help your company reach its goals, Azure's database services are globally distributed, and Azure supports many of the industry standard databases and APIs.

In this module, you'll learn about several of the primary database services that are available on Azure, and you'll analyze some of the reasons why each of these database services might be the right choice for you needs.

Learning objectives

After completing this module, you'll be able to describe the benefits and usage of:

- Azure Cosmos DB
- Azure SQL Database
- Azure Database for MySQL
- Azure Database for PostgreSQL
- Azure Synapse Analytics
- Azure HDInsight
- Azure Databricks
- Azure Data Lake Analytics

Prerequisites

- You should be familiar with basic computing concepts and terminology
- Familiarity with cloud computing is helpful, but isn't necessary
- You should be familiar with basic database concepts and terminology

Explore Azure Cosmos DB

Over the years, Tailwind Traders has acquired several smaller companies. Each of these companies had teams of developers who used different database services and various APIs to work with their data. While a long term plan might be to eventually move all of the disparate data to a common database service, for now you'd like to enable each of these teams to work with an environment where they can leverage their existing skillsets. Fortunately for you, Azure's Cosmos DB can help out.

Azure Cosmos DB supports schema-less data, which lets you build highly responsive and Always On applications to support constantly changing data. You can use this feature to store data that is updated and maintained by users around the world.Azure Cosmos DB is Microsoft's globally distributed, multi-model database service. With a click of a button, Cosmos DB enables you to elastically and independently scale throughput and storage across any number of Azure regions worldwide. You can elastically scale throughput and storage, and take advantage of fast, single-digit-millisecond data access using any one of several popular APIs. Cosmos DB provides comprehensive service level agreements (SLAs) for throughput, latency, availability, and consistency guarantees, something no other database service offers.

For example, Tailwind Traders provides a public training portal that is used by customers across the globe to learn about the different tools that Tailwind Traders creates, and the data is maintained and updated by Tailwind Traders' developers. The following illustration shows a sample Azure Cosmos DB database that's used to store data for Tailwind Traders training portal website.

Azure Cosmos DB makes a great choice in a variety of scenarios because it is flexible. At the lowest level, Azure Cosmos DB stores data in atom-record-sequence (ARS) format. The data is then abstracted and projected as an API, which you specify when you are creating your database. Your choices include SQL, MongoDB, Cassandra, Tables, and Gremlin. This level of flexibility means that as you migrate your company's databases to Azure Cosmos DB, your developers can stick with the API where they're most comfortable.

Explore Azure SQL Database

Azure SQL Database is a relational database that is based on the latest stable version of the Microsoft SQL Server database engine. SQL Database is a high-performance, reliable, fully managed and secure database. You can use it to build data-driven applications and websites in the programming language of your choice without needing to manage infrastructure.

SQL features

Azure SQL Database is a fully managed platform as a service (PaaS) database engine that handles most of the database management functions such as upgrading, patching, backups, and monitoring without user involvement. Azure SQL Database is always running on the latest stable version of the SQL Server data-

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

base engine and patched OS with 99.99% availability. PaaS capabilities that are built into Azure SQL Database enable you to focus on the domain-specific database administration and optimization activities that are critical for your business. SQL Database is a fully managed service that has built-in high availability, backups, and other common maintenance operations. Microsoft handles all patching and updating of the SQL and operating system code; you don't have to manage the underlying infrastructure.

With Azure SQL Database, you can create a highly available and high-performance data storage layer for the applications and solutions in Azure. SQL Database can be the right choice for a variety of modern cloud applications because it enables you to process both relational data and non-relational structures, such as graphs, JSON, spatial, and XML.

Since Azure SQL Database is based on the latest stable version of the Microsoft SQL Server database engine, you can use advanced query processing features, such as high-performance in-memory technologies and intelligent query processing. In fact, the newest capabilities of SQL Server are released first to SQL Database, and then to SQL Server itself. You get the newest SQL Server capabilities with no overhead for patching or upgrading, tested across millions of databases.

SQL migration

Tailwind Traders currently uses several on-premises SQL servers, which provide data storage for your public-facing website (for example: customer data, order history, product catalogs, and so on.) In addition, your on-premises SQL servers also provide data storage for your internal-only training portal website that Tailwind Traders uses for new employee training materials (for example: study materials, certification details, training transcripts, and so on.) The following illustration shows the types of data that your company might store in the Azure SQL database training portal website.

You can migrate your existing SQL Server databases with minimal downtime using the Azure Database Migration Service. The Microsoft Data Migration Assistant can generate assessment reports that provide recommendations to help guide you through required changes prior to performing a migration. Once you assess and resolve any remediation required, you're ready to begin the migration process. The Azure Database Migration Service performs all of the required steps. You just change the connection string in your apps.

Exercise - Create a SQL database

In this walkthrough, we will create a SQL database in Azure and then query the data in that database.

Task 1: Create the database.

In this task, we will create a new SQL database using the AdventureWorksLT sample database.

Task 2: Query the database.

In this task, we will configure the SQL server and run a SQL query.

Congratulations! You have created a SQL database in Azure and successfully queried the data in that database.

Note: To avoid additional costs, you can remove this resource group. Search for resource groups, click your resource group, and then click **Delete resource group**. Verify the name of the resource group and then click **Delete**. Monitor the **Notifications** to see how the delete is proceeding.

Explore Azure database for MySQL

Tailwind Traders currently manages several websites on-premises that use the LAMP stack (Linux, Apache, MySQL, PHP). As part of your planning for your migration strategy, the different teams at Tailwind Traders have been researching the available service offerings that Azure provides. You've already discovered that Azure Web Apps provides built in functionality to create web applications that use PHP on a Linux server running Apache, and you've been tasked with investigating whether the database needs for the web development team will continue to be met after the migration to Azure.

The good news is, the Azure Database for MySQL is a relational database service in the Microsoft cloud, which is based on the MySQL Community Edition database engine, versions 5.6, 5.7, and 8.0. Azure's industry leading 99.99% availability service level agreement (SLA), powered by a global network of Microsoft-managed datacenters, helps keep your app running 24/7. With every Azure Database for MySQL server, you take advantage of built-in security, fault tolerance, and data protection that you would otherwise have to buy or design, build, and manage. With Azure Database for MySQL, you can use point-in-time restore to recover a server to an earlier state, as far back as 35 days.

Azure Database for MySQL delivers:

- Built-in high availability with no additional cost.
- Predictable performance, using inclusive pay-as-you-go pricing.
- Scale as needed within seconds.
- Secured to protect sensitive data at-rest and in-motion.
- Automatic backups and point-in-time-restore for up to 35 days.
- Enterprise-grade security and compliance.

These capabilities require almost no administration and all are provided at no additional cost. They allow you to focus on rapid app development and accelerating your time to market rather than allocating precious time and resources to managing virtual machines and infrastructure. In addition, you can migrate your existing MySQL databases with minimal downtime using the Azure Database Migration Service. Once you have completed your migration, you can continue to develop your application with the open-source tools and platform of your choice to deliver with the speed and efficiency your business demands, all without having to learn new skills.

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

The Azure Database for MySQL service offers several service tiers, and each tier offers different performance and capabilities to support lightweight to heavyweight database workloads. You can build your first app on a small database for a few dollars a month, and then adjust the scale to meet the needs of your solution. Dynamic scalability enables your database to transparently respond to rapidly changing resource requirements. You only pay for the resources you need, and only when you need them.

Explore Azure Database for PostgreSQL

As part of its overall data strategy, Tailwind Traders has been using PostgreSQL for several years. As existing PostgreSQL users, you may already know the benefits of PostgreSQL. Part of your migration is to use Azure Database for PostgreSQL, and you want to make sure that you'll have access to the same benefits as your on-premises server before moving to the cloud.

Azure Database for PostgreSQL is a relational database service in the Microsoft cloud. The server software is based on the community version of the open-source PostgreSQL database engine. Your familiarity with tools and expertise with PostgreSQL is applicable when using Azure Database for PostgreSQL.

Moreover, Azure Database for PostgreSQL delivers the following benefits:

- Built-in high availability compared to on-premises resources. There is no additional configuration, replication, or cost required to make sure your applications are always available.
- Simple and flexible pricing. You have predictable performance based on a selected pricing tier choice that includes software patching, automatic backups, monitoring, and security.
- Scale up or down as needed within seconds. You can scale compute or storage independently as needed, to make sure you adapt your service to match usage.
- Adjustable automatic backups and point-in-time-restore for up to 35 days.
- Enterprise-grade security and compliance to protect sensitive data at-rest and in-motion that covers data encryption on disk and SSL encryption between client and server communication.

Azure Database for PostgreSQL is available in two deployment options: **Single Server** and **Hyperscale (Citus)**.

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

Azure Database for PostgreSQL - Single Server	Azure Database for PostgreSQL - Hyperscale (Citus)
The Single Server deployment option delivers: • Built-in high availability with no additional cost (99.99% SLA) • Predictable performance, using inclusive pay-as-you-go pricing • Vertical scale as needed within seconds • Monitoring and alerting to assess your server • Enterprise-grade security and compliance • Secured to protect sensitive data at-rest and in-motion • Automatic backups and point-in-time-restore for up to 35 days All those capabilities require almost no administration, and all are provided at no additional cost. They allow you to focus on rapid application development and accelerating your time to market, rather than spending precious time and resources to manage virtual machines and infrastructure. You can continue to develop your application with the open-source tools and platform of your choice, without having to learn new skills. The Single Server deployment option offers three pricing tiers: Basic, General Purpose, and Memory Optimized. Each tier offers different resource capabilities to support your database workloads. You can build your first app on a small database for a few dollars a month, and then adjust the scale to meet the needs of your solution. Dynamic scalability enables your database to transparently respond to rapidly changing resource requirements. You only pay for the resources you need, and only when you need them.	The Hyperscale (Citus) option horizontally scales queries across multiple machines using sharding. Its query engine parallelizes incoming SQL queries across these servers for faster responses on large datasets. It serves applications that require greater scale and performance, generally workloads that are approaching -- or already exceed -- 100 GB of data. The Hyperscale (Citus) deployment option delivers: • Horizontal scaling across multiple machines using sharding • Query parallelization across these servers for faster responses on large datasets • Excellent support for multi-tenant applications, real time operational analytics, and high throughput transactional workloads Applications built for PostgreSQL can run distributed queries on Hyperscale (Citus) with standard connection libraries and minimal changes.

Explore big data and analytics

Several years ago, Tailwind Traders rolled out a new GPS tracking system for all of their delivery vehicles, which provides real-time tracking data to your primary datacenter. Your CTO would like your team to look at several years of tracking data in order to determine trends, such as a spike in deliveries around the holidays that would require hiring additional headcount. Through an in-depth analysis of the tracking data that you've recorded, your CTO would like predict when changes are necessary and proactively take the steps that are necessary to manage spikes appropriately.

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

Data comes in all types of forms and formats. When we talk about big data, we're referring to *large* volumes of data. In this Tailwind Traders scenario, data is collected from the GPS sensors, which includes location information, data from weather systems, and many other sources that generate large amounts of data. This amount of data becomes increasingly hard to make sense of and make decisions around. The volumes are so large that traditional forms of processing and analysis are no longer appropriate.

Open source cluster technologies have been developed, over time, to try to deal with these large data sets. Microsoft Azure supports a broad range of technologies and services to provide big data and analytic solutions. Some of the most common big data and analytic service types in Azure are Azure Synapse Analytics, HDInsight, Databricks, and Data Lake Analytics.

Azure Synapse Analytics **Azure Synapse Analytics** *(https://docs.microsoft.com/azure/sql-data-warehouse/?azure-portal=true)* (formerly Azure SQL Data Warehouse) is a limitless analytics service that brings together enterprise data warehousing and Big Data analytics. Azure Synapse gives you the freedom to query data on your terms, using either serverless or provisioned resources at scale. Azure Synapse brings these two worlds together with a unified experience to ingest, prepare, manage, and serve data for immediate BI and machine learning needs.	

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

	Azure HDInsight **Azure HDInsight** *(https://azure.microsoft.com/services/hdinsight/?azure-portal=true)* is a fully managed, open-source analytics service for enterprises. It is a cloud service that makes it easier, faster, and more cost-effective to process massive amounts of data. HDInsight allows you to run popular open-source frameworks and create cluster types such as **Apache Spark** *(https://docs.microsoft.com/azure/hdinsight/spark/apache-spark-overview?azure-portal=true)*, **Apache Hadoop** *(https://docs.microsoft.com/azure/hdinsight/hadoop/apache-hadoop-introduction?azure-portal=true)*, **Apache Kafka** *(https://docs.microsoft.com/azure/hdinsight/kafka/apache-kafka-introduction?azure-portal=true)*, **Apache HBase** *(https://docs.microsoft.com/azure/hdinsight/hbase/apache-hbase-overview?azure-portal=true)*, **Apache Storm** *(https://docs.microsoft.com/azure/hdinsight/storm/apache-storm-overview?azure-portal=true)*, **Machine Learning Services** *(https://docs.microsoft.com/azure/hdinsight/r-server/r-server-overview?azure-portal=true)*. HDInsight also supports a broad range of scenarios such as extraction, transformation, and loading (ETL); data warehousing; machine learning; and IoT.
Azure Databricks **Azure Databricks** *(https://azure.microsoft.com/services/databricks/?azure-portal=true)* helps you unlock insights from all your data and build artificial intelligence (AI) solutions. You can set up your Apache Spark™ environment in minutes, then autoscale and collaborate on shared projects in an interactive workspace. Azure Databricks supports Python, Scala, R, Java, and SQL, as well as data science frameworks and libraries including TensorFlow, PyTorch, and scikit-learn.	

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

	Azure Data Lake Analytics **Azure Data Lake Analytics** *(https://azure.microsoft.com/services/data-lake-analytics/?azure-portal=true)* is an on-demand analytics job service that simplifies big data. Instead of deploying, configuring, and tuning hardware, you write queries to transform your data and extract valuable insights. The analytics service can handle jobs of any scale instantly by setting the dial for how much power you need. You only pay for your job when it is running, making it more cost-effective.

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

Explore Azure compute services

Introduction

Imagine that you work as a development lead at Tailwind Traders, a company that specializes in hardware manufacturing. Your management team tells you that the company's website has been having a difficult time keeping up with the application demands, and they want you to investigate a solution. The front-end webservers are operating near capacity during peak periods of the day, and time is of the essence to get a solution in place. But there's a problem: you don't have any free servers to scale out your application.

Of course, you could ask to buy new equipment, but your department's budget is tight. And even if you were able to procure several servers, you'd need to invest a lot of time to set them up and install software. Plus, you don't want to buy more hardware than needed, not only because you want to make a good impression with leadership, but also because you just don't know how many servers are necessary for this project.

Ideally, you'd obtain the resources you need to do the work without too much administration, and configure them to do the work. In addition, you'd pay only for the compute resources you need while you're using them.

This scenario is exactly what you can do in Azure. You can create compute resources, configure them to do the work that is needed, and pay for only what you use.

Learning objectives

After completing this module, you'll be able to describe the benefits and usage of:

- Azure Virtual Machines (VMs)
- Azure App Services
- Azure Container Instances (ACI)
- Azure Kubernetes Service (AKS)
- Azure Functions
- Windows Virtual Desktop

Prerequisites

- You should be familiar with basic computing concepts and terminology
- Familiarity with cloud computing is helpful, but isn't necessary

Overview of Azure compute services

Azure compute is an on-demand computing service for running cloud-based applications. It provides computing resources such as disks, processors, memory, networking and operating systems. The resourc-

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

es are available on-demand and can typically be made available in minutes or even seconds. You pay only for the resources you use, and only for as long as you're using them.

Azure supports a wide range of computing solutions for development and testing, running applications, and extending your datacenter, including Linux, Windows Server, Microsoft SQL Server, Oracle, IBM, and SAP. Azure also has many services that can run virtual machines, each providing different options depending on your requirements. Some of the most prominent services are Virtual Machines, Container Instances, App Services, and Functions (or *serverless computing*).

Virtual machines Virtual machines (VMs) are software emulations of physical computers. They include a virtual processor, memory, storage, and networking resources. VMs host an operating system, and you're able to install and run software just like a physical computer. When using a remote desktop client, you can use and control the virtual machine as if you were sitting in front it. **Azure virtual machines** *(https://azure.microsoft.com/services/virtual-machines/?azure-portal=true)* let you create and use virtual machines in the cloud. It provides IaaS and can be used in a variety of different ways. When you need total control over an operating system and environment, Azure VMs are an ideal choice. Just like a physical computer, you're able to customize all the software running on the VM. This ability is helpful when you are running custom software or custom hosting configurations.	

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

	Virtual machine scale sets **Virtual machine scale sets** *(https://azure.microsoft.com/services/virtual-machine-scale-sets?azure-portal=true)* are an Azure compute resource that you can use to deploy and manage a set of identical VMs. With all VMs configured the same, virtual machine scale sets are designed to support true autoscale; no pre-provisioning of VMs is required; and as such makes it easier to build large-scale services targeting big compute, big data, and containerized workloads. So, as demand goes up more virtual machine instances can be added, and as demand goes down virtual machines instances can be removed. The process can be manual, automated, or a combination of both.
Containers and Kubernetes **Azure Container Instances** *(https://azure.microsoft.com/services/container-instances?azure-portal=true)* and **Azure Kubernetes Service (AKS)** *(https://azure.microsoft.com/services/kubernetes-service?azure-portal=true)* are Azure compute resources that you can use to deploy and manage containers, which are lightweight, virtualized application environments that are designed to be quickly created, scaled out, and stopped dynamically. You can run multiple instances of a containerized application on a single host machine.	

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

	App Services With **App Services** *(https://azure.microsoft.com/services/app-service?azure-portal=true)*, you can quickly build, deploy, and scale enterprise-grade web, mobile, and API apps running on any platform. You can meet rigorous performance, scalability, security, and compliance requirements while using a fully managed platform to perform infrastructure maintenance. App Services is a platform as a service (PaaS) offering.
Functions **Azure Functions** *(https://azure.microsoft.com/services/functions?azure-portal=true)* are ideal when you're concerned only about the code running your service and not the underlying platform or infrastructure. They're commonly used when you need to perform work in response to an event (often via a REST request), timer, or message from another Azure service, and when that work can be completed quickly, within seconds or less.	

When to use Azure Virtual Machines

One possible solution to Tailwind Traders' lack of physical servers is through the use of virtual machines.

Azure Virtual Machines (VMs) let you create and use virtual machines in the cloud. They provide Infrastructure as a Service (IaaS) in the form of a virtualized server and can be used in many ways. Just like a physical computer, you can customize all of the software running on the VM. VMs are an ideal choice when you need:

- Total control over the operating system (OS)
- The ability to run custom software, or
- To use custom hosting configurations

An Azure VM gives you the flexibility of virtualization without having to buy and maintain the physical hardware that runs the VM. However, you still need to configure, update, and maintain the software that runs on the VM.

You can create and provision a VM in minutes when you select a pre-configured VM image. Selecting an image is one of the most important decisions you'll make when creating a VM. An image is a template used to create a VM. These templates already include an OS and often other software, like development tools or web hosting environments.

Examples of when to use virtual machines

- During testing and development. VMs provide a quick and easy way to create different OS and application configurations. Test and development personnel can then easily delete the VMs when they no longer need them.
- When running applications in the cloud. The ability to run certain applications in the public cloud as opposed to creating a traditional infrastructure to run them can provide substantial economic benefits. For example, if an application needs to handle fluctuations in demand, being able to shut down VMs when you don't need them or quickly start them up to meet a suddenly increased demand means you pay only for the resources you use.
- When extending your datacenter to the cloud. An organization can extend the capabilities of its own on-premises network by creating a virtual network in Azure and adding VMs to that virtual network. Applications like SharePoint can then run on an Azure VM instead of running locally, making it easier or less expensive to deploy than in an on-premises environment.
- During disaster recovery. As with running certain types of applications in the cloud and extending an on-premises network to the cloud, you can get significant costs savings by using an IaaS-based approach to disaster recovery. If a primary datacenter fails, you can create VMs running on Azure to run your critical applications and then shut them down when the primary datacenter becomes operational again.

Moving to the cloud with VMs

VMs are also an excellent choice when moving from a physical server to the cloud (“lift and shift”). You can create an image of the physical server and host it within a VM with little or no changes. Just like a physical on-premises server, you must maintain the VM. You update the installed OS and the software it runs.

Scaling VMs in Azure

You can run single VMs for testing, development, or minor tasks; or you can group VMs together to provide high availability, scalability, and redundancy. Azure has several features such that, no matter what your uptime requirements are, Azure can meet them. These features include:

- Virtual Machine Scale Sets
- Azure Batch

What are virtual machine scale sets?

Azure Virtual Machine Scale Sets let you create and manage a group of identical, load balanced VMs. Imagine you're running a website that enables scientists to upload astronomy images that need to be processed. If you duplicated the VM, you'd normally need to configure an additional service to route

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

requests between multiple instances of the website. Virtual Machine Scale Sets could do that work for you.

Scale sets allow you to centrally manage, configure, and update a large number of VMs in minutes to provide highly available applications. The number of VM instances can automatically increase or decrease in response to demand or a defined schedule. With Virtual Machine Scale Sets, you can build large-scale services for areas such as compute, big data, and container workloads.

What is Azure Batch?

Azure Batch enables large-scale parallel and high-performance computing (HPC) batch jobs with the ability to scale to tens, hundreds, or thousands of VMs.

When you're ready to run a job, Batch does the following:

- Starts a pool of compute VMs for you
- Installs applications and staging data
- Runs jobs with as many tasks as you have
- Identifies failures
- Requeues work
- Scales down the pool as work completes

There may be situations in which you need raw computing power or supercomputer level compute power. Azure provides these capabilities.

When to use Azure Container Instances or Azure Kubernetes Service

While virtual machines are an excellent way to reduce costs versus the investments that are necessary for physical hardware, they are still limited to a single operating system per virtual machine. If you wish to run multiple instances of an application on a single host machine, containers are an excellent choice.

What are containers?

Containers are a virtualization environment, and much like running multiple virtual machines on a single physical host, you can run multiple containers on a single physical or virtual host. However, unlike virtual machines, you do not manage the operating system for a container. Whereas virtual machines appear to be an instance of an operating system that you can connect to and manage, containers are lightweight and are designed to be created, scaled out, and stopped dynamically. While it is possible to create and deploy virtual machines as application demand increases, containers are designed to allow you to respond to changes on demand, and quickly restart in case of a crash or hardware interruption. One of the most popular container engines is Docker, which is supported by Microsoft Azure.

Comparing virtual machines to containers

The following video highlights several of the important differences between virtual machines and containers.

https://www.microsoft.com/videoplayer/embed/RE2yuaq

Managing containers

Containers are managed through a container orchestrator, which can start, stop, and scale out application instances as needed. There are two ways to manage both Docker and Microsoft-based containers in Azure: *Azure Container Instances* and *Azure Kubernetes Service*.

Azure Container Instances (ACI) **Azure Container Instances** *(https://azure.microsoft.com/services/container-instances?azure-portal=true)* offers the fastest and simplest way to run a container in Azure without having to manage any virtual machines or adopt any additional services. It is a PaaS offering that allows you to upload your containers, which it will run for you.	
Azure Kubernetes Service (AKS) The task of automating, managing, and interacting with a large number of containers is known as orchestration. **Azure Kubernetes Service (AKS)** *(https://azure.microsoft.com/services/kubernetes-service?azure-portal=true)* is a complete orchestration service for containers with distributed architectures and large volumes of containers. Orchestration is the task of automating and managing a large number of containers and how they interact.	

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

What is Kubernetes?

The following video discusses some important details about Kubernetes container orchestration.

https://www.microsoft.com/videoplayer/embed/RE2yEuX

Use containers in your solutions

Containers are often used to create solutions using a *microservice architecture*. This architecture is where you break solutions into smaller, independent pieces. For example, you may split a website into a container hosting your front end, another hosting your back end, and a third for storage. This split allows you to separate portions of your app into logical sections that can be maintained, scaled, or updated independently.

Imagine your website backend has reached capacity but the front end and storage aren't being stressed. You could scale the back end separately to improve performance, or you could decide to use a different storage service, or you could even replace the storage container without affecting the rest of the application.

What is a microservice?

The following video discusses some important details about microservices.

https://www.microsoft.com/videoplayer/embed/RE2yual

When to use Azure App Service

In your research for Tailwind Traders so far, you've looked at two different ways that you can virtualize your application. However, another alternative is to deploy your application's front-end websites to Azure App Service, which makes it easy to respond to application demand.

Azure App Service enables you to build and host web apps, background jobs, mobile backends, and RESTful APIs in the programming language of your choice without managing infrastructure. It offers automatic scaling and high availability. App Service supports both Windows and Linux, and enables automated deployments from GitHub, Azure DevOps, or any Git repo to support a continuous deployment model.

This Platform as a Service (PaaS) allows you to focus on the website and API logic while Azure handles the infrastructure to run and scale your web applications.

Azure App Service costs

You pay for the Azure compute resources your app uses while it processes requests based on the App Service Plan you choose. The App Service plan determines how much hardware is devoted to your host - for example, whether it's dedicated or shared hardware, and how much memory is reserved for it. There is even a *free* tier you can use to host small, low-traffic sites.

Types of app services

With Azure App Service, you can host most common app service styles, including:

- Web Apps
- API Apps
- WebJobs
- Mobile Apps

Azure App Service handles most of the infrastructure decisions you deal with in hosting web-accessible apps: deployment and management are integrated into the platform, endpoints can be secured, sites can be scaled quickly to handle high traffic loads, and the built-in load balancing and traffic manager provide high availability. All of these app styles are hosted in the same infrastructure and share these benefits. This flexibility makes App Service the ideal choice to host web-oriented applications.

Web apps

App Service includes full support for hosting web apps using ASP.NET, ASP.NET Core, Java, Ruby, Node.js, PHP, or Python. You can choose either Windows or Linux as the host operating system.

API apps

Much like hosting a website, you can build REST-based Web APIs using your choice of language and framework. You get full Swagger support, and the ability to package and publish your API in Azure Marketplace. The produced apps can be consumed from any HTTP(S)-based client.

Web jobs

WebJobs allows you to run a program (.exe, Java, PHP, Python, or Node.js) or script (.cmd, .bat, PowerShell, or Bash) in the same context as a web app, API app, or mobile app. They can be scheduled, or run by a trigger. WebJobs are often used to run background tasks as part of your application logic.

Mobile app back-ends

Use the Mobile Apps feature of Azure App Service to quickly build a back-end for iOS and Android apps. With just a few clicks in the Azure portal you can:

- Store mobile app data in a cloud-based SQL database
- Authenticate customers against common social providers such as MSA, Google, Twitter, and Facebook
- Send push notifications

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

- Execute custom back-end logic in C# or Node.js

On the mobile app side, there is SDK support for native iOS & Android, Xamarin, and React native apps.

When to use Azure Functions

After consulting with several of your fellow developers at Tailwind Traders, you've determined that some of your application logic is event driven. In other words, for a large amount of time, your application is waiting for a particular input before performing any processing. You'd like to find a way where you can reduce your costs so that you're not paying for the time that your application is waiting for input. With that in mind, you've decided to investigate Azure Functions to see if that can help.

Serverless computing is the abstraction of servers, infrastructure, and OSs. With *serverless* computing, Azure takes care of managing the server infrastructure and allocation/deallocation of resources based on demand. Infrastructure isn't your responsibility. Scaling and performance are handled automatically, and you are billed only for the exact resources you use. There's no need to even reserve capacity.

Serverless computing encompasses three ideas: the abstraction of servers, an event-driven scale, and micro-billing:

1. **Abstraction of servers**: Serverless computing abstracts the servers you run on. You never explicitly reserve server instances; the platform manages that for you. Each function execution can run on a different compute instance, and this execution context is transparent to the code. With serverless architecture, you simply deploy your code, which then runs with high availability.
2. **Event-driven scale**: Serverless computing is an excellent fit for workloads that respond to incoming events. Events include triggers by timers (for example, if a function needs to run every day at 10:00 AM UTC), HTTP (API and webhook scenarios), queues (for example, with order processing), and much more. Instead of writing an entire application, the developer authors a function, which contains both code and metadata about its triggers and bindings. The platform automatically schedules the function to run and scales the number of compute instances based on the rate of incoming events. Triggers define how a function is invoked and bindings provide a declarative way to connect to services from within the code.
3. **Micro-billing**: Traditional computing has the notion of billing for a block of time - like paying a monthly or annual rate for website hosting. This is a convenient method of billing, but quite often that isn't very cost effective. Even if a customer's website gets only one hit a day, they still pay for a full day's worth of availability. With serverless computing, they pay only for the time their code runs. If no active function executions occur, they're not charged. For example, if the code runs once a day for two minutes, they're charged for one execution and two minutes of computing time.

Serverless computing in Azure

https://www.microsoft.com/videoplayer/embed/RE2yzjL

Azure has two implementations of serverless compute:

- **Azure Functions**, which can execute code in almost any modern language.

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

- **Azure Logic Apps**, which are designed in a web-based designer and can execute logic triggered by Azure services without writing any code.

Azure Functions

When you're concerned only about the code running your service, and not the underlying platform or infrastructure, Azure Functions are ideal. They're commonly used when you need to perform work in response to an event, often via a REST request, timer, or message from another Azure service and when that work can be completed quickly, within seconds or less.

Azure Functions scale automatically based on demand, so they're a solid choice when demand is variable. For example, you may be receiving messages from an IoT solution used to monitor a fleet of delivery vehicles. You'll likely have more data arriving during business hours.

Using a VM-based approach, you'd incur costs even when the VM is idle. With functions, Azure runs your code when it's triggered and automatically deallocates resources when the function is finished. In this model, you're only charged for the CPU time used while your function runs.

Furthermore, Azure Functions can be either stateless (the default), where they behave as if they're restarted every time they respond to an event, or stateful (called “Durable Functions”), where a context is passed through the function to track prior activity.

Functions are a key component of serverless computing, but they're also a general compute platform for running any type of code. If the needs of the developer's app change, you can deploy the project in an environment that isn't serverless, which provides the flexibility to manage scaling, run on virtual networks, and even completely isolate the functions.

Azure Logic Apps

Azure Logic Apps are similar to Functions - both enable you to trigger logic based on an event. Where Functions execute code, Logic Apps execute *workflows* designed to automate business scenarios and built from predefined logic blocks. Every logic app workflow starts with a trigger, which fires when a specific event happens or when newly available data meets specific criteria. Many triggers include basic scheduling capabilities, so developers can specify how regularly their workloads will run. Each time the trigger fires, the Logic Apps engine creates a logic app instance that runs the actions in the workflow. These actions can also include data conversions and flow controls, such as conditional statements, switch statements, loops, and branching.

You create Logic App workflows using a visual designer on the Azure portal or in Visual Studio. The workflows are persisted as a JSON file with a known workflow schema.

Azure provides over 200 different connectors and processing blocks to interact with different services - including most popular enterprise apps. You can also build custom connectors and workflow steps if the service you need to interact with isn't covered. You then use the visual designer to link connectors and blocks together, passing data through the workflow to do custom processing - often all without writing any code.

As an example, let's say a ticket arrives in ZenDesk. You could:

- Detect the intent of the message with cognitive services
- Create an item in SharePoint to track the issue
- If the customer isn't in your database, add them to your Dynamics 365 CRM system
- Send a follow-up email to acknowledge their request

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

All of that could be designed in a visual designer making it easy to see the logic flow, which is ideal for a business analyst role.

Functions vs. Logic Apps

Functions and Logic Apps can both create complex orchestrations, which is a collection of functions or steps that are executed to accomplish a complex task.

- With Azure Functions, you write code to complete each step.
- With Logic Apps, you use a GUI to define the actions and how they relate to one another.

You can mix and match services when you build an orchestration, calling functions from logic apps and calling logic apps from functions. Here are some common differences between the two.

	Functions	Logic Apps
State	Normally stateless, but Durable Functions provide state	Stateful
Development	Code-first (imperative)	Designer-first (declarative)
Connectivity	About a dozen built-in binding types, write code for custom bindings	Large collection of connectors, Enterprise Integration Pack for B2B scenarios, build custom connectors
Actions	Each activity is an Azure function; write code for activity functions	Large collection of ready-made actions
Monitoring	Azure Application Insights	Azure portal, Log Analytics
Management	REST API, Visual Studio	Azure portal, REST API, PowerShell, Visual Studio
Execution context	Can run locally or in the cloud	Runs only in the cloud.

When to use Windows Virtual Desktop

In addition to the challenges that Tailwind Traders has been facing with application scale, your manager has asked you to put together a new development team of remote workers. This task would normally require setting up several new computers with all of the requisite development tools for your new team, and then shipping them to the respective developers across the country. The time to procure, set up, and ship each of these computers would be rather costly, and all of your new developers have their own computing devices that are running a mixture of Windows, Android, and macOS operating systems. You'd like to find a way to expedite the deployment process for your remote workers, and keep your management costs to a minimum. With that in mind, you want to see how Windows Virtual Desktop can help your organization.

What is Windows Virtual Desktop?

Windows Virtual Desktop on Microsoft Azure is a desktop and application virtualization service that runs on the cloud, which enables your users to use a cloud-hosted version of Windows from any location. Windows Virtual Desktop works across devices - like Windows, Mac, iOS, Android, and Linux - with apps that you can use to access remote desktops and apps. You can also use most modern browsers to access Windows Virtual Desktop-hosted experiences.

The following video gives you an overview of Windows Virtual Desktop.

Why should you use Windows Virtual Desktop?

To provide the best user experience

Users have the freedom to connect to Windows Virtual Desktop with any device over the internet. They use a Windows Virtual Desktop client to connect to their published Windows desktop and applications. This client could either be a native application on the device or the Windows Virtual Desktop HTML5 web client.

You can make sure your session host virtual machines (VMs) run near apps and services that connect to your datacenter or the cloud. So users stay productive and don't encounter long load times.

User sign-in to Windows Virtual Desktop is extremely fast because user profiles are containerized by using FSLogix. At sign-in, the user profile container is dynamically attached to the computing environment. The user profile is immediately available and appears in the system exactly like a native user profile.

You can provide individual ownership through personal (persistent) desktops. For example, you may want to provide personal remote desktops for members of an engineering team. They'd be able to add or remove programs without impacting other users on that remote desktop.

To enhance security

Windows Virtual Desktop provides centralized security management for users' desktops with Azure Active Directory (Azure AD). You can enable multi-factor authentication to secure user sign-ins. You can also secure access to data by assigning granular role-based access controls to users.

With Windows Virtual Desktop, the data and apps are separated from the local hardware and runs them instead on a remote server. So the risk of confidential data being left on a personal device is reduced.

User sessions are isolated in both single and multi-session environments.

Windows Virtual Desktop also improves security by using reverse connect technology which is a more secure connection type than the Remote Desktop Protocol. We don't open inbound ports to the session host VMs.

What are some key features of Windows Virtual Desktop?

Simplified management

Windows Virtual Desktop is an Azure service which will be familiar to Azure administrators. You use Azure Active Directory and role-based access controls to manage access to resources. Also with Azure, you get tools to automate VM deployments, manage VM updates, and provide disaster recovery. As with other Azure services, Windows Virtual Desktop uses Azure Monitor for monitoring and alerts. This lets admins identify issues through a single interface.

Performance management

Windows Virtual Desktop gives you options to load balance users on your VM host pools. **Host pools** are collections of VMs with the same configuration assigned to multiple users. For the best performance, you can configure load balancing to occur as users sign in (breadth mode). With breadth mode, users are sequentially allocated across the host pool for your workload. To save costs, you can configure your VMs for depth mode load balancing where users are fully allocated on one VM before moving to the next.

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

Windows Virtual Desktop provides tools to automatically provision additional VMs when incoming demand exceeds a specified threshold.

Multi-session Windows 10 deployment

Windows Virtual Desktop lets you use Windows 10 Enterprise multi-session, the only Windows client-based operating system that enables multiple concurrent users on a single virtual machine (VM). Windows Virtual Desktop also provides a more consistent experience with broader application support compared to Windows Server-based operating systems.

How can you reduce costs with Windows Virtual Desktop?

Bring your own licenses

Windows Virtual Desktop is available to you at no additional cost if you have an eligible Microsoft 365 license. Just pay for the Azure resources used by Windows Virtual Desktop.

- Bring your eligible Windows or Microsoft 365 license to get Windows 10 Enterprise and Windows 7 Enterprise desktops and apps at no additional cost.
- If you're an eligible Microsoft Remote Desktop Services (RDS) Client Access License (CAL) customer, Windows Server Remote Desktop Services desktops and apps are available at no additional cost.

Save on compute costs

Buy one-year or three-year Azure Reserved Virtual Machine Instances to save you up to 72 percent versus pay-as-you-go pricing. You can pay for a reservation up front or monthly. Reservations provide a billing discount and don't affect the runtime state of your resources.

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

Explore Azure Storage services

Introduction

Suppose your company, Tailwind Traders, has a number of product brochures, datasheets, product images, and other files related that are related to marketing, sales, and support. In the past, your company has been hosting these files on standalone web servers in your datacenter. Your company is in the process of migrating its applications to the cloud, and your development team is currently architecting new applications. Your Chief Technology Officer (CTO) would like to migrate all of your marketing, sales, and support files to the cloud in order to take advantage of geographic distribution of your files, and to reduce the number of physical servers that your company is maintaining in your datacenter. As part of your migration strategy, you need to determine the correct approach for your cloud-based storage infrastructure.

In this module, you'll learn about the different Azure storage options and the scenarios in which each is appropriate.

Note: Azure storage is not the same as Azure database services.

Learning objectives

After completing this module, you'll be able to describe the benefits and usage of:

- Azure Blob Storage
- Azure Disk Storage
- Azure File Storage
- Azure Storage Tiers

Prerequisites

- You should be familiar with basic computing concepts and terminology
- Familiarity with cloud computing is helpful, but isn't necessary

Azure Storage account fundamentals

The Chief Technology Officer (CTO) for your company, Tailwind Traders, has tasked your team with migrating all of your files to the cloud, and your team has chosen **Azure Storage**[1], which is a service that you can use to store files, messages, tables, and other types of information. You can use Azure Storage on its own (for example as a file share), but developers also often use it as a repository for working data. Such repositories can be used by websites, mobile apps, desktop applications, and many other types of custom solutions. Azure Storage is also used by Infrastructure as a Service (IaaS) virtual machines, and Platform as a Service (PaaS) cloud services.

1 https://azure.microsoft.com/product-categories/storage?azure-portal=true

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

Your first step to begin using Azure Storage is to create an Azure Storage account to store your data objects. You can create an Azure Storage account using the Azure portal, PowerShell, or the Azure Command Line Interface (CLI).

Your storage account will contain all of your Azure Storage data objects; for example: containers, blobs, files, queues, tables, and disks.

A storage account provides a unique namespace for your Azure Storage data that is accessible from anywhere in the world over HTTP or HTTPS. Data in your Azure storage account is secure, highly available, durable, and massively scalable.

To learn how to create an Azure storage account, see **Create a storage account**[2].

Disk storage fundamentals

Disk storage provides disks for virtual machines, applications, and other services to access and use as they need, similar to how they would in on-premises scenarios. Disk storage allows data to be persistently stored and accessed from an attached virtual hard disk. The disks can be managed or unmanaged by

2 https://docs.microsoft.com/azure/storage/common/storage-account-create?azure-portal=true

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

Azure, and therefore managed and configured by the user. Typical scenarios for using disk storage are if you want to lift and shift applications that read and write data to persistent disks, or if you are storing data that is not required to be accessed from outside the virtual machine to which the disk is attached.

Disks come in many different sizes and performance levels, from solid-state drives (SSDs) to traditional spinning hard disk drives (HDDs), with varying performance tiers. You can use standard SSD and HDD disks for less critical workloads, premium SSD disks for mission-critical production applications, and ultra disks for data-intensive workloads such as SAP HANA, top tier databases, and transaction-heavy workloads. Azure has consistently delivered enterprise-grade durability for infrastructure as a service (Iaas) disks, with an industry-leading ZERO% annualized failure rate.

The following illustration shows an Azure virtual machine using separate disks to store different data.

Azure Blob Storage and container storage fundamentals

Azure Blob storage is Microsoft's object storage solution for the cloud. Blob storage is optimized for storing massive amounts of unstructured data, such as text or binary data. Azure Blob Storage is unstructured, meaning that there are no restrictions on the kinds of data it can hold. Blobs are highly scalable and apps work with blobs in much the same way as they would work with files on a disk, such as reading and writing data. Blob Storage can manage thousands of simultaneous uploads, massive amounts of video data, constantly growing log files, and can be reached from anywhere with an internet connection.

Blobs aren't limited to common file formats. A blob could contain gigabytes of binary data streamed from a scientific instrument, an encrypted message for another application, or data in a custom format for an app you're developing. One advantage of blob storage over disk storage is that does not require developers to think about or manage disks; data is uploaded as blobs, and Azure takes care of the physical storage needs.

Blob storage is ideal for:

- Serving images or documents directly to a browser.
- Storing files for distributed access.
- Streaming video and audio.
- Storing data for backup and restore, disaster recovery, and archiving.
- Storing data for analysis by an on-premises or Azure-hosted service.

Azure Blob storage lets you stream large video or audio files directly to the user's browser from anywhere in the world. Blob storage is also used to store data for backup, disaster recovery, and archiving. It has the ability to store up to 8 TB of data for virtual machines.

Blobs are stored in *containers*, which you can use to organize your blobs depending on your business needs.

The following illustration from an earlier unit shows an example usage of Azure accounts, containers, and blobs.

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

File storage fundamentals

Azure Files offers fully managed file shares in the cloud that are accessible via the industry standard Server Message Block (SMB) protocol. Azure file shares can be mounted concurrently by cloud or on-premises deployments of Windows, Linux, and macOS. Applications running in Azure virtual machines or cloud services can mount a file storage share to access file data, just as a desktop application would mount a typical SMB share. Any number of Azure virtual machines or roles can mount and access the file storage share simultaneously. Typical usage scenarios would be to share files anywhere in the world, diagnostic data, or application data sharing.

Azure Files can be used for many common scenarios:

- Many on-premises applications use file shares. This feature makes it easier to migrate those applications that share data to Azure. If you mount the file share to the same drive letter that the on-premises application uses, the part of your application that accesses the file share should work with minimal, if any, changes.
- Configuration files can be stored on a file share and accessed from multiple VMs. Tools and utilities used by multiple developers in a group can be stored on a file share, ensuring that everybody can find them, and that they use the same version.
- Diagnostic logs, metrics, and crash dumps are just three examples of data that can be written to a file share and processed or analyzed later.

The following illustration shows Azure Files being used to share data between two geographical locations. Azure Files ensures the data is encrypted at rest, and the Server Message Block (SMB) protocol ensures the data is encrypted in transit.

One thing that distinguishes Azure Files from files on a corporate file share is that you can access the files from anywhere in the world using a URL that points to the file. You can also use Shared Access Signature (SAS) tokens to allow access to a private asset for a specific amount of time.

Here's an example of a service SAS URI, showing the resource URI and the SAS token:

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

Understanding storage tiers

Data stored in the cloud can grow at an exponential pace. To manage costs for your expanding storage needs, it's helpful to organize your data based on attributes like frequency-of-access and planned retention period to optimize costs. Data stored in the cloud can be different based on how it's generated, processed, and accessed over its lifetime. Some data is actively accessed and modified throughout its lifetime. Some data is accessed frequently early in its lifetime, with access dropping drastically as the data ages. Some data remains idle in the cloud and is rarely, if ever, accessed after it's stored. To accommodate these different access needs, Azure provides several *access tiers*, which you can use to balance your storage costs with your access needs.

Azure storage offers different access tiers for your blob and file storage, which allow you to store object data in the most cost-effective manner. The available access tiers include:

- *Hot storage tier*: optimized for storing data that is accessed frequently. (For example: images for your website.)
- *Cool storage tier*: optimized for data that is infrequently accessed and stored for at least 30 days. (For example: invoices for your customers.)
- *Archive storage tier*: for data that is rarely accessed and stored for at least 180 days with flexible latency requirements. (For example: long-term backups.)

The following considerations apply to the different access tiers:

- Only the hot and cool access tiers can be set at the account level. The archive access tier isn't available at the account level.
- Hot, cool, and archive tiers can be set at the blob level during upload or after upload.
- Data in the cool access tier can tolerate slightly lower availability, but still requires high durability, retrieval latency, and throughput characteristics similar to hot data. For cool data, a slightly lower availability service-level agreement (SLA) and higher access costs compared to hot data are acceptable trade-offs for lower storage costs.
- Archive storage stores data offline and offers the lowest storage costs but also the highest data rehydrate and access costs.

The following illustration demonstrates choosing between the Hot and Cool storage tiers on a general purpose storage account.

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

Explore Azure networking services

Introduction

Suppose your company, Tailwind Traders, has migrated some applications to the cloud and is architecting new ones. The servers that host Tailwind Traders's customer and product data are based in Silicon Valley, and your company has several branch offices that are located in different geographic regions. As part of your migration strategy, your company needs to be able to determine the correct approach to configure its network infrastructure.

To help save costs, you convince your team to move your website and several of your other networked resources to the cloud. With that in mind, you'll need to provide secure access to private company data for each of its branch locations, and you would like to know how can Azure help you manage your network more effectively. As it turns out, managing networks on Azure isn't entirely different from managing on-premises networks.

In this module, you'll learn about the different Azure networking options and the scenarios in which each is appropriate.

Learning objectives

After completing this module, you'll be able to:

- Describe the core networking resources that are available in Azure
- Describe the benefits and usage of Virtual Networks, VPN Gateway, and ExpressRoute

Prerequisites

- You should be familiar with basic network concepts and terminology
- Familiarity with cloud computing is helpful, but isn't necessary

Azure Virtual Network fundamentals

Tailwind Traders has an on-premises datacenter that you plan to keep, but you want to use Azure to offload peak traffic using virtual machines (VMs) hosted in Azure. You want to keep your existing IP addressing scheme and network appliances, while ensuring that any data transfer is secure.

The good news is, Azure virtual networking can help you reach your goals.

What is Azure virtual networking?

Azure virtual networks enable Azure resources - such as virtual machines, web apps, and databases - to communicate with each other, with users on the Internet, and with your on-premises client computers. You can think of an Azure network as a set of resources that links other Azure resources.

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

Azure virtual networks provide the following key networking capabilities:

- Isolation and segmentation
- Internet communications
- Communicate between Azure resources
- Communicate with on-premises resources
- Route network traffic
- Filter network traffic
- Connect virtual networks

Network configurations for virtual machines

Isolation and segmentation

Azure allows you to create multiple isolated virtual networks. When you set up a virtual network, you define a private Internet Protocol (IP) address space, using either public or private IP address ranges. You can divide that IP address space into subnets, and allocate part of the defined address space to each named subnet.

For name resolution, you can use the name resolution service that's built in to Azure, or you can configure the virtual network to use either an internal or an external Domain Name System (DNS) server.

Internet communications

A VM in Azure can connect out to the Internet by default. You can enable incoming connections from the Internet by defining a public IP address or a public load balancer. For VM management, you can connect via the Azure Command Line Interface (CLI), Remote Desktop Protocol (RDP), or Secure Shell (SSH).

Communicate between Azure resources

You'll want to enable Azure resources to communicate securely with each other. You can do that in one of two ways:

- **Virtual networks** Virtual networks can connect not only VMs, but other Azure resources, such as the App Service Environment, Azure Kubernetes Service, and Azure virtual machine scale sets.
- **Service endpoints** You can use service endpoints to connect to other Azure resource types, such as Azure SQL databases and storage accounts. This approach enables you to link multiple Azure resources to virtual networks, thereby improving security and providing optimal routing between resources.

Communicate with on-premises resources

Azure virtual networks enable you to link resources together in your on-premises environment and within your Azure subscription, in effect creating a network that spans both your local and cloud environments. There are three mechanisms for you to achieve this connectivity:

- **Point-to-site Virtual Private Networks** This approach is like a Virtual Private Network (VPN) connection that a computer outside your organization makes back into your corporate network, except that it's working in the opposite direction. In this case, the client computer initiates an encrypted VPN connection to Azure, connecting that computer to the Azure virtual network.

- **Site-to-site Virtual Private Networks** A site-to-site VPN links your on-premises VPN device or gateway to the Azure VPN gateway in a virtual network. In effect, the devices in Azure can appear as being on the local network. The connection is encrypted and works over the Internet.
- **Azure ExpressRoute** For environments where you need greater bandwidth and even higher levels of security, Azure ExpressRoute is the best approach. Azure ExpressRoute provides dedicated private connectivity to Azure that does not travel over the Internet. (You'll learn more about ExpressRoute in a separate unit later in this module.)

Route network traffic

By default, Azure will route traffic between subnets on any connected virtual networks, on-premises networks, and the Internet. However, you can control routing and override those settings as follows:

- **Route tables** A route table allows you to define rules as to how traffic should be directed. You can create custom route tables that control how packets are routed between subnets.
- **Border Gateway Protocol** Border Gateway Protocol (BGP) works with Azure VPN gateways or ExpressRoute to propagate on-premises BGP routes to Azure virtual networks.

Filter network traffic

Azure virtual networks enable you to filter traffic between subnets by using the following approaches:

- **Network security groups** A network security group is an Azure resource that can contain multiple inbound and outbound security rules. You can define these rules to allow or block traffic, based on factors such as source and destination IP address, port, and protocol.
- **Network virtual appliances** A network virtual appliance is a specialized VM that can be compared to a hardened network appliance. A network virtual appliance carries out a particular network function, such as running a firewall or performing Wide Area Network (WAN) optimization.

Connect virtual networks

You can link virtual networks together using virtual network *peering*. Peering enables resources in each virtual network to communicate with each other. These virtual networks can be in separate regions, allowing you to create a global interconnected network through Azure.

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

Azure Virtual Network settings

You can create and configure Azure virtual networks from the Azure portal, Azure PowerShell on your local computer, or Azure Cloud Shell.

Create a virtual network

When you create an Azure virtual network, you configure a number of basic settings. You'll have the option to configure advanced settings, such as multiple subnets, distributed denial of service (DDoS) protection, and service endpoints.

You'll configure the following settings for a basic virtual network:

- **Network name** The network name must be unique in your subscription, but does not need to be globally unique. Make the name a descriptive one that is easy to remember and identified from other virtual networks.
- **Address space** When you set up a virtual network, you define the internal address space in Classless Inter-Domain Routing (CIDR) format. This address space needs to be unique within your subscription and any other networks that you connect to. Let's assume, you choose an address space of 10.0.0.0/24 for your first virtual network. The addresses defined in this address space ranges from 10.0.0.1 - 10.0.0.254. You then create a second virtual network and choose an address space of 10.0.0.0/8. The address in this address space ranges from 10.0.0.1 - 10.255.255.254. Some of the address overlap and can't be used for the two virtual networks. However, you can use 10.0.0.0/16, with addresses ranging

from 10.0.0.1 - 10.0.255.254, and 10.1.0.0/16, with addresses ranging from 10.1.0.1 - 10.1.255.254. You can assign these address spaces to your virtual networks since there's no address overlap.

Note: You can add address spaces after creating the virtual network.

- **Subscription** This option only applies if you have multiple subscriptions to choose from.
- **Resource group** Like any other Azure resource, a virtual network needs to exist in a resource group. You can either select an existing resource group or create a new one.
- **Location** Select the location where you want the virtual network to exist.
- **Subnet** Within each virtual network address range, you can create one or more subnets that partition the virtual network's address space. Routing between subnets will then depend on the default traffic routes, or you can define custom routes. Alternatively, you can define one subnet that encompasses all the virtual networks' address ranges.

Note: Subnet names must begin with a letter or number, end with a letter, number or underscore, and may contain only letters, numbers, underscores, periods, or hyphens.

- **Distributed Denial of Service (DDoS) protection** You can select either Basic or Standard DDoS protection. Standard DDoS Protection is a premium service. The **Azure DDoS Protection Standard**[3] provides for more information on Standard DDoS protection.
- **Service Endpoints** Here, you enable service endpoints, and then select from the list which Azure service endpoints you want to enable. Options include Azure Cosmos DB, Azure Service Bus, Azure Key Vault, and so on.

When you have configured these settings, click the **Create** button.

Define additional settings

After creating a virtual network, you can then define further settings. These include:

- **Network security group** Network security groups have security rules that enable you to filter the type of network traffic that can flow in and out of virtual network subnets and network interfaces. You create the network security group separately, and then associate it with the virtual network.
- **Route table** Azure automatically creates a route table for each subnet within an Azure virtual network and adds system default routes to the table. However, you can add custom route tables to modify traffic between virtual networks.

You can also amend the service endpoints.

3 https://docs.microsoft.com/azure/virtual-network/ddos-protection-overview?azure-portal=true

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

Configure virtual networks

When you have created a virtual network, you can change any further settings from the Virtual Networks pane in the Azure portal. Alternatively, you can use PowerShell commands or commands in Cloud Shell to make changes.

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

You can then review and change settings in further sub-panes. These settings include:

- **Address spaces**: You can add additional address spaces to the initial definition
- **Connected devices**: Use the virtual network to connect machines
- **Subnets**: You can add additional subnets
- **Peerings**: Link virtual networks in peering arrangements

You can also monitor and troubleshoot virtual networks, or create an automation script to generate the current virtual network.

Virtual networks are powerful and highly configurable mechanisms for connecting entities in Azure. You can connect Azure resources to one another or to resources you have on-premises. You can isolate, filter and route your network traffic, and Azure allows you to increase security where you feel you need it.

Azure VPN Gateway fundamentals

A virtual private network (VPN) is a type of private interconnected network. VPNs use an encrypted tunnel within another network. They're typically deployed to connect two or more trusted private networks to one another over an untrusted network (typically the public Internet). Traffic is encrypted while traveling over the untrusted network to prevent eavesdropping or other attacks.

For our Tailwind Traders scenario, VPNs can enable branch offices to share sensitive information between locations. For example, let's say that your offices on the East Coast region of North America need to

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

access your company's private customer data, which is stored on servers that are physically located in West Coast region. A VPN that connects your East Coast offices to your West Coast servers allows your company to securely access your private customer data.

Azure VPN gateways

A VPN gateway is a type of Virtual Network Gateway. VPN gateways are deployed in Azure virtual networks and enable the following connectivity:

- Connect on-premises datacenters to Azure virtual networks through a *site-to-site* connection.
- Connect individual devices to Azure virtual networks through a *point-to-site* connection.
- Connect Azure virtual networks to other Azure virtual networks through a *network-to-network* connection.

All transferred data is encrypted in a private tunnel as it crosses the internet. You can deploy only one VPN gateway in each virtual network, but you can use one gateway to connect to multiple locations, including other Azure virtual networks or on-premises datacenters.

When you deploy a VPN gateway, you specify the VPN type: either *policy-based* or *route-based*, and the main difference between these two types of VPNs is how traffic to be encrypted is specified. In Azure, both types of VPN gateways use pre-shared key as the only method of authentication. Both types also rely on Internet Key Exchange (IKE) in either version 1 or version 2 and Internet Protocol Security (IPSec). IKE is used to set up a security association (an agreement of the encryption) between two endpoints. This association is then passed to the IPSec suite, which encrypts and decrypts data packets encapsulated in the VPN tunnel.

Policy-based VPNs

Policy-based VPN gateways specify statically the IP address of packets that should be encrypted through each tunnel. This type of device evaluates every data packet against those sets of IP addresses to choose the tunnel where that packet is going to be sent through.

Key features of policy-based VPN gateways in Azure include:

- Support for IKEv1 only.
- Use of *static routing*, where combinations of address prefixes from both networks control how traffic is encrypted and decrypted through the VPN tunnel. The source and destination of the tunneled networks are declared in the policy and don't need to be declared in routing tables.
- Policy-based VPNs must be used in specific scenarios that require them, such as for compatibility with legacy on-premises VPN devices.

Route-based VPNs

If defining which IP addresses are behind each tunnel is too cumbersome, route-based gateways can be used. With route-based gateways, IPSec tunnels are modeled as a network interface or Virtual Tunnel

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

Interface (VTI). IP routing (either static routes or dynamic routing protocols) decide which one of these tunnel interfaces to use when sending each packet. Route-based VPNs are the preferred connection method for on-premises devices, since they are more resilient to topology changes such as the creation of new subnets.

Use a route-based VPN gateway if you need any of the following types of connectivity:

- Connections between virtual networks
- Point-to-site connections
- Multisite connections
- Coexistence with an Azure ExpressRoute gateway

Key features of route-based VPNs gateways in Azure include:

- Supports IKEv2
- Uses any-to-any (wildcard) traffic selectors
- Can use *dynamic routing protocols*, where routing/forwarding tables direct traffic to different IPSec tunnels. In this case, the source and destination networks are not statically defined as they are in policy-based VPNs or even in route-based VPNs with static routing. Instead, data packets are encrypted based on network routing tables that are created dynamically using routing protocols such as BGP (Border Gateway Protocol).

VPN gateway sizes

The capabilities of your VPN gateway are determined by the SKU or size that you deploy. This table shows the main capabilities of each available SKU:

SKU	Site-to-site/VNet-to-VNet tunnels	Aggregate throughput benchmark	Border Gateway Protocol (BGP) support
Basic [See Note]	Maximum: 10	100 Mbps	Not supported
VpnGw1/Az	Maximum: 30	650 Mbps	Supported
VpnGw2/Az	Maximum: 30	1 Gbps	Supported
VpnGw3/Az	Maximum: 30	1.25 Gbps	Supported

Note: Basic VPN Gateway should only be used for Dev/Test workloads. In addition, it is unsupported to migrate from Basic to the VpnGW1/2/3/Az skus at a later time without having to remove the gateway and redeploy.

Deploying VPN gateways

Before you can deploy a VPN gateway, you'll need some Azure and on-premises resources.

Required Azure resources

You'll need these Azure resources before you can deploy an operational VPN gateway:

- **Virtual network**. Deploy an Azure virtual network with enough address space for the additional subnet that you'll need for the VPN gateway. The address space for this virtual network must not overlap with the on-premises network that you'll be connecting to. Remember that you can deploy only one VPN gateway within a virtual network.

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

- **GatewaySubnet**. Deploy a subnet called `GatewaySubnet` for the VPN gateway. Use at least a **/27** address mask to make sure you have enough IP addresses in the subnet for future growth. You can't use this subnet for any other services.
- **Public IP address**. Create a Basic-SKU dynamic public IP address if using a non-zone-aware gateway. This address provides a public-routable IP address as the target for your on-premises VPN device. This IP address is dynamic, but it won't change unless you delete and re-create the VPN gateway.
- **Local network gateway**. Create a local network gateway to define the on-premises network's configuration: where the VPN gateway will connect and what it will connect to. This configuration includes the on-premises VPN device's public IPv4 address and the on-premises routable networks. This information is used by the VPN gateway to route packets that are destined for on-premises networks through the IPSec tunnel.
- **Virtual network gateway**. Create the virtual network gateway to route traffic between the virtual network and the on-premises datacenter or other virtual networks. The virtual network gateway can be either a VPN or ExpressRoute gateway, but this unit only with VPN virtual network gateways. (You'll learn more about ExpressRoute in a separate unit later in this module.)
- **Connection**. Create a Connection resource to create a logical connection between the VPN gateway and the local network gateway.
  - The connection is made to the on-premises VPN device's IPv4 address as defined by the local network gateway.
  - The connection is made from the virtual network gateway and its associated public IP address.

  You can create multiple connections.

The following diagram shows this combination of resources and their relationships to help you better understand what's required to deploy a VPN gateway:

Required on-premises resources

To connect your datacenter to a VPN gateway, you'll need these on-premises resources:

- A VPN device that supports policy-based or route-based VPN gateways
- A public-facing (internet-routable) IPv4 address

High availability scenarios

There are several ways to ensure you have a fault-tolerant configuration.

Active/standby

By default, VPN gateways are deployed as two instances in an *active/standby* configuration, even if you only see one VPN gateway resource in Azure. When planned maintenance or unplanned disruption affects the active instance, the standby instance automatically assumes responsibility for connections without any user intervention. Connections are interrupted during this failover, but they're typically restored within a few seconds for planned maintenance and within 90 seconds for unplanned disruptions.

Active/active

With the introduction of support for the BGP routing protocol, you can also deploy VPN gateways in an *active/active* configuration. In this configuration, you assign a unique public IP address to each instance. You then create separate tunnels from the on-premises device to each IP address. You can extend the high availability by deploying an additional VPN device on-premises.

ExpressRoute failover

Another high availability option is to configure a VPN gateway as a secure failover path for ExpressRoute connections. ExpressRoute circuits have resiliency built in, but aren't immune to physical problems that affect the cables delivering connectivity, or outages affecting the complete ExpressRoute location. In high availability scenarios, where there's risk associated with an outage of an ExpressRoute circuit, you can also provision a VPN gateway which uses the internet as an alternative method of connectivity, thus ensuring there's always a connection to the Azure virtual networks.

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

Zone-redundant gateways

In regions that support availability zones, VPN and ExpressRoute gateways can be deployed in a zone-redundant configuration. This brings resiliency, scalability, and higher availability to virtual network gateways. Deploying gateways in Azure Availability Zones physically and logically separates gateways within a region, while protecting your on-premises network connectivity to Azure from zone-level failures. These require different gateway SKUs and leverage Standard public IP addresses instead of Basic public IP addresses.

Azure ExpressRoute fundamentals

Azure ExpressRoute lets you seamlessly extend your on-premises networks into the Microsoft cloud. This connection between your organization and Azure is dedicated and private. Establishing an ExpressRoute connection enables you to connect to Microsoft cloud services like Azure, Office 365, and Dynamics 365. Security is enhanced, connections are more reliable, latency is minimal, and throughput is greatly increased.

As part of your work for Tailwind Traders, you should understand what Azure ExpressRoute is, and how ExpressRoute integrates with on-premises and Azure networks. In this unit, you'll learn about the benefits that ExpressRoute provides compared to other site-to-site connectivity options, and whether ExpressRoute can provide your company with the best possible network performance.

Throughout this unit, we will focus on two different layers of the Open Systems Interconnection (OSI) model:

- **Layer 2 (L2)**: This is the *Data Link Layer*, which provides node-to-node communication between two nodes on the same network.
- **Layer 3 (L3)**: This is the *Network Layer*, which provides addressing and routing between nodes on a multi-node network.

Features and benefits of ExpressRoute

There are several benefits to using ExpressRoute as the connection service between Azure and on-premises networks.

Layer 3 connectivity

ExpressRoute provides Layer 3 (address-level) connectivity between your on-premises network and the Microsoft cloud through connectivity partners. These connections can be from a point-to-point, any-to-any network, or they can be virtual cross-connections through an exchange.

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

Built-in redundancy

Each connectivity provider uses redundant devices to ensure that connections established with Microsoft are highly available. You can configure multiple circuits to complement this feature. All redundant connections are configured with Layer 3 connectivity to meet SLAs.

Connectivity to Microsoft cloud services

ExpressRoute enables direct access to the following services in all regions:

- Microsoft Office 365
- Microsoft Dynamics 365
- Azure compute services, such as Azure Virtual Machines
- Azure cloud services, such as Azure Cosmos DB and Azure Storage

Office 365 was created to be accessed securely and reliably via the internet. Because of this, we recommend ExpressRoute for specific scenarios. The "Learn more" section at the end of this module includes a link about using ExpressRoute to access Office 365.

Across on-premises connectivity with ExpressRoute Global Reach

You can enable ExpressRoute Global Reach to exchange data across your on-premises sites by connecting your ExpressRoute circuits. For example, assume that you have a private datacenter in California connected to ExpressRoute in Silicon Valley. You have another private datacenter in Texas connected to ExpressRoute in Dallas. With ExpressRoute Global Reach, you can connect your private datacenters through two ExpressRoute circuits. Your cross-datacenter traffic will travel through the Microsoft network.

Dynamic routing

ExpressRoute uses the Border Gateway Protocol (BGP) routing protocol. BGP is used to exchange routes between on-premises networks and resources running in Azure. This protocol enables dynamic routing between your on-premises network and services running in the Microsoft cloud.

ExpressRoute connectivity models

ExpressRoute supports three models that you can use to connect your on-premises network to the Microsoft cloud:

- CloudExchange colocation
- Point-to-point Ethernet connection
- Any-to-any connection

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

Colocation at a cloud exchange

Co-located providers can normally offer both Layer 2 and Layer 3 connections between your infrastructure, which might be located in the colocation facility, and the Microsoft cloud. For example, if your datacenter is co-located at a cloud exchange such as an internet service provider (ISP), you can request a virtual cross-connection to the Microsoft cloud.

Point-point Ethernet connection

Point-to-point connections provide Layer 2 and Layer 3 connectivity between your on-premises site and Microsoft Azure. You can connect your offices or datacenters to Azure by using the point-to-point links. For example, if you have an on-premises datacenter, you can use a point-to-point Ethernet link to connect to Microsoft.

Any-to-any networks

With any-to-any connectivity, you can integrate your wide area network (WAN) with Microsoft Azure by providing connections to your offices and datacenters. Azure will integrate with your WAN connection to provide a seamless connection, just like you would have between your datacenter and any branch offices.

With any-to-any connections, all WAN providers offer Layer 3 connectivity. For example, if you already use Multiprotocol Label Switching (MPLS) to connect to your branch offices or other sites in your organization, an ExpressRoute connection to Microsoft will behave just like another location on your private WAN.

Security considerations

With ExpressRoute, your data doesn't travel over the public internet, so it's not exposed to the potential risks associated with internet communications. ExpressRoute is a private connection from your on-premises infrastructure to your Azure infrastructure. Even if you have an ExpressRoute connection, DNS queries, certificate revocation list checking, and Azure Content Delivery Network requests are still sent over the public internet.

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

Module 2 Review Questions

Module 02 Review Questions

Review Question 1

Your development team is interested in writing Graph-based applications that take advantage of the Gremlin API. Which option would be ideal for that scenario?

- ☐ Azure SQL Database
- ☐ Azure Databricks
- ☐ Azure Cosmos DB
- ☐ Azure Database for PostgreSQL

Review Question 2

Tailwind Traders uses the LAMP stack for several of its websites. Which option would be ideal for migration?

- ☐ Azure Database for MySQL
- ☐ Azure Cosmos DB
- ☐ Azure SQL Database
- ☐ Azure Database for PostgreSQL

Review Question 3

Tailwind Traders has millions of log entries that it wants to analyze. Which option would be ideal for analysis?

- ☐ Azure Cosmos DB
- ☐ Azure SQL Database
- ☐ Azure Database for PostgreSQL
- ☐ Azure Synapse Analytics

Review Question 4

Which Azure compute resource can be deployed to manage a set of identical virtual machines?

- ☐ Virtual machine availability sets
- ☐ Virtual machine scale sets
- ☐ Virtual machine availability zones

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

Review Question 5

Which of the following services should be used when the primary concern is to perform work in response to an event (often via a REST command) that needs a response in a few seconds?

- ☐ Azure Functions
- ☐ Azure App Service
- ☐ Azure Container Instances

Review Question 6

Your company has a team of remote workers that need to use Windows-based software to develop your company's applications, but your team members are using various operating systems like MacOS, Linux, and Windows. Which Azure compute service would help resolve this scenario?

- ☐ Azure App Service
- ☐ Windows Virtual Desktop
- ☐ Azure Container Instances

Review Question 7

What is the first step that you would take in order to share an image file as a blob in Azure Storage?

- ☐ Create an Azure Storage container to store the image.
- ☐ Upload the image file and create a container.
- ☐ Use a Shared Access Signature (SAS) token to restrict access to the image.
- ☐ Create an Azure Storage account.

Review Question 8

Which Azure Storage option is better for storing data for backup and restore, disaster recovery, and archiving?

- ☐ Azure Blob Storage
- ☐ Azure Files Storage
- ☐ Azure Disk Storage

Review Question 9

Tailwind Traders wants to create a secure communication tunnel between its branch offices. Which of the following technologies can't be used?

- ☐ Point-to-site virtual private network
- ☐ Implicit FTP over SSL
- ☐ Azure ExpressRoute
- ☐ Site-to-site virtual private network

Review Question 10

Tailwind Traders wants to use Azure ExpressRoute to connect its on-premises network to the Microsoft cloud. Which of the following choices isn't an ExpressRoute model that Tailwind Traders can use?

- ☐ Site-to-site virtual private network
- ☐ Any-to-any connection
- ☐ Point-to-point Ethernet connection
- ☐ CloudExchange colocation

Review Question 11

Which of the following options can you use to link virtual networks?

- ☐ Network address translation
- ☐ Multi-chassis link aggregation
- ☐ Dynamic Host Control Protocol
- ☐ Virtual network peering

Review Question 12

Which of the following options isn't a benefit of ExpressRoute?

- ☐ Redundant connectivity
- ☐ Consistent network throughput
- ☐ Encrypted network communication
- ☐ Access to Microsoft cloud services

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

Module 2 Summary

Module 02 Summary

Explore Azure database and analytics services

In this lesson, you learned how to help Tailwind Traders migrate their database workloads to Microsoft Azure. You saw how Azure SQL Database, Azure Database for MySQL, and Azure Database for PostgreSQL will enable your company to migrate their existing SQL Server, MySQL, and PostgreSQL databases to the cloud while preserving your company's development and database administration strengths.

In addition, you saw how Azure Cosmos DB a variety of popular APIs - SQL, MongoDB, Cassandra, Tables, and Gremlin - which you can use to migrate your data to the cloud and retain or enhance your developer skillsets. You also learned how you can use Azure's big data and analysis services like Azure Synapse Analytics, Azure HDInsight, Azure Databricks, and Azure Data Lake Analytics to analyze large volumes of data.

Explore Azure compute services

In this lesson, you learned how you can use several of Azure's Compute services to help Tailwind Traders resolve its application demand challenges through the use of virtualization services like Azure Virtual Machines (VMs), Azure Container Instances (ACI), and Azure Kubernetes Service (AKS). You also learned how you can use Azure App Services to create your website front-ends, and Azure Functions to create event drive application logic that only runs when you need it. Lastly, you learned how you can use Windows Virtual Desktop to quickly provide a customized operating system and software environment for your remote workers.

Explore Azure Storage services

In this lesson, you discovered how Azure Storage can provide your company with a variety of options for storing your data.

For example, you learned that your first step when using Azure Storage is to create a storage account. Once you have done so, Azure provides you with several options for storing your data:

- Azure Disk Storage
- Azure Blob/Container Storage
- Azure File Storage

Explore Azure networking services

In this lesson, you used the Tailwind Traders scenario to learn about the core networking resources that are available in Azure, and you learned about the benefits and usage of Virtual Networks, Virtual Private Network (VPN) gateways, and Azure ExpressRoute.

Armed with this new knowledge, you can apply this information to help your business use Azure's networking resources to configure its network infrastructure.

Answers

Review Question 1

Your development team is interested in writing Graph-based applications that take advantage of the Gremlin API. Which option would be ideal for that scenario?

- ☐ Azure SQL Database
- ☐ Azure Databricks
- ■ Azure Cosmos DB
- ☐ Azure Database for PostgreSQL

Explanation
Azure Cosmos DB supports SQL, MongoDB, Cassandra, Tables, and Gremlin APIs.

Review Question 2

Tailwind Traders uses the LAMP stack for several of its websites. Which option would be ideal for migration?

- ■ Azure Database for MySQL
- ☐ Azure Cosmos DB
- ☐ Azure SQL Database
- ☐ Azure Database for PostgreSQL

Explanation
Azure Database for MySQL is the logical choice for existing LAMP stack applications.

Review Question 3

Tailwind Traders has millions of log entries that it wants to analyze. Which option would be ideal for analysis?

- ☐ Azure Cosmos DB
- ☐ Azure SQL Database
- ☐ Azure Database for PostgreSQL
- ■ Azure Synapse Analytics

Explanation
Azure Synapse Analytics is the logical choice for analyzing large volumes of data.

Review Question 4

Which Azure compute resource can be deployed to manage a set of identical virtual machines?

- ☐ Virtual machine availability sets
- ■ Virtual machine scale sets
- ☐ Virtual machine availability zones

Explanation
Virtual machine scale sets let you deploy and manage a set of identical virtual machines.

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

Review Question 5

Which of the following services should be used when the primary concern is to perform work in response to an event (often via a REST command) that needs a response in a few seconds?

- ■ Azure Functions
- ☐ Azure App Service
- ☐ Azure Container Instances

Explanation
Azure Functions is used when you need to perform work in response to an event (often via a REST request), timer, or message from another Azure service, and when that work can be completed quickly, within seconds or less.

Review Question 6

Your company has a team of remote workers that need to use Windows-based software to develop your company's applications, but your team members are using various operating systems like MacOS, Linux, and Windows. Which Azure compute service would help resolve this scenario?

- ☐ Azure App Service
- ■ Windows Virtual Desktop
- ☐ Azure Container Instances

Explanation
That's correct. Windows Virtual Desktop enables your team members to run Windows in the cloud, with access to the required applications for your company's needs.

Review Question 7

What is the first step that you would take in order to share an image file as a blob in Azure Storage?

- ☐ Create an Azure Storage container to store the image.
- ☐ Upload the image file and create a container.
- ☐ Use a Shared Access Signature (SAS) token to restrict access to the image.
- ■ Create an Azure Storage account.

Explanation
You must create an Azure Storage account before you can use any Azure Storage features.

Review Question 8

Which Azure Storage option is better for storing data for backup and restore, disaster recovery, and archiving?

- ■ Azure Blob Storage
- ☐ Azure Files Storage
- ☐ Azure Disk Storage

Explanation
Azure Blob Storage is your best option for storing disaster recovery files and archives.

Review Question 9

Tailwind Traders wants to create a secure communication tunnel between its branch offices. Which of the following technologies can't be used?

- ☐ Point-to-site virtual private network
- ■ Implicit FTP over SSL
- ☐ Azure ExpressRoute
- ☐ Site-to-site virtual private network

Explanation
FTP over SSL can't be used to create a secure communication tunnel.

Review Question 10

Tailwind Traders wants to use Azure ExpressRoute to connect its on-premises network to the Microsoft cloud. Which of the following choices isn't an ExpressRoute model that Tailwind Traders can use?

- ■ Site-to-site virtual private network
- ☐ Any-to-any connection
- ☐ Point-to-point Ethernet connection
- ☐ CloudExchange colocation

Explanation
A site-to-site virtual private network isn't an ExpressRoute model.

Review Question 11

Which of the following options can you use to link virtual networks?

- ☐ Network address translation
- ☐ Multi-chassis link aggregation
- ☐ Dynamic Host Control Protocol
- ■ Virtual network peering

Explanation
Virtual network peering can be used to link virtual networks.

Review Question 12

Which of the following options isn't a benefit of ExpressRoute?

- ☐ Redundant connectivity
- ☐ Consistent network throughput
- ■ Encrypted network communication
- ☐ Access to Microsoft cloud services

Explanation
Correct. ExpressRoute does provide private connectivity, but it isn't encrypted.

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

Module 3 Describe core solutions and management tools on Azure

Learning Objectives

Learning Objectives

After completing this module, you'll be able to:

- Choose the correct Azure Artificial Intelligence service to address different kinds of business challenges.
- Choose the best software development process tools and services for a given business scenario.
- Choose the correct cloud monitoring service to address different kinds of business challenges.
- Choose the correct Azure management tool to address different kinds of technical needs and challenges.
- Choose the right serverless computing technology for your business scenario.
- Choose the best Azure IoT service for a given business scenario.

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

Choose the best AI service for your needs

Introduction

Artificial Intelligence (AI) is a category of computing that adapts and improves its decision-making ability over time based on its successes and failures. Microsoft Azure provides several different AI solutions to choose from, depending on the problem you're trying to solve.

Tailwind Traders, a traditional brick-and-mortar retailer who has experienced explosive online sales growth, faces exciting challenges as they seek to improve their ecommerce and service operations. Microsoft's AI services might be a good fit for one of the company's new initiatives, but Tailwind Traders needs help to better understand which product option is best for each scenario.

In this module, you'll learn about Microsoft's different AI services, and will analyze decision criteria that experts use to select the right service for a given scenario.

Learning objectives

By the end of this module, you will be able to:

- Choose the correct Azure Artificial Intelligence service to address different kinds of business challenges.

Prerequisites

- You should be familiar with the idea of an Application Programming Interface, or API. Programmers use APIs to utilize functionality contained in code libraries.
- You should be familiar with what a “web API” is. You should understand that a web API is an API that is accessible from servers that accept requests via HTTP. Also, you should understand that a "web API endpoint" is the location of the code library and that REST APIs refer to the design of the URL style used to expose the API's functionality.

Identify the product options

Artificial Intelligence (AI) is a broad classification of computing that allows a software system to perceive its environment and take action that maximizes its chance of successfully achieving its goals. A goal of AI is to create a software system that is able to adapt, or learn something on its own without being explicitly programmed to do it.

There are two basic approaches to AI. The first is to employ a “deep learning” system that is modeled on the neural network of the human mind, enabling it to discover, learn, and grow through experience.

The second approach is “machine learning”, which is a data science technique that uses existing data to train and test a model, then apply that model to new data to forecast future behaviors, outcomes, and trends.

Forecasts or predictions from machine learning can make apps and devices smarter. For example, when you shop online, machine learning powers product recommendation systems that offer a shopper additional products based on what they've bought and what other shoppers bought who have purchased similar items in the past. Machine learning is also used to detect credit card fraud by analyzing each new transaction using what it has learned from analyzing millions of fraudulent transactions.

Virtually every device or software system that collects textual, visual, and audio data could feed a machine learning model that makes that device or software system smarter about how it functions in the future.

Azure Product Options

At a high level, there are three primary offerings from Microsoft, each of which are designed for a specific audience and use case. Furthermore, each product option provides a diverse set of tools, services, and programmatic APIs. We will merely be scratching the surface of what each option is capable of in this module.

Azure Machine Learning

Azure Machine Learning[1] is a platform for making predictions. It consists of tools and services that allow you to connect to data to train and test models to find one that will most accurately predict a future result. Once you've run experiments to test the model, you can then deploy the model and use it in real time via a web API endpoint.

With Azure Machine Learning, you can:

- Create a process that defines how to obtain data, how to handle missing or bad data, how to split the data into either a training set or test set, and deliver the data to the training process
- Train and evaluate predictive models using tools and programming languages familiar to data scientists
- Create pipelines that define where and when to run the compute-intensive experiments required to score the algorithms based on the training and test data
- Deploy the best-performing algorithm as an API to an endpoint so it can be consumed in real time by other applications

Choose Azure Machine Learning when your data scientists need complete control over the design and training of an algorithm using your own data.

Azure Cognitive Services

Azure Cognitive Services[2] provides pre-built machine learning models that enable applications to see, hear, speak, understand, and even begin to reason. Use Azure Cognitive Services to solve general problems such as analyzing text for emotional sentiment or analyzing images to recognize objects or faces. You don't need special machine learning or data science knowledge to use these services. Developers access Azure Cognitive Services via APIs and can easily include these features in just a few lines of code.

While Azure Machine Learning requires you to bring your own data and train models over that data, Azure Cognitive Services, for the most part, provides you with pre-trained models so that you can bring in your live data to get predictions on.

Azure Cognitive Services can be divided into the following categories:

- **Language** services - Allow your apps to process natural language with pre-built scripts, evaluate sentiment, and learn how to recognize what users want.
- **Speech** services - Convert speech into text and text into natural-sounding speech. Translate from one language to another and enable speaker verification and recognition.
- **Vision** services - Add recognition and identification capabilities when analyzing pictures, videos, and other visual content.

1 https://azure.microsoft.com/services/machine-learning/?azure-portal=true
2 https://azure.microsoft.com/services/cognitive-services/?azure-portal=true

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

- **Decision** services - Add personalized recommendations for each user that automatically improve each time they're used, moderate content to monitor and remove offensive or risky content, and detect abnormalities in your time series data.

Azure Bot Service

The **Azure Bot Service**[3] and Bot Framework is a platform for creating virtual agents that understand and reply to questions just like a human. Azure Bot Service is a bit different from Azure Machine Learning and Azure Cognitive Services in that it has a specific use case: namely, creating a virtual agent that can intelligently communicate with humans. Behind the scenes, the bot you build uses other Azure services, like Azure Cognitive Services, to understand what their human counterparts are asking for.

Bots can be used to shift simple, repetitive tasks, such as taking a dinner reservation or gathering profile information, on to automated systems that may no longer require direct human intervention. Users converse with a bot using text, interactive cards, and speech. A bot interaction can be a quick question and answer, or it can be a sophisticated conversation that intelligently provides access to services.

Analyze the decision criteria

In this unit, you'll analyze the criteria experts employ when choosing an Azure artificial intelligence (AI) service for a given business need. Understanding the criteria can also help you better understand the nuanced differences between each product.

Are you building a virtual agent that interfaces with humans via natural language?

Use the Bot Service when you need to create a virtual agent to interact with humans using natural language. The Bot Service integrates knowledge sources, natural language processing, and form factors to allow interaction across different channels.

Bot Service solutions usually rely on other AI services for things like natural language understanding or even translation for localizing replies into the customer's preferred language.

Before jumping in to build a custom chat experience using Azure Bot Service, it might make sense to search for pre-built, no-code solutions that cover common scenarios. For example, QnA Maker, available from Azure Marketplace, allows you to build, train, and publish a sophisticated bot using FAQ pages, support websites, product manuals, SharePoint documents, or editorial content through an easy-to-use UI or via REST APIs. Likewise, Power Virtual Agents integrates with Microsoft's Power Platform allowing you to use hundreds of prebuilt connectors for data input. You can extend the Power Virtual Agent by building custom workflows with Power Automate, and if you feel that the out-of-the-box experience is too limiting, you can still build more complex interactions with Microsoft Bot Framework.

Do you need a service that can understand the content and meaning of images, video, audio, or translate text into a different language?

Use Azure Cognitive Services when it comes to general purpose tasks like performing speech to text, integrating with search, identifying the objects in an image, and so on. Azure Cognitive Services is

3 https://azure.microsoft.com/services/bot-service/?azure-portal=true

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

"general purpose", meaning that many different kinds of customers can benefit from the work Microsoft has already done to train and test these models and offer them inexpensively at scale.

Do you need to predict user behavior or provide users with personalized recommendations in your app?

Azure Cognitive Services' Personalizer service watches your users' actions within an application and can be used to predict their behavior and provide relevant experiences as it identifies usage patterns. Here again, you could capture and store user behavior and create your own custom Azure Machine Learning solution to do these things, but this approach would require much effort and expense.

Will your app predict future outcomes based on private historical data?

Choose Azure Machine Learning when you need to analyze data to predict future outcomes. For example, suppose you need to analyze years worth of financial transactions to discover new patterns that could help you create new products and services for your company's clients and offer those new services during routine customer service calls. When you're working with proprietary data then you will likely need to build a more custom, tailored machine learning model.

Do you need to build a model using your own data, or perform a different task than those listed above?

Use Azure Machine Learning for maximum flexibility. Data scientists or AI engineers can use tools they are familiar with, and data that you provide, to develop deep learning and machine learning models tuned for your particular requirements.

Use Machine Learning for decision support systems

Tailwind Traders' ecommerce website allows customers to browse and purchase items that can be delivered or can be picked-up from a retail store nearest to their location.

The Marketing department is convinced that they can increase sales dramatically by suggesting add-on products from their catalog that complement the items in the shopper's cart at the moment of checkout. They could hard-code these suggestions, but they feel a more organic approach would be to use years' worth of sales data as well as new shopping trends to decide what products to display to the shopper. Furthermore, the suggestions could be influenced by factors like product availability, product profitability, and other factors.

The Marketing department's existing data science experts have already done some initial analysis of the problem domain, and have determined that it may take months to prototype, and possibly a year to roll out.

Which service should we choose?

Let's apply the decision criteria we learned about in the previous unit to find the right option.

First, is Tailwind Traders building a virtual agent that interfaces with humans via natural language? No, Azure Bot Service is not a good candidate for this scenario.

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

Second, does Tailwind Traders need a service that can understand the content and meaning of images, video, audio, or translate text into a different language? No, so those relevant Cognitive Services will not help us.

Third, does Tailwind Traders need to predict user behavior or provide users with personalized recommendations? Yes! However, creating recommendations based on user behavior is only part of the requirement. Tailwind Traders needs to create a complex model that incorporates historical sales data, trending sales data, inventory, and more. It's possible that Azure Cognitive Service's Personalizer service could play a role, but it couldn't handle the entire breadth of the project alone.

Finally, will the Tailwind Trader app predict future outcomes based on private historical data? Yes, and that is why in this scenario, Azure Machine Learning is likely the best choice.

The success of this effort would depend primarily on the strength of the model to select just the right up-sale products to suggest to the shopper. Given that the model would need to be tweaked and tuned over time, an off-the-shelf model would likely not suffice.

Furthermore, it sounds like the Marketing department already employs some data science experts, and they are willing to make at least a year-long commitment to building, testing, and tweaking the models to be used.

Use Cognitive Services for data analysis

The first generation of the Tailwind Trader's ecommerce website was available exclusively in English. However, the Marketing department sponsored a demographics study for their brick-and-mortar locations. On average, only 80% of potential customers spoke English, and that proportion falls to 50% in some neighborhoods. The Marketing department sees the addition of multiple languages as a wonderful opportunity to serve non-English speakers with the same online ecommerce experience as English speakers.

Which service should we choose?

Just like we did in the previous unit, let's apply the decision criteria we learned about in the previous unit to find the right option.

First, is Tailwind Traders building a virtual agent that interfaces with humans via natural language? No, so Azure Bot Service is not a good candidate for this scenario. However, should Tailwind Traders ever implement a customer service agent, they may want to consider using the Translator's APIs to provide real-time translation to help customers who are not English speakers.

Second, does Tailwind Traders need a service that can understand the content and meaning of images, video, audio, or translate text into a different language? Yes! Translating textual content from one language into another is a general purpose task that is made easy using Azure Cognitive Service's Translator service. It's easy to integrate in your applications, websites, tools, and solutions. It allows you to add multi-language user experiences in more than 60 languages, and can be used on any hardware platform with any operating system for text-to-text language translation.

Azure Cognitive Services is likely the best option for this scenario, but let's continue applying the decision criteria to make sure.

Third, does Tailwind Traders need to predict user behavior or provide users with personalized recommendations? No, the Azure Cognitive Services Personalizer is not a good candidate for this scenario.

Finally, will the Tailwind Trader app predict future outcomes based on private historical data? No. While it would be possible to create a Machine Learning model to perform multi-language translation, it would be expensive and time consuming for Tailwind Traders to attempt to do build translation models them-

selves. They do not have the deep learning competency, nor the linguistic data required to train the models.

Now that we've examined all of the expert criteria, we can confidently select Cognitive Services as the best product option for this scenario.

Use Bot Service for interactive chat experiences

The Customer Service department has long asked for a virtual agent to handle the vast majority of questions they get asked. As it turns out, no matter how prominent they make the answers to the most frequently asked questions on the website, shoppers are impatient and perceive contact in a chat window as saving them time.

The Customer Service team would want the shopper to feel as though they were interacting with a real human. When it becomes clear that the virtual agent cannot provide an answer to the question, the chat session should be transferred to a human.

A virtual agent would decrease the amount of time it takes for all shoppers to receive answers. The virtual agent could answer the vast majority of questions, which would free up human customer service agents to provide support for more difficult questions or thorny account-related issues.

Which service should we choose?

Once again, let's apply the decision criteria we learned about in the previous unit to find the right product.

First, is Tailwind Traders building a virtual agent that interfaces with humans via natural language? Yes! Azure Bot Service should be used in this scenario to implement a virtual agent chat experience. The Bot Service could benefit from the Frequently Asked Questions page on the website along with thousands of chat sessions that have been stored between shoppers and customer service representatives. Customer Service supervisors can test and tweak the answers to continue to refine the chat experience.

Even though we've likely found the best option for this scenario, let's keep applying our decision criteria to see if there's any additional options that we might also employ.

Second, does Tailwind Traders need a service that can understand the content and meaning of images, video, audio, or translate text into a different language? Possibly, yes. In this scenario, Azure Cognitive Services could be used along with Bot Services to build the solution. The developers could explore using pre-built solutions like QnA Maker (part of Cognitive Services) or Power Virtual Agents to expedite implementing the feature. Also, any Azure Bot Solution would likely implement several Azure Cognitive Services like Language Understanding (LUIS) and possibly Translator to translate from the shopper's language to English and back again.

Third, does Tailwind Traders need to predict user behavior or provide users with personalized recommendations? No, the Azure Cognitive Services Personalizer is not a good candidate for this scenario.

Finally, will the Tailwind Trader app predict future outcomes based on private historical data? No. While it might be possible to create a chat solution using Azure Machine Learning given that Tailwind Traders does have historical data to feed into a model, there's already an existing option that is tailored for the chat bot experience.

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

Choose the best tools to help organizations build better solutions

Introduction

Modern software development practices are supported by tools encompassing virtually every aspect of the software development life cycle. Microsoft has created a comprehensive set of tools that help organizations implement DevOps practices, build solutions, and save money while developing solutions. In this module we'll learn how to choose the right tools to support those practices.

Tailwind Traders has experimented with various software development processes and tools, however until now there has been no organizational commitment to shift to a DevOps mindset. Likewise, there's been no planned, coordinated effort to standardize on a set of core tools and processes. Several new initiatives at the company accentuate the need for agile, repeatable, dependable management and deployment of software systems. Tailwind Traders believes that the adoption of DevOps tooling and practices to be critical to their future success.

In this module, you'll discover the different software development process tools from Microsoft. You'll explore the criteria experts would use to make the right choice. And you'll make key distinctions between similar offerings.

By the end of this module, you'll be able to choose the best software development process tools and services that align to your organization's goals and practices.

Learning objectives

By the end of this module, you will be able to:

- Choose the best software development process tools and services for a given business scenario.

Prerequisites

- A development or operations background is valuable but not required.
- It would be helpful for you to already be familiar with the concept of DevOps, it's larger purpose in the organization, it's goals, outcomes, and so on.
- Likewise, familiarity with concepts like the Software Development Lifecycle, Source Code Management / Version Control, the different forms of testing, Continuous Integration / Continuous Delivery, Continuous Deployment, Infrastructure as Code, and so on, will help you immediately understand the value of the tools covered in this module.

Understand your product options

Software developers and operations professionals strive to create working software systems that satisfy the needs of the organization. However, sometimes their short-term objectives are at cross purposes with each other resulting in technical issues, delays, and downtime.

DevOps is a new approach that helps to align technical teams to work towards their common goal. To accomplish this, organizations employ practices and processes that seek to automate the ongoing development, maintenance, and deployment of software systems to expedite the release of software changes, ensure the ongoing deployability of the system, and ensure all changes meet a high-quality bar. When done correctly, DevOps practices and processes touch nearly every aspect of the company, not to

mention the software development lifecycle, including planning, project management, and software developer collaboration with each other, as well as with operations and quality assurance teams. Tooling automates and enforces most of the practices and processes, making it both difficult and unnecessary to work around.

DevOps requires a fundamental mindset change from the top down. Organizations cannot merely install software tools or adopt services and hope to get all of the benefits promised by DevOps.

In this module, however, we will only focus on just the tools from Microsoft that can help accomplish some of the objectives of DevOps. Alternatively, for organizations that are not ready to fully embrace the power of DevOps, they can support technical teams in their cloud development activities. If you're interested in learning more about DevOps in general, Microsoft Learn has **several learning paths and modules**[4] that can help you.

Microsoft offers tools to enable source code management, Continuous Integration / Continuous Delivery, and automating the creation of testing environments. Sometimes it seems as though these tools overlap in functionality, so in this module you'll learn about the product options and when to choose one product over another.

Product options

At a high level, there are three primary offerings, each of which are aimed at a specific audience and use case, and provide a diverse set of tools, services, programmatic APIs, and more.

Azure DevOps Services

Azure DevOps is a suite of services that address every stage of the Software Development Lifecycle (SDL).

- **Azure Repos** is a centralized source code repository where software development, DevOps engineering, and documentation professionals can publish their code for review and collaboration.
- **Azure Boards** is an agile project management suite that includes Kanban boards, reporting, tracking ideas and work from high-level epics to work items and issues.
- **Azure Pipelines** is a Continuous Integration/Continuous Delivery (CI/CD) pipeline automation tool.
- **Azure Artifacts** is a repository for hosting artifacts (for example, the compiled source code), which can be fed into testing or deployment pipeline steps.
- **Azure Test Plans** is an automated test tool that can be used in a CI/CD pipeline to ensure quality before releasing the software.

Azure DevOps is a mature tool with a large feature set that began its live as on-prem server software and evolved into a software as a service (SaaS) offering from Microsoft.

GitHub and GitHub Actions

GitHub is arguably the world's most popular code repository for open-source software. While git is decentralized source code management tool, GitHub is a hosted version of git that serves as the primary remote. GitHub builds on top of git to provide related services for coordinating work, reporting and discussing issues, providing documentation, and more. It includes the following functionality:

- Shared source Code repository, including tools that enable developers to perform code reviews by adding comments and questions in a web-view of the source code before it can be merged into the main code base.

4 https://docs.microsoft.com/learn/browse/?terms=DevOps&azure-portal=true

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

- Project management, including Kanban boards
- Issue reporting, discussion, and tracking
- Continuous Integration / Continue Deployment (CI/CD) pipeline automation tooling
- A wiki for collaborative documentation
- Can be run from the cloud or on-prem

Most relevant for this module, GitHub Actions enables workflow automation with triggers for many lifecycle events, for example, automating a Continuous Integration / Continuous Deployment toolchain.

A **toolchain** is a combination of software tools that aid in the delivery, development, and management of software applications throughout the systems development life cycle. The output of one tool in the toolchain is the input of the next tool in the toolchain. Typical tools range from ones that perform automated dependency updates, to building and configuring the software, to delivery of the build artifacts to different locations, to various forms of testing, and so on.

With so many similar features to Azure DevOps, you might wonder which to choose for your organization. Unfortunately, the answer to this question may not be straightforward.

While both Azure DevOps and GitHub both allow public and private code repositories, GitHub has a long and trusted history with public repositories and is trusted by tens of thousands of open-source projects. GitHub is “lighter weight” than Azure DevOps, with a focus on individual developers contributing to open source. Azure DevOps, on the other hand, is more focused on enterprise development with heavier project management and planning tools, and finer-grained access control.

Note: It's important to note that you are not limited to choosing either Azure DevOps Services or GitHub and GitHub Actions. In practice, you can mix and match these services as needed. For example, you can use GitHub repos with Azure Boards for work item tracking.

Azure DevTest Labs

Azure DevTest Labs provides an automated means of managing the process of building, setting up, and tearing down Virtual Machines containing builds of your software projects so that developers and testers can perform tests across different environments and builds. And it's not limited to VMs. Anything you can deploy in Azure via an ARM template can be provisioned through DevTest Labs. Provisioning pre-created lab environments with required configurations and tools already installed is a huge timesaver for quality assurance professionals and developers.

Suppose you need to test a new feature on an old version of an operating system. Azure DevTest Labs can set up everything automatically upon request. Once the testing is complete, DevTest Labs can shut down and deprovision the VM to save money when not in use. Management can restrict how many labs can be created, how long they run, and so on, to control costs.

Analyze the decision criteria

In this unit, you'll analyze the criteria experts employ when choosing a DevOps tool or service for a given business need. Understanding the criteria can also help you better understand the nuanced differences between each product.

Do you need to automate and manage test lab creation?

If your aim is to automate the creation and management of test lab environments, you should chose Azure DevTest Labs. It is the only of the three tools/services that offer this functionality.

However, provisioning new labs can be automated as part of a toolchain using Azure Pipelines or GitHub Actions.

Are you building open-source software?

While Azure DevOps can publish public code repositories, GitHub has long been the defacto host for open-source software. If you are building open-source software, you would likely choose GitHub if for no other reason than visibility and general acceptance by the open-source development community.

The remainder of the decision criteria is specific to choosing between either Azure DevOps or GitHub.

Note: You are not limited to choosing either Azure DevOps Services or GitHub and GitHub Actions. In practice, you can mix and match these services as needed. For example, you can use GitHub repos with Azure Boards for work item tracking.

Regarding source code management and DevOps tools, what level granularity do you need for permissions?

GitHub works on a simple model of read/write permissions to every feature. Meanwhile, Azure DevOps has a much more granular set of permissions that allow organizations to refine who is able to perform most operations across the entire toolset.

Regarding source code management and DevOps tools, how sophisticated does your project management and reporting need to be?

While GitHub has work items, issues, and a Kanban board, project management and reporting is the area where Azure DevOps excels. Azure DevOps is highly customizable, allowing an administrator to add custom fields to capture metadata and other information along side each work item. By contrast, GitHub Issues uses tags as its primary means of helping a team categorize issues.

Regarding source code management and DevOps tools, how tightly do you need to integrate with third-party tools?

While there's no specific recommendation here, it's important to understand your organization's existing investments in tools and services and evaluate how these dependencies might impact your choice. It's likely that most vendors creating DevOps tools create hooks or APIs that can be leveraged by both Azure Pipelines and GitHub Actions. Even so, it's probably worth the effort to validate that assumption.

Use Azure DevOps to manage the application development lifecycle

The software development team at Tailwind Traders works on many different projects, both for internal and external usage. They need to provide project sponsors and managers executive level reporting, including burndown charts, track progress against epics, and track custom information specific to Tailwind Traders in each work item and bug report.

Furthermore, as Tailwind Traders grows and hires contractors and outside vendors for short-term work, upper management wants to ensure that these individuals have access to only the information they need to do their work.

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

Which services should we choose?

Let's apply the decision criteria we learned about in the previous unit to find the right option.

First, does Tailwind Traders need to automate and manage test lab creation? No. So, in this scenario, Azure DevTest Labs is not a candidate since it's not intended for this specific use case.

Second, is Tailwind Traders building open-source software? While it's not stated specifically, Tailwind Traders is building internal and external systems, like their eCommerce system, which is not open source. So, that is not a consideration in this scenario.

Third, what level granularity does Tailwind Traders need for permissions? In the opening paragraph, it stated that Tailwind Traders will hire temporary employees and vendors for short-term work, and so granular permissions is an important consideration to upper management. Given what we talked about in the previous unit, this feature would make Azure DevOps a leading candidate. Using Azure DevOps, administrators would also have a more robust set of options to control permissions across the entire portfolio of work.

Fourth, does Tailwind Traders require a sophisticated project management and reporting solution? Yes, robust project management and reporting features are one of the primary considerations. Here again, given the amount of work item customization and reporting they want, Azure DevOps would likely be a good choice.

Fifth, does Tailwind Traders require tight integration with any third-party DevOps tools? Tool integration was not listed as a primary consideration for this scenario. As stated in the previous unit, most third-party DevOps tools integrate with both Azure DevOps and GitHub, so it's likely that they'll find the tools they need for specific functionality they need.

Use GitHub to contribute to open-source software

Tailwind Traders hopes to publish an API that would allow third-parties to integrate their own inventories of new and used items that would allow Tailwind Traders to offer a wider variety of products directly from their ecommerce site.

While the internal implementation of the API is closed source, Tailwind Traders wants to create a set of examples that call the API to perform various actions. They need a platform to share example code, collect feedback on the API, allow contributors to report issues, and build a community around feature requests.

Which service should we choose?

Just like we did in the previous unit, let's apply the decision criteria we learned about in the previous unit to find the right option.

First, does Tailwind Traders need to automate and manage test lab creation? No. So, in this scenario, Azure DevTest Labs is not a candidate since it's not intended for this specific use case.

Second, is Tailwind Traders building open-source software? Yes! As we noted in a previous unit, developers are used to seeing this kind of content available on GitHub. With GitHub, Tailwind Traders can publish their code, accept community contributions to improve the code examples, accept feedback and bug reports, and more. The fact that this scenario involves open-source code, GitHub is a leading candidate.

Third, what level granularity does Tailwind Traders need for permissions? While not stated explicitly, the fact that Tailwind Traders will be accepting community contributions, issue reports, and generally attempting to build a community of developers around their API examples, the permission needs are basic:

users can either “view only” or "view and write". This is another reason why GitHub would be a good candidate for this scenario.

Fourth, does Tailwind Traders require a sophisticated project management and reporting solution? Again, given the nature of this project, it does not require a sophisticated project management and reporting solution. In this scenario, one of Azure DevOps Services' greatest strengths is not required.

Fifth, does Tailwind Traders require tight integration with any third-party DevOps tools? Tool integration was not listed as a primary consideration for this scenario and doesn't qualify or disqualify either tool.

GitHub is the best choice for this scenario. While Azure DevOps could be used to make the repository public, some of the other features that involve the development community like feedback, bug reports, and so on, would be less accessible.

Use Azure DevTest Labs to manage testing environments

Tailwind Traders wants to be more methodical and careful when pushing new versions of their ecommerce website to production. They will expand their quality assurance team, and use the cloud to create and host VMs to create testing environments that match the production environment.

Management has concerns around costs of a more automated test environment. For instance, they want to make sure that the QA professionals are not wasting time configuring the testing environment to match the production environment. They want to ensure that VMs are destroyed when no longer in use. They want to limit the number of VMs that each quality assurance professional is allowed to spin up. Also, they want to ensure that each environment is configured correctly and consistently with their production environment.

Which service should we choose?

Once again, let's start by applying the decision criteria we learned about in the previous unit to find the right product.

First, does Tailwind Traders need to automate and manage test lab creation? Yes! This looks like a job for Azure DevTest Labs since it literally will do everything that Tailwind Traders needs to accomplish in this scenario.

We could continue evaluating the decision criteria from earlier, however Azure DevOps nor GitHub are needed for this specific scenario. Remember that Azure DevOps or GitHub could be used to create product releases that can automatically be included in VMs created for testing purposes.

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

Choose the best monitoring service for visibility, insight, and outage mitigation

Introduction

Modern software systems running in the cloud are complex, and gaining visibility into the health and performance of your application hosting environment across all of its layers of services is challenging. Fortunately, there are several solutions from Microsoft that help you react quickly to outages, research intermittent issues, optimize your usage, and be proactive in handling future planned downtime.

Tailwind Traders, a traditional brick-and-mortar retailer who has experienced explosive growth due to selling products online, is seeking to tighten and operationalize control of their cloud environment. They face several challenges, from the desire to optimize their cloud spend and security posture to tracking down intermittent issues and planning ahead for upcoming outages. However, they need help with choosing the right product option for these different scenarios.

In this module, you will learn about Microsoft's different monitoring solutions, and will analyze decision criteria that experts use to select the right service for a given scenario.

Learning objectives

By the end of this module, you will be able to:

- Choose the correct cloud monitoring service to address different kinds of business challenges.

Prerequisites

- You should be familiar with basic computing concepts and terminology
- Familiarity with cloud computing is helpful, but isn't necessary

Identify your product options

There are several basic questions or concerns that all companies face when using the cloud.

- Are we using the cloud correctly? Can we squeeze more performance out of our cloud spend?
- Are we spending more than we need to?
- Do we have our systems properly secured?
- How resilient are our resources? If there was a regional outage, could we failover to another region?
- How can we diagnose and fix issues that occur intermittently?
- How can we quickly determine the cause of an outage?
- How can we learn about planned downtime?

Fortunately, using a combination of monitoring solutions on Azure, you can gain answers, insights, and alerts that help you ensure that you've optimized your cloud usage, that you're able to ascertain the root cause of unplanned issues, and can prepare ahead of time for planned outages.

Product options

At a high level, there are three primary monitoring offerings, each of which are aimed at a specific audience and use case, and provide a diverse set of tools, services, programmatic APIs, and more.

Azure Advisor

Azure Advisor[5] evaluates your Azure resources and makes recommendations to help you improve reliability, security, and performance, achieve operational excellence, and reduce costs. Advisor is designed to help you save you time on cloud optimization. The recommendation service includes suggested actions you can take right away, postpone, or dismiss.

The recommendations are available via the Azure portal, as well as via API, and you can set up notifications to alert you to new recommendations.

When in the Azure portal, the Advisor dashboard displays personalized recommendations for all your subscriptions, and you can use filters to hone into recommendations for specific subscriptions, resource groups, or services. The recommendations are divided into five categories:

- **Reliability** - Used to ensure and improve the continuity of your business-critical applications.
- **Security** - Used to detect threats and vulnerabilities that might lead to security breaches.
- **Performance** - Used to improve the speed of your applications.
- **Cost** - Used to optimize and reduce your overall Azure spending.
- **Operational Excellence** - Used to help you achieve process and workflow efficiency, resource manageability, and deployment best practices.

Azure Monitor

Azure Monitor[6] is a platform for collecting, analyzing, visualizing, and potentially taking action based on the metric and logging data from your entire Azure and on-prem environment.

The diagram below illustrates just how comprehensive Azure Monitor is.

5 https://azure.microsoft.com/services/advisor/?azure-portal=true
6 https://azure.microsoft.com/services/monitor/?azure-portal=true

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

First, on the left, you see the sources of logging and metric data can be collected at every layer in your application architecture from application to operating system and network.

In the center, you see how that logging and metric data is stored in central repositories.

On the right, the data is used in a number of different ways. You can view real-time and historic performance across each layer of your architecture, or aggregated and detailed information. The data is displayed at different levels for different audiences. You can view high-level reports on the Azure Monitor Dashboard or create custom views using Power BI and Kusto queries.

Furthermore, the data can be used to help you react to critical events in real time, whether through alerts delivered to teams via SMS, email and so on. Or, you can use thresholds to trigger autoscaling functionality to scale up or down to meet the demand.

Some popular products like Azure Application Insights, a service for sending telemetry information from application source code to Azure, uses Azure Monitor under the hood. Application Insights allows application developers to leverage the powerful data analysis platform in Azure Monitor to provide you with deep insights into an application's operations and diagnose errors without waiting for a user to report them.

Azure Service Health

Azure Service Health[7] provides a personalized view of the health of the Azure services, regions, and resources you rely on. The site status.azure.com doesn't provide the full picture because it only shows major issues broadly impacting Azure customers. On the other hand, Service Health shows you everything impacting you, including major issues and smaller, localized issues. Service issues are rare, but it's important to be prepared for the unexpected. You can set up alerts that help you triage outages and planned maintenance. After an outage, it provides official incident reports that you can share with stakeholders called “root cause analyses”, or RCAs.

7 https://azure.microsoft.com/features/service-health/?azure-portal=true

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

There are several different event types that you can keep an eye on:

- **Service issues** are problems in Azure that affect you right now. For example, outages. You can drill into the impacted services, regions, updates from the engineering teams, and ways you can share and track the latest information.
- **Planned maintenance** events can affect your availability. You can drill into the impacted services, regions, and details on how that will impact you, and what you need to do. Most of these events are performed without any impact to you and won't be shown here. In the rare case that a reboot will be required, Service Health will allow you to choose when to perform the maintenance to minimize the impacted downtime.
- **Health advisories** are issues that require you to act to avoid service interruption, including service retirements and breaking changes. Health advisories are announced far in advance to allow you to plan.

Analyze the decision criteria

In this unit, you'll analyze the criteria experts employ when choosing an Azure artificial intelligence (AI) service for a given business need. Understanding the criteria can also help you better understand the nuanced differences between each product.

Do you need an analysis of how you're using Azure in order to reduce costs? Improve resilience? Harden your security?

Choose Azure Advisor when you are looking for an analysis of your deployed resources. Azure Advisor analyzes your configuration and usage of your resources and provides suggestions on how to optimize for reliability, security, performance, costs, and operations based on expert best practices.

Do you want to monitor Azure's services or your usage of Azure?

If you want to keep tabs on Azure itself, especially those services and regions you depend on, you want to visit Azure Service Health. You'll see the current status of those Azure services you rely on, upcoming planned outages, and services that will be sunlit. You can set up alerts so you can stay on top of incidents and upcoming downtime without visiting the dashboard on a regular basis.

However, if you want to keep track of the performance or issues related to your specific VM or container instances, databases, your applications, and so on, then you want to visit Azure Monitor and create reports and notifications to help you understand how your services are performing or diagnose issues related to your specific usage of Azure.

Do you want to measure custom events along side other usage metrics?

Choose Azure Monitor when you want to measure custom events along side other collected telemetry data. Custom events, like those added in the source code of your software applications, could help identify and diagnose why your application is behaving a certain way.

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

Do you need to set up alerts for outages or when autoscaling is about to deploy new instances?

Here again, you would use Azure Monitor to set up alerts for key events related to your specific resources.

Use Azure Advisor

Tailwind Traders wants to optimize their cloud spend. Also, they're concerned about security breaches since they store customer data and historic purchase data in cloud-based databases. As they ramp up their cloud expertise, they want to better understand their use of the cloud, better understand best practices, and pinpoint "easy wins" where they can tighten up their cloud spend and their security practices.

Which service should we choose?

Let's apply the decision criteria we learned about in the previous unit to find the right option.

First, in this scenario, does Tailwind Traders need an analysis of their Azure usage for the sake of optimization? Yes, Tailwind Traders understands they may be spending too much and is concerned about their security practices and would like to have their use of the cloud analyzed against industry best practices. Therefore, Azure Advisor is the perfect option for this scenario.

While we may have found the right product option, let's continue evaluating our decision criteria for this scenario.

Second, in this scenario, does Tailwind Traders want to monitor the health of Azure's services affecting all customers or the resources deployed on Azure? This scenario is not concerned with operations. However, Azure Advisor does analyze and provide recommendations for achieving operational excellence.

Third, in this scenario, does Tailwind Traders want to measure custom events along side other usage metrics? No, measuring custom events is not mentioned as a requirement and is not a consideration in this scenario.

Fourth, in this scenario, does Tailwind Traders want to set up alerts for outages or when autoscaling is about to deploy new instances? Again, this scenario is not concerned with operations. However, Azure Advisor does analyze and provide recommendations for achieving operational excellence.

Azure Advisor is the right product option to help Tailwind Traders better understand and optimize both their cloud spend and their cloud security posture, and may help them with other areas of their cloud usage as well.

Use Azure Monitor

Tailwind Traders' ecommerce website is experiencing intermittent errors and they're unsure of the cause. Given the nature of the errors, they suspect it's either a database or caching issue. What are the circumstances surrounding the errors? Does it happen only during peak usage times? What is the state of their Azure SQL instance? What is the state of their Redis caching server? How can they trace down the issues to a root cause?

Which service should we choose?

Just like we did in the previous unit, let's apply the decision criteria we learned about in the previous unit to find the right option.

First, in this scenario, does Tailwind Traders need an analysis of their Azure usage for the sake of optimization? No, optimization is not their objective in this scenario, so Azure Advisor is not a candidate.

Second, in this scenario, does Tailwind Traders want to monitor the health of Azure's services affecting all customers or the resources deployed on Azure? Given that this issue happens intermittently, it's unlikely that it affects an entire Azure region or service. It's more likely that there's a logic issue somewhere in their ecommerce website code, or some other issue causing database failures or caching locks. In this scenario, Azure Monitor could be used to pinpoint a specific user session, and look at the performance of each service involved in the issue to identify the underlying issue.

Third, in this scenario, does Tailwind Traders want to measure custom events along side other usage metrics? Yes, software developers can send additional information about the state of the web application via Application Insights to help locate the root cause of the issue. Application Insights relies on the Azure Monitor platform to store custom event information.

Fourth, in this scenario, does Tailwind Traders want to set up alerts for outages or when autoscaling is about to deploy new instances? No, alerting is not their objective in this scenario.

Azure Monitor is the best option for helping Tailwind Traders track down this intermittent issue. They can use a wealth of tools to help them gain insight into the application's performance at a high level and dive deep into specific issues.

Use Azure Service Health

Tailwind Traders wants to operationalize their cloud environment. Specifically, their cloud operations team wants to let stakeholders know about upcoming planned downtime in advance. They also want their solution architectures to be forewarned about Microsoft's plans to sunset services so they can rearchitect their software products accordingly.

Furthermore, when outages do happen, they want to quickly ascertain whether the issue is specific to their services or if it's a service interruption affecting many Azure customers. They also want to provide key stakeholders with reports when outages happen explaining how and why the incident occurred, and so on.

Which service should we choose?

Once again, let's apply the decision criteria we learned about in the previous unit to find the right product.

First, in this scenario, does Tailwind Traders need an analysis of their Azure usage for the sake of optimization? No. Not in this scenario. In that case, Azure Advisor is not a candidate for this scenario.

Second, in this scenario, does Tailwind Traders want to monitor the health of Azure's services affecting all customers or the resources deployed on Azure? In this scenario, the requirement is to stay abreast of upcoming planned downtime. Furthermore, they want to capture official incident reports. For this reason, Azure Service Health is the strongest candidate to choose for this scenario.

While it's likely that Azure Service Health will be chosen, let's continue evaluating the remaining decision criteria.

Third, in this scenario, does Tailwind Traders want to measure custom events along side other usage metrics? No, measuring custom events is not mentioned as a requirement and is not a consideration in this scenario.

Fourth, in this scenario, does Tailwind Traders want to set up alerts for outages or when autoscaling is about to deploy new instances? Setting up alerts for outages is a requirement in this scenario, but creating alerts for other events like autoscaling are not in scope. Use Azure Service Health to set up alerts

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

specific to Azure outages that affect all Azure customers. Use Azure Monitor to set up alerts for outages and other events that only affect your specific resources.

In this scenario, Azure Service Health is the correct option to choose.

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

Choose the best tools for managing and configuring your Azure environment

Introduction

Management tools allow administrators, developers, and managers interact with the cloud environment to perform tasks like deploying dozens or hundreds of resources at a time, configuring individual services programmatically, or viewing rich reports across usage, health, costs, and more. Microsoft Azure provides a mix of management tooling options to choose from, depending on the situation.

Tailwind Traders, a traditional brick-and-mortar retailer who has found explosive growth due to selling products online, owes much of their success to their ability to quickly and efficiently manage their cloud environment. However, when they were getting started with their cloud journey, they initially had to choose the right management tool for each unique scenario.

In this module, you will learn about Microsoft Azure's different management tools, and will analyze decision criteria that experts use to select the right tool for a given scenario.

Learning objectives

By the end of this module, you will be able to:

- Choose the correct Azure management tool to address different kinds of technical needs and challenges.

Prerequisites

- You should be familiar with basic computing concepts and terminology
- Familiarity with cloud computing is helpful, but isn't necessary

Identify the product options

At a high level, there are two types of management tools: visual tools and code-based tools. The visual tools provide full access to all of the functionality of Azure in a friendly visual manner. However, visual tools may be less useful when trying to set up a large deployment of resources with interdependencies and configuration options.

When attempting to quickly set up and configure Azure resources, a code-based tool is usually the better choice. While it may take time to understand the right commands and parameters at first, once typed, they can be saved into files and used repeatedly as needed. Furthermore, the code that performs setup and configuration can be stored, versioned, and maintained along with application source code in a source code management tool like git. This approach to managing hardware and cloud resources using the same mindset that developers use when they write application code is referred to as “infrastructure as code”.

There are two approaches to “infrastructure as code”: imperative and declarative code. Imperative code details each individual step that should be performed to achieve the desired outcome. By contrast, declarative code details only the desired outcome, and allows an interpreter to decide how to best achieve that outcome. This distinction is important because tools that are based on declarative code can provide a more robust approach to deploying dozens or hundreds of resources simultaneously and reliably.

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

Product options

Microsoft offers several different tools and services to manage your cloud environment, each aimed at different scenarios and users.

Azure portal

The Azure portal is a web-based user interface that allows you access virtually every feature of Azure. The Azure portal provides a friendly GUI to view all the services you're using, create new services, configure your services, and view reports. The Azure portal is how most users first experience Azure, though as your Azure usage grows, you'll likely choose a more repeatable code-centric approach to managing your Azure resources.

Azure mobile app

The Azure mobile app provides iOS and Android access to your Azure resources when you're away from your computer. You can do things like:

- Monitor the health and status of your Azure resources
- Check for alerts, quickly diagnose and fix issues, restart a web app or VM
- Run Azure CLI or PowerShell commands to manage your Azure resources

Azure PowerShell

Azure PowerShell is a shell that allows developers, DevOps and IT professionals execute commands called cmdlets, or “command-lets”. These commands call the Azure Rest API to perform every possible management task in Azure. The cmdlets can be executed independently or combined into a script file and executed together to orchestrate routine setup, tear-down, and maintenance of a single resource, multiple connected resources, or orchestrate the deployment of an entire infrastructure containing dozens or hundreds of resources from imperative code. Capturing the commands in a script makes the process repeatable and automatable.

Azure PowerShell is available for Windows, Linux, and Mac, and can be accessed in a web browser via the Cloud Shell.

Windows PowerShell has helped Windows-centric IT organizations automate many of their on-prem operations for many years and have built up a large catalog of custom scripts and cmdlets, as well as expertise.

Azure CLI

The Azure CLI (Command Line Interface) is an executable program that allows developers, DevOps, and IT professionals execute commands using bash. The commands call the Azure Rest API to perform every possible management task in Azure. The commands can be run independently or combined into a script and executed together to orchestrate routine setup, tear-down, and maintenance of a single resource or an entire environment.

In many respects, it is almost identical to Azure PowerShell in what you can do. Both run on Windows, Linux, and Mac, and can be accessed in a web browser via the Cloud Shell. The primary difference is the syntax. Those users who are already proficient in PowerShell can remain productive using their PowerShell expertise, while those users proficient in bash can continue using it.

Azure Resource Manager Templates

While it's possible to write imperative code in Azure PowerShell or the Azure CLI to setup and tear-down one Azure resource or orchestrate an entire infrastructure containing dozens or hundreds of resources, there's a better way implement this functionality. Azure Resource Manager (ARM) Templates allow you to describe the resources you want to use in a declarative JSON format. The benefit is that the entire ARM template is verified first before any code is executed to ensure the resources will be created and connected correctly, then it orchestrates the creation of those resources in parallel, meaning, if you need 50 instances of the same resource, all 50 instances are created at the same time. Ultimately, the developer, DevOps, or IT professional just needs to define the desired state and configuration of each resource in a template, and the Azure Resource Manager does the rest. Templates can even execute PowerShell and Bash scripts before or after the setup of a resource.

Analyze the decision criteria

In this unit, you'll analyze the criteria experts employ when choosing which Azure management tool to use for a given business need. Understanding the criteria can also help you better understand the nuanced differences between each product.

Do you need to perform one-off management / administrative / reporting actions?

Use either PowerShell or the Azure CLI if you need to quickly obtain the IP address of a VM you deployed, need to reboot a VM, or scale an app. You may keep custom scripts handy on your local hard drive for these types of operations that you perform occasionally.

By contrast, ARM templates express the infrastructure requirements for your application for a repeatable deployment. ARM templates not intended for one-time or one-off scenarios, though depending on the scenario it's possible to use them for this purpose. Still, you should prefer PowerShell / Azure CLI scripts (or the Azure portal).

Also, ARM templates can include PowerShell / Azure CLI scripts, and PowerShell / Azure CLI scripts can trigger the execution of ARM templates, so you have flexibility in choosing the right tool for your particular needs.

You could perform most (if not all) management and administrative actions via the Azure portal. If you're just learning Azure, or infrequently need to set up and manage resources, or prefer the visual interface to view reports, then it makes sense to take advantage of the visual presentation of data and settings of the Azure portal.

However, if you're a in cloud management or administrative role, relying solely on the Azure portal would require visual scanning and clicking to find the settings or information you want to work with. In these cases, it is often quicker and more repeatable to use Azure CLI or PowerShell.

The last option in this case is the Azure mobile app, which can be accessed via iOS or Android phone or tablet. While it is full featured, it's likely the best choice when a laptop is not readily available and you need to view and triage issues.

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

Do you need a way to repeatedly set up one or more resources and ensure that all the dependencies are created in the proper order?

ARM templates express the infrastructure requirements for your application for a repeatable deployment. A validation step ensures that all resources can be created, then the resources are created in the proper order based on dependencies, in parallel, and are idempotent.

By contrast, it is entirely possible to use PowerShell / Azure CLI to set up all of the resources for a desired deployment. However, there's no validation step, so if a script encounters an error, you cannot easily roll back the dependency resources, deployments happen serially, and only some operations are idempotent.

When scripting, do you come from a Windows administration or Linux administration background?

If you or your cloud administrators come from a Windows administration background, it's likely they will prefer PowerShell. If you or your cloud administrators come from a Linux administration background, it's likely they will prefer the Azure CLI. Pragmatically, either one can be used to perform most one-off administration tasks.

Use the Azure portal to visually understand and manage your cloud environment

Tailwind Traders uses Azure extensively throughout their entire organization. To make sure both the technical team and the executive team is aware of their cloud spend, the director of cloud operations will begin to meet weekly with the Chief Financial Officer (CFO) to talk about their cloud spend. Conversations may begin at a high level, but the two may want to dive in deep during the meeting to gain more insight on how Azure resources are being used. Ideally, they would be able to see the data displayed visually, but also be able to run custom reports in real time. Which tool can they use during their meeting?

Which service should we choose?

Let's apply the decision criteria we learned about in the previous unit to find the right option.

First, in this scenario, does Tailwind Traders need to perform one-off management / administrative / reporting actions? Yes, and given the requirement to view data visually and create custom reports during the meeting, the Azure portal is the best choice. The meeting attendees can quickly find answers to questions that they're looking for using a wealth of reporting options.

The next two decision criteria do not apply to this scenario since the director of cloud operations and the CFO will not be deploying or configuring any resources.

The Azure portal is the correct product option for this scenario.

Use Azure PowerShell for one-off administrative tasks

Tailwind Traders employs technologists with many different skills. A team of developers and admins build and maintain a collection of intranet applications that are vital to the business. This team has a strong background in Windows development and network administration. They moved their applications to the

cloud and need a way to perform one-off testing, management, and administrative tasks on their intranet environment. They quickly realized that managing Azure from the Portal takes too much time and is not repeatable. Which tool should they use for one-off tasks?

Which service should we choose?

Just like we did in the previous unit, let's apply the decision criteria we learned about in the previous unit to find the right option.

First, in this scenario, does Tailwind Traders need to perform one-off management / administrative / reporting actions? Yes. However, they already identified that they do not want to rely on the Azure portal for these one-off administration tasks. Therefore, either PowerShell or the Azure CLI are candidates. We'll hone in on the specific tool they should use in a moment.

Second, in this scenario, does Tailwind Traders need a repeatable and reliable means of deploying their entire infrastructure? No, not in this scenario. Therefore, ARM templates are not the right choice.

When scripting, does this team at Tailwind Traders come from a Windows administration or Linux administration background? This team has a Windows administration background, therefore they would likely be most comfortable using Azure PowerShell since it allows them to use the syntax they're most comfortable with to perform their one-off administration tasks.

Azure PowerShell is the best choice for this scenario.

Use the Azure CLI for one-off administrative tasks

As we noted in the previous scenario, Tailwind Traders employs technologists with many different skills. The DevOps team is primarily concerned with keeping external systems, like the ecommerce site, up and running. This team has a Linux administration background. They frequently need to perform administration tasks related to the health of their cloud environment. They quickly realized that managing Azure from the Portal takes too much time and isn't repeatable. Which tool should they use for one-off tasks?

Which service should we choose?

Once again, we'll apply the decision criteria we learned about in a previous unit to find the right option.

Given that this scenario is almost identical to the one in the previous unit, we can skip over the first two criteria. In other words, we can quickly eliminate ARM templates and the Azure portal as viable options for this scenario. So, let's skip to the third decision criteria.

Choosing the right option in this scenario should be determined by the team's background. Since this team has a Linux administration background, they would likely be most comfortable using the Azure CLI. The Azure CLI allows them to use the Bash shell and its syntax to perform their one-off administration tasks.

The Azure CLI is the best choice for this scenario.

Use the Azure mobile app to manage Azure on the go

Tailwind Traders experiences a surge in ecommerce traffic at certain times of the year that coincide with national holidays and weekends. The first few years, the director of cloud operations has requested that

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

everyone who manages a critical system come into the office during these important dates. However, now that Tailwind Traders has successfully operationalized most critical systems, the director wants to relax this requirement and allow employees to spend these dates with their families. Is there a product that can help in this scenario?

Which service should we choose?

Let's run through our decision criteria again.

First, does Tailwind Traders need to perform one-off management / administrative / reporting actions? Yes. The real question is, how? In this case, a phone or tablet solution could help key employees keep an eye on the health of the cloud environment. The Azure mobile app is likely a good compromise, allowing employees the freedom to be away from the office while still having the capability to perform one-off management and administrative tasks.

Frankly, we can skip the rest of the decision criteria in this unique scenario. The Azure mobile app is the right choice.

Use ARM templates to deploy an entire cloud infrastructure

Tailwind Traders wants to operationalize their cloud deployments. They need a repeatable and reliable way to scale their operations during peak sales dates. Since we'll be choosing a process for scaling our production environment, we need to ensure that our choice:

- Is efficient and can potentially create many resources in parallel.
- Creates all dependencies in the correct order.
- Can be used without worrying that it failed in the middle of provisioning the necessary infrastructure.

Which service should we choose?

Let's run through our decision criteria one more time.

First, in this scenario, does Tailwind Traders need to perform one-off management / administrative / reporting actions? This time, we're not looking for one-time or one-off management or administration tasks. In other words, we're looking for a technology we can use to automate the deployment of our entire infrastructure as needed.

Second, does Tailwind Traders need a repeatable and reliable means of deploying their entire infrastructure? Yes, repeatable and reliable deployment is exactly what we need. Our decision criteria leads us to choose Azure ARM templates for this scenario.

We could possibly use Azure PowerShell or the Azure CLI, however these scripting technologies have significant limitations when it comes to deploying your infrastructure. ARM templates overcome these limitations.

The third decision criteria assumes we need to write a script using imperative code. However, using ARM templates, you define your infrastructure declaratively using JSON. In some instances, you still may need imperative code for configuration or clean-up tasks. In these cases, you can trigger the execution of scripts, either Azure PowerShell or Azure CLI, to perform these tasks.

In this scenario, Azure ARM templates is the correct choice.

Choose the best Azure serverless technology for your business scenario

Introduction

Serverless computing is a term used to describe an execution environment that is set up and managed for you. You merely specify what you want to happen by writing code or connecting and configuring components in a visual editor, and specify the action that triggers your functionality, like a timer or an HTTP request. Best of all, you never have to worry about an outage, your code can scale instantly to meet demand, and you only pay based on the actual usage of your code.

Tailwind Traders, a traditional brick-and-mortar retailer who has found success selling online. They see several opportunities to improve their ecommerce website. For example, they want to provide more accurate real-time inventory information online for those customers who want to visit their local store to purchase an item. They also want to respond more proactively to customers who had a negative experience with a new customer retention program. They suspect that serverless computing can help them, but they need help understanding which Azure solution is right for a given business scenario.

In this module, you will learn about two serverless computing solutions on Azure; Azure Functions and Azure Logic Apps. You'll learn what they are, how they're different, and when you should choose one over the other.

By the end of this module, you will be able to choose the right serverless computing service from Azure for a specific business scenario.

Learning objectives

By the time you finish this module, you will be able to:

- Choose the right serverless computing technology for your business scenario.

Prerequisites

- You should understand the idea of orchestration and workflows.
- You should understand what an API, or Application Programming Interface is.
- You should be familiar with other Microsoft products at a high level, like Dynamics 365 and Office 365.

Identify the product options

Serverless computing is a cloud-hosted execution environment that runs your code but abstracts the underlying hosting environment. The term “serverless computing” is a misnomer. After all, there *is* a server (or a group of servers) that executes your code or desired functionality. The key idea is that you are not responsible for setting up or maintaining that server. You don't have to worry about scaling the server when there's an increased demand, and you don't have to worry about outages. The cloud vendor takes care of all of maintenance and scaling concerns for you.

You create an instance of the service and you add your code. No infrastructure configuration or maintenance is required, or even allowed. You configure your serverless apps to respond to events. An event could be a REST endpoint, a periodic timer, or even a message received from another Azure service. The serverless app runs only when it's triggered by an event. Scaling and performance are handled automatically, and you are billed only for the exact resources you use. You don't even need to reserve resources.

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

Typically “serverless computing” is used to handle "backend" scenarios. In other words, it's responsible for sending message from one system to another, or processing messages that were sent from other systems. It's not used for end-user facing systems, but rather works in the background.

There are two Azure serverless computing services that we'll cover in this module: Azure Functions and Azure Logic Apps.

Azure Functions

Azure Functions[8] allows you to host a single method or function using a popular programming language in the cloud that runs in response to an event, like an HTTP request, a new message on a queue, or on a timer. Due to their atomic nature, Azure Functions can serve many purposes in an application's design. They can be written using many common programming languages like C#, Python, JavaScript, Typescript, Java, and PowerShell.

Azure Functions scale automatically, and charges accrue only when a function is triggered, so they're a solid choice when demand is variable. For example, you may be receiving messages from an IoT solution that monitors a fleet of delivery vehicles. You'll likely have more data arriving during business hours. Azure Functions can scale out to accommodate these busier times.

Furthermore, Azure Functions is a stateless environment; Functions behave as if they're restarted every time they respond to an event. This feature is ideal for processing incoming data. And if state is required, they can be connected to an Azure storage service.

Azure Functions can perform orchestration tasks using an extension called Azure Durable Functions, which allows developers to chain Functions together while maintaining state.

Azure Functions is ideal when you're only concerned with the code running your service and not the underlying platform or infrastructure. Azure Functions is commonly used when you need to perform work in response to an event, often via a REST request, timer, or message from another Azure service, and when that work can be completed quickly, within seconds or less.

Azure Logic Apps

Logic Apps[9] is a low-code/no-code development platform hosted as a cloud service that helps you automate and orchestrate tasks, business processes, and workflows when you need to integrate apps, data, systems, and services across enterprises or organizations. Logic Apps simplifies how you design and build scalable solutions, whether in the cloud, on premises, or both, for app integration, data integration, system integration, enterprise application integration (EAI), and business-to-business (B2B) integration.

Azure Logic Apps is designed in a web-based designer and can execute logic triggered by Azure services without writing any code. You build an app by linking triggers to actions with connectors. A trigger is an event that causes your app to execute, like a timer, a new message sent to a queue, or an HTTP request. An action is a task or step that can execute. There are logic actions like you would find in most programming languages like working with variables, decision statements and loops, as well as tasks to parse and modify data.

To build enterprise integration solutions with Azure Logic Apps, you can choose from a growing gallery of over 200 connectors. These include services such as Salesforce, SAP, Oracle DB, and file shares.

If you can't find the action or connector you need, you can build your own using custom code.

8 https://azure.microsoft.com/services/functions/?azure-portal=true
9 https://azure.microsoft.com/services/logic-apps/?azure-portal=true

What's the difference between these services?

You can call Azure Functions from Azure Logic Apps, and vice versa. The primary difference is the intent of each service. Azure Functions is a serverless compute service, while Azure Logic Apps is intended to be a serverless orchestration service. While there's nothing stopping you from using Azure Functions to orchestrate a long running business process involving many different types of connections, this was not its primary use case when it was designed. Furthermore, you can see a difference in how the two services are priced. Azure Functions is priced based on the number of executions and the running-time of each execution while Logic Apps is priced by the number of executions and the type of connectors that are utilized.

Analyze the decision criteria

With two viable serverless options, it can be difficult to know which is the best one for the job. In this unit, we'll analyze the criteria that experts employ when deciding which serverless service to use for a given business need. Understanding the criteria can also help you better understand the nuanced differences between each product.

Do you need to perform an orchestration across well-known APIs?

As we noted previously, Azure Logic Apps was designed with orchestration in mind, from the web-based visual configurator to the pricing model. It excels at connecting a large array of disparate services via their APIs to pass and process data through many steps in a workflow.

It's possible to create the same workflow using Azure Functions, but it might take a considerable amount of time researching which APIs to call and how to call them. Azure Logic Apps has already componentized these API calls so that you only supply a few details and the details of calling the necessary APIs is abstracted away.

Do you need to execute custom algorithms or perform specialized data parsing and data lookups?

Azure Functions allows you to use the full expressiveness of a programming language in a compact form, allowing you to concisely build complex algorithms, or data lookup and parsing operations. You would be responsible for maintaining the code, handling exceptions resiliently, and so on.

While Azure Logic Apps has the ability to perform logic (loops, decisions, and so on) if you had a logic intensive orchestration that required a complex algorithm, the implementation of that algorithm might be more verbose and visually overwhelming.

Do you have existing automated tasks written in an imperative programming language?

If you already have your orchestration or business logic expressed in C#, Java, Python, or other popular programming language, it might be easier to port your code into the body of an Azure Function than re-create it using Azure Logic Apps.

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

Do you prefer a visual (declarative) workflow or writing (imperative) code?

Your ultimate choice will really come down to whether you prefer to work in a declarative environment or an imperative environment. Developers who have expertise in an imperative programming language may prefer to think about automation and orchestration from an imperative mindset. IT Professionals and business analysts may prefer to work in a more visual low-code/no-code environment.

Use Azure Functions

Data about each product that's sold at Tailwind Traders is packaged up as a JSON message and sent to an event hub. The event hub distributes the JSON message to subscribers allowing different systems to be notified.

Tailwind Traders wants to upgrade their eCommerce site to include real-time inventory tracking. Currently, the website updates product availability each night at 2:00 AM. A Windows Service written in C# contains all of the necessary logic to retrieve the messages, parse the JSON, perform a look-up across multiple databases to find additional product information and potentially send notifications to the purchasing department so that they can reorder quantities that fall below certain levels. The Windows Service runs in a VM hosted on Azure.

Most of the time, this system works fine. However, some products are in high demand, and some products are kept in low quantities at each store. Several times a day, customers drive to the store to pick up an item only to find that it is no longer in stock.

Instead of running the algorithm on a nightly basis, they want to run the inventory updater each time a product is purchased.

Which service should we choose?

Since Tailwind Traders already has the logic written in C#, it would make sense to copy the relevant C# code from the Windows Service and port it to an Azure Function. The developers would bind the function to trigger each time a new message appears on a specific queue.

Why not choose Azure Logic Apps?

It's possible that the same logic could be implemented in Azure Logic Apps. However, since the team has already invested time in building the service in C#, they can leverage it for use in an Azure Function.

Use Azure Logic Apps

Tailwind Traders sends out invitations to participate in a customer satisfaction survey randomly after a purchase. Currently, the customer satisfaction is aggregated, averaged, and charted. However, the customer service department sees an opportunity to be proactive and reach out to customers who provide low scores and leave comments with a negative sentiment.

Ideally, responses with negative customer satisfaction scores would trigger a customer retention workflow. First, a sentiment analysis would be generated based on the free-form comments, an email sent to the customer with an apology and a coupon code, and the message would be routed to a Dynamics 365 Customer Service so that a follow-up email could be scheduled.

Unfortunately, there's no developer resources available to take on this project, however the customer service team works with several cloud and IT professionals who might be able to construct a solution.

Which service should we choose?

In this scenario, Azure Logic Apps would likely be the best solution. A cloud or IT professional could use existing connectors to perform a sentiment analysis using the Cognitive Services connector, send an email using the Office 365 Outlook connector, and create a new record and follow-up using the Dynamics 365 Customer Service connector.

Since Azure Logic Apps is a low-code/no-code service, no developers would be needed. A cloud or IT professional should be able to build and support this workflow.

Why not choose Azure Functions?

While it is possible to build this entire solution using Azure Functions, it might be challenge given that no software developers can be committed to this project. Furthermore, it's an ideal scenario for Azure Logic Apps. Connectors already exist for each of the steps outlined in the workflow. It would take quite a bit of research, development, and testing for a developer to build a solution that utilizes all of these disparate software systems.

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

Choose the best Azure IoT service for your application

Introduction

The Internet of Things (IoT) bridges the physical world and digital world by enabling devices with sensors and an internet connection to communicate with cloud-based system via the internet.

Tailwind Traders sees many opportunities to use Azure's IoT services across many different facets of their operations, from new product development to logistics to point-of-sale.

In this module, you'll help Tailwind Traders select the right Azure IoT service offering for a given business scenario. You will learn about the various services, what they do, how they're different or complimentary, and when to use them by evaluating a set of decision criteria.

By the end of this module, you will be able to choose the best Azure IoT service for a given business scenario.

Learning objectives

By the end of this module, you will be able to:

- Choose the best Azure IoT service for a given business scenario.

Prerequisites

- You should be familiar with basic computing concepts and terminology
- Familiarity with cloud computing is helpful, but isn't necessary

Identify the product options

The Internet of Things (IoT) is the ability for devices to gather and then relay information for data analysis. Smart devices are equipped with sensors that collect data. A few common sensors that measure attributes of the physical world include:

- Environmental sensors that capture temperature and humidity levels
- Barcode, QR code, or Optical Character Recognition (OCR) scanners
- Geo-location and proximity sensors
- Light, color, and infrared sensors
- Sound and ultrasonic sensors
- Motion and touch sensors
- Accelerometer and tilt sensors
- Smoke, gas, and alcohol sensors
- Error sensors to detect when there's a problem with the device
- Mechanical sensors that detect anomalies or deformations
- Flow, level, and pressure sensors for measuring gasses and liquids

Using Azure IoT services, devices that are equipped with these kinds of sensors and that can connect to the internet could send their sensor readings to a specific endpoint in Azure via a message, where the message's data is collected, aggregated, and can be converted into reports and alerts. Or, all devices could be updated with new firmware to fix issues or add new functionality by sending software updates from Azure's IoT services to each device.

Let's suppose your company manufactures and operates smart refrigerated vending machines. What kinds of information would you want to monitor? You may want to ensure that each machine is operating without any errors, make sure the machine has not been compromised, you may want to make sure that its refrigeration system is keeping the contents within a certain temperature range, and you want to be notified when products reach a certain inventory level so you can restock the machine. Assuming the hardware of your vending machine can collect and send this information in a standard message, the messages each machine sends can be received, stored, organized and displayed using Azure's IoT services.

The data collected from these devices could be combined with Azure's AI services to predict when machines need pro-active maintenance, or predict when inventories will need to be replenished and new product ordered from vendors.

There are many services that can assist and drive end-to-end solutions for IoT on Azure.

Azure IoT Hub

Azure IoT Hub[10] is a managed service hosted in the cloud that acts as a central message hub for bi-directional communication between your IoT application and the devices it manages. You can use Azure IoT Hub to build IoT solutions with reliable and secure communications between millions of IoT devices and a cloud-hosted solution backend. You can connect virtually any device to your IoT Hub.

IoT Hub supports communications both from the device to the cloud and from the cloud to the device. It also supports multiple messaging patterns such as device-to-cloud telemetry, file upload from devices, and request-reply methods to control your devices from the cloud. Once the IoT Hub receives messages from a device it can route that message to other Azure services.

From a cloud-to-device perspective, IoT Hub allows for “command and control”, in other words, either manual or automated remote control of connected devices so you can instruct the device to open valves, setting target temperatures, restarting stuck devices, and so on.

IoT Hub monitoring helps you maintain the health of your solution by tracking events such as device creation, device failures, and device connections.

Azure IoT Central

Azure IoT Central[11] builds on top of IoT Hub by adding a dashboard that allows you to connect, monitor, and manage your IoT devices. The visual user interface (UI) makes it easy to quickly connect new devices and watch as they begin sending telemetry or error messages. You can watch the overall performance across all devices in aggregate, and set up alerts that send notifications when a specific device needs maintenance. Finally, you can push hardware updates to the device.

To help you get up and running quickly, IoT Central provides starter templates for common scenarios across different industries, like retail, energy, healthcare, and government. You then customize the design starter templates directly in the UI by choosing from existing themes or creating your own custom theme,

10 https://azure.microsoft.com/services/iot-hub/?azure-portal=true
11 https://azure.microsoft.com/services/iot-central/?azure-portal=true

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

setting the logo, and so on. IoT Central allows you to tailor the starter templates for the specific data that's sent from your devices, the reports you want to see, and the alerts you want to send.

You can use the UI to control your devices remotely. This feature allows you to push a software update or modify a property of the device. You could update the desired temperature for one or all of your refrigerated vending machines from directly inside of IoT Central.

A key part of IoT Central is the use of device templates. Device templates let you connect a device without any service-side coding. IoT Central uses the templates to construct the dashboards, alerts, and so on. Device developers still need to create code to run on the devices and that code must match the device template specification.

Azure Sphere

Azure Sphere[12] creates an end-to-end highly secure IoT solution for customers that encompasses everything from the hardware and operating system on the device, to the secure method of sending messages from the device to the message hub. It has built-in communication and security features for internet-connected devices.

There are three parts to Azure Sphere:

- The first part is the Azure Sphere MCU (micro-controller unit) which is responsible for processing the operating system and signals from attached sensors. The following is a picture of the Seeed Azure Sphere MT3620 Development Kit MCU, one of several different starter kits available for prototyping and developing Azure Sphere applications.

- The second part is a customized Linux operating system (OS) that handles communication with the security service and can run the vendor's software.

12 https://azure.microsoft.com/services/azure-sphere/?azure-portal=true

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

- The third part is the Azure Sphere Security Service, also known as AS3. Its job is to make sure the device has not been maliciously compromised. When the device attempts to connect to Azure, it first must authenticate itself (per-device) which it does using certificate-based authentication. If it authenticates successfully, AS3 checks to ensure that the device has not been tampered with. Once it has established a secure channel of communication, it will push any OS or (approved) customer developed software updates to the device.

Once the Azure Sphere system has validated the authenticity of the device and authenticated it, the device can then interact with other Azure IoT services, sending telemetry and error information.

Analyze the decision criteria

In this unit, we'll analyze the criteria that experts employ when deciding which IoT service to use for a given business need. Understanding the criteria can also help you better understand the nuanced differences between each product.

Is it critical to ensure that the device is not compromised?

While no manufacturer or customer wants their devices to be maliciously compromised and used for nefarious purposes, it's more critical to ensure the integrity of an ATM than, say, a washing machine. When security is a critical consideration in your product's design, the best product option is Azure Sphere, which provides a comprehensive end-to-end solution for IoT devices. As we covered in the previous unit, Azure Sphere ensures a secure channel of communication between the device and Azure by controlling everything from the hardware to the operating system to the authentication process, ensuring that the integrity of the device is uncompromised. Once a secure channel is established, messages can be received from the device securely, and messages or software updates can be sent to the device remotely.

Do I need a dashboard for reporting and management?

The next decision will be the level of services you require from your IoT solution. If you merely want to connect to your remote devices to receive telemetry and occasionally push updates, and do not need any reporting capabilities, then you may prefer to just implement IoT Hub by itself. Your programmers can still create a customized set of management tools and reports using IoT Hub's RESTful API.

However, if you want a pre-built customizable user interface that allows you to view and control your devices remotely, whether individually or all your devices, and set up alerts for certain conditions like a device failure, then you might prefer to start with IoT Central. IoT Central integrates with many different Azure products, including IoT Hub, to create a dashboard with reports and management features. The dashboard is based on starter templates for common industry and usage scenarios. You can use the dashboard generated by the starter template as-is or customize to suit your needs.

Furthermore, you can have multiple dashboards targeted at different users.

Use IoT Hub

Tailwind Traders' senior leadership team has decided to partner with a leading appliance manufacture to create an exclusive high-end brand that promises a preemptive maintenance service agreement. This unique feature would differentiate their appliances in a crowded competitive market. It also makes the appliances lucrative since a yearly subscription would be necessary. To build a strong brand reputation, the appliances will send telemetry information to a centralized location where it can be analyzed and maintenance can be scheduled.

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

The devices will not require remote control. They will merely be sending their telemetry data for analysis and pro-active maintenance.

Since Tailwind Traders already has software in place for managing appliance maintenance requests, they want to integrate all functionality into this existing system.

Which service should we choose?

Let's apply the decision criteria from the previous unit.

Is it critical to ensure that the device, in this case, each appliance, isn't compromised? It's preferable that the devices aren't compromised, however it isn't critical. The worst that could happen is that a hacker reads the current temperature of the customer's refrigerator or the number of loads of laundry the washing machine has completed.

Even if the customer calls and reports strange behavior with their appliance, a technician could reset or replace the microcontroller. It may not warrant the extra expense or engineering resources required to employ Azure Sphere.

Next decision criteria: do I need a dashboard for reporting and management? In this case, no. Tailwind Traders wants to integrate the telemetry data and all other functionality into an existing maintenance request system. In this case Azure IoT Central is not required.

So, given the responses to the decision criteria, Azure IoT Hub is the best choice in this scenario.

Why not use Azure IoT Central?

Azure IoT Central provides a dashboard that allows companies to manage IoT devices individually and in aggregate, view reports and set up error notifications via a GUI. But in this scenario, Tailwind Traders wants to integrate the telemetry they collect and other analysis functionality into an existing software application. Furthermore, their appliances will only be collecting data via sensors, and do not need the ability update settings or software remotely. Therefore, they do not need Azure IoT Central.

Why not use Azure Sphere?

Azure Sphere provides a complete solution for scenarios where security is critical. In this scenario, security is not critical, it is preferred. The appliances cannot be updated with new software remotely. The sensors merely report usage data. As a result, Azure Sphere is not necessary.

Use IoT Central

Tailwind Traders owns a fleet of delivery vehicles that transport products from warehouses to distribution centers, and from distribution centers to stores and homes. They're looking for a complete logistics solution that takes data sent from an onboard vehicle computer and turns it into actionable information.

Furthermore, shipments can be outfitted with sensors from a third-party vendor to collect and monitor ambient conditions. These sensors might collect information like the temperature, humidity, tilt, shock, light, and the location of a shipment.

A few goals of this logistics system include:

- Shipment monitoring with real-time tracing and tracking.
- Shipment integrity with real-time ambient condition monitoring.
- Security from theft, loss, or damage of shipments.

- Geo-fencing, route optimization, fleet management, and vehicle analytics.
- Forecasting for predictable departure and arrival of shipments.

They would prefer a pre-built solution to collect the sensor and vehicle computer data, and provide a graphical user interface where they can view reports about shipments and vehicles.

Which service should we choose?

Here again, let's apply the decision criteria from a previous unit.

Is it critical to ensure that the device, in this case, each appliance, is not compromised? Ideally, each sensor and vehical computer would be impervious to interference. However, security was not mentioned as a critical concern at this point. The vehical computers and sensors are built by a third-party vendor, and unless Tailwind Traders wants to manufacture their own devices (which they don't), they will be forced to use the hardware already available.

Next, do they need a dashboard for reporting and management? Yes, a reporting and management dashboard is a requirement from Tailwind Traders.

So, given the responses to the decision criteria, Azure IoT Central is the best choice in this scenario. The Connected Logistics starter template provides an out-of-the-box dashboard that will accomplish many of these requirements. This dashboard is pre-configured to showcase the critical logistics device operations activity. Admittedly, it might need to be reconfigured to remove sea vessel gateways, but the truck gateway functionality would be almost exactly what Tailwind Traders needs.

Why not use IoT Hub?

Actually, if Tailwind Traders uses IoT Central, they would be using IoT Hub, preconfigured for their specific needs by the Connected Logistics starter template. Otherwise, they would need to do a lot of custom development to build their own cloud-based dashboards and management systems on top of IoT Hub.

Why not use Azure Sphere?

Azure Sphere provides a complete solution for scenarios where security is critical. In this scenario, security is ideal, but not a critical priority. Azure Sphere provides an end-to-end solution including hardware. However, Tailwind Traders will use hardware from a third-party vendor. So, in this scenario, Azure Sphere is not necessary.

Use Azure Sphere

Tailwind Traders wants to implement a touchless point-of-sale solution for self-checkout. These self-checkout terminals should be, above all else, secure. Each terminal must be impervious to malicious code that could create fraudulent transactions, force the company to take the systems offline during a heavy shopping period, or send transactional data to a spying organization. The terminals should also report back vital information on their health and allow secure updates to their software remotely.

After reviewing many possible solutions during a Request For Proposal process, they decided they needed features that vendors have yet to implement. Instead of using an existing solution, Tailwind Traders decides to work with a leading engineering firm that specializes in IoT solutions. This approach will allow them to build a uniquely secure terminal that gives them the retail platform to build on going forward.

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

While most of their focus is on the terminal itself, they realize they want a solution that can help them make sense of all the data that will be generated by these terminals across all of their retail stores, and an easy way to push software updates to their terminals.

Which service should we choose?

Here again, let's apply the decision criteria from a previous unit.

Is it critical to ensure that the device, in this case, each point-of-sale terminal, is not compromised? Absolutely. Device security is the primary requirement.

Next, do they need a dashboard for reporting and management? Yes, a reporting and management dashboard is a requirement from Tailwind Traders.

So, given the responses to the decision criteria, the IoT engineering firm will build a platform on top of both Azure IoT Central and Azure Sphere. Even though there's no specific starter template available in Azure IoT Central designed for this scenario, it can be easily adapted to accommodate the kinds of reports they want to see and management operations they want to perform.

Why not choose IoT Hub?

Actually, by using IoT Central, Tailwind Traders would be using IoT Hub behind the scenes as well.

Module 3 Review Questions

Module 03 Review Questions

Review Question 1

You need to predict future behavior based on previous actions. Which product option should you eliminate as a candidate?

- ☐ Azure Machine Learning
- ☐ Azure Bot Service
- ☐ Azure Cognitive Services

Review Question 2

You need to create a human-computer interface that uses natural language to answer customer questions. Which product option should you eliminate as a candidate?

- ☐ Azure Machine Learning
- ☐ Azure Cognitive Services
- ☐ Azure Bot Service

Review Question 3

You need to identify the content of product images to automatically create alt tags for images formatted properly. Which production option is the best candidate?

- ☐ Azure Machine Learning
- ☐ Azure Cognitive Services
- ☐ Azure Bot Service

Review Question 4

Which of the following choices would not be used to automate a CI/CD process?

- ☐ Azure Pipelines
- ☐ GitHub Actions
- ☐ Azure Boards

Review Question 5

Which service could help you manage the VMs that your developers and testers need to ensure that your new app works across various operating systems?

- ☐ Azure DevTest Labs
- ☐ Azure Test Labs
- ☐ Azure Repos

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

Review Question 6

Which service lacks features to assign individual developers tasks to work on?

- ☐ Azure Boards
- ☐ GitHub
- ☐ Azure Pipelines

Review Question 7

You want to be alerted when new recommendations to improve your cloud environment are available. Which service will do this?

- ☐ Azure Advisor
- ☐ Azure Monitor
- ☐ Azure Service Health

Review Question 8

Which service provides official outage root cause analyses (RCAs) for Azure incidents?

- ☐ Azure Advisor
- ☐ Azure Monitor
- ☐ Azure Service Health

Review Question 9

Which service is a platform that powers Application Insights, monitoring for VMs, containers, and Kubernetes?

- ☐ Azure Advisor
- ☐ Azure Monitor
- ☐ Azure Service Health

Review Question 10

As an administrator, you need to retrieve the IP address from a particular VM by using Bash. Which of the following tools should you use?

- ☐ ARM templates
- ☐ Azure PowerShell
- ☐ The Azure portal
- ☐ The Azure CLI

Review Question 11

You're a developer who needs to set up your first VM to host a process that runs nightly. Which of the following tools is your best choice?

- ☐ ARM templates
- ☐ Azure PowerShell
- ☐ The Azure portal
- ☐ The Azure CLI

Review Question 12

What is the best infrastructure-as-code option for quickly and reliably setting up your entire cloud infrastructure declaratively?

- ☐ ARM templates
- ☐ Azure PowerShell
- ☐ The Azure portal
- ☐ The Azure CLI

Review Question 13

You need to process messages from a queue, parse them by using some existing imperative logic written in Java, and then send them to a third-party API. Which serverless option should you choose?

- ☐ Azure Functions
- ☐ Azure Logic Apps

Review Question 14

You want to orchestrate a workflow by using APIs from several well-known services. Which is the best option for this scenario?

- ☐ Azure Functions
- ☐ Azure Logic Apps

Review Question 15

Your team has limited experience with writing custom code, but it sees tremendous value in automating several important business processes. Which of the following options is your team's best option?

- ☐ Azure Functions
- ☐ Azure Logic Apps

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

Review Question 16

A company wants to build a new voting kiosk for sales to governments around the world. Which IoT technologies should the company choose to ensure the highest degree of security?

- ☐ IoT Hub
- ☐ IoT Central
- ☐ Azure Sphere

Review Question 17

A company wants to quickly manage its individual IoT devices by using a web-based user interface. Which IoT technology should it choose?

- ☐ IoT Hub
- ☐ IoT Central
- ☐ Azure Sphere

Review Question 18

You want to send messages from the IoT device to the cloud and vice versa. Which IoT technology can send and receive messages?

- ☐ IoT Hub
- ☐ IoT Central
- ☐ Azure Sphere

Module 3 Summary

Module 03 Summary

Choose the best AI service for your needs

Our goal in this lesson was to help Tailwind Traders explore several AI service offerings from Azure that it can apply to various business opportunities.

You identified a few product options and their capabilities, including Azure Bot Service, Azure Cognitive Services, and Azure Machine Learning. You analyzed certain decision criteria to help yourself choose one option over another depending on the scenario. Then you applied those decision criteria to three Tailwind Traders initiatives, helping the company find the best service option for each scenario.

Without AI services, Tailwind Traders would spend more time and effort on manual tasks, respond to customers less quickly, offer weak product recommendations, and be unable to fully support customers who speak languages other than English.

AI is one focus that could transform every area of a business. Such transformation is limited only by the creativity and imagination of the organization.

This lesson discussed several products and services that you can learn more about:

- For an exhaustive list of services available in Azure Cognitive Services, see **What are Azure Cognitive Services?** [13].
- The Cognitive Services Personalizer service was mentioned as a possible solution for one of the scenarios. For more information, see **Cognitive Services Personalizer** [14].
- Azure Language Understanding (LUIS) was mentioned as a way to interact with the Bot Service by using natural language. For more information, see **Azure Language Understanding** [15].
- QnA Maker was mentioned as a pre-packaged virtual assistant solution available from Azure Marketplace. For more information, see **QnA Maker** [16].

Choose the best tools to help organizations build better solutions

The goal in this lesson was to help Tailwind Traders choose the best DevOps solution for a set of requirements across various software development and testing needs.

We identified various product options and capabilities, including Azure DevOps Services, GitHub (including GitHub Actions), and Azure DevTest Labs. We analyzed the criteria for choosing one option over another for each scenario. Then we applied those criteria to three separate challenges at Tailwind Traders, helping the team determine the best service option for the scenarios.

Without software development services and tools from Microsoft, the Tailwind Traders team might have difficulty in realizing the benefits of such DevOps practices as continuous integration and continuous delivery (CI/CD), source-code management, and work-item management.

13 https://docs.microsoft.com/en-us/azure/cognitive-services/what-are-cognitive-services
14 https://azure.microsoft.com/services/cognitive-services/personalizer/
15 https://www.luis.ai/
16 https://www.qnamaker.ai/

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

DevOps practices and processes have changed the software development landscape, helping to accelerate software development and improve the deployability and quality of software systems. Microsoft offers a wealth of tools that can help organizations implement DevOps practices, experience better collaboration among technical teams, and achieve more consistent results from those teams.

Choose the best monitoring service for visibility, insight, and outage mitigation

Our goal in this lesson was to help Tailwind Traders explore several monitoring service offerings from Azure to apply to a variety of business scenarios.

We identified three product options and their capabilities: Azure Advisor, Azure Monitor, and Azure Service Health. We analyzed decision criteria for choosing one option over another for certain scenarios. Then we applied those decision criteria to three different challenges faced by Tailwind Traders, helping them find the best service option for the scenario.

Without monitoring services, Tailwind Traders would spend more money on its cloud environment, be unsure about its cloud security posture, have difficulty pinpointing issues in its application logic, and be unable to plan ahead for outages or supply formal outage reports to stakeholders.

Azure monitoring services provide a comprehensive array of features to help improve your cloud operations.

Choose the best tools for managing and configuring your Azure environment

Our goal in this lesson was to help Tailwind Traders choose the right cloud management tools from Microsoft for its various technical needs.

We identified a variety of product options and their capabilities, including the Azure portal, the Azure mobile app, Azure PowerShell, the Azure CLI, and Azure Resource Manager templates (ARM templates).

We analyzed decision criteria for choosing one option over another in specific scenarios.

We then applied those decision criteria to three different Tailwind Traders initiatives, helping the company find the best service option for each scenario.

Without a full suite of management tools, the company would be severely limited in how it interacts with Azure. Fortunately, Azure provides a powerful mix of visual management tools, imperative scripting tools, and declarative infrastructure-as-code tools.

Choose the best Azure serverless technology for your business scenario

In this lesson, we wanted to help Tailwind Traders choose the right serverless computing technology for its business scenarios.

When the company needed to build a solution that pulls code logic from an existing C# Windows service, we helped it choose Azure Functions.

When the company needed to orchestrate a workflow to improve customer retention after a negative shopping experience, we helped it choose Azure Logic Apps.

In both cases, we noted how choosing the other serverless computing service would be possible. However, we tried to help the company consider the decision criteria we outlined and choose the right service for the scenario.

Without serverless computing, Tailwind Traders would be forced to set up and manage its own computing infrastructure for these business scenarios. The team would have needed to closely monitor the services to determine whether it needed to scale the service. And it likely would have wasted money in the process, with either too many or too few computing resources dedicated to the solution.

Additionally, it might have had to design, write, test, and maintain custom code to get similar results.

By helping Tailwind Traders select the right serverless computing solutions, we were able to deploy new functionality to help the company improve customer satisfaction with its e-commerce platform.

Choose the best Azure IoT service for your application

Our goal in this lesson was to help Tailwind Traders explore various IoT services from Azure and choose the best service for the company's business scenarios.

Tailwind Traders was able to capture telemetry data from appliances, combine it with some machine learning to predict future maintenance, and create a significant value-added service for customers by using Azure IoT Hub. The company was able to implement a complete real-time logistics system to track deliveries and vehicles by using Azure IoT Central and the Connected Logistics starter template. And, finally, it was able to design and build a secure, modern, point-of-sale self-checkout terminal by using Azure Sphere.

Without Azure IoT services, receiving messages from devices might still be possible, but it would likely be much less secure and require custom development to implement a dashboard for reporting and management. It would also be more difficult to push software or firmware updates to each device.

IoT is an exciting evolution in computing that bridges the physical and digital worlds. Azure IoT services provide a significant amount of functionality for organizations that want to build device-driven and sensor-driven solutions.

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

Answers

Review Question 1

You need to predict future behavior based on previous actions. Which product option should you eliminate as a candidate?

- ☐ Azure Machine Learning
- ■ Azure Bot Service
- ☐ Azure Cognitive Services

Explanation
Azure Bot Service will not help with prediction. It should be eliminated as a candidate.

Review Question 2

You need to create a human-computer interface that uses natural language to answer customer questions. Which product option should you eliminate as a candidate?

- ■ Azure Machine Learning
- ☐ Azure Cognitive Services
- ☐ Azure Bot Service

Explanation
Although Azure Machine Learning could be used to create a natural language model, it would likely be cost and time prohibitive. It should be eliminated as a candidate.

Review Question 3

You need to identify the content of product images to automatically create alt tags for images formatted properly. Which production option is the best candidate?

- ☐ Azure Machine Learning
- ■ Azure Cognitive Services
- ☐ Azure Bot Service

Explanation
Azure Cognitive Services includes Vision services that can identify the content of an image. Azure Cognitive Services is the best candidate.

Review Question 4

Which of the following choices would not be used to automate a CI/CD process?

- ☐ Azure Pipelines
- ☐ GitHub Actions
- ■ Azure Boards

Explanation
Azure Boards is an agile project-management tool. It would not be used to automate a CI/CD process.

Review Question 5

Which service could help you manage the VMs that your developers and testers need to ensure that your new app works across various operating systems?

- ■ Azure DevTest Labs
- ☐ Azure Test Labs
- ☐ Azure Repos

Explanation
Azure DevTest Labs is used to manage VMs for testing, including configuration, provisioning, and automatic de-provisioning.

Review Question 6

Which service lacks features to assign individual developers tasks to work on?

- ☐ Azure Boards
- ☐ GitHub
- ■ Azure Pipelines

Explanation
Azure Pipelines is a CI/CD tool for building an automated toolchain. It lacks features to assign tasks for individual developers to work on. However, it can automate other tools to assign tasks to users.

Review Question 7

You want to be alerted when new recommendations to improve your cloud environment are available. Which service will do this?

- ■ Azure Advisor
- ☐ Azure Monitor
- ☐ Azure Service Health

Explanation
Azure Advisor can alert you when new recommendations are available.

Review Question 8

Which service provides official outage root cause analyses (RCAs) for Azure incidents?

- ☐ Azure Advisor
- ☐ Azure Monitor
- ■ Azure Service Health

Explanation
Azure Service Health provides incident history and RCAs to share with your stakeholders.

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

Review Question 9

Which service is a platform that powers Application Insights, monitoring for VMs, containers, and Kubernetes?

- ☐ Azure Advisor
- ■ Azure Monitor
- ☐ Azure Service Health

Explanation
Azure Monitor is the platform used by Application Insights.

Review Question 10

As an administrator, you need to retrieve the IP address from a particular VM by using Bash. Which of the following tools should you use?

- ☐ ARM templates
- ☐ Azure PowerShell
- ☐ The Azure portal
- ■ The Azure CLI

Explanation
The Azure CLI enables you to use Bash to run one-off tasks on Azure.

Review Question 11

You're a developer who needs to set up your first VM to host a process that runs nightly. Which of the following tools is your best choice?

- ☐ ARM templates
- ☐ Azure PowerShell
- ■ The Azure portal
- ☐ The Azure CLI

Explanation
The Azure portal is a great place for newcomers to learn about Azure and set up their first resources.

Review Question 12

What is the best infrastructure-as-code option for quickly and reliably setting up your entire cloud infrastructure declaratively?

- ■ ARM templates
- ☐ Azure PowerShell
- ☐ The Azure portal
- ☐ The Azure CLI

Explanation
ARM templates are the best infrastructure-as-code option for quickly and reliably setting up your entire cloud infrastructure declaratively.

Review Question 13

You need to process messages from a queue, parse them by using some existing imperative logic written in Java, and then send them to a third-party API. Which serverless option should you choose?

■ Azure Functions

☐ Azure Logic Apps

Explanation
Azure Functions is the correct choice because you can use existing Java code with minimal modification.

Review Question 14

You want to orchestrate a workflow by using APIs from several well-known services. Which is the best option for this scenario?

☐ Azure Functions

■ Azure Logic Apps

Explanation
Azure Logic Apps makes it easy to create a workflow across well-known services with less effort than writing code and manually orchestrating all the steps yourself.

Review Question 15

Your team has limited experience with writing custom code, but it sees tremendous value in automating several important business processes. Which of the following options is your team's best option?

☐ Azure Functions

■ Azure Logic Apps

Explanation
Azure Logic Apps is best suited for users who are more comfortable in a visual environment that allows them to automate their business processes. Logic Apps is the best option in this scenario.

Review Question 16

A company wants to build a new voting kiosk for sales to governments around the world. Which IoT technologies should the company choose to ensure the highest degree of security?

☐ IoT Hub

☐ IoT Central

■ Azure Sphere

Explanation
Azure Sphere provides the highest degree of security to ensure the device has not been tampered with.

Review Question 17

A company wants to quickly manage its individual IoT devices by using a web-based user interface. Which IoT technology should it choose?

☐ IoT Hub

■ IoT Central

☐ Azure Sphere

Explanation
IoT Central quickly creates a web-based management portal to enable reporting and communication with IoT devices.

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

Review Question 18

You want to send messages from the IoT device to the cloud and vice versa. Which IoT technology can send and receive messages?

- ■ IoT Hub
- ☐ IoT Central
- ☐ Azure Sphere

Explanation
An IoT hub communicates to IoT devices by sending and receiving messages.

Module 4 Describe general security and network security features

Learning Objectives

Learning Objectives

After completing this module, you'll be able to:

- Strengthen your security posture and protect against threats by using Azure Security Center.
- Collect and act on security data from many different sources by using Azure Sentinel.
- Store and access sensitive information such as passwords and encryption keys securely in Azure Key Vault.
- Manage dedicated physical servers to host your Azure VMs for Windows and Linux by using Azure Dedicated Host.
- Identify the layers that make up a *defense in depth* strategy.
- Explain how Azure Firewall enables you to control what traffic is allowed on the network.
- Configure network security groups to filter network traffic to and from Azure resources within a Microsoft Azure virtual network.
- Explain how Azure DDoS Protection helps protect your Azure resources from DDoS attacks.

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

Protect against security threats on Azure

Introduction

In this module, you'll learn about some of the security tools that can help keep your infrastructure and data safe when you work in the cloud.

Security is a small word for a significant concept. There are so many factors to consider in order to protect your applications and your data. How does Azure help you protect workloads you run in the cloud and in your on-premises datacenter?

Meet Tailwind Traders

Tailwind Traders [1] is a fictitious home improvement retailer. It operates retail hardware stores across the globe and online.

Tailwind Traders specializes in competitive pricing, fast shipping, and a large range of items. It's looking at cloud technologies to improve business operations and support growth into new markets. By moving to the cloud, the company plans to enhance its shopping experience to further differentiate itself from competitors.

How will Tailwind Traders run securely in the cloud and in the datacenter?

Tailwind Traders runs a mix of workloads on Azure and in its datacenter.

The company needs to ensure that all of its systems meet a minimum level of security and that its information is protected from attacks. The company also needs a way to collect and act on security events from across its digital estate.

Let's explore how Tailwind Traders can use some of the tools and features in Azure as part of its overall security strategy.

Learning objectives

After completing this module, you'll be able to:

- Strengthen your security posture and protect against threats by using Azure Security Center.
- Collect and act on security data from many different sources by using Azure Sentinel.
- Store and access sensitive information such as passwords and encryption keys securely in Azure Key Vault.
- Manage dedicated physical servers to host your Azure VMs for Windows and Linux by using Azure Dedicated Host.

Prerequisites

- You should be familiar with basic computing concepts and terminology

1 https://www.tailwindtraders.com/

- Familiarity with cloud computing is helpful, but isn't necessary

Protect against security threats by using Azure Security Center

Tailwind Traders is broadening their use of Azure services. They still have on-premises workloads with current security-related configuration best practices and business procedures. How do they ensure that all of their systems meet a minimum level of security and that their information is protected from attacks?

Many Azure services include built-in security features. There are also tools on Azure that can help Tailwind Traders with this requirement. Let's start by looking at Azure Security Center.

What's Azure Security Center?

Azure Security Center[2] is a monitoring service that provides visibility of your security posture across all of your services, both on Azure and on-premises. The term *security posture* refers to cybersecurity policies and controls, as well as how well you can predict, prevent, and respond to security threats.

Security Center can:

- Monitor security settings across on-premises and cloud workloads.
- Automatically apply required security settings to new resources as they come online.
- Provide security recommendations that are based on your current configurations, resources, and networks.
- Continuously monitor your resources and perform automatic security assessments to identify potential vulnerabilities before those vulnerabilities can be exploited.
- Use machine learning to detect and block malware from being installed on your virtual machines and other resources. You can also use *adaptive application controls* to define rules that list allowed applications to ensure that only applications you allow can run.
- Detect and analyze potential inbound attacks and investigate threats and any post-breach activity that might have occurred.
- Provide just-in-time access control for network ports. Doing so reduces your attack surface by ensuring that the network only allows traffic that you require at the time that you need it to.

Understand your security posture

Tailwind Traders can use Security Center to get a detailed analysis of different components in their environment. Because their resources are analyzed against the security controls of any governance policies they have assigned, they can view their overall regulatory compliance from a security perspective all from one place.

Here's an example of what you might see in Azure Security Center:

2 https://azure.microsoft.com/services/security-center?azure-portal=true

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

Azure security center dashboard showing policy compliance, resource security hygiene, and threat protection.

Let's say that Tailwind Traders must comply with the Payment Card Industry's Data Security Standard (PCI DSS). This report shows that they have resources that they need to remediate.

Under the **Resource security hygiene** section, they can see the health of their resources from a security perspective. To help you prioritize remediation actions, recommendations are categorized as low, medium, and high. Here's an example:

Azure security center dashboard showing the resource security hygiene section. Recommendations are categorized as low, medium, and high.

What's secure score?

Secure score[3] is a measurement of an organization's security posture.

Secure score is based on *security controls*, or groups of related security recommendations. Your score is based on the percentage of security controls that you satisfy. The more security controls you satisfy, the higher the score you receive. Your score improves when you remediate all of the recommendations for a single resource within a control.

Here's an example from the Azure portal showing a score of 57 percent, or 34 out of 60 points:

3 https://docs.microsoft.com/azure/security-center/secure-score-security-controls/?azure-portal=true

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

A screenshot of the Azure portal showing a score of 57 percent, or 34 out of 60 points.

Following the secure score recommendations can protect your organization from threats. From a centralized dashboard in the Azure Security Center, organizations can monitor and work on the security of their Azure resources like identities, data, apps, devices, and infrastructure.

Secure score helps you:

- Report on the current state of your organization's security posture.
- Improve your security posture by providing discoverability, visibility, guidance, and control.
- Compare with benchmarks and establish key performance indicators (KPIs).

Protect against threats

Security Center also includes advanced cloud defense capabilities for virtual machines, network security, and file integrity. Let's take a look at how some of these capabilities apply to Tailwind Traders.

- **Just-in-time VM access** Tailwind Traders will configure just-in-time access to virtual machines (VMs), which blocks traffic by default to specific network ports of their virtual machines, but allows it for a specified time when requested and approved by an administrator.
- **Adaptive application controls** Tailwind Traders can also control which applications are allowed to run on their virtual machines. In the background, Security Center uses machine learning to look at the processes running on a virtual machine. It creates exception rules for each resource group that holds the virtual machines and provides recommendations. This process provides alerts that inform them about unauthorized applications that are running on their VMs.
- **Adaptive network hardening** Security Center can also monitor the internet traffic patterns of the VMs and compare those patterns with their current Network Security Group (NSG) settings. From there, Security Center can make recommendations on whether the NSGs should be locked down further and provide remediation steps.
- **File integrity monitoring** Tailwind Traders can also configure the monitoring of changes to important files on both Windows and Linux, registry settings, applications, and other aspects that might indicate a security attack.

Respond to security alerts

Tailwind Traders can use Security Center to get a centralized view of all of their security alerts. From there, Tailwind Traders can dismiss false alerts, investigate them further, remediate the alert manually, or use an automated response with a **Workflow automation**.

Workflow automation uses Logic Apps and Security Center connectors. The Logic App can be triggered by a threat detection alert or by a Security Center recommendation, filtered by name or by severity. You can then configure the Logic App to run an action such as sending an email or posting a message to a Microsoft Teams channel.

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

Detect and respond to security threats by using Azure Sentinel

Managing security on a large scale can benefit from a dedicated security information and event management system (SIEM). A SIEM aggregates security data from many different sources (as long as those sources support an open standard logging format) and provides additional capabilities for threat detection and response.

Azure Sentinel[4] is Microsoft's cloud-based SIEM, powered by Microsoft's intelligent security analytics and threat analysis.

Azure Sentinel capabilities

Azure Sentinel enables you to:

- **Collect cloud data at scale** Collect data across all users, devices, applications, and infrastructure, both on-premises and from multiple clouds.
- **Detect previously undetected threats** Minimize false positives by using Microsoft's comprehensive analytics and threat intelligence.
- **Investigate threats with artificial intelligence** Examine suspicious activities at scale, tapping into years of cybersecurity experience from Microsoft.
- **Respond to incidents rapidly** Utilize built-in orchestration and automation of common tasks.

Connect your data sources

Tailwind Traders decides to explore the capabilities of Azure Sentinel. First, they identify and connect their data sources.

Azure Sentinel supports a number of data sources, which it can analyze for security events. These connections are handled by built-in connectors or industry-standard log formats and APIs.

- **Connect Microsoft solutions** These connectors provide real-time integration for services like Microsoft Threat Protection solutions, Microsoft 365 sources (including Office 365), Azure Active Directory, Windows Defender Firewall, and more.
- **Connect other services and solutions** Connectors are available for a range of common non-Microsoft services and solutions, including AWS CloudTrail, Citrix Analytics (Security), Sophos XG Firewall, VMware Carbon Black Cloud, Okta SSO, and more.
- **Connect industry-standard data sources** Azure Sentinel supports data from other sources that use the Common Event Format (CEF) messaging standard, Syslog, or REST API.

Detect threats

Next, Tailwind Traders needs to be notified when something suspicious occurs. They decide to use both built-in analytics and custom rules to detect threats.

Built in analytics use templates designed by Microsoft's team of security experts and analysts based on known threats, common attack vectors, and suspicious activity escalation chains. These templates can be customized and search across the environment for any activity that looks suspicious. There are also

4 https://azure.microsoft.com/services/azure-sentinel/?azure-portal=true

templates that use machine learning behavioral analytics that are based on Microsoft's proprietary algorithms.

Custom analytics are rules you create to search for specific criteria within your environment. You can preview the number of results the query would generate (based on past log events) and set a schedule for the query to run, as well as set an alert threshold.

Investigate and respond

Finally, when Azure Sentinel detects suspicious events, Tailwind Traders can investigate specific alerts or *incidents* (a group of related alerts). With the investigation graph, they can review information from entities directly connected to the alert and see common exploration queries to help guide their investigation.

They'll also use **Azure Monitor Workbooks**[5] to automate responses to threats. For example, they can set an alert that looks for malicious IP addresses that access the network and create a workbook that does the following steps:

1. When the alert is triggered, open a ticket in the IT ticketing system.
2. Send a message to the security operations channel in Microsoft Teams or Slack to make sure the security analysts are aware of the incident.
3. Send all of the information in the alert to the senior network admin and to the security admin. The email message also includes two user option buttons: **Block** or **Ignore**.
4. The workbook continues to run after a response is received from the admins.
5. When an admin chooses **Block**, the IP address is blocked in the firewall and the user is disabled in Azure Active Directory.
6. When an admin chooses **Ignore**, the alert is closed in Azure Sentinel and the incident is closed in the IT ticketing system.

Workbooks can be run manually or automatically when a rule triggers an alert.

Store and manage secrets by using Azure Key Vault

As Tailwind Traders builds their workloads in the cloud, sensitive information such as passwords, encryption keys, and certificates need to be handled carefully. This information needs to be available for an application to function, but could allow an unauthorized person access to your application data.

Azure Key Vault[6] is a centralized cloud service for storing your applications' secrets in a single, central location. It provides secure access to sensitive information by providing access control and logging capabilities.

What can Azure Key Vault do?

Azure Key Vault can help you:

- **Manage secrets** You can use Key Vault to securely store and tightly control access to tokens, passwords, certificates, API keys, and other secrets.

5 https://docs.microsoft.com/azure/azure-monitor/platform/workbooks-overview/?azure-portal=true
6 https://azure.microsoft.com/services/key-vault?azure-portal=true

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

- **Manage encryption keys** You can use Key Vault as a key management solution. Key Vault makes it easier to create and control the encryption keys that are used to encrypt your data.
- **Manage SSL/TLS certificates** Key Vault enables you to provision, manage, and deploy your public and private Secure Sockets Layer / Transport Layer Security (SSL/TLS) certificates for both your Azure resources and for your internal resources.
- **Store secrets backed by hardware security modules (HSMs)** These secrets and keys can be protected either by software or by FIPS 140-2 Level 2 validated HSMs.

Here's an example that shows a certificate used for testing in Key Vault.

You'll add a secret to Key Vault later in this module.

What are the benefits of Azure Key Vault?

The benefits of using Key Vault include:

- **Centralized application secrets** Centralizing the storage for your application secrets enables you to control their distribution and reduces the chances that secrets are accidentally leaked.
- **Securely stored secrets and keys** Azure uses industry-standard algorithms, key lengths, and HSMs. Access to Key Vault requires proper authentication and authorization.
- **Access monitoring and access control** By using Key Vault, you can monitor and control access to your application secrets.
- **Simplified administration of application secrets** Key Vault makes it easier to enroll and renew certificates from public Certificate Authorities (CAs). You can also scale up and replicate content within regions and use standard certificate management tools.
- **Integration with other Azure services** You can integrate Key Vault with storage accounts, container registries, event hubs, and many more Azure services. These services can then securely reference the secrets stored in the Key Vault.

Host your Azure virtual machines on dedicated physical servers by using Azure Dedicated Host

On Azure, virtual machines (VMs) run on shared hardware that's managed by Microsoft. Although the underlying hardware is shared, your VM workloads are isolated from workloads being run by other Azure customers.

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

However, some organizations must follow regulatory compliance that requires them to be the only customer using the physical machine that hosts their virtual machines. **Azure Dedicated Host**[7] provides dedicated physical servers to host your Azure VMs for Windows and Linux.

What are the benefits of Azure Dedicated Host?

Azure Dedicated Host:

- Gives you visibility into, and control over, the server infrastructure running your Azure VMs.
- Helps address compliance requirements by deploying your workloads on an isolated server.
- Lets you choose the number of processors, server capabilities, VM series, and VM sizes within the same host.

Availability considerations for Dedicated Host

After a dedicated host is provisioned, Azure assigns it to the physical server in Microsoft's cloud data-center.

For high availability, you can provision multiple hosts in a *host group* and deploy your virtual machines across this group. VMs on dedicated hosts can also take advantage of *maintenance control*, which enables you to control when regular maintenance updates occur, within a 35 day rolling window.

Pricing considerations

You are charged per dedicated host, independent of how many virtual machines you deploy to it. The host price is based on the VM family, type (hardware size), and region.

Software licensing, storage, and network usage are billed separately from the host and VMs. For more information. see **Azure Dedicated Host pricing**[8].

7 https://azure.microsoft.com/services/virtual-machines/dedicated-host/?azure-portal=true
8 https://aka.ms/ADHPricing/?azure-portal=true

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

Secure network connectivity on Azure

Introduction

Every application and service, whether on-premises or in the cloud, needs to be designed with security in mind. There's too much at risk. For example, a denial of service attack might prevent customers from reaching your website or services and block you from doing business. Or, your website could be defaced, causing damage to your reputation. A data breach would be even worse, as it can ruin hard-earned trust while causing significant personal and financial harm.

Meet Tailwind Traders

Tailwind Traders [9] is a fictitious home improvement retailer. It operates retail hardware stores across the globe and online.

Tailwind Traders specializes in competitive pricing, fast shipping, and a large range of items. It's looking at cloud technologies to improve business operations and support growth into new markets. By moving to the cloud, the company plans to enhance its shopping experience to further differentiate itself from competitors.

How will Tailwind Traders secure its networks?

As Tailwind Traders moves to the cloud, it needs to evaluate its security needs before it can deploy a single line of code to production.

Although security must be considered at every layer in the company's applications (all the way from the physical servers to the application data), some factors relate specifically to the network configuration and network traffic of cloud-based workloads.

In this module, you'll focus on the network security capabilities in Azure and review how they help you secure your solutions in the cloud, based on your business needs.

Learning objectives

By the end of this module, you'll able to:

- Identify the various layers that make up a *defense in depth* strategy.
- Explain how Azure Firewall enables you to control what traffic is allowed on the network.
- Configure network security groups to filter network traffic to and from Azure resources within a Microsoft Azure Virtual Network.
- Explain how Azure DDoS Protection helps protect your Azure resources from DDoS attacks.

Prerequisites

- You should be familiar with basic computing concepts and terminology
- Familiarity with cloud computing is helpful, but isn't necessary

9 https://www.tailwindtraders.com/

What is defense in depth?

Tailwind Traders currently runs their workloads on-premises, in their datacenter. Running on-premises means that they're responsible for all aspects of security - from physical access to buildings all the way down to how data travels in and out of the network. They want to know how their current defense in depth strategy compares to running in the cloud.

Protect virtual networks by using Azure Firewall

A *firewall* is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules. You can create firewall rules that specify ranges of IP addresses. Only clients granted IP addresses from within those ranges are allowed to access the destination server. Firewall rules can also include specific network protocol and port information.

Tailwind Traders currently runs firewall appliances, which combine hardware and software, to protect their on-premises network. These firewall appliances require a monthly licensing fee to operate, and require IT staff to perform routine maintenance. As Tailwind Traders moves to the cloud, the IT manager wants to know what Azure services can protect both their cloud networks as well as their on-premises networks.

In this part, you explore Azure Firewall.

What's Azure Firewall?

Azure Firewall[10] is a managed, cloud-based, network security service that protects resources in your Azure Virtual Networks. A virtual network is similar to a traditional network that you'd operate in your own datacenter. It's a fundamental building block for your private network that enables virtual machines and other compute resources to securely communicate with each other, the internet, and on-premises networks.

Here's a diagram that shows a basic Azure Firewall implementation:

Azure Firewall is a *stateful* firewall. A stateful firewall analyzes the complete context of a network connection, not just an individual packet of network traffic. Azure Firewall features high availability and unrestricted cloud scalability.

Azure Firewall provides a central location to create, enforce, and log application and network connectivity policies across subscriptions and virtual networks. Azure Firewall uses a static (unchanging) public IP

10 https://azure.microsoft.com/services/azure-firewall?azure-portal=true

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

address for your virtual network resources, which enables outside firewalls to identify traffic coming from your virtual network. The service is integrated with Azure Monitor to enable logging and analytics.

Azure Firewall provides many features, including:

- Built-in high availability.
- Unrestricted cloud scalability.
- Inbound and outbound filtering rules.
- Inbound Destination Network Address Translation (DNAT) support
- Azure Monitor logging.

You typically deploy Azure Firewall on a central virtual network to control general network access.

What can I configure with Azure Firewall?

With Azure Firewall, you can configure:

- Application rules that define fully qualified domain names (FQDNs) that can be accessed from a subnet.
- Network rules that define source address, protocol, destination port, and destination address.
- Network Address Translation (NAT) rules that define destination IP addresses and ports to translate inbound requests.

Azure Application Gateway[11] also provides a firewall, called the *web application firewall* (WAF). WAF provides centralized, inbound protection for your web applications against common exploits and vulnerabilities. **Azure Front Door**[12] and **Azure Content Delivery Network**[13] (CDN) also provide WAF services.

Protect from DDoS attacks by using Azure DDoS Protection

Any large company can be the target of a large-scale network attack. Tailwind Traders is no exception. Attackers might flood your network to make a statement or simply for the challenge. As they move to the cloud, Tailwind Traders wants to understand how Azure can help them prevent Distributed Denial of Service (DDoS) and other attacks.

In this part, you learn how Azure DDoS Protection (Standard service tier) helps protect your Azure resources from DDoS attacks. First, let's define what a DDoS attack is.

What are DDoS attacks?

A **Distributed Denial of Service**[14] (DDoS) attack attempts to overwhelm and exhaust an application's resources, making the application slow or unresponsive to legitimate users. DDoS attacks can target any resource that's publicly reachable through the internet, including websites.

11 https://azure.microsoft.com/services/application-gateway?azure-portal=true
12 https://azure.microsoft.com/services/frontdoor/?azure-portal=true
13 https://azure.microsoft.com/services/cdn/?azure-portal=true
14 https://azure.microsoft.com/services/ddos-protection?azure-portal=true

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

What is Azure DDoS Protection?

Azure DDoS Protection[15] (Standard) helps protect your Azure resources from DDoS attacks.

When you combine DDoS Protection with recommended application design practices, you help provide a defense against DDoS attacks. DDoS Protection utilizes the scale and elasticity of Microsoft's global network to bring DDoS mitigation capacity to every Azure region. The DDoS Protection service protects your Azure applications by analyzing and discarding DDoS traffic at the Azure network edge, before it can impact your service's availability.

This diagram shows network traffic flowing into Azure from both customers and an attacker:

DDoS Protection identifies the attacker's attempt to overwhelm the network and blocks further traffic from them, ensuring that traffic never reaches Azure resources. Legitimate traffic from customers still flows into Azure without any interruption of service.

DDoS Protection can also help you manage your cloud consumption. When you run on-premises, you have a fixed number of compute resources. But in the cloud, elastic computing means that you can automatically scale out your deployment to meet demand. A cleverly designed DDoS attack can cause you to increase your resource allocation, which incurs unneeded expense. DDoS Protection Standard helps ensure that the network load you process reflects customer usage. You can also receive credit for any costs accrued for scaled-out resources during a DDoS attack.

What service tiers are available to DDoS Protection?

DDoS Protection provides these service tiers:

- **Basic** The Basic service tier is automatically enabled for free as part of your Azure subscription. Always-on traffic monitoring and real-time mitigation of common network-level attacks provide the same defenses that Microsoft's online services use. The Basic service tier ensures that Azure infrastructure itself is not impacted during a large-scale DDoS attack. Azure's global network is used to distribute and mitigate attack traffic across Azure regions.
- **Standard** The Standard service tier provides additional mitigation capabilities that are tuned specifically to Azure Virtual Network resources. DDoS Protection Standard is relatively easy to enable and requires no changes to your applications. The Standard tier provides always-on traffic monitoring and real-time mitigation of common network-level attacks. It provides the same defenses that Microsoft's online services use. Protection policies are tuned through dedicated traffic monitoring and machine learning algorithms. Policies are applied to public IP addresses, which are associated with resources deployed in virtual networks such as Azure Load Balancer and Application Gateway. Azure's global network is used to distribute and mitigate attack traffic across Azure regions.

15 https://azure.microsoft.com/services/ddos-protection/?azure-portal=true

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

What kinds of attacks can DDoS Protection help prevent?

The Standard service tier can help prevent:

- **Volumetric attacks** The goal of this attack is to flood the network layer with a substantial amount of seemingly legitimate traffic.
- **Protocol attacks** These attacks render a target inaccessible by exploiting a weakness in the layer 3 and layer 4 protocol stack.
- **Resource (application) layer attacks (only with web application firewall)** These attacks target web application packets to disrupt the transmission of data between hosts. You need a web application firewall to protect against L7 attacks. DDoS Protection Standard protects the web application firewall (WAF) from volumetric and protocol attacks.

Filter network traffic by using network security groups

While Azure Firewall and Azure DDoS Protection can help control what traffic can come from outside sources, Tailwind Traders would also like to understand how to protect their internal networks on Azure. Doing so will give them an extra layer of defense against attacks.

In this part, you examine network security groups.

What are network security groups?

A **network security group**[16] (NSG) enables you to filter network traffic to and from Azure resources within an Azure Virtual Network. You can think of network security groups like an internal firewall. An NSG can contain multiple inbound and outbound security rules that enable you to filter traffic to and from resources by source and destination IP address, port, and protocol.

How do I specify network security groups rules?

A network security group can contain as many rules as you need, within Azure subscription limits. Each rule specifies these properties:

Property	Description
Name	A unique name for the NSG.
Priority	A number between 100 and 4096. Rules are processed in priority order, with lower numbers processed before higher numbers.
Source or Destination	A single IP address or IP address range, service tag, or application security group.
Protocol	TCP, UDP, or Any.
Direction	Whether the rule applies to inbound or outbound traffic.
Port Range	A single port or range of ports.
Action	Allow or Deny.

16 https://docs.microsoft.com/azure/virtual-network/security-overview#network-security-groups?azure-portal=true

When you create a network security group, Azure creates a series of default rules to provide a baseline level of security. You cannot remove the default rules, but you can override them by creating new rules with higher priorities.

Combine Azure services to create a complete network security solution

When considering your Azure security solution, consider all the elements of defense in depth.

Here are some recommendations on how to combine Azure services to create a complete network security solution.

Secure the perimeter layer

The perimeter layer is about protecting your organization's resources from network-based attacks. Identifying these attacks, alerting the appropriate security teams, and eliminating their impact is important to keep your network secure. To do this:

- Use Azure DDoS Protection to filter large-scale attacks before they can cause a denial of service for end users.
- Use perimeter firewalls with Azure Firewall to identify and alert on malicious attacks against your network.

Secure the network layer

At this layer, the focus is on limiting network connectivity across all of your resources to allow only what's required. Segment your resources and use network-level controls to restrict communication to only what's needed.

By restricting connectivity, you reduce the risk of lateral movement throughout your network from an attack. Use network security groups to create rules that define allowed inbound and outbound communication at this layer. Here are some recommended practices:

- Limit communication between resources by segmenting your network and configuring access controls.
- Deny by default.
- Restrict inbound internet access and limit outbound where appropriate.
- Implement secure connectivity to on-premises networks.

Combine services

You can also combine Azure networking and security services to manage your network security and provide increased layered protection. Here are a few ways you can combine services:

- **Network security groups and Azure Firewall**

  Azure Firewall complements the functionality of network security groups. Together, they provide better defense-in-depth network security.

  Network security groups provide distributed network-layer traffic filtering to limit traffic to resources within virtual networks in each subscription.

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

Azure Firewall is a fully stateful, centralized network firewall as a service. It provides network-level and application-level protection across different subscriptions and virtual networks.

- **Azure Application Gateway web application firewall and Azure Firewall**

  Web application firewall (WAF) is a feature of Azure Application Gateway that provides your web applications with centralized, inbound protection against common exploits and vulnerabilities.

  Azure Firewall provides:

  - Inbound protection for non-HTTP/S protocols (for example, RDP, SSH, and FTP).
  - Outbound network-level protection for all ports and protocols.
  - Application-level protection for outbound HTTP/S.

  Combining them provides more layers of protection.

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

Module 4 Review Questions

Module 04 Review Questions

Review Question 1

How can companies enforce having only certain applications run on its VMs?

- ☐ Connect your VMs to Azure Sentinel.
- ☐ Create an application control rule in Azure Security Center.
- ☐ Periodically run a script that lists the running processes on each VM. The IT manager can then shut down any applications that shouldn't be running.

Review Question 2

What's the easiest way for companies to combine security data from all of its monitoring tools into a single report that it can take action on?

- ☐ Collect security data in Azure Sentinel.
- ☐ Build a custom tool that collects security data and displays a report through a web application.
- ☐ Look through each security log daily and email a summary to your team.

Review Question 3

Which is the best way for companies to safely store its certificates so that they're accessible to cloud VMs?

- ☐ Place the certificates on a network share.
- ☐ Store them on a VM that's protected by a password.
- ☐ Store the certificates in Azure Key Vault.

Review Question 4

How can companies ensure that certain VM workloads are physically isolated from workloads being run by other Azure customers?

- ☐ Configure the network to ensure that VMs on the same physical host are isolated.
- ☐ This is not possible. These workloads need to be run on-premises.
- ☐ Run the VMs on Azure Dedicated Host.

Review Question 5

An attacker can bring down your website by sending a large volume of network traffic to your servers. Which Azure service can help companies protect its App Service instance from this kind of attack?

- ☐ Azure Firewall
- ☐ Network security groups
- ☐ Azure DDoS Protection

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

Review Question 6

What's the best way for companies to limit all outbound traffic from VMs to known hosts?

- ☐ Configure Azure DDoS Protection to limit network access to trusted ports and hosts.
- ☐ Create application rules in Azure Firewall.
- ☐ Ensure that all running applications communicate with only trusted ports and hosts.

Review Question 7

How can companies most easily implement a deny by default policy so that VMs can't connect to each other?

- ☐ Allocate each VM on its own virtual network.
- ☐ Create a network security group rule that prevents access from another VM on the same network.
- ☐ Configure Azure DDoS Protection to limit network access within the virtual network.

Module 4 Summary

Module 04 Summary

Protect against security threats on Azure

Tailwind Traders faces a number of security challenges. In today's digital world, its needs aren't unique.

Azure provides tools and services that can help you detect and act on important security events. It also provides ways to help keep your data safe, which can prevent security incidents from happening to begin with.

In this lesson, you learned about Azure services that relate to security. Here's a brief summary:

- Azure Security Center provides visibility of your security posture across all of your services, both on Azure and on-premises.
- Azure Sentinel aggregates security data from many different sources and provides additional capabilities for threat detection and response.
- Azure Key Vault stores your applications' secrets, such as passwords, encryption keys, and certificates, in a single, central location.
- Azure Dedicated Host provides dedicated physical servers to host your Azure VMs for Windows and Linux.

Secure network connectivity on Azure

In this lesson, you learned about some of the ways you can secure network traffic both on Azure and in your on-premises datacenter.

Defense in depth is the overriding theme. Think about security as a multiple-layer, multiple-vector concern. Threats come from places we don't expect, and they can come with surprising strength.

Tailwind Traders now has a few tools and services that it can use to secure its networks. Here's a brief summary:

- Azure Firewall is a managed, cloud-based network security service that helps protect resources in Azure virtual networks.
- An Azure virtual network is similar to a traditional network that you'd operate in your own datacenter. It enables virtual machines and other compute resources to securely communicate with each other, the internet, and on-premises networks.
- A network security group (NSG) enables you to filter network traffic to and from Azure resources within a virtual network.
- Azure DDoS Protection helps protect Azure resources from DDoS attacks.

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

Answers

Review Question 1

How can companies enforce having only certain applications run on its VMs?

- ☐ Connect your VMs to Azure Sentinel.
- ■ Create an application control rule in Azure Security Center.
- ☐ Periodically run a script that lists the running processes on each VM. The IT manager can then shut down any applications that shouldn't be running.

Explanation
With Azure Security Center, you can define a list of allowed applications to ensure that only applications you allow can run. Azure Security Center can also detect and block malware from being installed on your VMs.

Review Question 2

What's the easiest way for companies to combine security data from all of its monitoring tools into a single report that it can take action on?

- ■ Collect security data in Azure Sentinel.
- ☐ Build a custom tool that collects security data and displays a report through a web application.
- ☐ Look through each security log daily and email a summary to your team.

Explanation
Azure Sentinel is Microsoft's cloud-based SIEM. A SIEM aggregates security data from many different sources to provide additional capabilities for threat detection and responding to threats.

Review Question 3

Which is the best way for companies to safely store its certificates so that they're accessible to cloud VMs?

- ☐ Place the certificates on a network share.
- ☐ Store them on a VM that's protected by a password.
- ■ Store the certificates in Azure Key Vault.

Explanation
Azure Key Vault enables you to store your secrets in a single, central location. Key Vault also makes it easier to enroll and renew certificates from public certificate authorities (CAs).

Review Question 4

How can companies ensure that certain VM workloads are physically isolated from workloads being run by other Azure customers?

- ☐ Configure the network to ensure that VMs on the same physical host are isolated.
- ☐ This is not possible. These workloads need to be run on-premises.
- ■ Run the VMs on Azure Dedicated Host.

Explanation
Azure Dedicated Host provides dedicated physical servers to host your Azure VMs for Windows and Linux.

Review Question 5

An attacker can bring down your website by sending a large volume of network traffic to your servers. Which Azure service can help companies protect its App Service instance from this kind of attack?

- ☐ Azure Firewall
- ☐ Network security groups
- ■ Azure DDoS Protection

Explanation
DDoS Protection helps protect your Azure resources from DDoS attacks. A DDoS attack attempts to overwhelm and exhaust an application's resources, making the application slow or unresponsive to legitimate users.

Review Question 6

What's the best way for companies to limit all outbound traffic from VMs to known hosts?

- ☐ Configure Azure DDoS Protection to limit network access to trusted ports and hosts.
- ■ Create application rules in Azure Firewall.
- ☐ Ensure that all running applications communicate with only trusted ports and hosts.

Explanation
Azure Firewall enables you to limit outbound HTTP/S traffic to a specified list of fully qualified domain names (FQDNs).

Review Question 7

How can companies most easily implement a deny by default policy so that VMs can't connect to each other?

- ☐ Allocate each VM on its own virtual network.
- ■ Create a network security group rule that prevents access from another VM on the same network.
- ☐ Configure Azure DDoS Protection to limit network access within the virtual network.

Explanation
A network security group rule enables you to filter traffic to and from resources by source and destination IP address, port, and protocol.

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

Module 5 Describe identity, governance, privacy, and compliance features

Learning Objectives

Learning Objectives

After completing this module, you'll be able to:

- Explain the difference between authentication and authorization.
- Describe how Azure Active Directory provides identity and access management.
- Explain the role single sign-on (SSO), multifactor authentication, and Conditional Access play in managing user identity.
- Make organizational decisions about your cloud environment by using the Cloud Adoption Framework for Azure.
- Define who can access cloud resources by using Azure role-based access control.
- Apply a resource lock to prevent accidental deletion of your Azure resources.
- Apply tags to your Azure resources to help describe their purpose.
- Control and audit how your resources are created by using Azure Policy.
- Enable governance at scale across multiple Azure subscriptions by using Azure Blueprints.
- Explain the types of compliance offerings that are available on Azure.
- Access the Microsoft Privacy Statement, the Online Services Terms, and the Data Protection Addendum to learn what personal data Microsoft collects, how Microsoft uses it, and for what purposes.
- Gain insight into regulatory standards and compliance on Azure from the Trust Center and from the Azure compliance documentation.
- Explain Azure capabilities that are specific to government agencies.

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

Secure access to your applications by using Azure identity services

Introduction

Traditionally, protecting access to systems and data involved the on-premises network perimeter and physical access controls.

With people increasingly being able to work from anywhere, the rise of bring your own device (BYOD) strategies, mobile applications, and cloud applications, many of those access points are now outside of the company's physical networks.

Identity has become the new primary security boundary. Accurately proving that someone is a valid user of your system, with an appropriate level of access, is critical to maintaining control of your data. This identity layer is now more often the target of attack than the network.

Meet Tailwind Traders

Tailwind Traders [1] is a fictitious home improvement retailer. It operates retail hardware stores across the globe and online.

How will Tailwind Traders secure access to their cloud applications?

Tailwind Traders' mobile workforce is increasing, as are the number of applications Tailwind Traders runs in the cloud.

Retail employees located around the world are issued tablet devices from which they can create custom orders for customers, track delivery schedules, and plan their work schedules.

Delivery drivers are permitted to use their own mobile devices to access scheduling and logistics applications. Some delivery drivers are permanent employees of Tailwind Traders; others work on short-term contract.

Tailwind Traders uses Active Directory to secure their on-premises environments. They need to ensure that only employees can sign in and access their business applications. Tailwind Traders also needs to ensure that short-term staff can access these applications only when they're under active contract.

How can Azure Active Directory (Azure AD) help Tailwind Traders consistently secure all of their applications, both when accessed from their intranet and from public networks?

Learning objectives

After completing this module, you'll be able to:

- Explain the difference between authentication and authorization.
- Describe how Azure Active Directory provides identity and access management.
- Explain the role single sign-on (SSO), multi-factor authentication (MFA), and Conditional Access play in managing user identity.

1 https://www.tailwindtraders.com/

Prerequisites

- You should be familiar with basic computing concepts and terminology
- Familiarity with cloud computing is helpful, but isn't necessary

Compare authentication and authorization

Recall that Tailwind Traders must ensure that only employees can sign in and access their business applications.

Tailwind Traders also needs to ensure that employees can access only authorized applications. For example, all employees can access inventory and pricing software, but only store managers can access payroll and certain accounting software.

Two fundamental concepts you need to understand when talking about identity and access are *authentication* (AuthN) and *authorization* (AuthZ).

Authentication and authorization both support everything else that happens and occur sequentially in the identity and access process.

Let's take a brief look at each.

What is authentication?

Authentication is the process of establishing the identity of a person or service that wants to access a resource. It involves the act of challenging a party for legitimate credentials and provides the basis for creating a security principal for identity and access control. It establishes whether the user is who they say they are.

What is authorization?

Authentication establishes the user's identity, but authorization is the process of establishing what level of access an authenticated person or service has. It specifies what data they're allowed to access and what they can do with it.

How are authentication and authorization related?

Here's a diagram that shows the relationship between authentication and authorization:

The identification card represents credentials that the user has to prove their identity (you'll learn more about the types of credentials later in this module.) Once authenticated, authorization defines what kinds of applications, resources, and data that user can access.

What is Azure Active Directory?

In this part, you learn how Azure Active Directory (Azure AD) provides identity services that enable your users to sign in and access both Microsoft cloud applications and cloud applications you develop. You also learn how supports single sign-on (SSO).

Tailwind Traders already uses Active Directory to secure their on-premises environments and they don't want their users to have a different username and password to remember for accessing applications and

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

data in the cloud. Can they integrate their existing Active Directory with cloud identity services to create a seamless experience for their users?

Let's start with how Azure AD compares to Active Directory.

How does Azure AD compare to Active Directory?

Active Directory is related to Azure AD, but they have some key differences.

Microsoft introduced Active Directory in Windows 2000 to give organizations the ability to manage multiple on-premises infrastructure components and systems by using a single identity per user.

For on-premises environments, Active Directory running on Windows Server provides an identity and access management service that's managed by your own organization. Azure AD is Microsoft's cloud-based identity and access management service. With Azure AD, you control the identity accounts, but Microsoft ensures that the service is available globally. If you've worked with Active Directory, Azure AD will be familiar to you.

When you secure identities on-premises with Active Directory, Microsoft doesn't monitor sign-in attempts. When you connect Active Directory with Azure AD, Microsoft can help protect you by detecting suspicious sign-in attempts at no extra cost. For example, Azure AD can detect sign-in attempts from unexpected locations or unknown devices.

Who uses Azure AD?

Azure AD is for:

- **IT administrators** Administrators can use Azure AD to control access to applications and resources based on their business requirements.
- **App developers** Developers can use Azure AD to provide a standards-based approach for adding functionality to applications that they build, such as adding SSO functionality to an app or enabling an app to work with a user's existing credentials.
- **End users** End users can manage their identity. For example, self-service password reset enables users to change or reset their password with no involvement from an IT administrator or help desk.
- **Online service subscribers** Microsoft 365, Microsoft Office 365, Azure, and Microsoft Dynamics CRM Online subscribers are already using Azure AD. A *tenant* is a representation of an organization. A tenant is typically separated from other tenants and has its own identity. Each Microsoft 365, Office 365, Azure, and Dynamics CRM Online tenant is automatically an Azure AD tenant.

What services does Azure AD provide?

Azure AD provides services such as:

- **Authentication** This includes verifying identity to access applications and resources, and providing functionality such as self-service password reset, multi-factor authentication (MFA), a custom banned password list, and smart lockout services.
- **Single sign-on (SSO)** SSO enables you to remember only one username and one password to access multiple applications. A single identity is tied to a user, which simplifies the security model. As users change roles or leave an organization, access modifications are tied to that identity, which greatly reduces the effort needed to change or disable accounts.

- **Application management** You can manage your cloud and on-premises apps by using Azure AD. Features like Application Proxy, SaaS apps, the My Apps portal (also referred to as *Access panel*), and single-sign on provide a better user experience.
- **Device management** As well as accounts for individual people, Azure AD also supports the registration of devices. This enables devices to be managed through tools like Microsoft Intune. It also allows for device-based conditional access policies to restrict access attempts to only those coming from known, registered devices, regardless of the requesting user account.

What kinds of resources can Azure AD help secure?

Azure AD helps users access both external and internal resources.

External resources might include Microsoft Office 365, the Azure portal, and thousands of other software as a service (SaaS) applications.

Internal resources might include apps on your corporate network and intranet, along with any cloud applications developed within your organization.

What's single sign-on (SSO)?

Single sign-on enables a user to sign in one time and use that credential to access multiple resources and applications from different providers.

More identities mean more passwords to remember and change. Password policies can vary among applications and, as complexity requirements increase, it becomes increasingly difficult for users to remember them. The more passwords a user has to manage, the greater the risk of a credential-related security incident.

Consider the process of managing all those identities. Additional strain is placed on help desks as they deal with account lockouts and password reset requests. If a user leaves an organization, tracking down all those identities and ensuring they are disabled can be challenging. If an identity is overlooked, this could allow access when it should have been eliminated.

With SSO, you need to remember only one ID and one password. Access across applications is granted to a single identity that's tied to the user, which simplifies the security model. As users change roles or leave an organization, access is tied to a single identity, which greatly reduces the effort needed to change or disable accounts. Using SSO for accounts makes it easier for users to manage their identities and increases your security capabilities.

You'll find resources at the end of this module about how to enable SSO through Azure AD.

How can I connect Active Directory with Azure AD?

Connecting Active Directory with Azure AD enables you to provide a consistent identity experience to your users.

There are a few ways to connect your existing Active Directory installation with Azure AD. Perhaps the most popular method is to use Azure AD Connect.

Azure AD Connect synchronizes user identities between Active Directory running on-premises and Azure AD. Azure AD Connect synchronizes changes between both identity systems, which enables you to use features like SSO, MFA, and self-service password reset under both systems. Self-service password reset prevents users from using known compromised passwords.

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

Here's a diagram that shows how Azure AD Connect fits between your on-premises Active Directory and Azure AD:

A diagram showing two environments: Active Directory running on-premises and Azure AD. Azure AD Connect joins the two environments. Azure AD includes SSO, MFA, and self-service password reset.

As Tailwind Traders integrates its existing Active Directory instance with Azure AD, they create a consistent access model across their organization. Doing so greatly simplifies their ability to sign in to different applications, manage changes to user identities and control, and monitor and block unusual access attempts.

What are multifactor authentication and Conditional Access?

Tailwind Traders allows delivery drivers to use their own mobile devices to access scheduling and logistics applications. Some delivery drivers are permanent employees of Tailwind Traders; others work on short-term contract. How can the IT department ensure that an access attempt is really from a valid Tailwind Traders worker?

In this part, you'll learn about two processes that enable secure authentication: Azure Multi-Factor Authentication and Conditional Access. Let's start with a brief look at what multi-factor authentication is in general.

What's multi-factor authentication (MFA)?

Multi-factor authentication is a process where a user is prompted during the sign-in process for an additional form of identification, such as to enter a code on their cellphone or to provide a fingerprint scan.

Think about how you sign in to websites, email, or online gaming services. In addition to your username and password, have you ever needed to enter an additional code that was sent to your phone? If so, you've used MFA to sign in.

MFA provides additional security for your identities by requiring two or more elements to fully authenticate.

These elements fall into three categories:

- **Something you know** This could be your email address and password.
- **Something you have** This might be a code that's sent to your mobile phone.
- **Something you are** This is typically some sort of biometric property, such as a fingerprint or face scan that's used on many mobile devices.

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

MFA increases identity security by limiting the impact of credential exposure (for example, stolen usernames and passwords). With MFA enabled, an attacker who has a user's password would also need to have possession of their phone or their fingerprint to fully authenticate.

Compare MFA with single-factor authentication. Under single-factor authentication, an attacker would only need your username and password to authenticate. Therefore, MFA should be enabled wherever possible as MFA adds enormous benefits to security.

What's Azure Multi-Factor Authentication?

Azure Multi-Factor Authentication is a Microsoft service that provides MFA capabilities. Azure Multi-Factor Authentication enables users to choose an additional form of authentication during sign-in, such as a phone call or mobile app notification.

Which Microsoft services provide Azure Multi-Factor Authentication?

These services provide Azure Multi-Factor Authentication capabilities:

- **Azure Active Directory** The Azure Active Directory free edition enables Azure Multi-Factor Authentication for administrators with the *Global Admin* level of access, via the Microsoft Authenticator app, phone call, or SMS code. Azure Multi-Factor Authentication can also be enforced for all users via the Microsoft Authenticator app only, by enabling *security defaults* in your Azure AD tenant. Azure Active Directory Premium (P1 or P2 licenses) allows for comprehensive and granular configuration of Azure Multi-Factor Authentication through Conditional Access policies (explained below).
- **Multi-factor authentication for Office 365** A subset of Azure Multi-Factor Authentication capabilities is part of your Office 365 subscription.

For more information on licenses and Azure Multi-Factor Authentication capabilities, see **Available versions of Azure Multi-Factor Authentication**[2].

What's Conditional Access?

Conditional Access is a tool that's used by Azure Active Directory to allow (or deny) access to resources based on identity *signals*. These signals include who the user is, the user's location, and what device the user is requesting access from.

Conditional Access helps IT administrators:

- Empower users to be productive wherever and whenever.
- Protect the organization's assets.

2 https://docs.microsoft.com/azure/active-directory/authentication/concept-mfa-licensing#available-versions-of-azure-multi-factor-authentication?azure-portal=true

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

Conditional Access also provides a more granular MFA experience for end users. For example, end users might not be challenged for second authentication factor if they are at a known location. However, they might be challenged for a second authentication factor if their sign-in signals are unusual or the user is at an unexpected location.

During sign-in, Conditional Access collects signals from the user, makes decisions based on those signals, and then enforces that decision by allowing or denying the access request or challenging for an MFA response.

Here's a diagram that illustrates this flow:

Here, the signal might be the user's location, device, or the application the user is trying to access.

Based on these signals, the decision might be to allow full access if the user is signing in from their usual location. If the user is signing in from an unusual location or a location that's marked as high-risk, then access might be blocked entirely or possibly granted after the user provides a second form of authentication.

Enforcement is the action that carries out the decision; for example, to allow access or require the user to provide a second form of authentication.

When can I use Conditional Access?

Conditional Access is useful when you need to:

- Require MFA to access an application. You can configure whether all users require MFA or only certain users, such as administrators. You can also configure whether MFA applies to access from all networks or only untrusted networks.
- Require access to services only through approved client applications. For example, you might want to allow users to access Office 365 services from a mobile device as long as they use approved client apps, like Outlook mobile.
- Require the user to access your application only from managed devices. A *managed device* is a device that meets your standards for security and compliance.
- Block access from untrusted sources, such as access from unknown or unexpected locations.

Conditional Access comes with a *What If* tool, which helps you plan and troubleshoot your Conditional Access policies. You can use this tool to model your proposed conditional access policies across recent sign-in attempts from your users to see what the impact would have been if those policies had been enabled. The *What If* tool enables you to test your proposed conditional access policies before you implement them.

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

Where is Conditional Access available?

To use Conditional Access, you need an Azure AD Premium P1 or P2 license. If you have a Microsoft 365 Business Premium license, you also have access to Conditional Access features.

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

Build a cloud governance strategy on Azure

Introduction

The term *governance* describes the general process of establishing rules and policies and ensuring that those rules and policies are enforced.

When running in the cloud, a good governance strategy helps you maintain control over the applications and resources that you manage in the cloud. Maintaining control over your environment ensures that you stay compliant with:

- Industry standards, like **PCI DSS**[3].
- Corporate or organizational standards, such as ensuring that network data is encrypted.

Governance is most beneficial when you have:

- Multiple engineering teams working in Azure.
- Multiple subscriptions to manage.
- Regulatory requirements that must be enforced.
- Standards that must be followed for all cloud resources.

Meet Tailwind Traders

Tailwind Traders [4] is a fictitious home improvement retailer. It operates retail hardware stores across the globe and online.

Tailwind Traders specializes in competitive pricing, fast shipping, and a large range of items. It's looking at cloud technologies to improve business operations and support growth into new markets. By moving to the cloud, the company plans to enhance its shopping experience to further differentiate itself from competitors.

How will Tailwind Traders improve agility while maintaining control?

Tailwind Traders is continuing its migration to the cloud. For its existing datacenter, development and test teams must submit support tickets to request access to virtual machines, storage, and networking components. It can take IT staff anywhere from two weeks to two months to purchase, provision, and configure these components.

By working in the cloud, you essentially have immediate access to compute, storage, and networking components. Many kinds of groups and users, including people from development, test, operations, and security teams, can potentially have direct access to cloud resources.

Going forward, Tailwind Traders could enforce similar processes that prevent teams from directly creating or configuring resources on Azure, similar to its existing approach where central IT provisions infrastructure. But the company knows that these restrictions reduce team agility and the ability to innovate. How can they enable innovation while still maintaining control?

3 https://docs.microsoft.com/microsoft-365/compliance/offering-pci-dss?view=o365-worldwide?azure-portal=true
4 https://www.tailwindtraders.com/

In this module, you'll help the company explore ways it can enforce standards while still enabling teams to create and manage the cloud resources they need.

Learning objectives

After completing this module, you'll be able to:

- Make organizational decisions about your cloud environment by using the Cloud Adoption Framework.
- Define who can access cloud resources by using Azure RBAC.
- Apply a resource lock to prevent accidental deletion of your Azure resources.
- Apply tags to your Azure resources to help describe their purpose.
- Control and audit how your resources are created by using Azure Policy.
- Enable governance at scale across multiple Azure subscriptions by using Azure Blueprints.

Accelerate your cloud adoption journey by using the Cloud Adoption Framework for Azure

The **Microsoft Cloud Adoption Framework for Azure**[5] provides you with proven guidance to help with your cloud adoption journey. The Cloud Adoption Framework helps you create and implement the business and technology strategies needed to succeed in the cloud.

Tailwind Traders needs to control their cloud environment so that they comply with several industry standards, but they're not sure where to start. They have existing business requirements and they understand how these requirements relate to their on-premises workloads. These requirements also need to be met by any workloads they run in the cloud.

You've been tasked with investigating what's available on Azure and to define and implement the governance strategy for Tailwind Traders. You decide to start with Microsoft's Cloud Adoption Framework for Azure.

What's in the Cloud Adoption Framework?

The Cloud Adoption Framework consists of tools, documentation, and proven practices. The Cloud Adoption Framework breaks down into these stages:

1. Define your strategy
2. Make a plan
3. Ready your organization
4. Adopt the cloud
5. Govern and manage your cloud environments

5 https://docs.microsoft.com/azure/cloud-adoption-framework/?azure-portal=true

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

The Govern stage focuses on cloud governance. You can refer back to the Cloud Adoption Framework for recommended guidance as you build your cloud governance strategy.

To help build your adoption strategy, the Cloud Adoption Framework breaks down each stage into further exercises and steps. Let's take a brief look at each stage.

Define your strategy

Here, you answer why you're moving to the cloud and what you want to get out of cloud migration. Do you need to scale to meet demand or reach new markets? Will it reduce costs or increase business agility?

Here are the steps that make up this stage:

	Define and document your motivations: Meeting with stakeholders and leadership can help you answer why you're moving to the cloud.

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

2	**Document business outcomes**: Meet with leadership from your finance, marketing, sales, and human resource groups to help you document your goals.
3	**Develop a business case**: Validate that moving to the cloud give you the right return on investment (ROI) for your efforts.

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

	Choose the right first project: Choose a project that is achievable but also shows progress towards your cloud migration goals.

Make a plan

Here, you build a plan that maps your aspirational goals to specific actions. A good plan helps ensure that your efforts map to the desired business outcomes.

Here are the steps that make up this stage:

Digital estate: Create an inventory of the existing digital assets and workloads that you plan to migrate to the cloud.	

Initial organizational alignment: Ensure that the right people are involved in your migration efforts, both from a technical standpoint as well as from a cloud governance standpoint.	
Skills readiness plan: Build a plan that helps individuals build the skills they need to operate in the cloud.	

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

Cloud adoption plan: Build a comprehensive plan that brings together the development, operations, and business teams towards a shared cloud adoption goal.	

Ready your organization

Here, you create a *landing zone*, or an environment in the cloud to begin hosting your workloads.

Here are the steps that make up this stage:

	Azure setup guide: Review the Azure setup guide to become familiar with the tools and approaches you need to use to create a landing zone.

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

2	**Azure landing zones**: Begin to build out the Azure subscriptions that support each of the major areas of your business. A landing zone includes cloud infrastructure as well as governance, accounting, and security capabilities.
3	**Expand the landing zone**: Refine your landing zones to ensure that it meets your operations, governance, and security needs.

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

	Best practices: Start with recommended and proven practices to help ensure that your cloud migration efforts are scalable and maintainable.

Adopt the cloud

Here, you begin to migrate your applications to the cloud. Along the way, you might find ways to modernize your applications and build innovative solutions that use cloud services.

In fact, the Cloud Adoption Framework breaks this stage into two parts: migrate and innovate.

Migrate: Here are the steps that make up the migrate part of this stage:

Migrate your first workload: Use the Azure migration guide to deploy your first project to the cloud.	

Migration scenarios: Use additional in-depth guides to explore more complex migration scenarios.	2
Best practices: Check in with the Azure cloud migration best practices checklist to verify that you're following recommended practices.	3

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

Process improvements: Identify ways to make the migration process scale while requiring less effort.	

Innovate: Here are the steps that make up the innovate part of this stage:

	Business value consensus: Verify that investments in new innovations add value to the business and meet customer needs.

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

2	**Azure innovation guide**: Use this guide to accelerate development and build a minimum viable product (MVP) for your idea.
3	**Best practices**: Verify that your progress maps to recommended practices before you move forward.

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

	Feedback loops: Check in frequently with your customers to verify that you're building what they need.

Govern and manage your cloud environments

Here, you begin to form your cloud governance and cloud management strategies. As the cloud estate changes over time, so do cloud governance processes and policies. Therefore, you need to create resilient solutions that are constantly optimized.

Govern: Here are the steps that make up the govern part of this stage:

Methodology: Consider your end state solution. Then define a methodology incrementally takes you from your first steps all the way to full cloud governance.	

Benchmark: Use the **governance benchmark tool** *(https://cafbaseline.com/?azure-portal=true)* to assess your current state and future state to establish a vision for applying the framework.	
Initial governance foundation: Create an MVP that captures the first steps of your governance plan.	

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

Improve the initial governance foundation: Iteratively add governance controls that address tangible risks as you progress toward your end state solution.	

Manage: Here are the steps that make up the manage part of this stage:

	Establish a management baseline: Define your minimum commitment to operations management. A management baseline is the minimum set of tools and processes that should be applied to every asset in an environment.

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

2	**Define business commitments**: Document supported workloads to establish operational commitments with the business and agree on cloud management investments for each workload.
3	**Expand the management baseline**: Apply recommended best practices to iterate on your initial management baseline.

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

	Advanced operations and design principles: For workloads that require a higher level of business commitment, perform a deeper architecture review to deliver on your resiliency and reliability commitments.

Create a subscription governance strategy

In Plan and discuss Azure deployments, you learned that the organizing structure for resources in Azure has four levels: management groups, subscriptions, resource groups, and resources.

The beginning of any cloud governance implementation involves identifying a cloud organization structure that meets your business needs. This step often involves setting up a *cloud center of excellence team* (also referred to as a *cloud enablement team* or a *cloud custodian team*) and empowering this team to implement governance practices from a centralized location for the entire organization.

Teams often start their Azure governance strategy at the subscription level. There are three main aspects to consider when creating and managing subscriptions: billing, access control, and subscription limits.

Let's look at each of these aspects in more detail.

Billing

You can create one billing report per subscription. If you have multiple departments and need to do a “chargeback” of cloud costs, one possible solution is to organize subscriptions by department or by project.

Resource tags can also help here, and you'll explore tags later in this module. When defining how many subscriptions you need and what to name them, take into account your internal billing requirements.

Access control

A subscription is a deployment boundary for Azure resources. Every subscription is associated with an Azure Active Directory (Azure AD) tenant. Each tenant provides administrators the ability to set up granular access through defined roles by using Azure role-based access control (Azure RBAC).

When designing your subscription architecture, consider the deployment boundary factor. For example, do you need separate subscriptions for development and for production environments? Creating separate subscriptions enables you to control access to each one separately and therefore isolate their resources from one another.

Subscription limits

Subscriptions also have some resource limitations. For example, the maximum number of network Express Route circuits per subscription is 10. Those limits should be considered during your design phase. If you will need to exceed those limits, then you may need to add additional subscriptions. If you hit a hard limit maximum, there is no flexibility to increase it.

Management groups are also available to assist with managing subscriptions. A management group manages access, policies, and compliance across multiple Azure subscriptions. You'll learn more about management groups later in this module.

Control access to cloud resources by using Azure role-based access control

When you have multiple IT and engineering teams, how can you control what access they have to the resources in your cloud environment? It's a good security practice to grant users only the rights they need to perform their job, and only to the relevant resources.

Instead of defining the detailed access requirements for each individual, and then updating access requirements when new resources are created, Azure enables you to control access through **Azure role-based access control**[6] (Azure RBAC).

Azure provides built-in roles that describe common access rules for cloud resources. You can also define your own roles. Each role has an associated set of access permissions that relate to that role. When you assign individuals or groups to one or more roles, they receive all of the associated access permissions.

How is role-based access control applied to resources?

Role-based access control is applied to a *scope*, which is a resource or set of resources that this access applies to.

Here's a diagram that shows the relationship between roles and scopes:

Scopes include:

- A management group (a collection of multiple subscriptions.)
- A single subscription.
- A resource group.
- A single resource.

6 https://docs.microsoft.com/azure/role-based-access-control/overview?azure-portal=true

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

Observers, **Users managing resources**, **Admins**, and **Automated processes** illustrate the kinds of users or accounts who would typically be assigned each of the various roles.

When you grant access at a parent scope, those permissions are inherited by all child scopes. For example:

- When you assign the **Owner**[7] role to a user at the management group scope, that user can manage everything in all subscriptions within the management group.
- When you assign the **Reader**[8] role to a group at the subscription scope, the members of that group can view every resource group and resource within the subscription.
- When you assign the **Contributor**[9] role to an application at the resource group scope, the application can manage resources of all types within that resource group, but not other resource groups within the subscription.

When should I use Azure RBAC?

Use Azure RBAC when you need to:

- Allow one user to manage VMs in a subscription, and another user to manage virtual networks.
- Allow a database administrator (DBA) group to manage SQL databases in a subscription.
- Allow a user to manage all resources in a resource group, such as VMs, websites, and subnets.
- Allow an application to access all resources in a resource group.

These are just a few examples. You'll find the complete list of built-in roles at the end of this module.

How is Azure RBAC enforced?

Azure RBAC is enforced on any action that's initiated against an Azure resource that passes through Azure Resource Manager. Azure Resource Manager is a management service that provides a way to organize and secure your cloud resources.

You typically access the Azure Resource Manager from the Azure portal, Azure Cloud Shell, Azure PowerShell, and the Azure CLI. Azure RBAC does not enforce access permissions at the application or data level. Application security must be handled by your application.

RBAC uses an *allow model*. This means that when you are assigned a role, RBAC *allows* you to perform certain actions, such as read, write, or delete. Therefore, if one role assignment grants you read permissions to a resource group, and a different role assignment grants you write permissions to the same resource group, you have both read and write permissions on that resource group.

Who does Azure RBAC apply to?

You can apply Azure RBAC to an individual person or to a group. You can also apply Azure RBAC to other special identity types such as service principals and managed identities. These identity types are used by applications and services to automate access to Azure resources.

Tailwind Traders has the following teams with an interest in some part of their overall IT environment:

- IT Administrators This team has ultimate ownership of technology assets, both on-premises and in the cloud, and requires full control of all resources.

7 https://docs.microsoft.com/azure/role-based-access-control/built-in-roles?azure-portal=true#owner
8 https://docs.microsoft.com/azure/role-based-access-control/built-in-roles?azure-portal=true#reader
9 https://docs.microsoft.com/azure/role-based-access-control/built-in-roles?azure-portal=true#contributor

- Backup and Disaster Recovery This team is responsible for managing the health of regular backups and invoking any data or system recoveries.
- Cost and Billing People in this team track and report on technology-related spend and manage the organization's internal budgets.
- Security Operations This team monitors and responds to any technology-related security incidents, and require ongoing access to log files and security alerts.

How do I manage Azure RBAC permissions?

You manage access permissions on the **Access control (IAM)** blade in the Azure portal. This blade shows who has access to what scope and what roles apply. You can also grant or remove access from this blade.

The following screenshot shows an example of the **Access control (IAM)** blade for a resource group. In this example, Alain Charon has been assigned the **Backup Operator** role for this resource group.

A screenshot that shows the access control role assignment blade. In the access control pane, settings and permissions for a user are shown.

Prevent accidental changes by using resource locks

A **resource lock**[10] prevents resources from being accidentally deleted or changed.

Even with Azure RBAC policies in place, there's still a risk that people with the right level of access could delete critical cloud resources. Think of a resource lock as a warning system that reminds you that a resource should not be deleted or changed.

For example, at Tailwind Traders, an IT administrator was performing routine cleanup of unused resources in Azure. They accidentally deleted resources that appeared to be unused. However, these resources were critical to an application that's used for seasonal promotions. How can resource locks help prevent this kind of incident from happening in the future?

How do I manage resource locks?

You can manage resource locks from the Azure portal, PowerShell, the Azure CLI, or from an Azure Resource Manager template.

To view, add, or delete locks in the Azure portal, go to the **Settings** section of any resource's settings blade in the Azure portal.

Here's an example that shows how to add a resource lock from the Azure portal. You'll apply a similar resource lock in the next part.

10 https://docs.microsoft.com/azure/azure-resource-manager/management/lock-resources?azure-portal=true

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

A screenshot of the Azure portal showing how to add a resource lock.

What levels of locking are available?

You can apply locks to a subscription, to a resource group, or to an individual resource. You can set the lock level to **CanNotDelete** or **ReadOnly**.

- **CanNotDelete** means authorized people can still read and modify a resource, but they can't delete the resource without first removing the lock.
- **ReadOnly** means authorized people can read a resource, but they can't delete or change the resource. Applying this lock is like restricting all authorized users to the permissions granted by the **Reader** role in Azure RBAC.

How do I delete or change a locked resource?

Although locking helps prevent accidental changes, you can still make changes by following a two-step process.

To modify a locked resource, you must first remove the lock. After you remove the lock, you can apply any action you have permissions to perform. This additional step allows the action to be taken, but helps protect your administrators from doing something they may not have intended to do.

Resource locks apply regardless of RBAC permissions. Even if you are an owner of the resource, you must still remove the lock before you you can perform the blocked activity.

Combine resource locks with Azure Blueprints

What if a cloud administrator accidentally deletes a resource lock? If the resource lock is removed, its associated resources can be changed or deleted.

To make the protection process more robust, you can combine resource locks with Azure Blueprints. Azure Blueprints enables you to define the set of standard Azure resources that your organization requires. For example, you can define a blueprint that specifies that a certain resource lock must exist. Azure Blueprints can automatically replace the resource lock if that lock is removed.

You'll learn more about Azure Blueprints later in this module.

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

Exercise - Protect a storage account from accidental deletion by using a resource lock

In this exercise, you see how resource locks help prevent accidental deletion of your Azure resources.

To do so, you create a resource group from the Azure portal. Think of a resource group as a container for related Azure resources. Then you add a lock to your resource group and verify that you cannot delete the resource group.

You then add a storage account to your resource group and see how the lock from the parent resource group prevents the storage account from being deleted. A storage account is a container that groups a set of Azure Storage services together.

Important: *You need your own* ***Azure subscription***[11] *to complete the exercises in this module. If you don't have an Azure subscription, you can still read along.*

Create the resource group

Here you create a resource group that's named *my-test-rg*.

1. Go to the **Azure portal**[12] and sign in.
2. At the top of the page, select **Resource groups**.
3. Select **Add**. Then fill in these fields:

Setting	Value
Subscription	(Your Azure subscription)
Name	*my-test-rg*
Region	**(US) East US**

   You can also select a region that's closer to you.

4. Select **Review + create** and then select **Create**.

Add a lock to the resource group

Add a resource lock to the resource group. To do so:

1. From the Azure portal, select your resource group, *my-test-rg*.
2. Under **Settings**, select **Locks**, then select **Add**.

11 https://azure.microsoft.com/free/?azure-portal=true
12 https://portal.azure.com?azure-portal=true

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

3. Fill in these fields:

Setting	Value
Lock name	*rg-delete-lock*
Lock type	**Delete**

4. Select **OK**. You see that the resource lock is applied to your resource group.

Verify that the resource group is protected from deletion

Here, you verify protection by attempting to delete the resource group.

1. From the top of the page, select *my-test-rg* to go to your resource group's overview page.

2. Select **Delete resource group**.

3. At the prompt, enter *my-test-rg* and then select **OK**. You see a message that tells you that the resource group is locked and can't be deleted.

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

Protect a storage account from accidental deletion

Here you add a storage account to your resource group and see how the lock from the parent resource group prevents the storage account from being deleted. To do so:

1. From the Azure portal, at the top of the page, select **Home** to return to the start page.
2. Select **Storage accounts**. Then select **Add**.
3. Fill in these fields:

   Note: Replace**NNN** with a series of numbers. This helps ensure that your storage account name is unique.

Setting	Value
Subscription	(Your Azure subscription)
Resource group	**my-test-rg**
Storage account name	**mysaNNN**
Location	**(US) East US**
Performance	**Standard**
Account kind	**StorageV2 (general purpose v2)**
Replication	**Locally-redundant storage (LRS)**
Access tier (default)	**Hot**

   As before, you can also select a region that's closer to you.

4. Select **Review + Create** and then **Create**. The deployment might take a few moments to complete.
5. Select **Go to resource**.
6. At the top of the page, select **Delete**.

   You see a message that tells you the resource or its parent is locked and can't be deleted. Here's an example that shows the error message for a storage account that's named **mysa1234**:

Although you did not create a lock specifically for the storage account, the lock you created for the parent resource group prevents you from deleting the resource. In other words, the storage account inherits the lock from the parent resource group.

Delete the resource group and the storage account

You no longer need your resource group or storage account. Here you remove both.

When you delete a resource group, you also delete its child resources, such as the storage account you previously created.

To delete the resource group, you first need to remove the resource lock.

1. From the Azure portal, select **Home** > **Resource groups** > **my-test-rg** to go to your resource group.
2. Under **Settings**, select **Locks**.
3. Locate **rg-delete-lock** and select **Delete** on that same row.

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

4. Select **Overview**, then select **Delete resource group**.
5. At the prompt, enter *my-test-rg* and then select **OK**. The deletion operation might take a few moments to complete.
6. When the operation completes, select **Home** > **Resource groups**. You see that the **my-test-rg** resource group no longer exists in your account. Your storage account is also deleted.

Nice work. You can now apply resource locks to help prevent the accidental deletion of your Azure resources.

Organize your Azure resources by using tags

As your cloud usage grows, it's increasingly important to stay organized. Having a good organization strategy in place helps you understand your cloud usage and can help you manage costs.

For example, as Tailwind Traders prototypes new ways to deploy their applications on Azure, they need a way to mark their test environments so that they can easily identify and delete resources in these environments when they're no longer needed.

One way to organize related resources is to place them in their own subscriptions. You can also use resource groups to manage related resources. Resource *tags* are another way to organize resources. Tags provide extra information, or metadata, about your resources. This metadata is useful for:

- **Resource management** Tags enable you to locate and act on resources that are associated with specific workloads, environments, business units, and owners.
- **Cost management and optimization** Tags enable you to group resources so that you can report on costs, allocate internal cost centers, track budgets, and forecast estimated cost.
- **Operations management** Tags enable you to group resources according to how critical their availability is to your business. This helps you formulate service-level agreements (SLAs). An SLA is an uptime or performance guarantee between you and your users.
- **Security** Tags enable you to classify data by its security level (such as *public* or *confidential*).
- **Governance and regulatory compliance** Tags enable you to identify resources that align with governance or regulatory compliance requirements, such as ISO 27001. Tags can also be part of your standards enforcement efforts. For example, you might require that all resources be tagged with an owner or department name.
- **Workload optimization and automation** Tags can help you visualize all of the resources that participate in complex deployments. For example, you might tag a resource with its associated workload or application name and use software such as Azure DevOps to perform automated tasks on those resources.

How do I manage resource tags?

You can add, modify, or delete resource tags through PowerShell, the Azure CLI, Azure Resource Manager templates, the REST API, or the Azure portal.

You can also manage tags by using Azure Policy (you'll learn more about Azure Policy later in this module.) For example, you can apply tags to a resource group, but those tags are not automatically applied to the resources within that resource group. However, you can use Azure Policy to ensure that a resource inherits the same tags as its parent resource group.

You can also use Azure Policy to enforce tagging rules and conventions. For example, you can require that certain tags be added to new resources as they're provisioned. You can also define rules that reapply tags that have been removed.

An example tagging structure

A resource tag consists of a name and a value. You can assign one or more tags to each Azure resource.

After reviewing their business requirements, Tailwind Traders decides on the following tags:

Name	Value
AppName	The name of the application that the resource is part of.
CostCenter	The internal cost center code.
Owner	The name of the business owner who's responsible for the resource.
Environment	An environment name, such as "Prod", "Dev", or "Test".
Impact	How important the resource is to business operations, such as "Mission-critical", "High-impact", or "Low-impact".

Here's an example that shows these tags as they're applied to a virtual machine during provisioning:

Name		Value	Resource
AppName	:	SpecialOrders	Virtual machine
CostCenter	:	0224 - Infrastructure R&D	Virtual machine
Owner	:	tim@tailwindtraders.com	Virtual machine
Environment	:	Test	Virtual machine
Impact	:	High-impact	Virtual machine

The Tailwind Traders team can run queries, for example from PowerShell or the Azure CLI, to list all resources that contain these tags.

Keep in mind that you don't need to enforce that a specific tag is present on all of your resources. For example, you might decide that only mission-critical resources have the **Impact** tag. All non-tagged resources would then not be considered as mission-critical.

Control and audit your resources by using Azure Policy

Now that you've identified your governance and business requirements, how do you ensure that your resources *stay* compliant? How can you be alerted if a resource's configuration has changed?

Azure Policy[13] is a service in Azure that enables you to create, assign, and manage policies that control or audit your resources. These policies enforce different rules and effects over your resource configurations so that those configurations stay compliant with corporate standards.

13 https://azure.microsoft.com/services/azure-policy?azure-portal=true

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

How does Azure Policy define policies?

Azure Policy enables you to define both individual policies and groups of related policies, known as *initiatives*. Azure Policy evaluates your resources and highlights those which are not compliant with the policies you've created. Azure Policy can also prevent non-compliant resources from being created.

Azure Policy comes with a number of built-in policy and initiative definitions that you can use, under categories such as Storage, Networking, Compute, Security Center, and Monitoring.

For example, say you define a policy that allows only a certain stock keeping unit (SKU) size of virtual machines (VMs) to be used in your environment. After you enable this policy, that policy is applied when you create new VMs or resize existing VMs. Azure Policy also evaluates any current VMs in your environment.

In some cases, Azure Policy can automatically remediate non-compliant resources and configurations to ensure the integrity of the state of the resources. For example, if all resources in a certain resource group should be tagged with the **AppName** tag and a value of "SpecialOrders", Azure Policy can automatically reapply that tag if it has been removed.

Azure Policy also integrates with Azure DevOps by applying any continuous integration and delivery pipeline policies that apply to the pre-deployment and post-deployment phases of your applications.

Azure Policy in action

Implementing a policy in Azure Policy involves these three steps:

1. Create a policy definition.
2. Assign the definition to resources.
3. Review the evaluation results.

Let's examine each step in more detail.

1. Create a policy definition

A policy definition expresses what to evaluate and what action to take. For example, you could prevent VMs from being deployed in certain Azure regions. You also could audit your storage accounts to verify that they only accept connections from allowed networks.

Every policy definition has conditions under which it is enforced. A policy definition also has an accompanying effect that takes place when the conditions are met. Here are some example policy definitions:

- **Allowed Virtual Machine SKUs** This policy enables you to specify a set of VM SKUs that your organization can deploy.
- **Allowed locations** This policy enables you to restrict the locations that your organization can specify when deploying resources. Its effect is used to enforce your geographic compliance requirements.
- **MFA should be enabled accounts with write permissions on your subscription** This policy requires that Multi-Factor Authentication (MFA) be enabled for all subscription accounts with write privileges to prevent a breach of accounts or resources.
- **CORS should not allow every resource to access your Web Applications** CORS (Cross Origin Resource Sharing) is an HTTP feature that enables a web application running under one domain to access resources in another domain. For security reasons, modern web browsers restrict cross-site scripting by default. This policy allows only required domains to interact with your web app.

- **System updates should be installed on your machines** This policy enables Azure Security Center to recommend missing security system updates on your servers.

2. Assign the definition to resources

To implement your policy definitions, you assign definitions to resources. A *policy assignment* is a policy definition that takes place within a specific scope. This scope could be a management group (a collection of multiple subscriptions), a single subscription, or a resource group.

Policy assignments are inherited by all child resources within that scope. This means that if a policy is applied to a resource group, that policy is applied to all resources within that resource group. However, you can exclude a sub-scope from the policy assignment if there are specific child resources you need to be exempt from the policy assignment.

3. Review the policy evaluation results

When a condition is evaluated against your existing resources, each resource is marked as compliant or non-compliant. You can review the non-compliant policy results and take any action that's needed.

Policy evaluation happens about once per hour, which means that if you make changes to your policy definition and create a policy assignment, that policy is evaluated over your resources within the hour.

What are Azure Policy initiatives?

An Azure Policy initiative is a way of grouping related policies into one set. The initiative definition contains all of the policy definitions to help track your compliance state for a larger goal.

For example, Azure Policy includes an initiative named **Enable Monitoring in Azure Security Center**. Its goal is to monitor all of the available security recommendations for all Azure resource types in Azure Security Center.

Under this initiative, the following policy definitions are included:

- **Monitor unencrypted SQL Database in Security Center** This policy monitors for unencrypted SQL databases and servers.
- **Monitor OS vulnerabilities in Security Center** This policy monitors servers that do not satisfy the configured OS vulnerability baseline.
- **Monitor missing Endpoint Protection in Security Center** This policy monitors for servers that don't have an installed endpoint protection agent.

In fact, the **Enable Monitoring in Azure Security Center** initiative contains over 100 separate policy definitions.

Azure Policy also includes initiatives that support regulatory compliance standards such as HIPAA and ISO 27001.

How do I define an initiative?

You define initiatives by using the Azure portal or by using command-line tools. From the Azure portal, you can search the list of built-in initiatives that are already provided by Azure or you can create your own custom policy definition.

The following image shows a few example Azure Policy initiatives in the Azure portal.

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

How do I assign an initiative?

Like a policy assignment, an initiative assignment is an initiative definition that's assigned to a specific scope of a management group, a subscription, or a resource group.

Even if you have just a single policy, an initiative enables you to increase the number of policies over time. Because the associated initiative remains assigned, this makes it easier to add and remove policies without the need to change your resources' policy assignment.

Exercise - Restrict deployments to a specific location by using Azure Policy

In this exercise, you create a policy in Azure Policy that restricts the deployment of Azure resources to a specific location. You verify the policy by attempting to create a storage account in a location that violates the policy.

Tailwind Traders wants to limit the location where resources can be deployed to the **East US** region. They do for for two reasons:

- **Improved cost tracking** To track costs, Tailwind Traders uses different subscriptions to track deployments to each of their regional locations. The policy will ensure that all resources are deployed to the **East US** region.
- **Adhere to data residency and security compliance** Tailwind Traders must adhere to a compliance rule that states where customer data can be stored. Here, customer data must be stored in the **East US** region.

Recall that you can assign a policy to a management group, a single subscription, or a resource group. Here, you assign the policy to a resource group so that policy does not affect any other resources in your Azure subscription.

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

Important: *You need your own* ***Azure subscription***[14] *to complete the exercises in this module. If you don't have an Azure subscription, you can still read along.*

Create the resource group

Here you create a resource group that's named *my-test-rg*. This is the resource group to which you'll apply your location policy.

For learning purposes, you use the same resource group name that you used in the previous exercise. You can use the same name because you deleted the previous resource group.

1. Go to the **Azure portal**[15] and sign in.
2. Select **Create a resource**.
3. Enter *resource group* in the search box and select Enter.
4. If you are taken to a search results page, select **Resource group** from the results.
5. Select **Create**. Then fill in these fields:

Setting	Value
Subscription	(Your Azure subscription)
Subscription > Resource group	*my-test-rg*
Region	**(US) East US**

6. Select **Review + create** and then select **Create**.

Explore predefined policies

Before you configure your location policy, let's take a brief look at some predefined policies. As an example, you'll look at policies that relate to Azure Compute services.

1. From the Azure portal, at the top of the page, select **Home** to return to the start page.
2. At the top of the page, enter *policy* in the search bar. Then select **Policy** from the list of results to access Azure Policy.
3. Under **Authoring**, select **Definitions**.
4. From the **Category** drop-down list, select only **Compute**. Notice that the **Allowed virtual machine SKUs** definition enables you to specify a set of virtual machine SKUs that your organization can deploy.

14 https://azure.microsoft.com/free/?azure-portal=true
15 https://portal.azure.com?azure-portal=true

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

As an optional step, explore any other policies or categories that interest you.

Configure the location policy

Here you configure the allowed location policy by using Azure Policy and then you assign that policy to your resource group. To do so:

1. From the **Policy** page, under **Authoring**, select **Assignments**.

An assignment is a policy that has been assigned to take place within a specific scope. For example, a definition could be assigned to the subscription scope.

2. Select **Assign Policy**.

You are taken to the **Assign policy** page.

3. Under **Scope**, select the ellipsis. From the dialog that appears, set:
    1. The **Subscription** field to your Azure subscription.
    2. The **Resource Group** field to **my-test-rg**.
    3. Select the **Select** button.
4. Under **Policy definition**, select the ellipsis.
    1. In the search bar, enter *location*.
    2. Select the **Allowed locations** definition.
    3. Select the **Select** button.

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

This policy definition specifies the location into which all resources must be deployed. If a different location is chosen, deployment will fail.

5. Select **Next** to move to the **Parameters** tab.
6. From **Allowed locations** drop-down box, select **East US**.
7. Select **Review + create**, and then select **Create**. You see that the **Allowed locations** policy assignment is now listed on the **Policy | Assignments** pane. It enforces the policy on the **my-test-rg** resource group.

Verify the location policy

Here you attempt to add a storage account to your resource group at a location that violates your location policy.

1. From the Azure portal, at the top of the page, select **Home** to return to the start page.
2. Select **Create a resource**.
3. Enter *storage account* in the search box and select Enter.
4. If you are taken to a search results page, select **Storage account** from the results.
5. Select **Create**. Then fill in these fields:

   Replace **NNN** with a series of numbers. This helps ensure that your storage account name is unique.

Setting	Value
Subscription	(Your Azure subscription)

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

Setting	Value
Subscription > Resource group	**my-test-rg**
Storage account name	**mysaNNN**
Location	**(Asia Pacific) Japan East**
Performance	**Standard**
Account kind	**StorageV2 (general purpose v2)**
Replication	**Locally-redundant storage (LRS)**
Access tier (default)	**Hot**

If you previously selected **Japan East** in your location policy, select a different region from the list.

6. Select **Review + create** and then select **Create**. You see a message that states that the deployment failed due to the policy violation. Below you see the deployment details. Here's an example that shows

the deployment details for a storage account named **mysa1234**:]A screenshot of the Azure portal showing the deployment details message. The details include the resource name, its type, and a status of Forbidden.":::

Delete the policy assignment

You no longer need your policy assignment. Here you remove it from your subscription.

1. From the Azure portal, select **Home** > **Policy**.
2. Under **Authoring**, select **Assignments**.
3. On the **Allowed locations** row, select the ellipsis. Then select **Delete assignment**. When prompted, select **Yes**.

You see that the **Allowed locations** policy assignment no longer exists.

As an optional step, you can try creating the storage account a second time to verify that the policy is no longer in effect.

Delete the resource group

You no longer need your resource group. Here you remove it from your subscription.

1. From the Azure portal, select **Home** > **Resource groups** > **my-test-rg** to go to your resource group.
2. Select **Overview**, then select **Delete resource group**.

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

3. At the prompt, enter *my-test-rg* and then select **OK**. The deletion operation might take a few moments to complete.
4. After the operation completes, select **Home** > **Resource groups**. You see that the **my-test-rg** resource group no longer exists in your account.

Great work! You've successfully applied a policy by using Azure Policy to restrict the deployment of Azure resources to a specific location. You can now apply the policies that you need at the management group, subscription, or resource group level.

Govern multiple subscriptions by using Azure Blueprints

So far, you've explored a number of Azure features that can help you implement your governance decisions, monitor the compliance of your cloud resources, and control access and protect critical resource from accidental deletion.

What happens when your cloud environment starts to grow beyond just one subscription? How can you scale the configuration of these features, knowing they need to be enforced for resources in new subscriptions?

Instead of having to configure features like Azure Policy for each new subscription, **Azure Blueprints**[16] enables you to define a repeatable set of governance tools and standard Azure resources that your organization requires. This enables development teams to rapidly build and deploy new environments with the knowledge that they're building within organizational compliance with a set of built-in components that speed up the development and deployment phases.

Azure Blueprints orchestrates the deployment of various resource templates and other artifacts, such as:

- Role assignments
- Policy assignments
- Azure Resource Manager templates
- Resource groups

Azure Blueprints in action

When you form a cloud center of excellence team or a cloud custodian team, that team can use Azure Blueprints to scale their governance practices throughout the organization.

Implementing a blueprint in Azure Blueprints involves these three steps:

1. Create an Azure Blueprint.
2. Assign the blueprint.
3. Track the blueprint assignments.

With Azure Blueprints, the relationship between the blueprint definition (what should be deployed) and the blueprint assignment (what was actually deployed) is preserved. In other words, Azure creates a record that associates a resource with the blueprint that defines it. This connection helps you track and audit your deployments.

Blueprints are also versioned. Versioning enables you to track and comment on changes to your blueprint.

16 https://azure.microsoft.com/services/blueprints?azure-portal=true

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

What are blueprint artifacts?

Each component in the blueprint definition is known as an *artifact*.

Artifacts can either have no parameters (for example, the **Deploy threat detection on SQL servers** policy, which requires no further configuration), or they can contain one or more parameters that you can configure.

The following screenshot shows the **Allowed locations** policy. This policy includes a parameter that specifies the allowed locations.

A screenshot showing the Allowed locations policy. This policy includes a parameter that specifies the allowed locations.

You can specify a parameter's value when you crate the blueprint definition or when you assign the blueprint definition to a scope. This enables you to maintain one standard blueprint, but have the flexibility to specify the relevant configuration parameters at each scope where the definition is assigned.

How will Tailwind Traders use Azure Blueprints for ISO 27001 compliance?

ISO 27001[17] is a standard that applies to the security of Information Technology (IT) systems, published by the International Organization for Standardization. As part of its quality process, Tailwind Traders wants to certify that it complies with this standard. Azure Blueprints has several built-in blueprint definitions that relate to ISO 27001.

As an IT administrator, you decide to investigate the **ISO 27001: Shared Services Blueprint** definition. Here an outline of your plan:

1. Define a management group that's named **PROD-MG**. Recall that a management group manages access, policies, and compliance across multiple Azure subscriptions. Every new Azure subscription is added to this management group when the subscription is created.

17 https://www.iso.org/isoiec-27001-information-security.html?azure-portal=true

2. Create a blueprint definition that's based on the **ISO 27001: Shared Services Blueprint** template and then publish the blueprint.
3. Assign the blueprint to your **PROD-MG** management group.

The following image shows artifacts that are created when you run an ISO 27001 blueprint from a template:

Screenshot showing artifacts listed when creating an ISO 27001 blueprint from template.

You see that the blueprint template contains policy assignments, ARM templates, and resource groups. The blueprint deploys these artifacts to any existing subscriptions within the **PROD-MG** management group. The blueprint also deploys these artifacts to any new subscriptions as they are created and added to the management group.

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

Examine privacy, compliance, and data protection standards on Azure

Introduction

In this module, you'll learn about Microsoft's commitment to privacy and how Azure adheres to common regulatory and compliance standards.

If your organization is a government department or agency, or you need to deploy to regions of China, you'll also learn about some additional considerations that you need to make that don't apply to other Azure users.

In general, *compliance* means to adhere to some law, standard, or set of guidelines. *Regulatory compliance* refers to the discipline and process of ensuring that a company follows the laws that governing bodies enforce.

Meet Tailwind Traders

Tailwind Traders [18] is a fictitious home improvement retailer. It operates retail hardware stores across the globe and online.

Tailwind Traders specializes in competitive pricing, fast shipping, and a large range of items. It's looking at cloud technologies to improve business operations and support growth into new markets. By moving to the cloud, the company plans to enhance its shopping experience to further differentiate itself from competitors.

How will Tailwind Traders protect its data in the cloud and stay compliant?

Tailwind Traders is planning its migration to the cloud. It's used to having full control of all of its application data, which is stored on servers that it manages in its datacenter.

Tailwind Traders knows that moving an application to the cloud means that data is now outside of its own walls. The company also understands that the cloud provider has access to the server hardware and infrastructure. How is the privacy of its application data protected?

Tailwind Traders must also adhere to multiple regulatory and compliance frameworks. For example, it must follow certain rules to ensure that it properly handles credit card data. It will still need to ensure that its applications comply with applicable regulations and standards. How does infrastructure on Azure already adhere to these same standards?

To answer these questions, you'll start by learning about the types of compliance offerings that are available on Azure.

Learning objectives

After completing this module, you'll be able to:

- Explain the types of compliance offerings that are available on Azure.

18 https://www.tailwindtraders.com/

- Access the Microsoft Privacy Statement, the Online Services Terms, and the Data Protection Addendum to learn what personal data Microsoft collects, how Microsoft uses it, and for what purposes.
- Gain insight into regulatory standards and compliance on Azure from the Trust Center and from the Azure compliance documentation.
- Explain Azure capabilities that are specific to government agencies.

Prerequisites

- You should be familiar with basic computing concepts and terminology
- Familiarity with cloud computing is helpful, but isn't necessary

Explore compliance terms and requirements

In this part, you learn about the types of compliance offerings that are available on Azure.

As Tailwind Traders moves to running their applications in the cloud, they want to know how Azure adheres to applicable regulatory compliance frameworks. They ask:

- How compliant is Azure when it comes to the handling of personal data?
- How compliant are each of Azure's individual services?

Microsoft's online services build upon a common set of regulatory and compliance controls. Think of a *control* as a known good standard that you can compare your solution against to ensure security. These controls address today's regulations and adapt as regulations evolve.

Which compliance categories are available on Azure?

Although there are many more, the following image shows some of the more popular compliance offerings that are available on Azure. These offerings are grouped under four categories: Global, US Government, Industry, and Regional.

A screenshot of some of the Azure compliance offerings grouped under categories of Global, US Government, Industry, and Regional.

To get a sense of the variety of the compliance offerings available on Azure, let's take a closer look at a few of them.

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

While not all of these compliance offerings will be relevant to you or your team, they show that Microsoft's commitment to compliance is comprehensive, ongoing, and independently tested and verified.

Criminal Justice Information Service (CJIS)

Any US state or local agency that wants to access the FBI's Criminal Justice Information Services (CJIS) database is required to adhere to the CJIS Security Policy.

Azure is the only major cloud provider that contractually commits to conformance with the CJIS Security Policy, which commits Microsoft to adhering to the same requirements that law enforcement and public safety entities must meet.

Cloud Security Alliance (CSA) STAR Certification

Azure, Intune, and Microsoft Power BI have obtained STAR Certification, which involves a rigorous independent third-party assessment of a cloud provider's security posture.

The STAR certification is based on achieving ISO/IEC 27001 certification and meeting criteria specified in the Cloud Controls Matrix (CCM). This certification demonstrates that a cloud service provider conforms to the applicable requirements of ISO/IEC 27001, has addressed issues critical to cloud security as outlined in the CCM, and has been assessed against the STAR Capability Maturity Model for the management of activities in CCM control areas.

European Union (EU) Model Clauses

Microsoft offers customers EU Standard Contractual Clauses that provide contractual guarantees around transfers of personal data outside of the EU.

Microsoft is the first company to receive joint approval from the EU's Article 29 Working Party that the contractual privacy protections Azure delivers to its enterprise cloud customers meet current EU standards for international transfers of data, which ensures that Azure customers can use Microsoft services to move data freely through Microsoft's cloud, from Europe to the rest of the world.

Health Insurance Portability and Accountability Act (HIPAA)

The Health Insurance Portability and Accountability Act (HIPAA) is a US federal law that regulates patient Protected Health Information (PHI).

Azure offers customers a HIPAA Business Associate Agreement (BAA), stipulating adherence to certain security and privacy provisions in HIPAA and the HITECH Act. To assist customers in their individual compliance efforts, Microsoft offers a BAA to Azure customers as a contract addendum.

International Organization of Standards/International Electrotechnical Commission (ISO/IEC) 27018

Microsoft is the first cloud provider to have adopted the ISO/IEC 27018 code of practice, covering the processing of personal information by cloud service providers.

Multi-Tier Cloud Security (MTCS) Singapore

After rigorous assessments conducted by the MTCS Certification Body, Microsoft cloud services received MTCS 584:2013 Certification across all three service classifications: infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS).

Microsoft is the first global cloud solution provider to receive this certification across all three classifications.

Service Organization Controls (SOC) 1, 2, and 3

Microsoft-covered cloud services are audited at least annually against the SOC report framework by independent third-party auditors.

The Microsoft cloud services audit covers controls for data security, availability, processing integrity, and confidentiality as applicable to in-scope trust principles for each service.

National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF)

NIST CSF is a voluntary Framework that consists of standards, guidelines, and best practices to manage cybersecurity-related risks.

Microsoft cloud services have undergone independent, third-party Federal Risk and Authorization Management Program (FedRAMP) Moderate and High Baseline audits and are certified according to the FedRAMP standards.

Additionally, through a validated assessment performed by the Health Information Trust Alliance (HITRUST), a leading security and privacy standards development and accreditation organization, Office 365 is certified to the objectives specified in the NIST CSF.

United Kingdom (UK) Government G-Cloud

The UK Government G-Cloud is a cloud computing certification for services used by government entities in the United Kingdom. Azure has received official accreditation from the UK Government.

Access the Microsoft Privacy Statement, the Online Services Terms, and the Data Protection Addendum

In this part, you learn how the Microsoft Privacy Statement, the Online Services Terms, and the Data Protection Addendum explain what personal data Microsoft collects, how Microsoft uses it, and for what purposes.

For Tailwind Traders, understanding Microsoft's commitment to privacy helps ensure that their customer and application data will be protected.

Let's begin with a brief look at the Microsoft Privacy Statement.

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

What's in the Microsoft Privacy Statement?

The **Microsoft Privacy Statement**[19] explains what personal data Microsoft collects, how Microsoft uses it, and for what purposes.

The privacy statement covers all of Microsoft's services, websites, apps, software, servers, and devices. This list ranges from enterprise and server products to devices that you use in your home to software that students use at school.

Microsoft's privacy statement also provides additional information that's relevant to specific products such as Windows and Xbox.

What's in the Online Services Terms?

The **Online Services Terms**[20] (OST) is a legal agreement between Microsoft and the customer. The OST details the obligations by both parties with respect to the processing and security of customer data and personal data. The OST applies specifically to Microsoft's online services that you license through a subscription, including Azure, Dynamics 365, Office 365, and Bing Maps.

What is the Data Protection Addendum?

The Data Protection Addendum (DPA) further defines the data processing and security terms for online services. These terms include:

- Compliance with laws.
- Disclosure of processed data.
- Data Security, which includes security practices and policies, data encryption, data access, customer responsibilities, and compliance with auditing.
- Data transfer, retention, and deletion.

To access the DPA:

1. Go to the **Licensing Terms and Documentation**[21].
2. In the search bar, enter *DPA*.
3. From the search results, locate the link to the DPA in your preferred language.

   Alternatively, in the search bar that appears, enter your preferred language to filter the results. Here's an example that retrieves the English version of the DPA.

19 https://privacy.microsoft.com/privacystatement?azure-portal=true
20 https://www.microsoft.com/licensing/terms/product/ForallOnlineServices?azure-portal=true
21 https://www.microsoftvolumelicensing.com/DocumentSearch.aspx?azure-portal=true

Search for Documents:
DPA

Note: This page does not include any signed Volume Licensing agreements, enrollments or Microsoft Business and Services Agreement, and is intended solely for reference purposes.

Show Archived

Search: English

Title	Language	Sectors	Regions
MicrosoftOnlineServicesDPA(WW)(English)(July212020)	English	Commercial, Public Sector, Third Party, Common Document, Academic, Government, Nonprofit	North America, EU-EFTA (European Union and EFTA), MEA-EE (Middle East, Africa - Eastern Europe, Asia , WW (World

Transparency is important when it comes to how a cloud provider communicates its privacy policies and how it treats your data. The Microsoft Privacy Statement, the OST, and the DPA detail Microsoft's commitment to protecting data and privacy in the cloud.

Explore the Trust Center

Tailwind Traders needs to stay up to date on the latest security standards for protecting their data. Today, the security team needs to verify whether Azure meets ISO 27001, a commonly-used information security standard. Where can they access this information?

The **Trust Center**[22] showcases Microsoft's principles for maintaining data integrity in the cloud and how Microsoft implements and supports security, privacy, compliance, and transparency in all Microsoft cloud products and services. The Trust Center is an important part of the Microsoft Trusted Cloud Initiative and provides support and resources for the legal and compliance community.

22 https://www.microsoft.com/trustcenter?azure-portal=true

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

The Trust Center provides:

- In-depth information about security, privacy, compliance offerings, policies, features, and practices across Microsoft cloud products.
- Additional resources for each topic.
- Links to the security, privacy, and compliance blogs and upcoming events.

The Trust Center is a great resource for other people in your organization who may play a role in security, privacy, and compliance. These people include business managers, risk assessment and privacy officers, and legal compliance teams.

As an optional exercise, let's take a brief look at the Trust Center's entry for ISO 27001.

Access to the Trust Center doesn't require an Azure subscription or a Microsoft account.

1. Go to the **Trust Center**[23].
2. Locate the **Additional resources** section on the page. Under **Compliance offerings**, select **Learn more**.

23 https://www.microsoft.com/trustcenter?azure-portal=true

You're taken to **Microsoft compliance offerings**[24].

The offerings are grouped into these categories: **Global**, **US Government**, **Industry**, and **Regional**.

3. Under **Global**, select **ISO 27001**.

The ISO 27001 Information Security Management Standards page is typical of the type of compliance information we provide.

4. Briefly review the documentation for ISO/IEC 27001.

You see:

- An overview of the standard.
- Which cloud services are in scope.
- An overview of the audit cycle and links to audit reports.
- Answers to frequently asked questions.
- Additional resources and white papers.

The areas of documentation for other compliance offerings will vary, but this is the typical format that you'll find.

Access Azure compliance documentation

Here, you learn how to access detailed documentation about legal and regulatory standards and compliance on Azure.

E-commerce is an important part of Tailwind Traders' sales strategy. Their **online retail store**[25] enables customers to easily browse and order products. Customers typically pay by credit card, so Tailwind Traders has a responsibility under the Payment Card Industry (PCI) Data Security Standard (DSS). This global standard, known as PCI DSS, seeks to prevent fraud through increased control of credit card data and applies to any organization that stores, processes, or transmits payment and cardholder data.

You've been tasked with investigating whether hosting their e-commerce application on Azure would be compliant with PCI DSS. You start with the Azure compliance documentation.

24 https://docs.microsoft.com/microsoft-365/compliance/offering-home?azure-portal=true
25 https://www.tailwindtraders.com/?azure-portal=true

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

What is the Azure compliance documentation?

The **Azure compliance documentation**[26] provides you with detailed documentation about legal and regulatory standards and compliance on Azure.

Here you find compliance offerings across these categories:

- Global
- US government
- Financial services
- Health
- Media and manufacturing
- Regional

There are also additional compliance resources, including audit reports, privacy information, compliance implementations and mappings, and white papers and analyst reports, as well as country and region privacy and compliance guidelines. Some resources may require you to be signed in to your cloud service to access them.

Examine PCI DSS compliance

The legal team at Tailwind Traders wants to learn more about how PCI DSS relates to their e-commerce application on Azure.

As an optional exercise, here you follow along.

1. Go to the **Azure compliance documentation**[27].
2. Under **Financial services**, select **PCI DSS**.

There you see:

- An overview of the PCI DSS standard.
- How PCI DSS applies to Microsoft.
- Which cloud services are in scope.

26 https://docs.microsoft.com/azure/compliance/?azure-portal=true
27 https://docs.microsoft.com/azure/compliance/?azure-portal=true

- An overview of the audit cycle.
- Answers to frequently asked questions.
- Additional resources and white papers.

Access additional compliance resources

From the **Azure compliance documentation**[28], you can access additional compliance resources.

For example, from the **Audit reports** section, you find a link to audit reports for **PCI DSS**[29].

Audit reports

CCSL/IRAP
CDSA
ENS
ISO 27001
FedRAMP
PCI DSS
SOC 1, 2, 3

From there you can access several different files including the Attestation of Compliance reports and the PCI DSS Shared Responsibility Matrix.

Under **Compliance blueprints**, you find reference blueprints, or policy definitions, for common standards that you can apply to your Azure subscription. The **PCI-DSS**[30] blueprint deploys a core set of policies that map to PCI DSS compliance and help you govern your Azure workloads against this standard.

Compliance blueprints

Azure Security Benchmark
Canada Federal PBMM
CIS benchmarks
FedRAMP Moderate
FedRAMP High
HIPAA HITRUST
IRS 1075
ISO 27001
NIST SP 800-53 R4
PCI-DSS v3.2.1
SWIFT CSP-CSCF v2020
UK NHS and UK OFFICIAL (G-Cloud)

You can then see if the Azure resources in your application architecture have been configured correctly for PCI DSS compliance, or which resources you need to remediate.

Because standards evolve, the Tailwind Traders team might check the audit report periodically to ensure that Azure has kept up with any recent changes.

28 https://docs.microsoft.com/azure/compliance/?azure-portal=true
29 https://servicetrust.microsoft.com/ViewPage/MSComplianceGuideV3?docTab=7027ead0-3d6b-11e9-b9e1-290b1eb4cdeb_PCI_DSS?azure-portal=true
30 https://docs.microsoft.com/azure/governance/blueprints/samples/pci-dss-3.2.1/?azure-portal=true

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

What is Azure Government?

Azure Government[31] is a separate instance of the Microsoft Azure service. It addresses the security and compliance needs of US federal agencies, state and local governments, and their solution providers. Azure Government offers physical isolation from non-US government deployments and provides screened US personnel.

Azure Government services handle data that is subject to certain government regulations and requirements:

- Federal Risk and Authorization Management Program (FedRAMP)
- National Institute of Standards and Technology (NIST) 800.171 Defense Industrial Base (DIB)
- International Traffic in Arms Regulations (ITAR)
- Internal Revenue Service (IRS) 1075
- Department of Defense (DoD) L4
- Criminal Justice Information Service (CJIS)

To provide the highest level of security and compliance, Azure Government uses physically isolated datacenters and networks located only in the US. Azure Government customers, such as the US federal, state, and local government or their partners, are subject to validation of eligibility.

Azure Government provides the broadest compliance and Level 5 DoD approval. Azure Government is **available in eight geographies** [32] and offers the most compliance certifications of any cloud provider.

31 https://azure.microsoft.com/global-infrastructure/government?azure-portal=true
32 https://azure.microsoft.com/global-infrastructure/geographies/#geographies?azure-portal=true

What is Azure China 21Vianet?

Azure China 21Vianet[33] is operated by 21Vianet is a physically separated instance of cloud services located in China, independently operated and transacted by Shanghai Blue Cloud Technology Co., Ltd. ("21Vianet"), a wholly owned subsidiary of Beijing 21Vianet Broadband Data Center Co., Ltd.

According to the China Telecommunication Regulation, providers of cloud services (IaaS and PaaS) must have value-added telecom permits. Only locally registered companies with less than 50-percent foreign investment qualify for these permits. To comply with this regulation, the Azure service in China is operated by 21Vianet, based on the technologies licensed from Microsoft.

As the first foreign public cloud service provider offered in China in compliance with government regulations, Azure China 21Vianet provides world-class security as discussed on the **Trust Center**[34], as required by Chinese regulations for all systems and applications built on its architecture.

Azure products and services available in China

The Azure services are based on the same Azure, Office 365, and Power BI technologies that make up the Microsoft global cloud service, with comparable service levels. Azure agreements and contracts in China, where applicable, are signed between customers and 21Vianet.

Azure includes the core components of IaaS, PaaS, and SaaS. These components include network, storage, data management, identity management, and many other services.

Azure China 21Vianet supports most of the same services that global Azure has, such as geosynchronous data replication and autoscaling. Even if you already use global Azure services, to operate in China you may need to rehost or refactor some or all your applications or services.

33 https://docs.microsoft.com/azure/china?azure-portal=true
34 https://www.trustcenter.cn/compliance/default.html?azure-portal=true

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

Module 5 Review Questions

Module 05 Review Questions

Review Question 1

How can the IT department ensure that employees at the company's retail stores can access company applications only from approved tablet devices?

- ☐ SSO
- ☐ Conditional Access
- ☐ Multifactor authentication

Review Question 2

How can the IT department use biometric properties, such as facial recognition, to enable delivery drivers to prove their identities?

- ☐ SSO
- ☐ Conditional Access
- ☐ Multifactor authentication

Review Question 3

How can the IT department reduce the number of times users must authenticate to access multiple applications?

- ☐ SSO
- ☐ Conditional Access
- ☐ Multifactor authentication

Review Question 4

How can companies allow some users to control the virtual machines in each environment but prevent them from modifying networking and other resources in the same resource group or Azure subscription?

- ☐ Create a role assignment through Azure role-based access control (Azure RBAC).
- ☐ Create a policy in Azure Policy that audits resource usage.
- ☐ Split the environment into separate resource groups.

Review Question 5

Which is the best way for companies to ensure that they only deploy cost-effective virtual machine SKU sizes?

- ☐ Create a policy in Azure Policy that specifies the allowed SKU sizes.
- ☐ Periodically inspect the deployment manually to see which SKU sizes are used.
- ☐ Create an Azure RBAC role that defines the allowed virtual machine SKU sizes.

Review Question 6

Which is likely the best way for companies to identify which billing department each Azure resource belongs to?

- ☐ Track resource usage in a spreadsheet.
- ☐ Split the deployment into separate Azure subscriptions, where each subscription belongs to its own billing department.
- ☐ Apply a tag to each resource that includes the associated billing department.

Review Question 7

Where can the company access details about the personal data Microsoft processes and how the company processes it, including for Cortana?

- ☐ Microsoft Privacy Statement
- ☐ The Azure compliance documentation
- ☐ Microsoft compliance offerings

Review Question 8

Where can a legal team access information around how the Microsoft cloud helps them secure sensitive data and comply with applicable laws and regulations?

- ☐ Microsoft Privacy Statement
- ☐ Trust Center
- ☐ Online Services Terms

Review Question 9

Where can the IT department find reference blueprints that it can apply directly to its Azure subscriptions?

- ☐ Online Services Terms
- ☐ Azure compliance documentation
- ☐ Microsoft Privacy Statement

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

Module 5 Summary

Module 05 Summary

Secure access to your applications by using Azure identity services

Tailwind Traders needs to ensure that only its workforce can access its growing set of cloud applications, both from any location and from any device.

In building out its plan, Tailwind Traders learns that:

- Authentication (AuthN) establishes the user's identity.
- Authorization (AuthZ) establishes the level of access that an authenticated user has.
- Single sign-on (SSO) enables a user to sign in one time and use that credential to access multiple resources and applications.
- Azure Active Directory (Azure AD) is a cloud-based identity and access management service. Azure AD enables an organization to control access to apps and resources based on its business requirements.
- Azure Multi-Factor Authentication provides additional security for identities by requiring two or more elements to fully authenticate. In general, multifactor authentication can include something the user knows, something the user has, and something the user is.
- Conditional Access is a tool that Azure AD uses to allow or deny access to resources based on identity signals such as the user's location.

With these ideas in place, the software development and IT administrator teams can begin to replace their existing authentication systems with ones that use multiple factors and allow access to multiple applications.

Build a cloud governance strategy on Azure

You've been tasked with defining and implementing the governance strategy for Tailwind Traders.

Cloud governance requires good analysis and requirement gathering. Luckily, the Cloud Adoption Framework for Azure can help you define and implement your governance strategy. There are several services and features in Azure to support these efforts:

- Azure role-based access control (Azure RBAC) enables you to create roles that define access permissions.
- Resource locks prevent resources from being accidentally deleted or changed.
- Resource tags provide extra information, or metadata, about your resources.
- Azure Policy is a service in Azure that enables you to create, assign, and manage policies that control or audit your resources.
- Azure Blueprints enables you to define a repeatable set of governance tools and standard Azure resources that your organization requires.

With these points in mind, you're ready to take the next step toward building a good cloud governance strategy.

Examine privacy, compliance, and data protection standards on Azure

In this lesson, you learned about Microsoft's approach to privacy, security, and compliance. You explored resources specific to online services, including Azure, and how governments can use Azure to meet their specific security and compliance needs.

The security team at Tailwind Traders now has a better understanding of what resources are available to help it protect its data in the cloud and stay compliant:

- The **Microsoft Privacy Statement** [35] provides trust in how Microsoft collects, protects, and uses customer data.
- The **Trust Center** [36] provides you with documentation about compliance standards and how Azure can support your business.
- The **Azure compliance documentation** [37] includes detailed information about legal and regulatory standards and compliance on Azure.

Keep in mind that compliance status for Azure products and services doesn't automatically translate to compliance for the service or application you build or host on Azure. You're responsible for ensuring that you achieve compliance with the legal and regulatory standards that you must follow.

Most services are the same on both Azure Government and global Azure. But there are some differences that you should be aware of. To learn more, **compare Azure Government and global Azure** [38].

35 https://privacy.microsoft.com/privacystatement
36 https://www.microsoft.com/trustcenter
37 https://docs.microsoft.com/en-us/azure/compliance/
38 https://docs.microsoft.com/en-us/azure/azure-government/compare-azure-government-global-azure

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

Answers

Review Question 1

How can the IT department ensure that employees at the company's retail stores can access company applications only from approved tablet devices?

- ☐ SSO
- ■ Conditional Access
- ☐ Multifactor authentication

Explanation
Conditional Access enables you to require users to access your applications only from approved, or managed, devices.

Review Question 2

How can the IT department use biometric properties, such as facial recognition, to enable delivery drivers to prove their identities?

- ☐ SSO
- ☐ Conditional Access
- ■ Multifactor authentication

Explanation
Authenticating through multifactor authentication can include something the user knows, something the user has, and something the user is.

Review Question 3

How can the IT department reduce the number of times users must authenticate to access multiple applications?

- ■ SSO
- ☐ Conditional Access
- ☐ Multifactor authentication

Explanation
SSO enables a user to remember only one ID and one password to access multiple applications.

Review Question 4

How can companies allow some users to control the virtual machines in each environment but prevent them from modifying networking and other resources in the same resource group or Azure subscription?

- ■ Create a role assignment through Azure role-based access control (Azure RBAC).
- ☐ Create a policy in Azure Policy that audits resource usage.
- ☐ Split the environment into separate resource groups.

Explanation
Azure RBAC enables you to create roles that define access permissions. You might create one role that limits access only to virtual machines and a second role that provides administrators with access to everything.

Review Question 5

Which is the best way for companies to ensure that they only deploy cost-effective virtual machine SKU sizes?

- ■ Create a policy in Azure Policy that specifies the allowed SKU sizes.
- ☐ Periodically inspect the deployment manually to see which SKU sizes are used.
- ☐ Create an Azure RBAC role that defines the allowed virtual machine SKU sizes.

Explanation
After you enable this policy, that policy is applied when you create new virtual machines or resize existing ones. Azure Policy also evaluates any current virtual machines in your environment.

Review Question 6

Which is likely the best way for companies to identify which billing department each Azure resource belongs to?

- ☐ Track resource usage in a spreadsheet.
- ☐ Split the deployment into separate Azure subscriptions, where each subscription belongs to its own billing department.
- ■ Apply a tag to each resource that includes the associated billing department.

Explanation
Tags provide extra information, or metadata, about your resources. They might create a tag that's named BillingDept whose value would be the name of the billing department. You can use Azure Policy to ensure that the proper tags are assigned when resources are provisioned.

Review Question 7

Where can the company access details about the personal data Microsoft processes and how the company processes it, including for Cortana?

- ■ Microsoft Privacy Statement
- ☐ The Azure compliance documentation
- ☐ Microsoft compliance offerings

Explanation
The Microsoft Privacy Statement provides information that's relevant to specific services, including Cortana.

Review Question 8

Where can a legal team access information around how the Microsoft cloud helps them secure sensitive data and comply with applicable laws and regulations?

- ☐ Microsoft Privacy Statement
- ■ Trust Center
- ☐ Online Services Terms

Explanation
The Trust Center is a great resource for people in your organization who might play a role in security, privacy, and compliance.

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

Review Question 9

Where can the IT department find reference blueprints that it can apply directly to its Azure subscriptions?

- ☐ Online Services Terms
- ■ Azure compliance documentation
- ☐ Microsoft Privacy Statement

Explanation
The compliance documentation provides reference blueprints, or policy definitions, for common standards that you can apply to your Azure subscription.

Module 6 Describe Azure cost management and service level agreements

Learning Objectives

Learning Objectives

After completing this module, you'll be able to:

- Use the Total Cost of Ownership Calculator to compare your current datacenter costs to running the same workloads on Azure.
- Describe the different ways you can purchase Azure products and services.
- Use the Pricing calculator to estimate the monthly cost of running your cloud workloads.
- Define some of the major factors that affect total cost and apply recommended practices to minimize cost.
- Describe what a service-level agreement (SLA) is and why SLAs are important.
- Identify factors, such as the service tier you choose, that can affect an SLA.
- Combine SLAs to compute a composite SLA.
- Describe the service lifecycle in Azure, including how to access new capabilities that are coming to Azure.

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

Plan and manage your Azure costs

Introduction

In this module, you'll learn about the major factors that influence the cost of running in the cloud. Along the way, you'll get hands-on experience with some of the tools you can use to estimate the costs of running your workloads on Azure to help ensure that you stay within budget and use only the services that you need.

Meet Tailwind Traders

Tailwind Traders [1] is a fictitious home improvement retailer. It operates retail hardware stores across the globe and online.

Tailwind Traders specializes in competitive pricing, fast shipping, and a large range of items. It's looking at cloud technologies to improve business operations and support growth into new markets. By moving to the cloud, the company plans to enhance its shopping experience to further differentiate itself from competitors.

How will Tailwind Traders manage cloud costs?

Tailwind Traders is planning its migration to the cloud. The company has run a few successful proof-of-concept projects and wants to better understand how to manage its costs before it moves its workloads to Azure.

Running in the datacenter requires you to maintain a facility and purchase, power, cool, and maintain your servers. Running in the cloud presents new ways to think about your IT expenses.

To answer the question of how much it will cost, you need to understand the factors that influence cost. You also need to understand what tools are available to you to help estimate and manage your cloud spend.

Learning objectives

After completing this module, you'll be able to:

- Use the Total Cost of Ownership (TCO) Calculator to compare your current datacenter costs to running the same workloads on Azure.
- Describe the different ways you can purchase Azure products and services.
- Use the Pricing calculator to estimate the monthly cost of running your cloud workloads.
- Define some of the major factors that affect total cost and apply recommended practices to minimize cost.

Prerequisites

- You should be familiar with basic computing concepts and terminology
- Familiarity with cloud computing is helpful, but isn't necessary

1 https://www.tailwindtraders.com/

Compare costs by using the Total Cost of Ownership Calculator

Before Tailwind Traders takes their next steps towards migrating to the cloud, they want to better understand what they spend today in their datacenter.

Having a firm understanding of where they are today will give them a greater sense of what cloud migration means in terms of cost.

In this part, you'll see how the Total Cost of Ownership (TCO) Calculator can help you compare the cost of running in the datacenter versus running on Azure.

What's the TCO Calculator?

The **TCO Calculator**[2] helps you estimate the cost savings of operating your solution on Azure over time, instead of in your on-premises datacenter.

While the term *total cost of ownership* is commonly used in finance, it can be hard to truly see all of the hidden costs related to operating a technology capability on-premises, in addition to the cost of software licenses and hardware.

With the TCO Calculator, you enter the details of your on-premises workloads and then review the suggested industry average cost (which you can adjust) for related operational costs, such as electricity, network maintenance, and IT labor. You're then presented with a side-by-side report, enabling you to compare those costs with the same workloads running on Azure.

The following image shows just one example:

Note: You don't need an Azure subscription to work with the TCO Calculator.

How does the TCO Calculator work?

The TCO Calculator breaks down into these three steps:

2 https://azure.microsoft.com/pricing/tco/calculator?azure-portal=true

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

Let's take a closer look at each step.

Step 1: Define your workloads

First, you enter the specifications of your on-premises infrastructure into the TCO calculator, according to these four categories:

- **Servers** This category includes operating systems, virtualization methods, CPU cores, and memory (RAM).
- **Databases** This category includes database types, server hardware, and the Azure service you would like to use, including the expected maximum concurrent user logins.
- **Storage** This category includes storage type and capacity, including any backup or archive storage.
- **Networking** This category includes the amount of network bandwidth you currently consume in your on-premises environment.

Step 2: Adjust assumptions

Next, you specify whether your current on-premises licenses are enrolled for **Software Assurance**[3], which can save you money by reusing those licenses on Azure. You also specify whether you need to replicate your storage to another Azure region for greater redundancy.

Then, you can see the key operating cost assumptions across several different areas, which vary among teams and organizations. These costs have been certified by Nucleus Research, an independent research company. For example, these include:

- Electricity price per kilowatt hour (KWh).
- Hourly pay rate for IT administration.
- Network maintenance cost as a percentage of network hardware and software costs.

To improve the accuracy of the TCO Calculator results, you adjust the values so that they match the costs of your current on-premises infrastructure.

Step 3: View report

Choose a time frame between one and five years; the TCO Calculator generates a report that's based on the information you've entered. Here's an example:

3 https://www.microsoft.com/licensing/licensing-programs/software-assurance-default?azure-portal=true

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

For each category (compute, datacenter, networking, storage, and IT labor), you can also view a side-by-side comparison of the cost breakdown of operating those workloads on-premises versus operating them on Azure. Here's an example:

Estimated on-premises cost (2 year(s))	Estimated Azure cost (2 year(s))
Compute cost	Azure compute cost
Data center cost	Azure data center cost
Networking cost	Azure networking cost
Storage cost	Azure storage cost

Hardware		Page Blob storage	
Local Disk/SAN-HDD		Usable storage volume in GB	1,024
Cost per GB	$1.69	Storage cost per GB/month	$0.045
Storage (RAID 10 configuration) volume in GB	3,072	Annual storage cost per usable volume	$552.96
Total storage procurement cost	$5,191.68	Total Page Blob LRS storage maintenance cost over two year(s)	$1,105.92

You can download, share, or save this report to review later in more detail.

In the next part, you'll use the TCO Calculator to help the Tailwind Traders team understand their total costs.

Exercise - Compare sample workload costs by using the TCO Calculator

In this exercise, you use the Total Cost of Ownership (TCO) Calculator to compare the cost of running a sample workload in the datacenter versus on Azure.

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

Tailwind Traders is interested in moving some of their on-premises workloads to the cloud. But first, their Chief Financial Officer wants to understand more about moving from a relatively fixed cost structure to an ongoing monthly cost structure.

You've been tasked to investigate whether there are any potential cost savings in moving your European datacenter to the cloud over the next three years. You need to take into account all of the potentially hidden costs involved with operating on-premises and in the cloud.

Instead of manually collecting everything you think might be included, you use the TCO Calculator as a starting point. You adjust the provided cost assumptions to match Tailwind Traders' on-premises environment.

Note: Remember, you don't need an Azure subscription to work with the TCO Calculator.

Let's say that:

- Tailwind Traders run two sets, or banks, of 50 virtual machines (VMs) in each bank.
- The first bank of VMs runs Windows Server under Hyper-V virtualization.
- The second bank of VMs runs Linux under VMware virtualization.
- There is also a storage area network (SAN) with 60 terabytes (TB) of disk storage.
- You consume an estimated 15 TB of outbound network bandwidth each month.
- There are also a number of databases involved, but for now, you'll omit those details.

Recall that the TCO Calculator breaks down into these three steps:

A visual representation of the three steps; define your workloads, adjust assumptions, view report.

Let's see how Tailwind Traders' existing workloads stack up in the datacenter versus on Azure.

Define your workloads

Enter the specifications of your on-premises infrastructure into the TCO calculator.

1. Go to the **Total Cost of Ownership (TCO) Calculator**[4].
2. Under **Define your workloads**, select **Add server workload** to create a row for your bank of Windows Server virtual machines.
3. Under **Servers**, set the value for each of these settings:

Setting	Value
Name	*Servers: Windows VMs*
Workload	**Windows/Linux Server**
Environment	**Virtual Machines**
Operating system	**Windows**
VMs	**50**

4 https://azure.microsoft.com/pricing/tco/calculator?azure-portal=true

Setting	Value
Virtualization	**Hyper-V**
Core(s)	**8**
RAM (GB)	**16**
Optimize by	**CPU**
Windows Server 2008/2008 R2	**Off**

4. Select **Add server workload** to create a second row for your bank of Linux virtual machines. Then specify these settings:

Setting	Value
Name	*Servers: Linux VMs*
Workload	**Windows/Linux Server**
Environment	**Virtual Machines**
Operating system	**Linux**
VMs	**50**
Virtualization	**VMware**
Core(s)	**8**
RAM (GB)	**16**
Optimize by	**CPU**

5. Under **Storage**, select **Add storage**. Then specify these settings:

Setting	Value
Name	*Server Storage*
Storage type	**Local Disk/SAN**
Disk type	**HDD**
Capacity	**60 TB**
Backup	**120 TB**
Archive	**0 TB**

6. Under **Networking**, set **Outbound bandwidth** to **15 TB**.
7. Select **Next**.

Adjust assumptions

Here, you specify your currency. For brevity, you leave the remaining fields at their default values.

In practice, you would adjust any cost assumptions and make any adjustments to match your current on-premises environment.

1. At the top of the page, select your currency. This example uses **US Dollar ($)**.
2. Select **Next**.

View report

Take a moment to review generated report.

Remember, you've been tasked to investigate cost savings for your European datacenter over the next three years.

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

To make these adjustments:

1. Set **Timeframe** to **3 Years**.
2. Set **Region** to **North Europe**.

Scroll to the summary at the bottom. You see a comparison of running your workloads in the datacenter versus on Azure. The prices you see might differ, but here's an example of the cost savings you might expect:

Select **Download** to download or print a copy of the report in PDF format.

Great work. You now have the information that you can share with your Chief Financial Officer. If you need to make adjustments, you can revisit the TCO Calculator to generate a fresh report.

Purchase Azure services

In this part, you learn how to purchase Azure services as well as get a sense for other factors that affect cost.

You meet with your Chief Financial Officer and some of the team leads. You learn about some assumptions you've missed and were able to quickly update your total estimated spend through the Total Cost of Ownership (TCO) Calculator.

During the meeting, some new questions come up as the discussion moves towards cloud migration:

[!div class="checklist"]

- What types of Azure subscriptions are available?
- How do we purchase Azure services?
- Does location or network traffic affect cost?
- What other factors affect the final cost?
- How can we get a more detailed estimate of the cost to run on Azure?

It's important to learn how costs are generated in Azure so that you can understand how your purchasing and solution design decisions can impact your final cost. You agree to research these questions, so let's review each one in greater detail.

What types of Azure subscriptions can I use?

You probably know that an Azure *subscription* provides you with access to Azure resources, such as virtual machines, storage, and databases. The types of resources you use impact your monthly bill.

Azure offers both free and paid subscription options to fit your needs and requirements. They are:

- **Free Trial** A Free Trial subscription provides you with 12 months of popular free services, a credit to explore any Azure service for 30 days, and 25+ services that are always free. Your Azure services are disabled when the trial ends or when your credit expires for paid products, unless you upgrade to a paid subscription.

- **Pay-As-You-Go** A Pay-As-You-Go subscription enables you to pay for what you use by attaching a credit or debit card to your account. Organizations can apply for volume discounts and pre-paid invoicing.
- **Member offers** Your existing membership to certain Microsoft products and services might provide you with credits for your Azure account and reduced rates on Azure services. For example, member offers are available to Microsoft Visual Studio subscribers, Microsoft Partner Network members, Microsoft for Startups members, and Microsoft Imagine members.

How do I purchase Azure services?

There are three main ways to purchase services on Azure. They are:

- **Through an Enterprise Agreement** Larger customers (known as Enterprise customers) can sign an Enterprise Agreement with Microsoft that commits them to spending a predetermined amount on Azure services over a period of 3 years, which is typically paid annually. As an Enterprise Agreement customer, you will receive the best, customized pricing based on the kinds and amounts of services you plan on using.
- **Directly from the web** Here, you purchase Azure services directly from the Azure portal website and pay standard prices. You're billed monthly, as a credit card payment or through an invoice. This purchasing method is known as Web Direct.
- **Through a Cloud Solution Provider (CSP)** A CSP is a Microsoft Partner who helps you build solutions on top of Azure. Your CSP bills you for your Azure usage at a price they determine. They also answer your support questions, escalating them to Microsoft as needed.

You can bring up, or *provision*, Azure resources from the Azure portal or from the command line. The Azure portal arranges products and services by category. You select the services that fit your needs, and your account is billed according to Azure's “pay for what you use” model.

Here's an example that shows the Azure portal:

At the end of each month, you're billed for what you've used. At any time, you can check the cost management and billing page in the Azure portal to get a summary of your current usage and review invoices from prior months.

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

What factors affect cost?

The way you use resources, your subscription type, and pricing from third-party vendors are common factors. Let's take a quick look at each.

Resource type

Azure resources have a number of factors which influence their cost, depending on the type of resource or how you customize it.

For example, with a storage account you would specify a type (such as block blob storage or table storage), a performance tier (standard or premium), and an access tier (hot, cool or archive). These selections present different costs.

Usage meters

When you provision a resource, Azure creates *meters* to track usage of that resource. Azure uses these meters to generate a usage record that's later used to help calculate your bill.

Think of usage meters similar to how you use electricity or water in your home. You might pay a base price each month for electricity or water service, but your final bill is based on the total amount that you have consumed.

Let's look at a single virtual machine as an example. The following kinds of meters are relevant to tracking its usage:

- Overall CPU time.
- Time spent with a public IP address.
- Incoming (ingress) and outgoing (egress) network traffic in and out of the VM.
- Disk size and amount of disk read and disk write operations.

Each meter tracks a specific type of usage. For example, a meter might track bandwidth usage (ingress or egress network traffic in bits-per-second), number of operations, or its size (storage capacity in bytes).

The usage that a meter tracks correlates to a quantity of billable units. Those are charged to your account for each billing period, and the rate per billable unit depends on the resource type you are using.

Resource usage

In Azure, you're always charged based on what you use. As an example, let's look at how this applies to deallocating a virtual machine (VM).

In Azure, you can delete or deallocate a VM. Deleting a VM means that you no longer need it; the VM is removed from your subscription and then it's prepared for another customer.

Deallocating a VM means that the VM is no longer running, but the associated hard disks and data are still kept in Azure. The VM is not assigned to a CPU or network in Azure's datacenter, so it doesn't generate the costs associated with compute time or the VM's IP address. However, because the disks and data are still stored, and the resource is present in your Azure subscription, you are still billed for disk storage.

Deallocating a VM when you don't plan on using it for some time is just one way to minimize costs. For example, you might deallocate the VMs you use for testing purposes on weekends when your testing team is not using them. You'll learn more about ways to minimize cost later in this module.

Azure subscription types

Some Azure subscription types also include usage allowances, which affect costs.

For example, an Azure Free Trial subscription provides access to a number of Azure products that are free for 12 months, as well as credit to spend within your first 30 days of sign-up, and access to more than 25 products that are always free (based on resource and region availability).

Azure Marketplace

You can also purchase Azure-based solutions and services from third-party vendors through the Azure Marketplace. Examples include managed network firewall appliances or connectors to third-party backup services. Billing structures are set by the vendor.

Does location or network traffic affect cost?

When you provision a resource in Azure, you need to define the location (known as the Azure region) of where it will be deployed. Let's see why this decision can have cost consequences.

Location

Azure infrastructure is distributed globally, which enables you to deploy your services centrally or provision your services closest to where your customers use them.

Different regions can have different associated prices. Because geographic regions can impact where your network traffic flows, network traffic is a cost influence to consider as well.

For example, say Tailwind Traders decides to provision their Azure resources in the Azure regions that offer the lowest prices. That would save them some money! However, if they need to transfer data between those regions, or if their users are located in different parts of the world, any potential savings could be offset by the additional network usage costs of transferring data between those resources.

Zones for billing of network traffic

Billing zones are a factor in determining the cost of some Azure services.

Bandwidth[5] refers to data moving in and out of Azure datacenters. Some inbound data transfers (data going into Azure datacenters), are free. For outbound data transfers (data leaving Azure datacenters), data transfer pricing is based on *Zones*.

A Zone is a geographical grouping of Azure regions for billing purposes. The following Zones include some of the regions as shown here:

- **Zone 1** – Australia Central, West US, East US, Canada West, West Europe, France Central and others.
- **Zone 2** – Australia East, Japan West, Central India, Korea South and others.

5 https://azure.microsoft.com/pricing/details/bandwidth?azure-portal=true

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

- **Zone 3** - Brazil South, South Africa North, South Africa West, UAE Central, UAE North.
- **DE Zone 1** - Germany Central, Germany Northeast.

How can I estimate the total cost?

As you've learned, an accurate cost estimate would take all of the above factors into account. Fortunately, the Azure Pricing calculator helps you do just that.

The Pricing calculator displays Azure products in categories, which you add to your estimate and then configure according to your specific requirements. You then receive a consolidated estimated price, with a detailed breakdown of the costs associated with each resource you've added to your solution. Then, you can export or share that estimate, or save it for later. You can load a saved estimate and modify it to match updated requirements.

You also can access pricing details, product details, and documentation for each product from within the Pricing calculator.

The options that you can configure in the Pricing calculator vary between products, but can include:

- **Region** A region is the geographical location in which you can provision a service. Southeast Asia, Central Canada, Western United States, and Northern Europe are a few examples.
- **Tier** Tiers such as the Free Tier, Basic Tier, and so on, have different levels of availability or performance, and therefore different associated costs.
- **Billing Options** Billing options highlight the different ways you can pay for a service. Options can vary based on your customer type and subscription type and can include options to save costs.
- **Support Options** These options enable you to select additional support pricing options for certain services.
- **Programs and Offers** Your customer or subscription type might enable you to choose from specific licensing programs or other offers.
- **Azure Dev/Test Pricing** This option lists the available prices for development and test workloads. Dev/Test pricing applies when you run resources within an Azure subscription that is based on a Dev/Test offer.

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

Keep in mind that the Pricing calculator provides estimates, and *not* actual price quotes. Actual prices can vary depending upon the date of purchase, the payment currency you are using, and the type of Azure customer you are.

Exercise - Estimate workload cost by using the Pricing calculator

In this exercise, you use the Pricing calculator to estimate the cost of running a basic web application on Azure.

With an understanding of the more important cost factors associated with running on Azure, Tailwind Traders wants to take a typical workload and estimate how much it would cost each month to run it on Azure.

The IT Manager at Tailwind Traders is faced with the decision about whether to replace some aging on-premises hardware or move the application to Azure. They need to know how much the ongoing monthly cost of the solution in Azure would be.

Let's start by defining which Azure services you need.

Note: The Pricing calculator is for information purposes only. The prices are only an estimate, and you won't be charged for any services you select.

Define your requirements

Before you run the Pricing calculator, you first need a sense of what Azure services you need.

You meet with the application development team to discuss their migration project.

In their datacenter, the team has an ASP.NET web application that runs on Windows. The web application provides information about product inventory and pricing. They have two virtual machines that are connected through a central load balancer. The web application connects to a SQL Server database that holds inventory and pricing information.

The team decides to:

- Use virtual machines on Azure, similar to what they use in the datacenter.
- Use Azure Application Gateway for load balancing.
- Use Azure SQL Database to hold inventory and pricing information.

Here's a diagram that shows the basic configuration:

In practice, you would define your requirements in greater detail. But here are some basic facts and requirements that came up during the meeting:

- The application is used by Tailwind Traders employees at their retail stores. It's not accessible to customers.

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

- This application doesn't require a massive amount of computing power.
- The virtual machines and the database run all the time (730 hours/month).
- The network processes about 1 TB of data per month.
- The database doesn't need to be configured for high-performance workloads and requires no more than 32 GB of storage.

Explore the Pricing calculator

Let's start with a quick tour of the Pricing calculator.

1. Go to the **Pricing calculator**[6].
2. Note the tabs at the top:

Here's what you'll find under each tab:

- **Products** This is where you choose the Azure services that you want to include in your estimate. You'll likely spend most of your time here.
- **Example Scenarios** Here you'll find several *reference architectures*, or common cloud-based solutions that you can use as a starting point.
- **Saved Estimates** Here you'll find your previously saved estimates.
- **FAQ** Here you'll discover answers to frequently asked questions about the Pricing calculator.

Estimate your solution

Here you add each Azure service that you need to the calculator and then configure each service to fit your needs.

Tip: Make sure you have a clean calculator with nothing listed in the estimate. You can reset the estimate by selecting the trash can icon next to each item.

Add services to the estimate

1. On the **Products** tab, select the service from each of these categories:

Category	Service
Compute	**Virtual Machines**
Databases	**Azure SQL Database**
Networking	**Application Gateway**

2. Scroll to the bottom of the page. You see that each service is listed with its default configuration.

6 https://azure.microsoft.com/pricing/calculator/?azure-portal=true

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

Configure services to match your requirements

1. Under **Virtual Machines**, set these values:

Setting	Value
Region	**West US**
Operating system	**Windows**
Type	**(OS Only)**
Tier	**Standard**
Instance	**D2 v3**
Virtual Machines	**2** x **730 Hours**

   Leave the remaining settings at their current values.

2. Under **Azure SQL Database**, set these values:

Setting	Value
Region	**West US**
Type	**Single Database**
Backup Storage Tier	**RA-GRS**
Purchase Model	**vCore**
Service Tier	**General Purpose**
Compute Tier	**Provisioned**
Generation	**Gen 5**
Instance	**8 vCore**

   Leave the remaining settings at their current values.

3. Under **Application Gateway**, set these values:

Setting	Value
Region	**West US**
Tier	**Web Application Firewall**
Size	**Medium**
Gateway hours	**2** x **730 Hours**
Data processed	**1 TB**
Outbound Data Transfer	**5 GB**

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

Leave the remaining settings at their current values.

Review, share, and save your estimate

At the bottom of the page, you see the total estimated cost of running the solution. You can change the currency type if you'd like.

At this point, you have a few options:

- Select **Export** to save your estimate as a Microsoft Excel document.
- Select **Save** or **Save as** to save your estimate to the **Saved Estimates** tab for later.
- Select **Share** to generate a URL so you can share the estimate with your team.

You now have a cost estimate that you can share with your team. You can make adjustments as you discover any changes to your requirements.

Try experimenting with some of the options you worked with here, or create a purchase plan for a workload you want to run on Azure.

Manage and minimize total cost on Azure

As a home improvement retailer, the proverb “measure twice, cut once” is fitting for the team at Tailwind Traders.

Here are some recommended practices that can help you minimize your costs.

Understand estimated costs before you deploy

To help you plan your solution on Azure, carefully consider the products, services, and resources you need, and read the relevant documentation to understand how each of your choices are metered and billed.

Calculate your projected costs by using the Pricing calculator and the Total Cost of Ownership (TCO) calculator. Only add the products, services, and resources that you need for your solution.

Use Azure Advisor to monitor your usage

Ideally, you want your provisioned resources to match your actual usage.

Azure Advisor identifies unused or under-utilized resources and recommends unused resources that you can remove. This helps you configure your resources to match your actual workload.

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

The following image shows some example recommendations from Azure Advisor:

Recommendations are sorted by impact: high, medium, or low. In some cases, Azure Advisor can automatically remediate, or fix, the underlying problem. Other issues, such as the two that are listed as high impact, require human intervention.

Use spending limits to restrict your spending

If you have a Free Trial or a credit-based Azure subscription, you can use spending limits to prevent accidental overrun.

For example, when you spend all the credit included with your Azure free account, Azure resources that you deployed are removed from production and your Azure virtual machines are stopped and deallocated. The data in your storage accounts are available as read-only. At this point, you can upgrade your Free Trial subscription to a Pay-As-You-Go subscription.

If you have a credit-based subscription and you reach your configured spending limit, Azure suspends your subscription until a new billing period begins.

A related concept is *quotas*, or limits on the number of similar resources you can provision within your subscription. For example, you can allocate up to 25,000 virtual machines per region. These limits mainly help Microsoft plan their datacenter capacity.

Use Azure Reservations to pre-pay in advance

Azure Reservations offers discounted prices on certain Azure services. Azure Reservations can save you up to 72% as compared to pay-as-you-go prices. To receive a discount, you reserve services and resources by paying in advance.

For example, you can pre-pay for one year or three years of use of virtual machines, database compute capacity, database throughput, and other Azure resources.

The following example shows estimated savings on virtual machines. In this example, you save an estimated 72% by committing to a three-year term.

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

Azure Reservations are available to customers with an Enterprise Agreement, Cloud Solution Providers, and Pay-As-You-Go subscriptions.

Choose low-cost locations and regions

The cost of Azure products, services, and resources can vary across locations and regions. If possible, you should use them in those locations and regions where they cost less.

But remember, some resources are metered and billed according to how much outgoing (egress) network bandwidth they consume. You should provision connected resources that are metered by bandwidth in the same Azure region to reduce egress traffic between them.

Research available cost-saving offers

Keep up-to-date with the latest Azure customer and subscription offers, and switch to offers that provide the greatest cost-saving benefit.

Use Azure Cost Management + Billing to control spending

Azure Cost Management + Billing is a free service that helps you understand your Azure bill, manage your account and subscriptions, monitor and control Azure spending, and optimize resource use.

The following image shows current usage broken down by service:

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

In this example, Azure App Service, a web application hosting service, generates the greatest cost.

Azure Cost Management + Billing features include:

- Reporting

  Use historical data to generate reports and forecast future usage and expenditure.

- Data enrichment

  Improve accountability by categorizing resources with tags that correspond to real-world business and organizational units.

- Budgets

  Create and manage cost and usage budgets by monitoring resource demand trends, consumption rates, and cost patterns.

- Alerting

  Get alerts based on your cost and usage budgets.

- Recommendations

  Receive recommendations to eliminate idle resources and to optimize the Azure resources you provision.

Apply tags to identify cost owners

Tags help you manage costs associated with the different groups of Azure products and resources. You can apply tags to groups of Azure resources to organize billing data.

For example, if you run several virtual machines for different teams, you can use tags to categorize costs by department, such as Human Resources, Marketing, or Finance, or by environment, such as Test or Production.

Tags make it easier to identify groups that generate the biggest Azure costs, which can help you adjust your spending accordingly.

The following image shows a year's worth of usage broken down by tags on the Azure Cost Management + Billing page:

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

Resize underutilized virtual machines

A common recommendation that you'll find from Azure Cost Management + Billing and Azure Advisor is to resize or shut down virtual machines that are underutilized or idle.

As an example, say you have a virtual machine whose size is **Standard_D4_v4**, a general-purpose virtual machine type with four vCPUs and 16 GB of memory. You might discover that this virtual machine is idle 90% of the time.

Virtual machine costs are linear and double for each size larger in the same series. So in this case, if you reduce the VM's size from **Standard_D4_v4** to **Standard_D2_v4**, which is the next size lower, you reduce your compute cost by 50%.

The following image shows this idea:

Keep in mind that resizing a VM requires it to be stopped, resized, and then restarted. This may take a few minutes depending on how significant the size change is. Be sure to properly plan for an outage, or shift your traffic to another instance while you perform resize operations.

Deallocate virtual machines during off hours

Recall that to *deallocate* a VM means to no longer run the VM, but preserve the associated hard disks and data in Azure.

If you have virtual machine workloads that are only used during certain periods, but you're running them every hour of every day, you're wasting money. These VMs are great candidates to shut down when not in use and start back when you need them, saving you compute costs while the VM is deallocated.

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

This approach is an excellent strategy for development and testing environments, where the virtual machines are needed only during business hours. Azure even provides a way to automatically start and stop your VMs on a schedule.

Delete unused resources

This might sound obvious, but if you aren't using a resource, you should shut it down. It's not uncommon to find non-production or proof-of-concept systems that are no longer needed following the completion of a project.

Regularly review your environment and work to identify these systems. Shutting down these systems can have a dual benefit by saving you not only on infrastructure costs but also potential savings on licensing and operating costs.

Migrate from IaaS to PaaS services

As you move your workloads to the cloud, a natural evolution is to start with infrastructure as a service (IaaS) services because they map more directly to concepts and operations you're already familiar with.

Over time, one way to reduce costs is to gradually move IaaS workloads to run on platform as a service (PaaS) services. While you can think of IaaS as direct access to compute infrastructure, PaaS provides ready-made development and deployment environments that are managed for you.

As an example, say you run SQL Server on a virtual machine running on Azure. This requires you to manage the underlying operating system, set up a SQL Server license, manage software and security updates, and so on. You also pay for the VM whether or not the database is processing queries. One way to potentially save costs is to move your database from SQL Server on a virtual machine to Azure SQL Database. Azure SQL Database is based on SQL Server.

Not only are PaaS services such as Azure SQL Database often less expensive to run, but because they're managed for you, you don't need to worry about software updates, security patches, or optimizing physical storage for read and write operations.

Save on licensing costs

Licensing is another area that can dramatically impact your cloud spending. Let's look at some ways you can reduce your licensing costs.

Choose cost-effective operating systems

Many Azure services provide a choice of running on Windows or Linux. In some cases, the cost depends on which you choose. When you have a choice, and your application doesn't depend on the underlying operating system, it's useful to compare pricing to see whether you can save money.

Use Azure Hybrid Benefit to re-purpose software licenses on Azure

If you've purchased licenses for Windows Server or SQL Server, and your licenses are covered by **Software Assurance**[7], you may be able to re-purpose those licenses on virtual machines on Azure.

7 https://www.microsoft.com/licensing/licensing-programs/software-assurance-default?azure-portal=true

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

Some of the details vary between Windows Server or SQL Server, and we'll provide resources at the end of this module where you can learn more.

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

Choose the right Azure services by examining SLAs and service lifecycle

Introduction

In this module, you'll learn about Azure's service-level agreements (SLAs) and how they can impact your application design decisions. You'll also learn about the lifecycle of new Azure services — from the preview phase to becoming generally available.

Meet Tailwind Traders

Tailwind Traders [8] is a fictitious home improvement retailer. It operates retail hardware stores across the globe and online.

Tailwind Traders specializes in competitive pricing, fast shipping, and a large range of items. It's looking at cloud technologies to improve business operations and support growth into new markets. By moving to the cloud, the company plans to enhance its shopping experience to further differentiate itself from competitors.

How will moving to the cloud affect availability agreements?

Moving to the cloud removes the burden of supporting IT infrastructure. When network connectivity is lost or a hard drive fails, you rely on the cloud provider to restore service.

Tailwind Traders' IT department hosts applications and services in its datacenter for the rest of the company. The IT department has agreements with other teams in place that state how available those services will be, which includes when and how planned maintenance can happen. As Tailwind Traders moves its workloads to Azure, it no longer has full control over the hardware and networks. How will its agreements around availability be affected?

Learning objectives

After completing this module, you'll be able to:

- Describe what a service-level agreement (SLA) is and why SLAs are important.
- Identify factors, such as the service tier you choose, that can impact an SLA.
- Combine SLAs to compute a composite SLA.
- Describe the service lifecycle in Azure, including how to access new capabilities that are coming to Azure.

Prerequisites

- You should be familiar with basic computing concepts and terminology
- Familiarity with cloud computing is helpful, but isn't necessary

8 https://www.tailwindtraders.com/

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

What are service-level agreements (SLAs)?

A *service-level agreement* (SLA) is a formal agreement between a service company and the customer. On Azure, this agreement defines the performance standards that Microsoft commits to for you, the customer.

In this part, you'll learn more about Azure SLAs, including why SLAs are important, where you can find the SLA for a specific Azure service, and what you'll find in a typical SLA.

Why are SLAs important?

Understanding the SLA for each Azure service you use helps you understand what guarantees you can expect.

When you build applications on Azure, the availability of the services that you use impact your application's uptime and performance. Understanding the SLAs involved can help you establish the SLA you set with your customers.

Later in this module, you'll learn about some strategies you can use when an Azure SLA doesn't meet your needs.

Where can I access SLAs for Azure services?

You can access SLAs from the **Service Level Agreements**[9] page on azure.microsoft.com.

Note: You don't need an Azure subscription to review service SLAs.

Each Azure service defines its own SLA. Azure services are organized by category.

Open the SLA for Azure Database for MySQL, a managed database that makes it easy for developers to work with MySQL databases. You'll refer back to this SLA in a moment.

To do so:

1. Go to **Service Level Agreements**[10].
2. From the **Databases** category, select **Azure Database for MySQL**.

What's in a typical SLA?

A typical SLA breaks down into these sections:

- **Introduction** This section explains what to expect in this SLA, including its scope and how subscription renewals can impact the terms.

9 https://azure.microsoft.com/support/legal/sla/?azure-portal=true
10 https://azure.microsoft.com/support/legal/sla/?azure-portal=true

- **General Terms** This section contains terms that are used throughout the SLA so that both parties (you and Microsoft) have a consistent vocabulary. For example, this section might define what's meant by downtime, incidents, error codes, and so on. This section also defines the general terms of the agreement, including how to submit a claim, receive credit for any performance or availability issues, and limitations of the agreement.
- **SLA details** This section defines the specific guarantees for the service. Performance commitments are commonly measured as a percentage. That percentage typically ranges from 99.9% ("three nines") to 99.99% ("four nines"). The primary performance commitment typically focuses on *uptime*, or the percentage of time that a product or service is successfully operational. Some SLAs focus on other factors as well, including *latency*, or how fast the service must respond to a request. This section also defines any additional terms that are specific to this service.

Take a moment to review the SLA for Azure Database for MySQL.

You see that this SLA focuses mainly on uptime. Azure Database for MySQL guarantees 99.99%, or "four nines", uptime. This means that the service is guaranteed to be running and available to process requests 99.99% of the time.

How do percentages relate to total downtime?

Downtime refers to the time duration that the service is unavailable.

The difference between 99.9% and 99.99% might seem minor, but it's important to understand what these numbers mean in terms of total downtime.

Here's a table to give you a sense of how total downtime decreases as the SLA percentage increases from 99% to 99.999%:

SLA percentage	Downtime per week	Downtime per month	Downtime per year
99	1.68 hours	7.2 hours	3.65 days
99.9	10.1 minutes	43.2 minutes	8.76 hours
99.95	5 minutes	21.6 minutes	4.38 hours
99.99	1.01 minutes	4.32 minutes	52.56 minutes
99.999	6 seconds	25.9 seconds	5.26 minutes

These amounts are cumulative, which means that the duration of multiple different service outages would be combined, or added together.

What are service credits?

A *service credit* is the percentage of the fees you paid that are credited back to you according to Microsoft's claim approval process.

An SLA describes how Microsoft responds when an Azure service fails to perform to its specification. For example, you may receive a discount on your Azure bill as compensation when a service fails to perform according to its SLA.

Credits typically increase as uptime decreases. Here's how credits are applied for Azure Database for MySQL according to uptime:

Monthly Uptime Percentage	Service Credit
< 99.99%	10%
< 99%	25%

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

Monthly Uptime Percentage	Service Credit
< 95%	100%

What's the SLA for free services?

Free products typically do not have an SLA.

For example, many Azure services provide a *Free* or *Shared* tier that provides more limited functionality. Services like Azure Advisor are always free. The **SLA for Azure Advisor**[11] states that because it's free, it does not have a financially backed SLA.

How do I know when there's an outage?

Azure status[12] provides a global view of the health of Azure services and regions. If you suspect there's an outage, this is often a good place to start your investigation.

Azure status provides an RSS feed of changes to the health of Azure services that you can subscribe to. You can connect this feed to communication software such as Microsoft Teams or Slack.

From the Azure status page, you can also access Azure Service Health, which provides a personalized view of the health of the Azure services and regions that you're using, directly from the Azure portal.

How can I request a service credit from Microsoft?

Typically, you need to file a claim with Microsoft to receive a service credit. If you purchase Azure services from a Cloud Solution Provider (CSP) partner, your CSP typically manages the claims process.

Each SLA specifies the timeline by which you must submit your claim and when Microsoft processes your claim. For many services, you must submit your claim by the end of the calendar month following the month in which the incident occurred.

Next, let's look at some other factors that Tailwind Traders needs to consider which might impact SLA performance targets.

Define your application SLA

An *application SLA* defines the SLA requirements for a specific application. This term typically refers to an application that *you* build on Azure.

Tailwind Traders runs an application that they built on Azure called Special Orders. The application tracks special orders that customers have placed in their retail stores. A special order includes an item and any customizations the customer needs. For example, a folding door might include customizations such as dimension and hinge placement. Because customizations typically require special handling, the customized item needs to be ordered from the supplier when a customer needs it.

There are many design decisions you could make to improve the availability and resiliency of the applications and services you build on Azure. These decisions extend beyond just Microsoft's SLA for a specific service. In this part, you'll explore a few of these considerations.

A good place to start is to have a discussion with your team about how important the availability of each application is to your business.

Here are a few factors that Tailwind Traders might consider:

11 https://azure.microsoft.com/support/legal/sla/advisor/?azure-portal=true
12 https://status.azure.com/status?azure-portal=true

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

Business impact

If the Special Orders application goes down, what would the business impact be? In this case, customers can't place new orders through the store and staff can't check the status of existing orders. This can make customers unhappy. They'll either need to try again later or possibly go to a competitor.

Effect on other business operations

The Special Orders application does not affect other operations. So the majority of the Tailwind Traders business would continue to function normally if the Special Orders application went down.

Usage patterns

Usage patterns define when and how users access your application.

One question to consider is whether the availability requirement differs between critical and non-critical time periods. For example, a tax-filing application can't fail during a filing deadline.

For Tailwind Traders, retail stores are not open 24 hours a day, so if the application were down in the middle of the night, the impact would be minimal. However, because Tailwind Traders has retail locations all over the world, they will need to ensure that each location has access to the service during its retail hours.

What does the team decide?

Let's say that Tailwind Traders decides that an SLA of 99.9% is acceptable for the Special Orders application. This gives them an estimated downtime of 10.1 minutes per week. But how will they ensure that their technology choices support their application SLA?

In the next part, you'll see how the team maps their application requirements to specific Azure services. You'll learn about some of the techniques you can use to help ensure that your technology choices meet your application SLA.

Design your application to meet your SLA

Tailwind Traders decides that an SLA of 99.9% is acceptable for the Special Orders application. Recall that this gives them an estimated downtime of 10.1 minutes per week.

Now you need to design an efficient and reliable solution for this application on Azure, keeping that application SLA in mind. You'll select the Azure products and services you need and provision your cloud resources according to those requirements.

In reality, failures will happen. Hardware can fail. The network can have intermittent timeout periods. While it's rare for an entire service or region to experience a disruption, you still need to plan for such events.

Let's follow the process Tailwind Traders uses to ensure that their technology choices meet their application SLA.

Identify your workloads

A *workload* is a distinct capability or task that's logically separated from other tasks, in terms of business logic and data storage requirements. Each workload defines a set of requirements for availability, scalability, data consistency, and disaster recovery.

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

On Azure, the Special Orders application will require:

- Two virtual machines.
- One instance of Azure SQL Database.
- One instance of Azure Load Balancer.

Here's a diagram that shows the basic architecture:

Combine SLAs to compute the composite SLA

After you've identified the SLA for the individual workloads in the Special Orders application, you might notice that those SLAs are not all the same. How does this impact our overall application SLA requirement of 99.9%? To work that out, you'll need to do some math.

The process of combining SLAs helps you compute the *composite SLA* for a set of services. Computing the composite SLA requires you to multiply the SLA of each individual service.

From the **Service Level Agreements**[13] page, you discover the SLA for each Azure service that you need. They are:

Service	SLA
Virtual Machines	99.9%
Azure SQL Database	99.99%
Azure Load Balancer	99.99%

Therefore, for the Special Orders application, the composite SLA would be:

99.9% × 99.9% × 99.99% × 99.99%

=0.999 × 0.999 × 0.9999 × 0.9999

=0.9978

=99.78%

Recall that you need two virtual machines. Therefore, you include the Virtual Machines SLA of 99.9 percent two times in the formula.

Note that even though all of the individual services have SLAs equal to or better than the application SLA, combining them results in an overall number that's *lower* than the 99.9 percent you need. Why? Because using multiple services adds an extra level of complexity and slightly increases the risk of failure.

You see here that the composite SLA of 99.78 percent doesn't meet the required SLA of 99.9 percent. You might go back to team and ask whether this is acceptable. Or you might implement some other strategies into your design to improve this SLA.

What happens when the composite SLA doesn't meet your needs?

For the Special Orders application, the composite SLA of doesn't meet the required SLA of 99.9 percent. Let's look at a few strategies that Tailwind Traders might consider.

13 https://azure.microsoft.com/support/legal/sla/?azure-portal=true

Choose customization options that fit your required SLA

Each of the workloads defined previously has its own SLA, and the customization choices you make when you provision each workload affects that SLA. For example:

- Disks

  With Virtual Machines, you can choose from a Standard HDD Managed Disk, a Standard SSD Managed Disk, or a Premium SSD or Ultra Disk. The SLA for a single VM would be either 95 percent, 99.5 percent or 99.9 percent, depending on the disk choice.

- Tiers

  Some Azure services are offered as both a free tier product and as a standard paid service. For example, Azure Automation provides 500 minutes of job runtime in an Azure free account, but is not backed by an SLA. The standard tier SLA for Azure Automation is 99.9 percent.

Make sure that your purchasing decisions take into account the impact on the SLA for the Azure services that you choose. Doing so ensures that the SLA supports your required application SLA.

Here, Tailwind Traders might choose the Ultra Disk option for its virtual machines to help guarantee greater uptime.

Build availability requirements into your design

There are application design considerations you can use that relate to the underlying cloud infrastructure.

For example, to improve the availability of the application, avoid having any single points of failure. So instead of adding more virtual machines, you can deploy one or more extra instances of the same virtual machine across the different availability zones in the same Azure region.

An *availability zone* is a unique physical location within an Azure region. Each zone is made up of one or more datacenters equipped with independent power, cooling, and networking. These zones use different schedules for maintenance, so if one zone is affected, your virtual machine instance in the other zone is unaffected.

Deploying two or more instances of an Azure virtual machine across two or more availability zones raises the virtual machine SLA to 99.99 percent. Recalculating your composite SLA above with this Virtual Machines SLA gives you an application SLA of:

99.99% × 99.99% × 99.99% × 99.99%

=99.96%

This revised SLA of 99.96 percent exceeds your target of 99.9 percent.

To learn more about the SLA for Virtual Machines, visit **SLA for Virtual Machines** [14].

Include redundancy to increase availability

To ensure high availability, you might plan for your application to have duplicate components across several regions, known as *redundancy*. Conversely, to minimize costs during non-critical periods, you might run your application only in a single region. Tailwind Traders might consider this if there's a trend that the special order rates are much higher during certain months or seasons.

To achieve maximum availability in your application, add redundancy to every single part of the application. This redundancy includes the application itself, as well as the underlying services and infrastructure.

14 https://azure.microsoft.com/support/legal/sla/virtual-machines

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

Be aware, however, that doing so can be difficult and expensive, and often results in solutions that are more complex than they need to be.

Consider how critical high availability is to your requirements before you add redundancy. There may be simpler ways to meet your application SLA.

Very high performance is difficult to achieve

Performance targets above 99.99 percent are very difficult to achieve. Recall that an SLA of 99.99 percent means 1.01 minutes of downtime per week. It's difficult for humans to respond to failures quickly enough to meet SLA performance targets above 99.99 percent. Instead, your application must be able to self-diagnose and self-heal during an outage.

Access preview services and preview features

Now that Tailwind Traders has their applications up and running, they want to start looking into new capabilities. One option is to look at preview services. In this part, you'll learn how Azure services go from the preview phase to being generally available.

For Tailwind Traders, migration from the datacenter to Azure is more about operational efficiency. The research and development team is looking into new features that will keep them ahead of the competition — features they can't achieve without the power of the cloud.

Tailwind Traders is experimenting with a custom drone delivery system for customers in rural areas. They need the ability to use real-time storm tracking in the drone guidance system, but the feature is not ready yet. They read about the new AI Storm Analyzer service that has just entered Public preview. So Tailwind Traders has decided to incorporate it into the early stages of their application testing.

Note: AI Storm Analyzer is a fictitious Azure service. We introduce it here for illustration.

Before the team moves forward, they want a better understanding of how preview services impact their SLA. Let's begin by defining the Azure service lifecycle.

What is the service lifecycle?

The *service lifecycle* defines how every Azure service is released for public use.

Every Azure service starts in the development phase. This is where the Azure team collects defines their requirements and begins to build out the service.

Next, the service is released to the Public preview phase. During this phase, the public can access and experiment with it so that they can provide feedback. Your feedback helps Microsoft to improve their services. More importantly, providing feedback gives you the opportunity to request new or different capabilities so that services better meet your needs.

After a new Azure service is validated and tested, it's released to all customers as a production-ready service. This is known as *general availability* (GA).

What terms and conditions can I expect?

Each Azure preview defines its own terms and conditions. All preview-specific terms and conditions supplement your existing Azure service agreement.

Some previews are not covered by customer support. Therefore, previews are not recommended for business-critical workloads.

How can I access preview services?

You can access preview services from the Azure portal.

Here's how to see what preview service are available. You can follow along if have an Azure subscription.

1. Go to the **Azure portal**[15] and sign in.
2. Select **Create a resource**.
3. Enter *preview* in the search box and select Enter.
4. Select a service to learn more about it. You can also launch the service if you'd like to try it out.

How can I access new features for an existing service?

Some preview features relate to a specific area of an existing Azure service. For example, a compute or database service that you use daily might provide enhanced functionality. These preview features are accessible when you deploy, configure, and manage the service.

Although you can use an Azure preview feature in production, make sure you're aware of any limitations around its use before deploying to production.

How can I access preview features for the Azure portal?

You can access preview features that are specific to the Azure portal from **preview.portal.azure.com**[16].

Typical portal preview features provide performance, navigation, and accessibility improvements to the Azure portal interface.

You see **Microsoft Azure (Preview)** near the menu bar to remind you that you're working with a preview version of the Azure portal.

How can I provide feedback on the Azure portal?

You can provide feedback:

- From the **Feedback** tab in the Azure portal.

15 https://portal.azure.com?azure-portal=true
16 https://preview.portal.azure.com?azure-portal=true

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

- From the **Azure portal feedback forum**[17].

How can I stay updated on the latest announcements?

The **Azure updates**[18] page provides information about the latest updates to Azure products, services, and features, as well as product roadmaps and announcements.

From the Azure updates page, you can:

- View details about all Azure updates.
- See which updates are in general availability, preview, or development.

- Browse updates by product category or update type.
- Search for updates by keyword.
- Subscribe to an RSS feed to receive notifications.
- Access the Microsoft Connect page to read Azure product news and announcements.

17 https://feedback.azure.com/forums/223579-azure-portal?azure-portal=true
18 https://azure.microsoft.com/updates?azure-portal=true

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

Module 6 Review Questions

Module 06 Review Questions

Review Question 1

Which is the best first step a team should take to compare the cost of running these environments on Azure versus in their datacenter?

- ☐ They're just test environments. Spin them up and check the bill at the end of the month.
- ☐ Assume that running in the cloud costs about the same as running in the datacenter.
- ☐ Run the Total Cost of Ownership Calculator.

Review Question 2

What's the best way to ensure that a development team doesn't provision too many virtual machines at the same time?

- ☐ Do nothing. Let the development team use what they need.
- ☐ Apply spending limits to the development team's Azure subscription.
- ☐ Verbally give the development lead a budget and hold them accountable for overages.

Review Question 3

Which is the most efficient way for a testing team to save costs on virtual machines on weekends, when testers are not at work?

- ☐ Delete the virtual machines before the weekend and create a new set the following week.
- ☐ Deallocate virtual machines when they're not in use.
- ☐ Just let everything run. Azure bills you only for the CPU time that you use.

Review Question 4

Resources in the Dev and Test environments are each paid for by different departments. What's the best way to categorize costs by department?

- ☐ Apply a tag to each virtual machine that identifies the appropriate billing department.
- ☐ Split the cost evenly between departments.
- ☐ Keep a spreadsheet that lists each team's resources.

Review Question 5

What's the SLA for Azure Maps in terms of guaranteed uptime?

- ☐ 99 percent
- ☐ 99.9 percent
- ☐ 99.99 percent

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

Review Question 6

What's the new composite SLA? Remember, the new SLA includes a third virtual machine and Azure Maps.

- ☐ 99.58 percent
- ☐ 99.78 percent
- ☐ 99.99 percent

Review Question 7

Adding a third virtual machine reduces the composite SLA. How can companies offset this reduction?

- ☐ Increase the size of each virtual machine.
- ☐ Deploy extra instances of the same virtual machines across the different availability zones in the same Azure region.
- ☐ Do nothing. Using Azure Load Balancer increases the SLA for virtual machines.

Review Question 8

What approach might the company take in adding the augmented reality (AR) preview service to its architecture?

- ☐ The Special Orders app is already in production. The company shouldn't look into the AR service until the service reaches general availability (GA).
- ☐ The Special Orders app is mainly for use by retail employees. The company can integrate the AR service now because potential downtime or failures aren't an important factor.
- ☐ The development team can create a prototype version of the app that includes the AR service that it tests out with select retail employees.

Module 6 Summary

Module 06 Summary

Plan and manage your Azure costs

Tailwind Traders is taking a methodical approach toward cloud migration. While proof-of-concept projects can help demonstrate technical feasibility, having a clear picture of the total cost of running in the cloud will further help the team validate its approach.

To start, the Tailwind Traders team used the Total Cost of Ownership Calculator to estimate the cost savings of operating its solution on Azure instead of in its on-premises datacenter.

From there, the team used the Pricing calculator to get a more detailed estimate for running a typical workload on Azure each month.

The team also created a checklist of cost-saving measures that it can use to help keep down costs. This list includes:

- Perform cost analysis before you deploy.
- Use Azure Advisor to monitor your usage.
- Use spending limits to prevent accidental spending.
- Use Azure Reservations to prepay.
- Choose low-cost locations and regions.
- Research available cost-saving offers.
- Apply tags to identify cost owners.

With these measures in place, the Tailwind Traders team is ready to take the next steps toward cloud migration.

Choose the right Azure services by examining SLAs and service lifecycle

A service-level agreement (SLA) is the formal agreement between a service company and the customer. For Azure, this agreement defines the performance standards that Microsoft commits to for its customers.

The Tailwind Traders team is working on quite a variety of projects! In addition to its main website, the team is adding a mapping feature to its Special Orders application so that it can calculate routes between suppliers and retail stores. The team is also exploring how severe weather tracking can improve its drone guidance system.

As requirements evolve, it's important for the team to understand how the SLA for each service it chooses affects the overall performance guarantees of its applications.

For example, the main website must be available as close to 100 percent of the time as possible. To accomplish that, Tailwind Traders might deploy extra instances of the same virtual machine across different availability zones in the same Azure region. Doing so helps ensure that if one zone is affected, virtual machine instances in the other zone can pick up the load.

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

The Special Orders application might have more flexible tolerances. As long as retail employees don't lose data and can quickly regain network access, the Special Orders application might have a lower SLA. Here, the team can choose to include less redundancy in its design.

When defining your SLA requirements, be sure to consider both your business needs and the time it takes to restore a component after a failure. Also consider how the use of preview services and preview features might affect your systems in production.

Next steps

Create a sketch or diagram for an application that you plan to migrate to the cloud. Include each Azure service that you plan to use.

Use the documented **Service Level Agreements** [19] to find out the SLA for each Azure service involved. Then compute the composite SLA for your application.

Does the composite SLA meet your requirements? If not, what can you do to improve it?

19 https://azure.microsoft.com/support/legal/sla/

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

Answers

Review Question 1

Which is the best first step a team should take to compare the cost of running these environments on Azure versus in their datacenter?

- ☐ They're just test environments. Spin them up and check the bill at the end of the month.
- ☐ Assume that running in the cloud costs about the same as running in the datacenter.
- ■ Run the Total Cost of Ownership Calculator.

Explanation
Running the Total Cost of Ownership Calculator is a great first step because it can provide an accurate comparison of running workloads in the datacenter versus on Azure, certified by an independent research company.

Review Question 2

What's the best way to ensure that a development team doesn't provision too many virtual machines at the same time?

- ☐ Do nothing. Let the development team use what they need.
- ■ Apply spending limits to the development team's Azure subscription.
- ☐ Verbally give the development lead a budget and hold them accountable for overages.

Explanation
If you exceed your spending limit, active resources are deallocated. You can then decide whether to increase your limit or provision fewer resources.

Review Question 3

Which is the most efficient way for a testing team to save costs on virtual machines on weekends, when testers are not at work?

- ☐ Delete the virtual machines before the weekend and create a new set the following week.
- ■ Deallocate virtual machines when they're not in use.
- ☐ Just let everything run. Azure bills you only for the CPU time that you use.

Explanation
When you deallocate virtual machines, the associated hard disks and data are still kept in Azure. But you don't pay for CPU or network consumption, which can help save costs.

Review Question 4

Resources in the Dev and Test environments are each paid for by different departments. What's the best way to categorize costs by department?

- ■ Apply a tag to each virtual machine that identifies the appropriate billing department.
- ☐ Split the cost evenly between departments.
- ☐ Keep a spreadsheet that lists each team's resources.

Explanation
You can apply tags to groups of Azure resources to organize billing data.

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

Review Question 5

What's the SLA for Azure Maps in terms of guaranteed uptime?

- ☐ 99 percent
- ■ 99.9 percent
- ☐ 99.99 percent

Explanation
The SLA for Azure Maps tells you the SLA.

Review Question 6

What's the new composite SLA? Remember, the new SLA includes a third virtual machine and Azure Maps.

- ■ 99.58 percent
- ☐ 99.78 percent
- ☐ 99.99 percent

Explanation
To compute the composite SLA for a set of services, you multiply the SLA of each individual service.

Review Question 7

Adding a third virtual machine reduces the composite SLA. How can companies offset this reduction?

- ☐ Increase the size of each virtual machine.
- ■ Deploy extra instances of the same virtual machines across the different availability zones in the same Azure region.
- ☐ Do nothing. Using Azure Load Balancer increases the SLA for virtual machines.

Explanation
If one availability zone is affected, your virtual machine instance in the other availability zone should be unaffected.

Review Question 8

What approach might the company take in adding the augmented reality (AR) preview service to its architecture?

- ☐ The Special Orders app is already in production. The company shouldn't look into the AR service until the service reaches general availability (GA).
- ☐ The Special Orders app is mainly for use by retail employees. The company can integrate the AR service now because potential downtime or failures aren't an important factor.
- ■ The development team can create a prototype version of the app that includes the AR service that it tests out with select retail employees.

Explanation
After the AR service reaches general availability (GA), the team can roll it out to production.

Module 7 Course Conclusion

Summary

Summary

In this course, you have learned about:

- The basics of cloud computing and Azure, and how to get started with Azure's subscriptions and accounts.
- The advantages of using cloud computing services, learning to differentiate between the categories and types of cloud computing, and how to examine the various concepts, resources, and terminology that are necessary to work with Azure architecture.
- The core services available with Microsoft Azure.
- The core solutions that encompass a wide array of tools and services from Microsoft Azure.
- The general security and network security features, and how you can use the various Azure services to help ensure that your cloud resources are safe, secure, and trusted.
- The identity, governance, privacy, and compliance features, and how Azure can help you secure access to cloud resources, what it means to build a cloud governance strategy, and how Azure adheres to common regulatory and compliance standards.
- The factors that influence cost, tools you can use to help estimate and manage your cloud spend, and how Azure's service-level agreements (SLAs) can impact your application design decisions.

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED