Microsoft

Microsoft Official Course

AZ-900T00

Microsoft Azure Fundamentals

AZ-900T00
Microsoft Azure Fundamentals

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.

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

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.

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,

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.

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.**

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

Contents

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

- Understand general cloud computing concepts.
- Understand core services available with Microsoft Azure.
- Understand security, privacy, compliance and trust with Microsoft Azure.
- Understand pricing and support models available with Microsoft.

Course Syllabus

Module 1 - Cloud Concepts

In this module, you will learn general cloud computing concepts.

- Lesson 1 - Learning Objectives
- Lesson 2 - Why Cloud Services
- Lesson 3 - Types of Cloud models
- Lesson 4 - Types of Cloud services
- Lesson 5 - Module 1 Review Questions
- Lesson 6 - Module 1 Summary

Module 2 - Core Azure Services

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

- Lesson 1 - Learning Objectives
- Lesson 2 - Core Azure architectural components
- Lesson 3 - Core Azure services and products
- Lesson 4 - Azure solutions
- Lesson 5 - Azure management tools
- Lesson 6 - Module 2 Review Questions
- Lesson 7 - Module 2 Summary

Module 3 - Security, Privacy, Compliance and Trust

In this module, learn security, privacy, compliance and trust with Microsoft Azure.

- Lesson 1 - Learning Objectives
- Lesson 2 - Securing network connectivity
- Lesson 3 - Core Azure Identity services
- Lesson 4 - Security tools and features
- Lesson 5 - Azure governance methodologies
- Lesson 6 - Monitoring and Reporting in Azure
- Lesson 7 - Privacy, compliance and data protection standards
- Lesson 8 - Module 3 Review Questions
- Lesson 9 - Module 3 Summary
- **Module 4 - Azure Pricing, Service Level Agreements (SLAs), and Lifecycle**

In this module you will learn pricing and support models available with Microsoft.

- Lesson 1 - Learning Objectives
- Lesson 2 - Azure subscriptions
- Lesson 3 - Planning and managing costs
- Lesson 5 - Azure Service Level Agreements (SLAs)

- Lesson 6 - Service lifecycle in Azure
- Lesson 7 - Module 4 Review Questions
- Lesson 8 - Module 4 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 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
Understand cloud concepts	15-20%
Understand core Azure services	30-35%
Understand security, privacy, compliance, and trust	25-30%
Understand Azure pricing and support	20-25%

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

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

Module 1 Cloud Concepts

Learning Objectives

Learning Objectives

After completing this module, you will be able to:

- Describe and understand cloud services and their benefits.
- Understand key terms you will encounter when working with cloud services.
- Understand public, private, and hybrid cloud models.
- Understand infrastructure as a service (IaaS).
- Understand platform as a service (PaaS).
- Understand software as a service (SaaS).

Why cloud services?

Cloud computing

Cloud Computing[1] is the delivery of computing services—servers, storage, databases, networking, software, analytics, intelligence and more—over the internet (the cloud), enabling faster innovation, flexible resources, and economies of scale. You typically pay only for cloud services you use, helping lower your operating costs, run your infrastructure more efficiently, and scale as your business needs change.

The company providing these services is referred to as a cloud provider. Some example providers are Microsoft Azure, Amazon Web Services (AWS), and the Google Cloud Platform (GCP). The cloud provider is responsible for the physical hardware required to execute your work, in addition to keeping it up to date. Every business is unique and has different needs. To meet those needs, cloud computing providers offer a wide range of services. Typically, these services include:

- **Compute power** - such as Linux servers or web applications.
- **Storage** - such as files and databases.
- **Networking** - such as secure connections between the cloud provider and your company.
- **Analytics** - such as visualizing telemetry and performance data.

Cloud computing services

The goal of cloud computing is to make running a business easier and more efficient, whether it's a small start-up or a large enterprise. Every business is unique and has different needs. To meet those needs, cloud computing providers offer a wide range of services.

You need to have a basic understanding of some of the services it provides. Let's briefly discuss the two most common services that all cloud providers offer – *compute power* and *storage*.

Compute power

When you send an email, book a reservation on the Internet, pay a bill online, or even take this Microsoft Learn module you're interacting with cloud-based servers that are processing each request and returning a response. As a consumer, we're all dependent on the computing services provided by the various cloud providers that make up the Internet.

When you build solutions using cloud computing, you can choose how you want work to be done based on your resources and needs. For example, if you want to have more control and responsibility over

1 https://azure.microsoft.com/overview/what-is-cloud-computing

maintenance, you could create a *virtual machine* (VM). A VM is an emulation of a computer - just like your desktop or laptop you're using now. Each VM includes an operating system and hardware that appears to the user like a physical computer running Windows or Linux. You can then install whatever software you need to do the tasks you want to run in the cloud.

The difference is that you don't have to buy any of the hardware or install the OS. The cloud provider runs your virtual machine on a physical server in one of their datacenters - often sharing that server with other VMs (isolated and secure). With the cloud, you can have a VM ready to go in minutes at less cost than a physical computer.

VMs aren't the only computing choice - there are two other popular options: *containers* and *serverless computing*.

What are containers?

Containers provide a consistent, isolated execution environment for applications. They're similar to VMs except they don't require a guest operating system. Instead, the application and all its dependencies is packaged into a "container" and then a standard runtime environment is used to execute the app. This allows the container to start up in just a few seconds, because there's no OS to boot and initialize. You only need the app to launch.

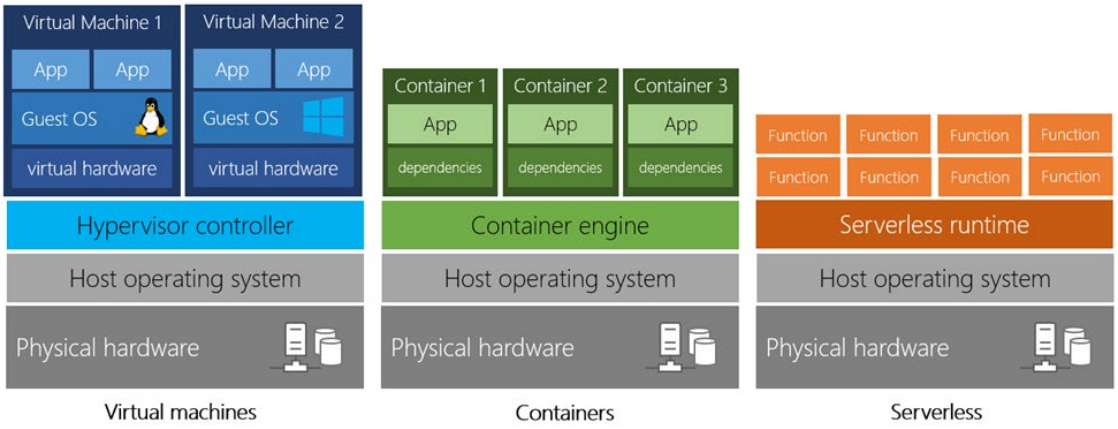
The open-source project, Docker, is one of the leading platforms for managing containers. Docker containers provide an efficient, lightweight approach to application deployment because they allow different components of the application to be deployed independently into different containers. Multiple containers can be run on a single machine, and containers can be moved between machines. The portability of the container makes it easy for applications to be deployed in multiple environments, either on-premises or in the cloud, often with no changes to the application.

What is serverless computing?

Serverless computing lets you run application code without creating, configuring, or maintaining a server. The core idea is that your application is broken into separate *functions* that run when triggered by some action. This is ideal for automated tasks - for example, you can build a serverless process that automatically sends an email confirmation after a customer makes an online purchase.

The serverless model differs from VMs and containers in that you only pay for the processing time used by each function as it executes. VMs and containers are charged while they're running - even if the applications on them are idle. This architecture doesn't work for every app - but when the app logic can be separated to independent units, you can test them separately, update them separately, and launch them in microseconds, making this approach the fastest option for deployment.

Here's a diagram comparing the three compute approaches we've covered.



Storage

Most devices and applications read and/or write data. Here are some examples:

- Buying a movie ticket online
- Looking up the price of an online item
- Taking a picture
- Sending an email
- Leaving a voicemail

In all of these cases, data is either *read* (looking up a price) or *written* (taking a picture). The type of data and how it's stored can be different in each of these cases.

Cloud providers typically offer services that can handle all of these types of data. For example, if you wanted to store text or a movie clip, you could use a file on disk. If you had a set of relationships such as an address book, you could take a more structured approach like using a database.

The advantage to using cloud-based data storage is you can scale to meet your needs. If you find that you need more space to store your movie clips, you can pay a little more and add to your available space. In some cases, the storage can even expand and contract automatically - so you pay for exactly what you need at any given point in time.

✓ Every business has different needs and requirements, and cloud computing is flexible and cost-efficient. The goal of cloud computing is to make running a business easier and more efficient, whether it's a small start-up or a large enterprise.

Key cloud concepts and benefits

Cloud services is a big shift from the traditional way businesses think about IT resources. Cloud services have characteristics and considerations, some of which are outlined and explained below:

- **High availability**. The ability to keep services up and running for long periods of time, with very little downtime, depending on the service in question.
- **Scalability**. The ability to increase or decrease resources for any given workload. You can add additional resources to service a workload (known as *scaling out*), or add additional capabilities to manage an increase in demand to the existing resource (known as *scaling up*). Scalability doesn't have to be done automatically
- **Elasticity**. The ability to automatically or dynamically increase or decrease resources as needed. Elastic resources match the current needs, and resources are added or removed automatically to meet future needs when it's needed, and from the most advantageous geographic location. A distinction between scalability and elasticity is that elasticity is done automatically
- **Agility**. The ability to react quickly. Cloud services can allocate and deallocate resources quickly. They are provided on-demand via self-service, so vast amounts of computing resources can be provisioned in minutes. There is no manual intervention in provisioning or deprovisioning services.
- **Fault tolerance**. The ability to remain up and running even in the event of a component or service no longer functioning. Typically, redundancy is built into cloud services architecture so if one component fails, a backup component takes its place. The type of service is said to be tolerant of faults.
- **Disaster recovery**. The ability to recover from an event which has taken down a cloud service. Cloud services disaster recovery can happen very quickly with automation and services being readily available to use.
- **Global reach**. The ability reach audiences around the globe. Cloud services can have presence in various regions across the globe which you can access, giving you a presence in those regions even though you may not have any infrastructure in that region.
- **Customer latency capabilities**. If customers are experiencing slowness with a particular cloud service, they are said to be experiencing some latency. Even though modern fiber optics are fast, it can still take time for services to react to customer actions if the service is not local to the customer. Cloud services have the ability deploy resources in datacenters around the globe, thus addressing customer latency issues.
- **Predictive cost considerations**. The ability for users to predict what costs they will incur for a particular cloud service. Costs for individual services are made available, and tools are provided to allow you predict what costs a service will incur. You can also perform analysis based on future growth.
- **Technical skill requirements and considerations**. Cloud services can provide and manage hardware and software for workloads. Therefore, getting a workload up and running with cloud services demands less technical resources than having IT teams build and maintain physical infrastructure for handling the same workload. A user can be expert in the application they want to run without having to need skills to build and maintain the underlying hardware and software infrastructure.
- **Increased productivity**. On-site datacenters typically require a lot of hardware setup (otherwise known as *racking and stacking*), software patching, and other time-consuming IT management chores.

Cloud computing eliminates the need for many of these tasks, so IT teams can spend time on achieving more important business goals.

- **Security**. Cloud providers offer a broad set of policies, technologies, controls, and expert technology skills that can provide better security than most organizations can otherwise achieve. The result is strengthened security, which helps to protect data, apps, and infrastructure from potential threats.

✓ Take a few minutes to review the **Cloud computing terms**[2] page.

Inline - Contoso, Ltd. Case Study

Wow, those are some great benefits to moving to cloud and the Contoso needs all of those capabilities. I bet your applications could as well. Lets take a quick look at several of these in the context of growth of Contoso Ltd:

- **High Availability** is a must. At Contoso, we make money and keep our customers happy when they can get to our products. When our site goes down, or our shipping systems and drones can't talk with each other it is a critical situation.
- **Scalability** and **Elasticity** is something we at Contoso have wished for in the past. We have purchased thousands of servers, had to manually set each one up and manage it, then many of them set there idle waiting on users to log-in. They were using power, heating / cooling, and had to be maintained. Then there was a rush of people logging in during seasonal parts of the year and things really bogged down.
- **Disaster Recorery** would be great to have. Right now we run an on-premises backup system, then transport the backup offsite for storage; this is time consuming and costly and really slow to restore if we ever have an issue. Backing up customers orders, history, and data the moment it is entered is an absolute must. We can't survive if we cannot get to our customers information.

We could keep going with all of these items. Why don't you take a moment and think about how each of these are applicable to your daily business.

Try This Exercise:

1. Grab a piece of paper.
2. Write down three of the key cloud concepts.
3. Next to each concept you listed, write out a scenario your company has experience where this capability would have helped.

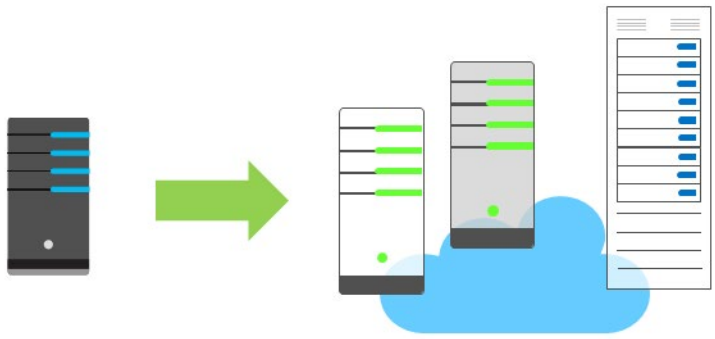
Economies of scale

The concept of **economies of scale** is the ability to reduce costs and gain efficiency when operating at a larger scale in comparison to operating at a smaller scale.

Cloud providers such as Microsoft, Google, and Amazon are large businesses, and are able to leverage the benefits of economies of scale, and then pass those benefits on to their customers.

This is apparent to end users in a number of ways, one of which is the ability to acquire hardware at a lower cost than if a single user or smaller business were purchasing it.

2 https://azure.microsoft.com/overview/cloud-computing-dictionary?azure-portal=true



Storage costs, for example, have decreased significantly over the last decade due in part to cloud providers' ability to purchase larger amounts of storage at significant discounts. They are then able to use that storage more efficiently and pass on those benefits to end users in the form of lower prices.

✓ There are limits to the benefits large organizations can realize through economies of scale. A product will inevitably have an underlying core cost, as it becomes more of a commodity, based on what it costs to produce. Competition is also another factor which has an effect on costs of cloud services.

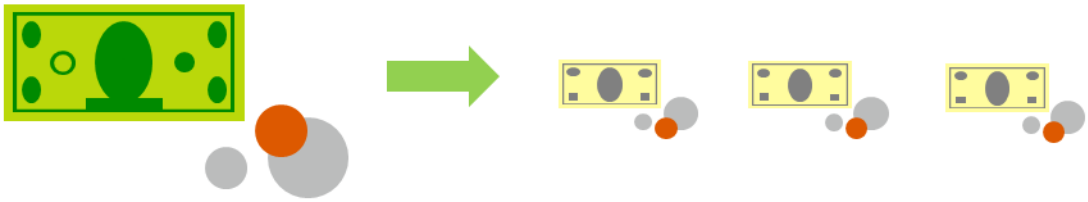
CapEx versus OpEx

In previous years, startup companies needed to acquire a physical premises and infrastructure to start their business and begin trading. Large amounts of money were need to get a new business up and running, or to grow an existing company. They would have to buy new datacenters or new servers to allow them build out new services, which they could then deliver to their customers. That is no longer the case.

Today, organizations can sign up for a service from a cloud provider to get up and running. This enables them to begin selling or providing services to their customers more quickly, without the need for significant up front costs.

These two approaches to investment are referred to as:

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



CapEx computing costs

A typical on-premises datacenter includes costs such as:

Server costs

This area includes all hardware components and the cost of supporting them. When purchasing servers, make sure to design fault tolerance and redundancy, such as server clustering, redundant power supplies, and uninterruptible power supplies. When a server needs to be replaced or added to a datacenter, you need to pay for the computer. This can affect your immediate cash flow because you must pay for the server up front.

Storage costs

This area includes all storage hardware components and the cost of supporting it. Based on the application and level of fault tolerance, centralized storage can be expensive. For larger organizations, you can create tiers of storage where more expensive fault-tolerant storage is used for critical applications and lower expense storage is used for lower priority data.

Network costs

Networking costs include all on-premises hardware components, including cabling, switches, access points, and routers. This also includes wide area network (WAN) and Internet connections.

Backup and archive costs

This is the cost to back up, copy, or archive data. Options might include setting up a backup to or from the cloud. There's an upfront cost for the hardware and additional costs for backup maintenance and consumables like tapes.

Organization continuity and disaster recovery costs

Along with server fault tolerance and redundancy, you need to plan for how to recover from a disaster and continue operating. Your plan should consist of creating a data recovery site. It could also include backup generators. Most of these are upfront costs, especially if you build a data recovery site, but there's an additional ongoing cost for the infrastructure and its maintenance.

Datacenter infrastructure costs

These are costs for construction and building equipment, as well as future renovation and remodeling costs that may arise as demands grow. Additionally, this infrastructure incurs operational expenses for electricity, floor space, cooling, and building maintenance.

Technical personnel

While not a capital expenditure, the personnel required to work on your infrastructure are specific to on-premises datacenters. You will need the technical expertise and workforce to install, deploy, and manage the systems in the datacenter and at the data recovery site.

OpEx cloud computing costs

With cloud computing, many of the costs associated with an on-premises datacenter are shifted to the service provider. Instead of thinking about physical hardware and datacenter costs, cloud computing has a different set of costs. For accounting purposes, all these costs are operational expenses:

Leasing software and customized features

Using a pay-per-use model requires actively managing your subscriptions to ensure users do not misuse the services, and that provisioned accounts are being utilized and not wasted. As soon as the provider provisions resources, billing starts. It is your responsibility to de-provision the resources when they aren't in use so that you can minimize costs.

Scaling charges based on usage/demand instead of fixed hardware or capacity.

Cloud computing can bill in various ways, such as the number of users or CPU usage time. However, billing categories can also include allocated RAM, I/O operations per second (IOPS), and storage space. Plan for backup traffic and data recovery traffic to determine the bandwidth needed.

Billing at the user or organization level.

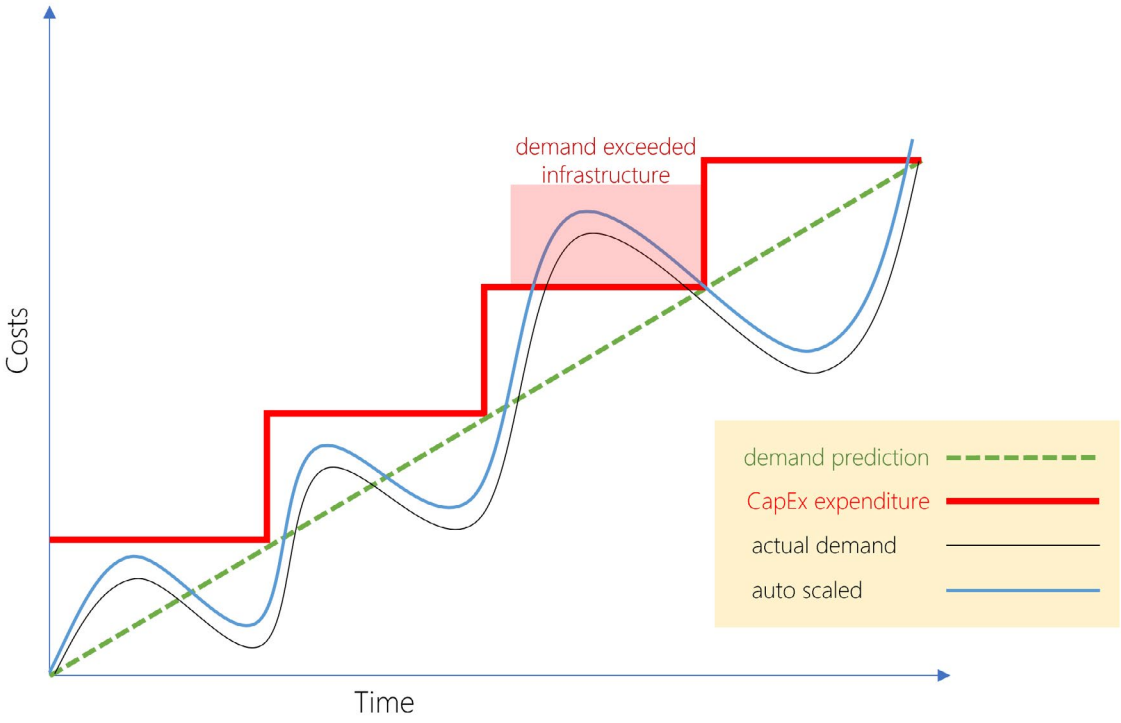
The subscription (pay-per-use) model is a computing billing method that is designed for both organizations and users. The organization or user is billed for the services used, typically on a recurring basis. You can scale, customize, and provision computing resources, including software, storage, and development platforms. For example, when using a dedicated cloud service, you could pay based on server hardware and usage.

Benefits of CapEx

With capital expenditures, you plan your expenses at the start of a project or budget period. Your costs are fixed, meaning you know exactly how much is being spent. This is appealing when you need to predict the expenses before a project starts due to a limited budget.

Benefits of OpEx

Demand and growth can be unpredictable and can outpace expectation, which is a challenge for the CapEx model as shown in the following graph.



With the OpEx model, companies wanting to try a new product or service don't need to invest in equipment. Instead, they pay as much or as little for the infrastructure as required.

OpEx is particularly appealing if the demand fluctuates or is unknown. Cloud services are often said to be *agile*. Cloud agility is the ability to rapidly change an IT infrastructure to adapt to the evolving needs of the business. For example, if your service peaks one month, you can scale to demand and pay a larger bill for the month. If the following month the demand drops, you can reduce the used resources and be charged less. This agility lets you manage your costs dynamically, optimizing spending as requirements change.

✓ Companies wanting to start a new business or grow their business do not have to incur up front costs to try out a new product or service for customers. Instead, they can get into a market immediately and pay as much or as little for the infrastructure as the business requires. They also can terminate that cost if and when they need to.

If your service is busy and you consume a lot of resources in a month, then you receive a large bill. If those services are minimal and don't use a lot of resources, then you will receive a smaller bill.

A business can still use the CapEx expenditure strategy if they wish, but it is no longer a requirement that they do so.

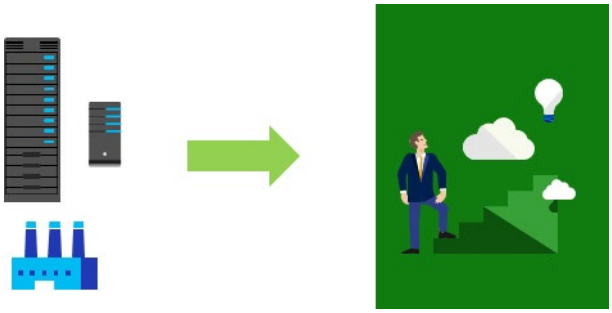
define-consumption-based-models

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.

This consumption-based model brings with it 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.



This also allows for better cost prediction. Prices for individual resources and services are provided so you can predict how much you will spend in a given billing period based on your expected usage. You can also perform analysis based on future growth using historical usage data tracked by your cloud provider.

Contoso Ltd. Case Study - Consumption-Based Usage

This is best capability ever for us here at the Contoso, only paying for what we consume!! We have systems designed to take a ton of load, but often they are sitting there idle. During the last shopping season we had more than a 1000 servers just waiting to collect and process data. Waiting being the operative word, because we were paying for them even when they set idle.

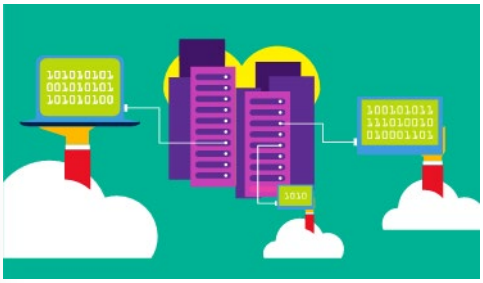
This ability to build out the application, deploy it to cloud, and only pay for it when and how it is being used is great. We can have one server deployed and waiting for users and pay for a small amount. Then when more users start connecting in peak shopping times, we just add a few extra servers to our site. Pay for them while they work, and then disconnect them, when not needed.

This model of just paying for what we use will save us money and time, and reduce the cost of our programs.

Types of cloud models

Public Cloud

A public cloud is owned by the cloud services provider (also known as a *hosting provider*). It provides resources and services to multiple organizations and users, who connect to the cloud service via a secure network connection, typically over the internet.



Public cloud models have the following characteristics:

- **Ownership** - Ownership refers to the resources that an organization or end user uses. Examples include storage and processing power. Resources do not belong to the organization that is utilizing them, but rather they are owned and operated by a third party, such as the cloud service provider.
- **Multiple End Users** - Public cloud modes may make their resources available to multiple organizations.
- **Public Access** - Public Access allows the public to access the desired cloud services.
- **Availability** - Availability is the most common cloud-type deployment model.
- **Connectivity** - Users and organizations are typically connected to the public cloud over the internet using a web browser.
- **Skills** - Public clouds do not require deep technical knowledge to set up and use its resources.

With a public cloud, there is no local hardware to manage or keep up to date; everything runs on the cloud provider's hardware. In some cases, cloud users can save additional costs by sharing computing resources with other cloud users.

A common use case scenario is deploying a web application or a blog site on hardware and resources that are owned by a cloud provider. Using a public cloud in this scenario allows cloud users to get their website/blog up and running quickly, and then focus on maintaining the site without having to worry about purchasing, managing, or maintaining the hardware on which it runs.

Businesses can use multiple public cloud service provider companies of varying scale. Microsoft Azure is an example of a public cloud provider.

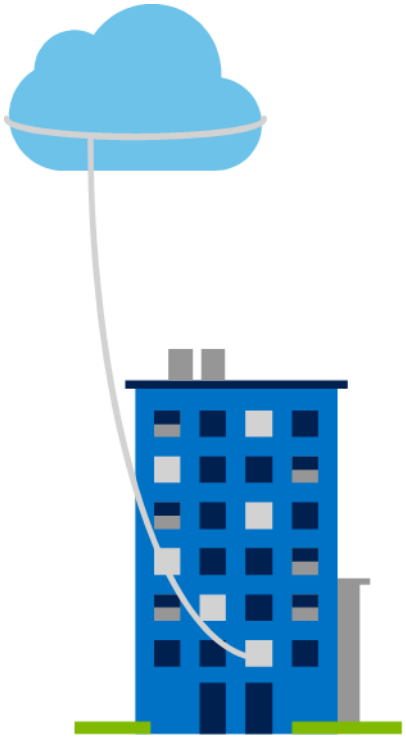
Private Cloud

A private cloud is owned and operated by the organization that uses the resources from that cloud. They create a cloud environment in their own datacenter and provide self-service access to compute resources to users within their organization. The organization remains the owner, entirely responsible for the operation of the services they provide.

Private cloud models have the following characteristics:

- **Ownership**. The owner and user of the cloud services are the same.

- **Hardware**. The owner is entirely responsible for the purchase, maintenance, and management of the cloud hardware.
- **Users**. A private cloud operates only within one organization and cloud computing resources are used exclusively by a single business or organization.
- **Connectivity**. A connection to a private cloud is typically made over a private network that is highly secure.
- **Public access**. Does not provide access to the public.
- **Skills**. Requires deep technical knowledge to set up, manage, and maintain.



A use case scenario for a private cloud would be when an organization has data that cannot be put in the public cloud, perhaps for legal reasons. For example, they may have medical data that cannot be exposed publicly.

Another scenario may be where government policy requires specific data to be kept in-country or privately.

A private cloud can provide cloud functionality to external customers as well, or to specific internal departments such as Accounting or Human Resources.

Hybrid Cloud

A hybrid cloud combines both public and private clouds, allowing you to run your applications in the most appropriate location.

Hybrid cloud models have the following characteristics:

- **Resource location**. Specific resources run or are used in a public cloud, and others run or are used in a private cloud.

- **Cost and efficiency**. Hybrid cloud models allow an organization to leverage some of the benefits of cost, efficiency, and scale that are available with a public cloud model.
- **Control**. Organizations retain management control in private clouds.
- **Skills**. Technical skills are still required to maintain the private cloud and ensure both cloud models can operate together.

An example of a hybrid cloud usage scenario would be hosting a website in the public cloud and linking it to a highly secure database hosted in a private cloud.

Hybrid cloud scenarios can be useful when organizations have some things that cannot be put in a public cloud, possibly for legal reasons. For example, you may have medical data that cannot be exposed publicly.

Another example is one or more applications that run on old hardware that can't be updated. In this case, you can keep the old system running locally in your private cloud and connect it to the public cloud for authorization or storage.

Comparing the Cloud Models

Below is an outline of some of the advantages and disadvantages for public, private, and hybrid clouds.

Public cloud

This is the most common deployment model. In this case, you have no local hardware to manage or keep up-to-date – everything runs on your cloud provider's hardware. In some cases, you can save additional costs by sharing computing resources with other cloud users.

Businesses can use multiple public cloud providers of varying scale. Microsoft Azure is an example of a public cloud provider.

Advantages:

- **No CapEx**. You don't have to buy a new server in order to scale.
- **Agility**. Applications can be made accessible quickly, and deprovisioned whenever needed.

- **Consumption-based model**. Organizations pay only for what they use, and operate under an OpEx model.
- **Maintenance**. Organizations have no responsibility for hardware maintenance or updates.
- **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.

Disadvantages:

- **Security**. There may be specific security requirements that cannot be met by using public cloud.
- **Compliance**. There may be government policies, industry standards, or legal requirements which public clouds cannot meet.
- **Ownership**. Organizations don't own the hardware or services and cannot manage them as they may wish.
- **Specific scenarios**. If organizations have a unique business requirement, such as having to maintain a legacy application, it may be hard to meet that requirement with public cloud services.

Private cloud

In a private cloud, you create a cloud environment in your own datacenter and provide self-service access to compute resources to users in your organization. This offers a simulation of a public cloud to your users, but you remain completely responsible for the purchase and maintenance of the hardware and software services you provide.

Advantages:

- **Control**. Organizations have complete control over the resources.
- **Security**. Organizations have complete control over security.
- **Compliance**. If organizations have very strict security, compliance, or legal requirements, a private cloud may be the only viable option.
- **Specific scenarios**. If an organization has a specific scenario not easily supported by a public cloud provider (such as having to maintain a legacy application), it may be preferable to run the application locally.

Disadvantages:

- **Upfront CapEx**. Hardware must be purchased for start-up and maintenance.
- **Agility**. Private clouds are not as agile as public clouds, because you need to purchase and set up all the underlying infrastructure before they can be leveraged.
- **Maintenance**. Organizations have the responsibility for hardware maintenance and updates.
- **Skills**. Private clouds require in-house IT skills and expertise that may be hard to get or be costly.

Hybrid cloud

A hybrid cloud combines public and private clouds, allowing you to run your applications in the most appropriate location. For example, you could host a website in the public cloud and link it to a highly secure database hosted in your private cloud (or on-premises datacenter).

Advantages:

- **Flexibility**. The most flexible scenario: with a hybrid cloud setup, an organization can decide to run their applications either in a private cloud or in a public cloud.
- **Costs**. Organizations can take advantage of economies of scale from public cloud providers for services and resources as they wish. This allows them to access cheaper storage than they can provide themselves.
- **Control**. Organizations can still access resources over which they have total control.
- **Security**. Organizations can still access resources for which they are responsible for security.
- **Compliance**. Organizations maintain the ability to comply with strict security, compliance, or legal requirements as needed.
- **Specific scenarios**. Organizations maintain the ability to support specific scenarios not easily supported by a public cloud provider, such as running legacy applications. In this case, they can keep the old system running locally, and connect it to the public cloud for authorization or storage. Additionally, they could host a website in the public cloud, and link it to a highly secure database hosted in their private cloud.

Disadvantages:

- **Upfront CapEx**. Upfront CapEx is still required before organizations can leverage a private cloud.
- **Costs**. Purchasing and maintaining a private cloud to use alongside the public cloud can be more expensive than selecting a single deployment model.
- **Skills**. Deep technical skills are still required to be able to set up a private cloud.
- **Ease of management**. Organizations need to ensure there are clear guidelines to avoid confusion, complications or misuse.

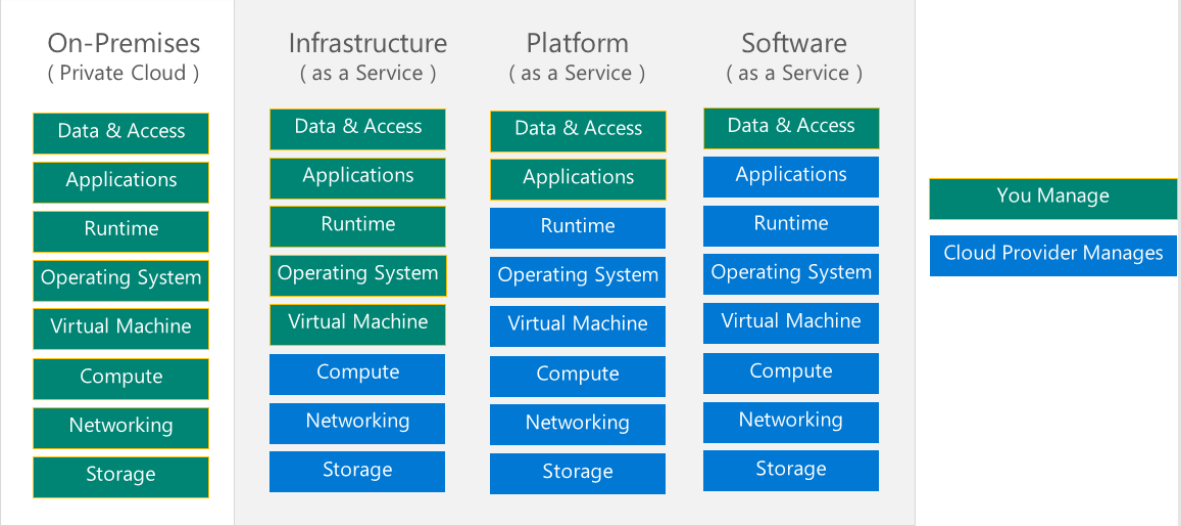
Types of cloud services

Shared Responsibility Model

The importance of understanding the **shared responsibility model** is essential for customers who are moving to the cloud. Cloud providers offer considerable advantages for security and compliance efforts, but these advantages do not absolve the customer from protecting their users, applications, and service offerings.

The shared responsibility model ensures cloud workloads are run securely and in a well-managed way. Depending on the service you are using, the cloud provider is responsible for some aspects of the workload management, and the customer or end user is responsible for other aspects of the workload management, and in some cases, both share a responsibility.

The following list of cloud service types describes the management responsibilities for the user and the cloud provider as compared to on-premises systems:

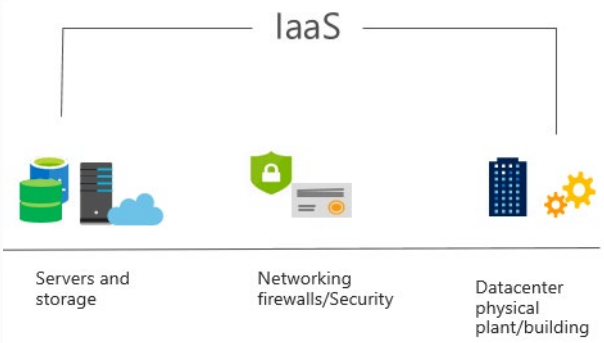


- IaaS requires the most user management of all the cloud services. The user is responsible for managing the operating systems, data, and applications.
- PaaS requires less user management. The cloud provider manages the operating systems, and the user is responsible for the applications and data they run and store.
- SaaS requires the least amount of management. The cloud provider is responsible for managing everything, and the end user just uses the software.

✓ It is important that cloud users understand what they are responsible for, to ensure their workloads are managed correctly and don't suffer any down time.

Infrastructure as a Service

Infrastructure as a Service (IaaS) is the most basic category of cloud computing services. With IaaS, you rent IT infrastructure servers and virtual machines (VMs), storage, networks, and operating systems from a cloud provider on a pay-as-you-go basis. It's an instant computing infrastructure, provisioned and managed over the internet.



IaaS characteristics

- **Upfront costs**. IaaS has no upfront costs. Users pay only for what they consume.
- **User ownership**. The user is responsible for the purchase, installation, configuration, and management of their own software operating systems, middleware, and applications.
- **Cloud provider ownership**. The cloud provider is responsible for ensuring that the underlying cloud infrastructure (such as virtual machines, storage and networking) is available for the user.

Common usage scenarios:

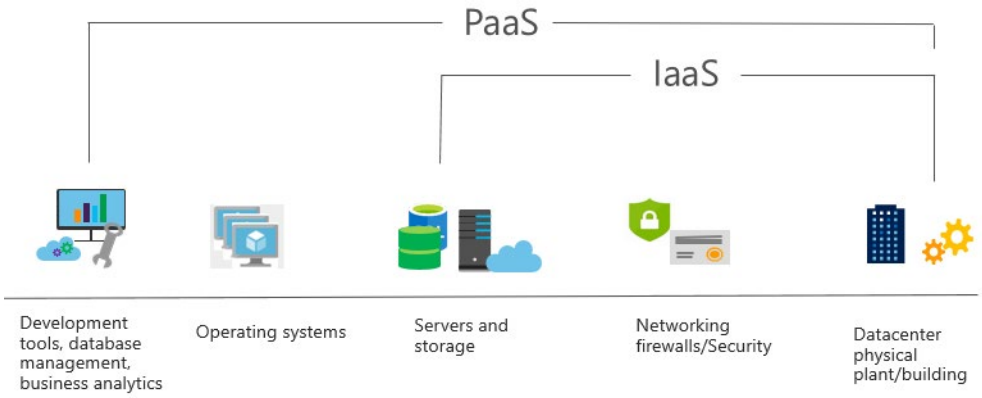
- **Migrating workloads**. Typically, IaaS facilities are managed in a similar way as on-premises infrastructure and provide an easy migration path for moving existing applications to the cloud.
- **Test and development**. Teams can quickly set up and dismantle test and development environments, bringing new applications to market faster. IaaS makes scaling development testing environments up and down fast and economical.
- **Website hosting**. Running websites using IaaS can be less expensive than traditional web hosting.
- **Storage, backup, and recovery**. Organizations avoid the capital outlay and complexity of storage management, which typically requires a skilled staff to manage data and meet legal and compliance requirements. IaaS is useful for managing unpredictable demand and steadily growing storage needs. It can also simplify the planning and management of backup and recovery systems.

✓ When using IaaS, ensuring that a service is up and running is a shared responsibility: the cloud provider is responsible for ensuring the cloud infrastructure is functioning correctly; the cloud customer is responsible for ensuring the service they are using is configured correctly, is up to date, and is available to their customers.

Platform as a Service

Platform as a Service (PaaS) provides an environment for building, testing, and deploying software applications. The goal of PaaS is to help create an application as quickly as possible without having to worry about managing the underlying infrastructure. For example, when deploying a web application using PaaS, you don't have to install an operating system, web server, or even system updates. PaaS is a complete development and deployment environment in the cloud, with resources that enable organizations to deliver everything from simple cloud-based apps to sophisticated cloud-enabled enterprise applications.

Resources are purchased from a cloud service provider on a pay-as-you-go basis and accessed over a secure Internet connection.



PaaS characteristics

- **Upfront costs**. There are no upfront costs, and users pay only for what they consume.
- **User ownership**. The user is responsible for the development of their own applications. However, they are not responsible for managing the server or infrastructure. This allows the user to focus on the application or workload they want to run.
- **Cloud provider ownership**. The cloud provider is responsible for operating system management, and network and service configuration. Cloud providers are typically responsible for everything apart from the application that a user wants to run. They provide a complete managed platform on which to run an application.

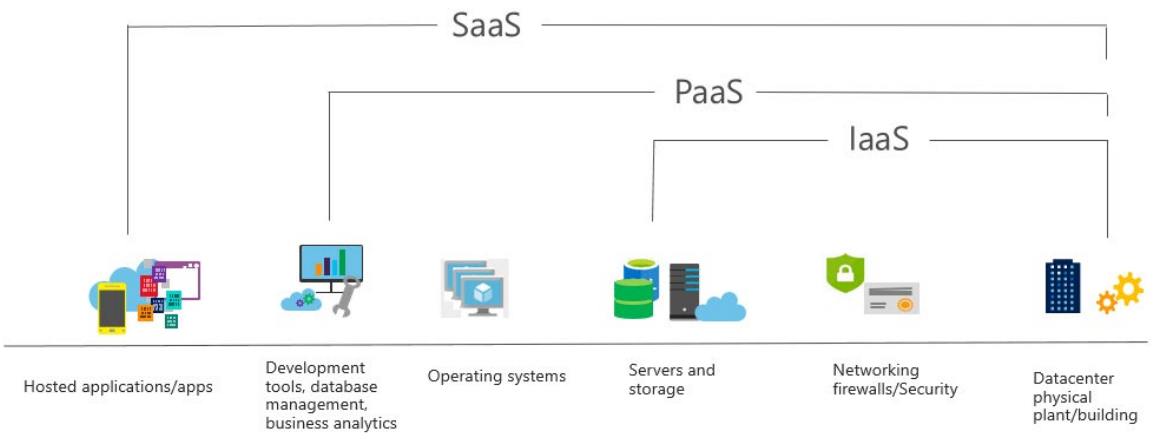
Common usage scenarios

- **Development framework**. PaaS provides a framework that developers can build upon to develop or customize cloud-based applications. Similar to the way you create a Microsoft Excel macro, PaaS lets developers create applications using built-in software components. Cloud features such as scalability, high-availability, and multi-tenant capability are included, reducing the amount of coding that developers must do.
- **Analytics or business intelligence**. Tools provided as a service with PaaS allow organizations to analyze and mine their data. They can find insights and patterns, and predict outcomes to improve business decisions such as forecasting, product design, and investment returns.

Software as a Service

Software as a Service (SaaS) is software that is centrally hosted and managed for the end customer. It allows users to connect to and use cloud-based apps over the internet. Common examples are email, calendars, and office tools such as Microsoft Office 365.

SaaS is typically licensed through a monthly or annual subscription, and Office 365 is an example of SaaS software.



SaaS characteristics

- **Upfront costs**. Users have no upfront costs; they pay a subscription, typically on a monthly or annual basis.
- **User ownership**. Users just use the application software; they are not responsible for any maintenance or management of that software.
- **Cloud provider ownership**. The cloud provider is responsible for the provision, management, and maintenance of the application software.

Common usage scenarios

- Examples of Microsoft SaaS services include Office 365, Skype, and Microsoft Dynamics CRM Online.

Comparing the types of cloud services

There are both advantages and disadvantages for IaaS, PaaS, and SaaS cloud services.

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.
- **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.
- **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.

Disadvantages:

- **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.

PaaS

PaaS provides the same benefits and considerations as IaaS, but there some additional benefits.

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.
- **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.

Disadvantages:

- **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.

SaaS

SaaS is software that is centrally hosted and managed for the end customer. It is usually based on an architecture where one version of the application is used for all customers, and licensed through a monthly or annual subscription

SaaS provides the same benefits as IaaS, but again there some additional benefits.

Advantages:

- **No CapEx**. Users don't have any upfront costs.
- **Agility**. Users can provide staff with access to the latest software quickly and easily.
- **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.
- **Flexibility**. Users can access the same application data from anywhere.

Disadvantages

- **Software limitations**. There may be some limitations to a software application that might affect how users work. Any limitations should be taken into consideration when considering which PaaS platform is best suited for a workload.

✓ IaaS, PaaS, and SaaS each contain different levels of managed services. You may easily use a combination of these types of infrastructure. You could use Office 365 on your company's computers (SaaS), and in Azure you could host your VMs (IaaS) and use Azure SQL Database (PaaS) to store your data. With the cloud's flexibility, you can use any combination that provides you with the maximum result.

Module 1 Review Questions

Module 01 Review Questions

Review Question 1

Which of the following describes a benefit of cloud services?

- ☐ Economies of scale
- ☐ Fixed workloads
- ☐ Unpredictable costs

Review Question 2

Which of the following refers to spending money upfront and then deducting that expense over time?

- ☐ Capital expenditure
- ☐ Operational expenditures
- ☐ Supply and demand

Review Question 3

Which of the following terms refer to making a service available with no downtime for an extended period of time?

- ☐ Agility
- ☐ Fault tolerance
- ☐ High availability

Review Question 4

Which term from the list below would be viewed as benefits of using cloud services?

- ☐ Unpredictable costs
- ☐ Local reach only
- ☐ Elasticity

Review Question 5

From the choices below, what is one of the advantages of moving your infrastructure to Azure?

- ☐ The move reduces Capital Expenditures. (CapEx)
- ☐ The move reduces Operational Expenses (OpEx).
- ☐ The move allows for complete control of infrastructure resources.

Review Question 6

Which cloud model provides the greatest degree of ownership and control?

- ☐ Hybrid
- ☐ Private
- ☐ Public

Review Question 7

Which cloud model provides the greatest degree of flexibility?

- ☐ Public
- ☐ Private
- ☐ Hybrid

Review Question 8

Which of the following describes a public cloud?

- ☐ Is owned and operated by the organization that uses the resources from that cloud.
- ☐ Lets organizations run applications in the cloud or on-premises.
- ☐ Provides resources and services to multiple organizations and users, who connect through a secure network connection.

Review Question 9

You have legacy applications that require specialized mainframe hardware and you have newer shared applications. Which cloud deployment model would be best for you?

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

Review Question 10

Which of the following requires the most user management of the cloud services?

- ☐ Infrastructure as a Service
- ☐ Platform as a Service
- ☐ Software as a Service

Review Question 11

Microsoft Office 365 is an example of?

- ☐ Infrastructure as a Service
- ☐ Platform as a Service
- ☐ Software as a Service

Review Question 12

Which of the following describes Platform as a Service (PaaS)?

- ☐ Users are responsible for purchasing, installing, configuring, and managing their own software (operating systems, middleware, and applications).
- ☐ Users create and deploy applications quickly without having to worry about managing the underlying infrastructure.
- ☐ Users pay an annual or monthly subscription.

Review Question 13

Which of the following requires the most user management of the cloud services?

- ☐ Infrastructure as a Service
- ☐ Platform as a Service
- ☐ Software as a Service

Review Question 14

You're developing an application and want to focus on building, testing, and deploying. You don't want to worry about managing the underlying hardware or software. Which cloud service type is best for you?

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

Review Question 15

You are running a virtual machine in a public cloud using IaaS. Which model correctly reflects how that resource is managed?

- ☐ Shared responsibility model
- ☐ Cloud user management model
- ☐ User management model

Module 1 Summary

Module 1 Summary

In this module you've learned about cloud computing, what it is and what its key characteristics are. You learned about the different types of cloud models that are available and the considerations of using those different models. You also learned about the different cloud services available, the benefits of using the different types, and the management responsibilities under each service type.

Why cloud services?

In this lesson you have learned about what cloud computing is, and why you should consider using cloud services. You've learned what some of the key terms and concepts are, such as high availability, agility, elasticity, fault tolerance, global reach, CapEx versus OpEX in the context of cloud computing, economies of scale, and the consumption-based cost model.

Types of cloud models

In this lesson you have learned about public cloud, private cloud, and hybrid cloud models, and what the key characteristics of each model are. You've also learned how they compare, what considerations you need to take into account when using them, and when you might use them.

Types of cloud services

In this lesson you have learned about the different types of cloud service available, IaaS, PaaS, and SaaS. You've learned what the key characteristics of each service are, how they compare, what considerations you need to take into account when using them, and when you might use them.

Answers

Review Question 1

Which of the following describes a benefit of cloud services?

■ Economies of scale

☐ Fixed workloads

☐ Unpredictable costs

Explanation
Economies of scale. Economies of scale is the ability to do things more cheaply and more efficiently when operating at a larger scale in comparison to operating at a smaller scale.

Review Question 2

Which of the following refers to spending money upfront and then deducting that expense over time?

■ Capital expenditure

☐ Operational expenditures

☐ Supply and demand

Explanation
Capital expenditure. Capital expenditure refers to spending of money on physical infrastructure up front, and then deducting that expense from your tax bill over time.

Review Question 3

Which of the following terms refer to making a service available with no downtime for an extended period of time?

☐ Agility

☐ Fault tolerance

■ High availability

Explanation
`High availability keeps services up and running for long periods of time, with little downtime, depending on the service in question.`

Review Question 4

Which term from the list below would be viewed as benefits of using cloud services?

☐ Unpredictable costs

☐ Local reach only

■ Elasticity

Explanation
Elasticity, agility and economies of scale are the correct answers, and would be seen as benefits that you can gain from using cloud services.

Review Question 5

From the choices below, what is one of the advantages of moving your infrastructure to Azure?

■ The move reduces Capital Expenditures. (CapEx)

☐ The move reduces Operational Expenses (OpEx).

☐ The move allows for complete control of infrastructure resources.

Explanation
Public Cloud deployments reduce Capital Expenditures because there is far less infrastructure to buy; you effectively rent only what you use as you use it – CapEx is the best answer.

Review Question 6

Which cloud model provides the greatest degree of ownership and control?

☐ Hybrid

■ Private

☐ Public

Explanation
The private cloud provides the greatest degree of ownership and control.

Review Question 7

Which cloud model provides the greatest degree of flexibility?

☐ Public

☐ Private

■ Hybrid

Explanation
The hybrid cloud model provides the greatest degree of flexibility, as you have the option to choose either public or private depending on your requirements.

Review Question 8

Which of the following describes a public cloud?

☐ Is owned and operated by the organization that uses the resources from that cloud.

☐ Lets organizations run applications in the cloud or on-premises.

■ Provides resources and services to multiple organizations and users, who connect through a secure network connection.

Explanation
The public cloud provides resources and services to multiple organizations and users, who connect through a secure network connection.

Review Question 9

You have legacy applications that require specialized mainframe hardware and you have newer shared applications. Which cloud deployment model would be best for you?

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

Explanation
Hybrid cloud. A hybrid cloud is a public and private cloud combined. You can run your newer applications on commodity hardware you rent from the public cloud and maintain your specialized mainframe hardware on-premises.

Review Question 10

Which of the following requires the most user management of the cloud services?

- ■ Infrastructure as a Service
- ☐ Platform as a Service
- ☐ Software as a Service

Explanation
Infrastructure as a Service. Infrastructure as a Service requires the most user management of cloud services.

Review Question 11

Microsoft Office 365 is an example of?

- ☐ Infrastructure as a Service
- ☐ Platform as a Service
- ■ Software as a Service

Explanation
SaaS is typically licensed through a monthly or annual subscription.

Review Question 12

Which of the following describes Platform as a Service (PaaS)?

- ☐ Users are responsible for purchasing, installing, configuring, and managing their own software (operating systems, middleware, and applications).
- ■ Users create and deploy applications quickly without having to worry about managing the underlying infrastructure.
- ☐ Users pay an annual or monthly subscription.

Explanation
PaaS lets users create and deploy applications quickly without having to worry about managing the underlying infrastructure.

Review Question 13

Which of the following requires the most user management of the cloud services?

■ Infrastructure as a Service

☐ Platform as a Service

☐ Software as a Service

Explanation
Infrastructure as a Service requires the most user management of cloud services.

Review Question 14

You're developing an application and want to focus on building, testing, and deploying. You don't want to worry about managing the underlying hardware or software. Which cloud service type is best for you?

☐ Infrastructure as a Service (IaaS)

☐ Software as a Service (SaaS)

■ Platform as a Service (PaaS)

Explanation
Platform as a Service is the best choice here because the PaaS services handle the IT management tasks for you, so you can focus on writing code.

Review Question 15

You are running a virtual machine in a public cloud using IaaS. Which model correctly reflects how that resource is managed?

■ Shared responsibility model

☐ Cloud user management model

☐ User management model

Explanation
The shared responsibility model is the correct answer. Under the shared responsibility model, management of the resource is shared between the cloud provider and the end user. The cloud provider being responsible for the cloud services infrastructure and the end user being responsible for the service being configured and managed correctly.

Module 2 Core Azure services

Learning Objectives

Learning Objectives

After completing this module, you will be able to:

- Understand and describe core Azure architectural components.
- Understand and describe core Azure services and products.
- Understand and describe Azure solutions.
- Understand and describe Azure management tools.

Core Azure architectural components

Regions

Microsoft Azure is made up of datacenters located around the globe. These datacenters are organized and made available to end users by region. A **region**[1] is a geographical area on the planet containing at least one, but potentially multiple datacenters that are in close proximity and networked together with a low-latency network. Azure intelligently assigns and controls the resources within each region to ensure workloads are appropriately balanced.

A few examples of regions are *West US*, *Canada Central*, *West Europe*, *Australia East*, and *Japan West*. At the time of writing this, Azure is generally available in 55 regions and available in 140 countries.

Things to know about regions

- Azure has more global regions than any other cloud provider.
- Regions provide customers the flexibility and scale needed to bring applications closer to their users.
- Regions preserve data residency and offer comprehensive compliance and resiliency options for customers.
- For most Azure services, when you deploy a resource in Azure, you choose the region where you want your resource to be 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.

1 https://azure.microsoft.com/global-infrastructure/regions

Special Azure regions

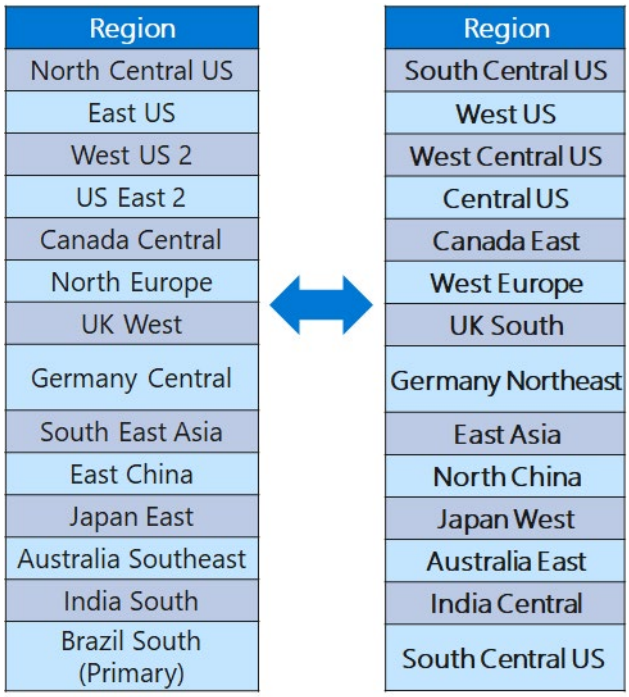
Azure has specialized regions that you might want to use when building out your applications for compliance or legal purposes. These include:

- *US DoD Central*, *US Gov Virginia*, *US Gov Iowa* and more: These 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.

✓ View the latest **Azure regions map.**[2]

Region Pairs

It's possible that a large enough disaster could cause an outage large enough to affect even two datacenters. That's why Azure creates region pairs. Each Azure region is paired with another region within the same geography (such as US, Europe, or Asia) at least 300 miles away, which together make a **region pair**[3]. The exception is Brazil South, which is paired with a region outside its geography.



Things to know about regional pairs:

- **Physical isolation**. When possible, Azure prefers at least 300 miles of separation between datacenters in a regional pair, although this isn't practical or possible in all geographies. Physical datacenter separation reduces the likelihood of natural disasters, civil unrest, power outages, or physical network outages affecting both regions at once.

2 https://azure.microsoft.com/global-infrastructure/regions
3 https://docs.microsoft.com/azure/best-practices-availability-paired-regions?azure-portal=true

- **Platform-provided replication**. Some services such as Geo-Redundant Storage provide automatic replication to the paired region.
- **Region recovery order**. In the event of a broad outage, recovery of one region is prioritized out of every pair. Applications that are deployed across paired regions are guaranteed to have one of the regions recovered with priority.
- **Sequential updates**. Planned Azure system updates are rolled out to paired regions sequentially (not at the same time) to minimize downtime, the effect of bugs, and logical failures in the rare event of a bad update.

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.

✓ View the complete list of **region pairs**[4].

Geographies

Azure divides the world into *geographies* that are defined by geopolitical boundaries or country borders. An Azure **geography**[5] is a discrete market typically containing two or more regions that preserves data residency and compliance boundaries.

This division has several benefits.

- Geographies allow customers with specific data residency and compliance needs to keep their data and applications close.
- Geographies ensure that data residency, sovereignty, compliance, and resiliency requirements are honored within geographical boundaries.
- Geographies are fault-tolerant to withstand complete region failure through their connection to dedicated high-capacity networking infrastructure.

Tip - Data residency refers to the physical or geographic location of an organization's data or information. It defines the legal or regulatory requirements imposed on data based on the country or region in which it resides and is an important consideration when planning out your application data storage.

Geographies are broken up into the following areas:

- Americas
- Europe
- Asia Pacific

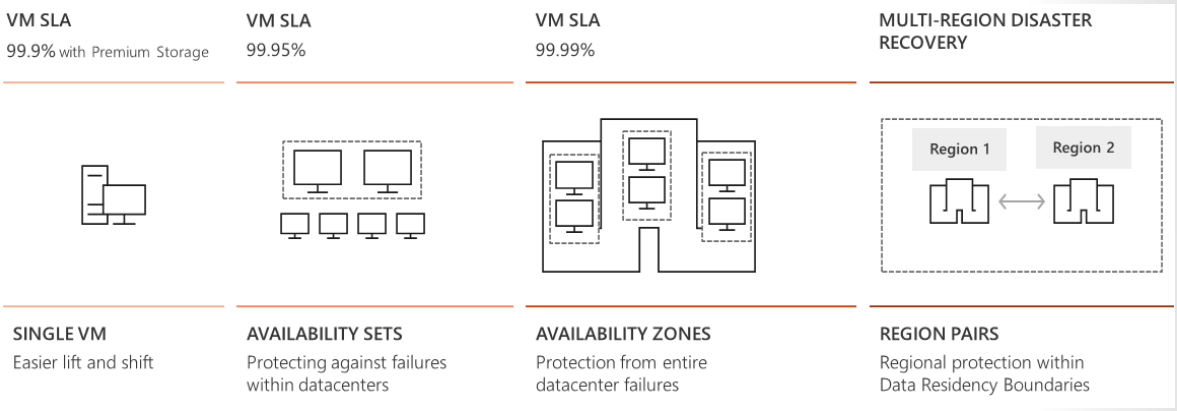
4 https://docs.microsoft.com/azure/best-practices-availability-paired-regions#what-are-paired-regions?azure-portal=true
5 https://azure.microsoft.com/global-infrastructure/geographies?azure-portal=true

- Middle East and Africa

✓ Each region belongs to a single geography and has specific service availability, compliance, and data residency/sovereignty rules applied to it. Check the documentation for more information (a link is available in the summary unit).

Availability options

Availability Options

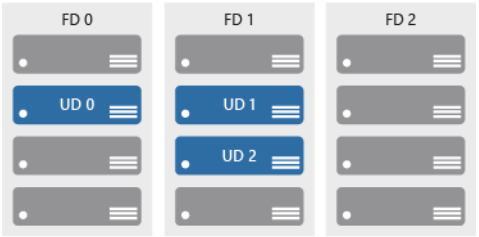


- A single virtual machine with premium storage has an SLA of 99.9%. You can quickly migrate existing virtual machines to Azure through "lift and shift". Lift and shift is a no-code option where each application is migrated as-is providing the benefits of the cloud without the risks or costs of making code changes.
- By placing virtual machines in an availability set you protect against datacenter failures and increases the SLA to 99.95%.
- Adding virtual machines to availability zones protects from entire datacenter failures and increases the SLA to 99.99%. This is highest level of protection that is provided.
- For multi-region disaster recovery region pairs protects and provides data residency boundaries.

Availability sets

Availability sets are a way for you to ensure your application remains online if a high-impact maintenance event is required, or a hardware a failure occurs.

Availability sets are made up of **Update domains (UD)** and **Fault domains (FD)**.



- **Update domains**. When a maintenance event occurs (such as a performance update or critical security patch applied to the host), the update is sequenced through update domains. Sequencing updates using update domains ensures that the entire datacenter isn't unavailable during platform

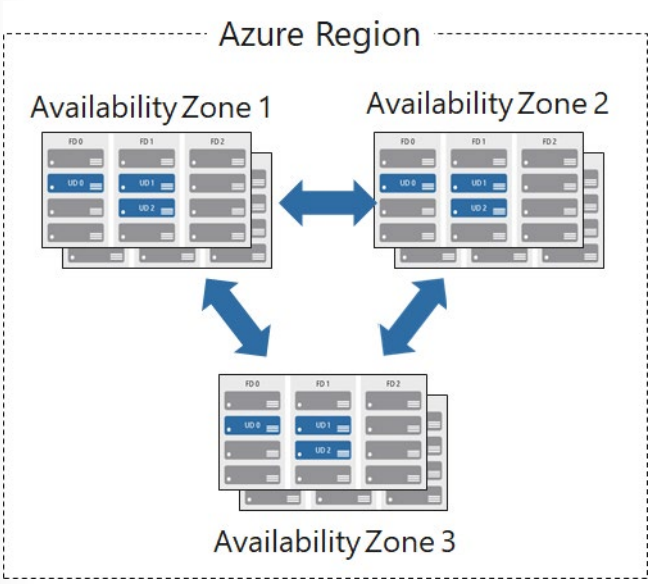
updates and patching. Update domains are a logical section of the datacenter, and they are implemented with software and logic.

- **Fault domains**. Fault domains provide for the physical separation of your workload across different hardware in the datacenter. This includes power, cooling, and network hardware that supports the physical servers located in server racks. In the event the hardware that supports a server rack becomes unavailable, only that rack of servers would be affected by the outage.

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, this requires creating duplicate hardware environments. Azure can help make your app highly available through Availability Zones.

Availability zones[6] are physically separate locations within an Azure region that use availability sets to provide additional fault tolerance.



Tip - The list of supported regions is expanding - check the documentation for the latest information.

Availability Zone features

- Each availability zone is an isolation boundary containing one or more datacenters equipped with independent power, cooling, and networking.
- If one availability zone goes down, the other continues working.
- The availability zones are typically connected to each other through very fast, private fiber-optic networks.
- Availability zones allow customers to run mission-critical applications with high availability and low-latency replication.
- Availability zones are offered as a service within Azure, and to ensure resiliency, there's a minimum of three separate zones in all enabled regions.

✓ Regions that support Availability Zones include *Central US*, *North Europe*, *SouthEast Asia*, and more.

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

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.

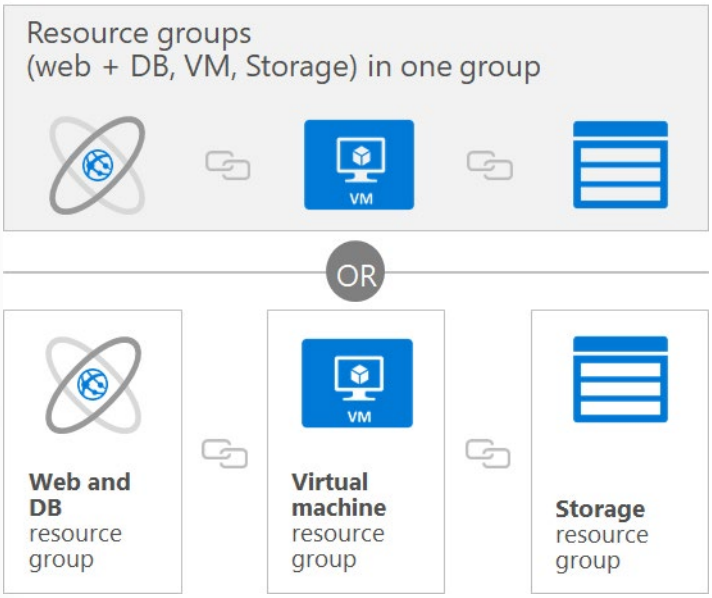
Resource Groups

A **resource group** is a unit of management for your resources in Azure. You can think of your resource group as a container that allows you to aggregate and manage all the resources required for your application in a single manageable unit. This allows you to manage the application collectively over its lifecycle, rather than manage components individually. Before any resource can be provisioned, you need a resource group for it to be placed in.

You can manage and apply the following resources at resource group level:

- Metering and billing
- Policies
- Monitoring and alerts
- Quotas
- Access control

Remember that when you delete a resource group you delete all resources contained within it.



Considerations

When creating and placing resources within resource groups there are a few considerations:

- Each resource must exist in one, and only one, resource group.
- A resource group can contain resources that reside in different regions.
- You decide how you want to allocate resources to resource groups based on what makes the most sense for your organization.
- You can add or remove a resource to a resource group at any time.
- You can move a resource from one resource group to another.
- Resources for an application do not need to exist in the same resource group. However, it is recommended that you keep them in the same resource group for ease of management.

✓ Do you have a strategy on how you will organize your Azure resources?

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 we'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.

Create a Resource Group

Resource groups can be created by using the following methods:

- Azure portal
- Azure PowerShell
- Azure CLI
- Templates
- Azure SDKs (like .NET, Java)

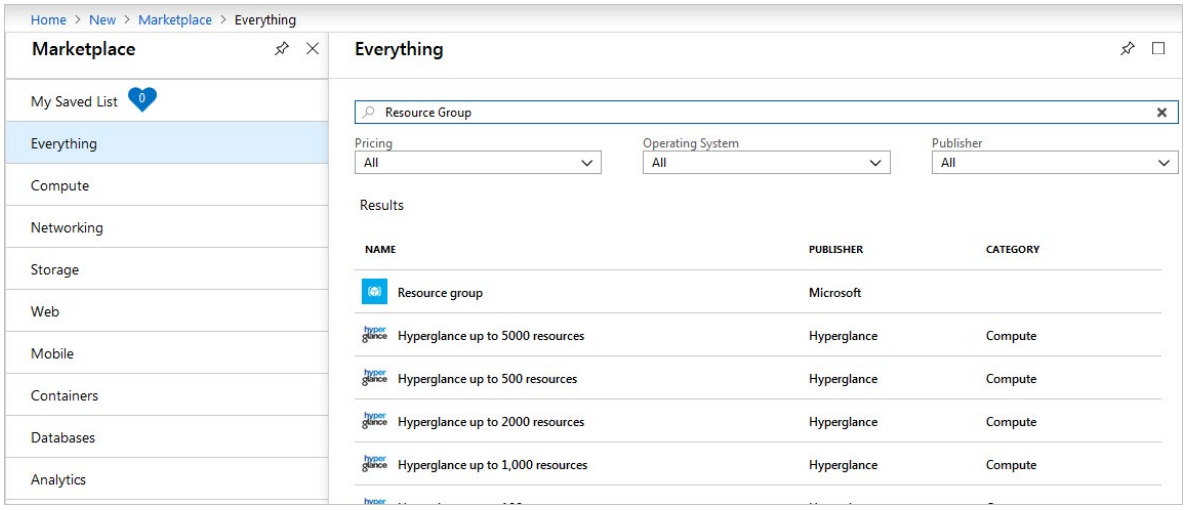
Let's walk through the steps you'd take to create a resource group in the Azure portal. If you'd like to follow along in your own subscription, you may.

1. Open a web browser and sign into the **Azure portal**[7].

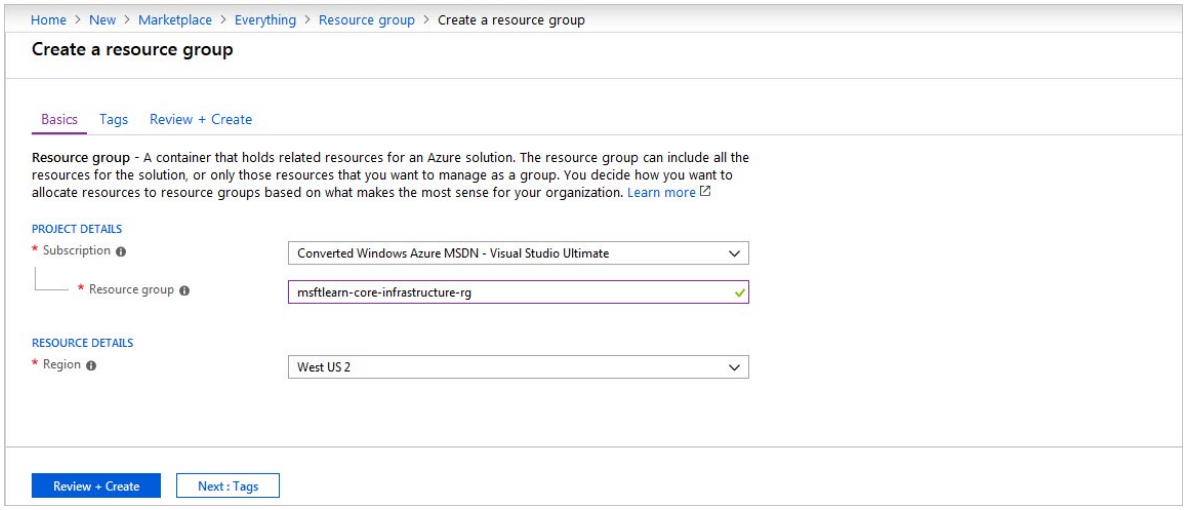
   Important - Make sure to use your *own* subscription. When you are in the free sandbox environment, it will not allow you to create resource groups. You can tell which subscription you are using by looking at the tenant name under your profile picture. You can switch tenants by selecting your profile picture and selecting **Switch Directory** from the options menu.

2. On the Azure portal menu or from the **Home** page, select **Create a resource**.
3. Type **Resource Group** in the search box and hit Enter.
4. The first item in the list should be the resource group resource. Select it and then select the **Create** button.

7 https://portal.azure.com/?azure-portal=true



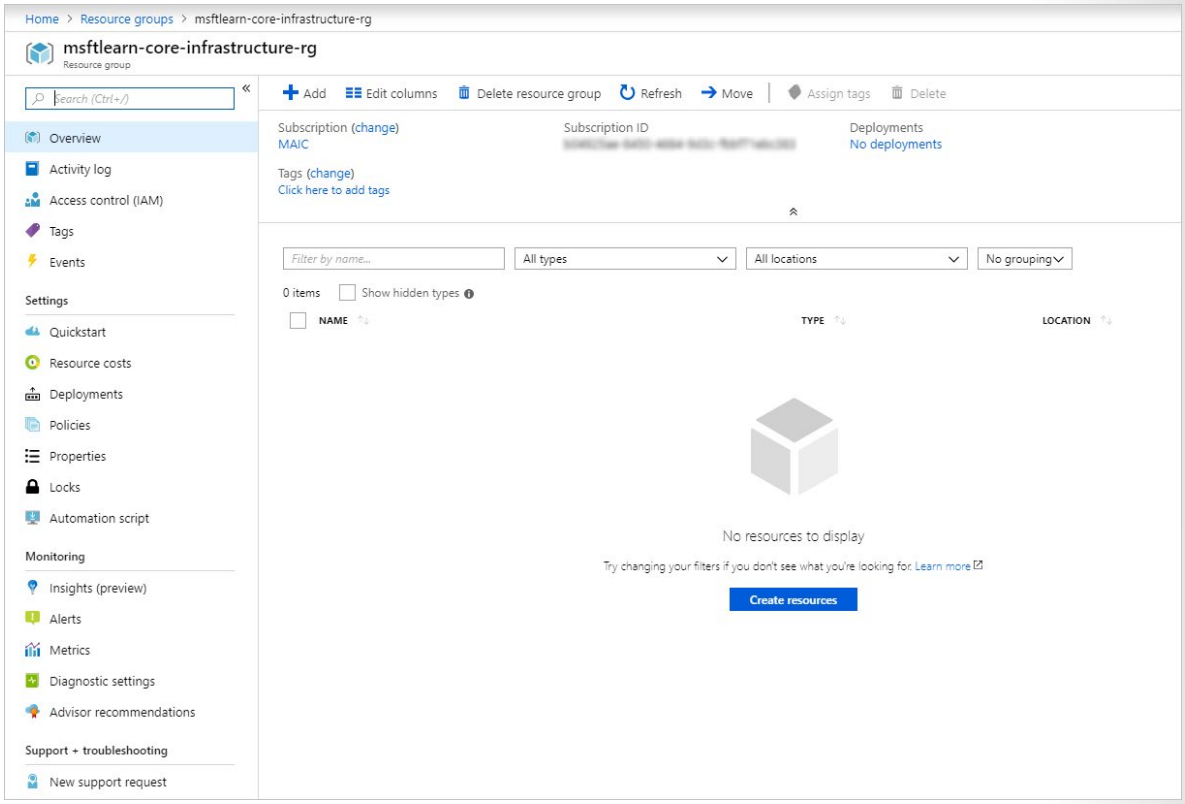
5. Enter your resource group name, let's use **msftlearn-core-infrastructure-rg**. Select the subscription it should be in, and select the region for the resource group. Select **Review + Create** and then **Create** to create the resource group.



That's it, you've created a resource group that you can now use when you deploy Azure resources. Let's take a closer look at this resource group and some important things to consider.

Explore a resource group and add a resource

On the Azure portal menu or from the **Home** page, select **Resource groups**, and select your newly created resource group. Note that you may also see a resource group called **NetworkWatcherRG**. You can ignore this resource group, it's created automatically to enable Network Watcher in Azure virtual networks.



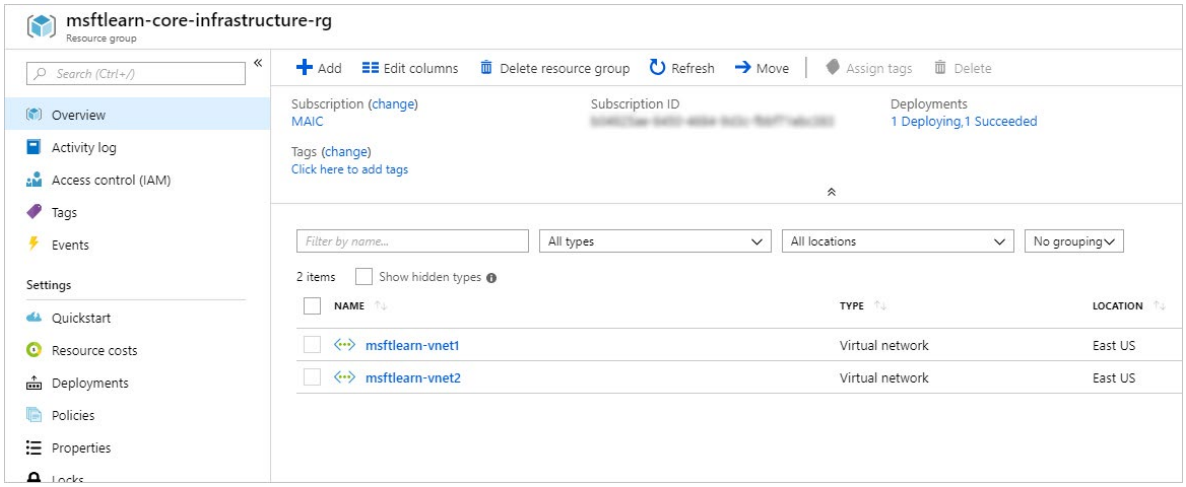
On the Overview panel, there's the basic information about the resource group like the subscription it's in, the subscription ID, any tags that are applied, and a history of the deployments to this resource group. We'll cover tags in the next unit. The deployments link takes you to a new panel with the history of all deployments to this resource group. Anytime you create a resource, it's a deployment, and you see that history for the resource group here.

Across the top you can add more resources, change the columns in the list, move the resource group to another subscription, or delete it entirely.

On the left menu, there are a number of options

We don't have any resources in this resource group yet, so the list at the bottom is empty. Let's create a couple resources inside the resource group.

1. Select **+ Add** at the top or select the **Create resources**, either will work.
2. Search for **Virtual network**. The first result should be the virtual network resource. Select it, and on the next screen select **Create**.
3. Name the virtual network **msftlearn-vnet1**. For the **Resource group** drop-down, select the resource group that you created earlier. Enter **192.168.0.0/24** for both the **Address space** and subnet **Address range**. Leave the defaults for all other options, and select **Create**.
4. Repeat the steps again to create one more VNet, where both the **Address space** and subnet **Address range** are for a different network than your previous network, (e.g. **192.168.100.0/24**). Name it **msftlearn-vnet2**, and make sure to place it in the resource group that you created earlier.
5. Go back to your resource group, and on the **Overview** panel you should see the two VNets you created.



Our resource group now contains two virtual network resources because we specified in our deployment (when we created the resources) which resource group we wanted the VNet to be placed in. We could create additional resources inside this resource group, or we could create additional resource groups in the subscription to deploy resources into.

When creating resources, you usually have the option to create a new resource group as an alternative to using an existing resource group. This simplifies the process a bit, but as you see in your new organization, can lead to resources spread across resource groups with little thought as to how to organize them.

Use resource groups for organization

So how can you use resource groups to your advantage in your new organization? There are some guidelines and best practices that can help with the organization.

Consistent naming convention

You can start with using an understandable naming convention. We named our resource group **msftlearn-core-infrastructure-rg**. We've given some indication of what it's used for (**msftlearn**), the types of resources contained within (**core-infrastructure**), and the type of resource it is itself (**rg**). This descriptive name gives us a better idea of what it is. If we had named it **my-resource-group** or **rg1**, we have no idea on a glance of what the usage may be. In this case, we can deduce that there are probably core pieces of infrastructure contained within. If we created additional VNets, storage accounts, or other resources the company may consider *core infrastructure*, we could place them here as well, to improve the organization of our resources. Naming conventions can vary widely between and even within companies, but some planning can help.

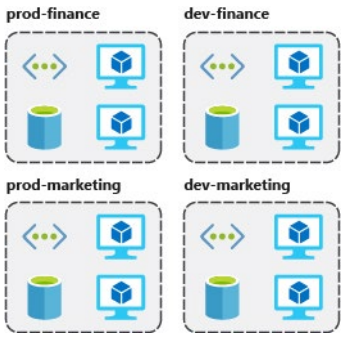
Organizing principles

Resource groups can be organized in a number of ways, let's take a look at a few examples. We might put all resources that are *core infrastructure* into this resource group. But we could also organize them strictly by resource type. For example, put all VNets in one resource group, all virtual machines in another resource group, and all Azure Cosmos DB instances in yet another resource group.

We could organize them by environment (prod, qa, dev). In this case, all production resources are in one resource group, all test resources are in another resource group, and so on.

We could organize them by department (marketing, finance, human resources). Marketing resources go in one resource group, finance in another resource group, and HR in a third resource group.

We could even use a combination of these strategies and organize by environment and department. Put production finance resources in one resource group, dev finance resources in another, and the same for the marketing resources.



There are a few factors that can play into the strategy you use to organize resources: authorization, resource life cycle, and billing.

Organizing for authorization

Since resource groups are a scope of RBAC, you can organize resources by *who* needs to administer them. If your database administration team is responsible for managing all of your Azure SQL Database instances, putting them in the same resource group would simplify administration. You could give them the proper permissions at the resource group level to administer the databases within the resource group. Similarly, the database administration team could be denied access to the resource group with virtual networks, so they don't inadvertently make changes to resources outside the scope of their responsibility.

Organizing for life cycle

We mentioned earlier that resource groups serve as the life cycle for the resources within it. If you delete a resource group, you delete all the resources in it. Use this to your advantage, especially in areas where

resources are more disposable, like non-production environments. If you deploy 10 servers for a project that you know will only last a couple of months, you might put them all in a single resource group. One resource group is easier to clean up than 10 or more resource groups.

Organizing for billing

Lastly, placing resources in the same resource group is a way to group them for usage in billing reports. If you're trying to understand how your costs are distributed in your Azure environment, grouping them by resource group is one way to filter and sort the data to better understand where costs are allocated.

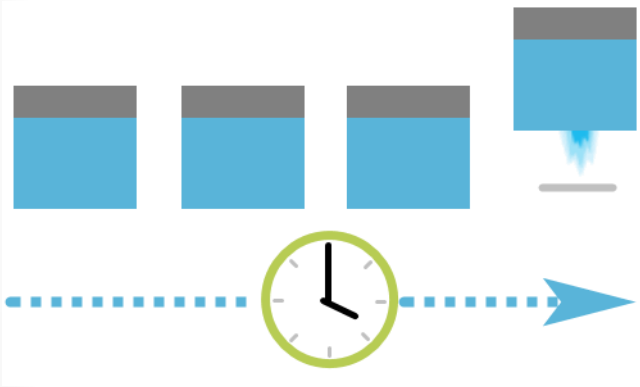
✓ The bottom line is that you have flexibility in how to organize resources in your resource groups. Put some thought into it so that you have a coherent approach to how you use resource groups in your Azure environment.

Azure Resource Manager

Azure Resource Manager[8] is a management layer in which resource groups and all the resources within it are created, configured, managed, and deleted. It provides a consistent management layer which allows you automate the deployment and configuration of resources using different automation and scripting tools, such as Microsoft Azure PowerShell, Azure Command-Line Interface (Azure CLI), Azure portal, REST API, and client SDKs.

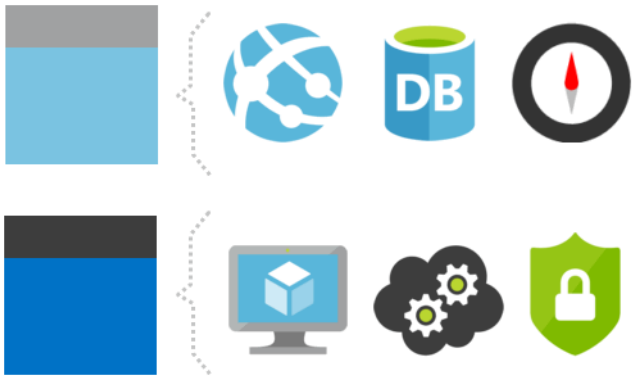
With Azure Resource Manager, you can:

- **Deploy Application resources**. Update, manage, and delete all the resources for your solution in a single, coordinated operation.



- **Organize resources**. Manage your infrastructure through declarative templates rather than scripts. You can view which resources are linked by a dependency, and you can apply tags to resources to categorize them for management tasks, such as billing.

8 https://azure.microsoft.com/features/resource-manager?azure-portal=true



- **Control access and resources**. You can control who in your organization can perform actions on the resources. You manage permissions by defining roles, adding users or groups to the roles, and applying policies at resource group level. Examples of elements you may wish to control are: enforcing naming convention on resources, limiting which types and instances of resources can be deployed, or limiting which regions can host a type of resource.

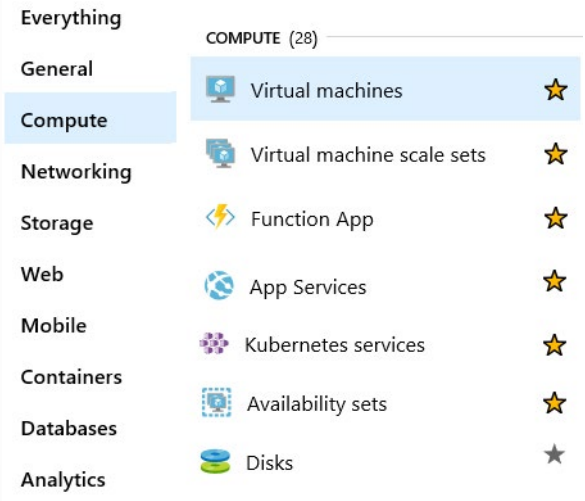
Core Azure services and products

Azure compute

Azure compute[9] 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 resources 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.

There are many compute services two of the most common are: virtual machines and containers.



Azure Compute Services

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 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 Machine Scale Sets, App Services, and Azure Functions.

Explore Azure virtual machines

9 https://azure.microsoft.com/product-categories/compute?azure-portal=true

Azure virtual machines[10] 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.

Virtual machine scale sets

Virtual machine scale sets[11] 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.

App services

With **App services**[12], 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[13] 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.

Walkthrough-Create a virtual machine

In this walkthrough, we will create a virtual machine in the Azure Portal, connect to the virtual machine, install the web server role and test.

10 https://azure.microsoft.com/services/virtual-machines/?azure-portal=true
11 https://azure.microsoft.com/services/virtual-machine-scale-sets?azure-portal=true
12 https://azure.microsoft.com/services/app-service?azure-portal=true
13 https://azure.microsoft.com/services/functions?azure-portal=true

Task 1: Create the virtual machine

In this task, we will create a Windows Server 2016 Datacenter virtual machine.

Task 2: Connect to the virtual machine

In this task, we will connect to our new virtual machine using RDP.

Task 3: Install the web server role and test

In this task, install the Web Server role on the server and ensure the default IIS welcome page can be displayed.

Congratulations! You have created a web server that can be connected to publicly via this IP address, or via the fully qualified domain name. If you had a web page to host you could deploy those source files to the virtual machine and host them for public access on the deployed virtual machine.

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.

Container Services

If you wish to run multiple instances of an application on a single host machine, containers are an excellent choice. The container orchestrator can start, stop, and scale out application instances as needed.

Containers are a virtualization environment.

- Containers reference the operating system of the host environment that runs the container.
- Unlike virtual machines you do not manage the operating system.
- Containers are lightweight and are designed to be created, scaled out, and stopped dynamically.
- Containers allows you to respond to changes on demand and quickly restart in case of a crash or hardware interruption.
- Azure supports Docker containers.

There are two ways to manage both Docker and Microsoft-based containers in Azure.

Azure Container Instances

Azure Container Instances[14] 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

14 https://azure.microsoft.com/services/container-instances?azure-portal=true

The task of automating, managing, and interacting with a large number of containers is known as orchestration. **Azure Kubernetes Service (AKS)**[15] 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.

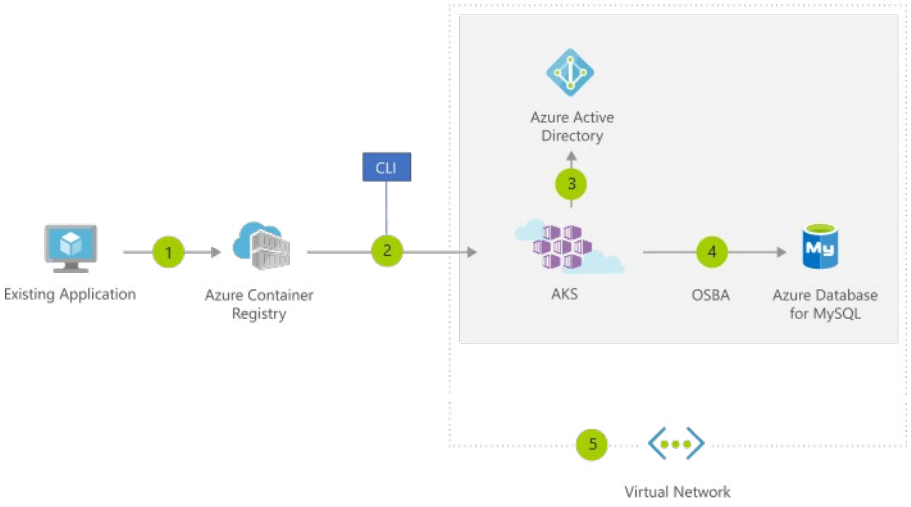
Using containers in your solutions

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.

Migrating apps to containers

You can move existing applications to containers and run them within AKS. You can control access via integration with Azure Active Directory (Azure AD) and access Service Level Agreement (SLA)–backed Azure services, such as Azure Database for MySQL for any data needs, via Open Service Broker for Azure (OSBA).



The preceding figure depicts this process as follows:

1. You convert an existing application to one or more containers and then publish one or more container images to the Azure Container Registry.
2. By using the Azure portal or the command line, you deploy the containers to an AKS cluster.
3. Azure AD controls access to AKS resources.
4. You access SLA-backed Azure services, such as Azure Database for MySQL, via OSBA.

15 https://azure.microsoft.com/services/kubernetes-service?azure-portal=true

5. Optionally, AKS is deployed with a virtual network.

Walkthrough-Deploy Azure Container Instances

In this walkthrough we create, configure, and deploy a Docker container to Azure Container Instances (ACI) in the Azure Portal. The container is a Welcome to ACI web application that displays a static HTML page.

Task 1: Create a container instance

In this task, we will create a new container instance for the web application.

Task 2: Deploy the container and test

In this task, we will deploy the container instance and ensure the welcome page displays.

Congratulations! You have used Azure Portal to successfully deploy an application to a container in Azure Container Instance.

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.

Azure Networking

Azure Networking[16] allows you to connect cloud and on-premises infrastructure and services to provide your customers and users the best possible experience. Once the resources move to Azure, they require the same networking functionality as an on-premises deployment. In specific scenarios, they may require some level of network isolation. Azure networking components offer a range of functionality and services that can help organizations design and build cloud infrastructure services that meet their requirements.

Some of the most common networking service types in Azure are discussed in the following sections.

Azure Virtual Network

Azure Virtual Network[17] enables many types of Azure resources such as Azure VMs to securely communicate with each other, the internet, and on-premises networks. A virtual network is scoped to a single region; however, multiple virtual networks from different regions can be connected using virtual network peering. With Azure Virtual Network you can provide isolation, segmentation, communication with on-premises and cloud resources, routing and filtering of network traffic.

Azure Load Balancer

16 https://azure.microsoft.com/product-categories/networking?azure-portal=true
17 https://docs.microsoft.com/azure/virtual-network?azure-portal=true

Azure Load Balancer[18] can provide scale for your applications and create high availability for your services. Load Balancer supports inbound and outbound scenarios, provides low latency and high throughput, and scales up to millions of flows for all Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) applications. You can use Load Balancer with incoming internet traffic, internal traffic across Azure services, port forwarding for specific traffic, or outbound connectivity for VMs in your virtual network.

VPN gateway

A **VPN gateway**[19] is a specific type of virtual network gateway that is used to send encrypted traffic between an Azure Virtual Network and an on-premises location over the public internet. It provides a more secure connection from on-premises to Azure over the internet.

Azure Application Gateway

Azure Application Gateway[20] is a web traffic load balancer that enables you to manage traffic to your web applications. It is the connection through which users connect to your application. With Application Gateway you can route traffic based on source IP address and port to a destination IP address and port. You also can help protect a web application with a web application firewall, redirection, session affinity to keep a user on the same server, and many more configuration options.

Content Delivery Network

A **Content Delivery Network (CDN)**[21] is a distributed network of servers that can efficiently deliver web content to users. It is a way to get content to users in their local region to minimize latency. CDN can be hosted in Azure or any other location. You can cache content at strategically placed physical nodes across the world and provide better performance to end users. Typical usage scenarios include web applications containing multimedia content, a product launch event in a region, or any event where you expect a high bandwidth requirement in a region.

Walkthrough-Create a virtual network

In this walkthrough, we will create a virtual network, deploy two virtual machines onto that virtual network and then configure them to allow one virtual machine to ping the other over that virtual network.

18 https://azure.microsoft.com/services/load-balancer?azure-portal=true
19 https://azure.microsoft.com/services/vpn-gateway?azure-portal=true
20 https://azure.microsoft.com/services/application-gateway?azure-portal=true
21 https://azure.microsoft.com/services/cdn?azure-portal=true

Task 1: Create a virtual network

In this task, we will create a new virtual network.

Task 2: Create two virtual machines

In this task, we will create two virtual machines in the virtual network.

Task 3: Test the connection

In this task, we will allow ICMP connections and test that the virtual machines can communicate (ping) each other.

Congratulations! You have configured and deployed two virtual machines in a virtual network. You have also configured the firewall so one of the virtual machines allows ping requests.

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.

Azure Data Categories

You can generally think of data as **structured**, **semi-structured**, and **unstructured**.

Structured data

- Structured data is data that adheres to a schema, so all the data has the same fields or properties.
- Structured data can be stored in a database table with rows and columns.
- Structured data relies on keys to indicate how one row in a table relates to data in another row of another table.
- Structured data is also known as *relational data*. The data's schema defines the table of data, the fields in the table, and the clear relationship between the two.
- Structured data is easy to enter, query, and analyze because all the data follows the same format.
- Examples of structured data include sensor data or financial data.

Semi-structured data

- Semi-structured data is less organized than structured data.
- Semi-structured data is not stored in a relational format, meaning the fields do not neatly fit into tables, rows, and columns.
- Semi-structured data contains tags that make the organization and hierarchy of the data apparent.
- Semi-structured data is also known as *non-relational* or *NoSQL* data.
- Examples of semi-structured data include books, blogs, and HTML documents.

Unstructured data

- Unstructured data has no designated structure.
- Unstructured data can hold any kind of data.
- Unstructured data is becoming more prominent as businesses try to tap into new data sources.

- Examples of unstructured data include a PDF document, a JPG image, a JSON file, and video content.

✓ There are different Azure products to support each data type.

Azure Storage

Azure Storage[22] 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 store for working data. Such stores can be used by websites, mobile apps, desktop applications, and many other types of custom solutions. Azure Storage is also used by IaaS virtual machines, and PaaS cloud services.

Some of the most common storage service types in Azure are **disks**, **files**, **objects**, **queues**, and **tables**.

Disk storage

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 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 abilities. Details on pricing are available on the Managed Disks pricing page.

Containers (Blobs)

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.

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.

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

Files

Azure Files enables you to set up highly available network file shares that can be accessed by using the standard Server Message Block (SMB) protocol. That means that multiple VMs can share the same files with both read and write access. You can also read the files using the REST interface or the storage client libraries.

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 and includes a shared access signature (SAS) token. You can generate SAS tokens; they allow specific access to a private asset for a specific amount of time.

File shares 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.

Queues

The Azure Queue service is used to store and retrieve messages. Queue messages can be up to 64 KB in size, and a queue can contain millions of messages. Queues are generally used to store lists of messages to be processed asynchronously.

For example, say you want your customers to be able to upload pictures, and you want to create thumbnails for each picture. You could have your customer wait for you to create the thumbnails while uploading the pictures. An alternative would be to use a queue. When the customer finishes their upload, write a message to the queue. Then have an Azure Function retrieve the message from the queue and create the thumbnails. Each of the parts of this processing can be scaled separately, giving you more control when tuning it for your usage.

Tables

Azure Table storage stores large amounts of structured data. The service is a NoSQL datastore which accepts authenticated calls from inside and outside the Azure cloud. Azure tables are ideal for storing structured, non-relational data. Common uses of Table storage include:

- Storing TBs of structured data capable of serving web scale applications.
- Storing datasets that don't require complex joins, foreign keys, or stored procedures and can be denormalized for fast access.
- Quickly querying data using a clustered index.

You can use Table storage to store and query huge sets of structured, non-relational data, and your tables will scale as demand increases.

Walkthrough-Create Blob storage

In this walkthrough, we will create a storage account, then work with blob storage files.

Task 1: Create a storage account

In this task, we will create a new storage account.

Task 2: Work with blob storage

In this task, we will create a Blob container and upload a blob file.

Task 3: Monitor the storage account

In this task, we will review the storage troubleshooter and Insights pages.

Congratulations! You have created a storage account, then worked with blob storage files.

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.

Azure Database Services

Azure database services are fully managed PaaS database services that free up valuable time you'd otherwise spend managing your database. Enterprise-grade performance with built-in high availability means you can scale quickly and reach global distribution without worrying about costly downtime. Developers can take advantage of industry-leading innovations such as built-in security with automatic monitoring and threat detection, automatic tuning for improved performance, and turnkey global distribution.

Some of the most common data service types in Azure as follows:

Azure Cosmos DB

Microsoft Azure Cosmos DB[23] is a globally distributed database service that enables you to elastically and independently scale throughput and storage across any number of Azure's geographic regions. It supports schema-less data that lets you build highly responsive and Always On applications to support

23 https://azure.microsoft.com/services/cosmos-db?azure-portal=true

constantly changing data. You can use Cosmos DB to store data that is updated and maintained by users around the world. It makes it easy to build scalable, highly responsive applications at global scale.

Azure SQL Database

Azure SQL Database[24] is a relational database as a service (DaaS) based on the latest stable version of Microsoft SQL Server database engine. SQL Database is a high-performance, reliable, fully managed and secure database that you can use to build data-driven applications and websites in the programming language of your choice without needing to manage infrastructure.

Azure Database Migration

The Azure Database Migration Service[25] is a fully managed service designed to enable seamless migrations from multiple database sources to Azure data platforms with minimal downtime (online migrations). The service uses the Microsoft Data Migration Assistant to generate assessment reports that provide recommendations to help guide you through required changes prior to performing a migration. Once you assess and perform any remediation required, you're ready to begin the migration process. The Azure Database Migration Service performs all of the required steps.

✓ These are just a few of our database service offerings. Take a minute to review other database services and **find the product you need**[26].

Walkthrough-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.

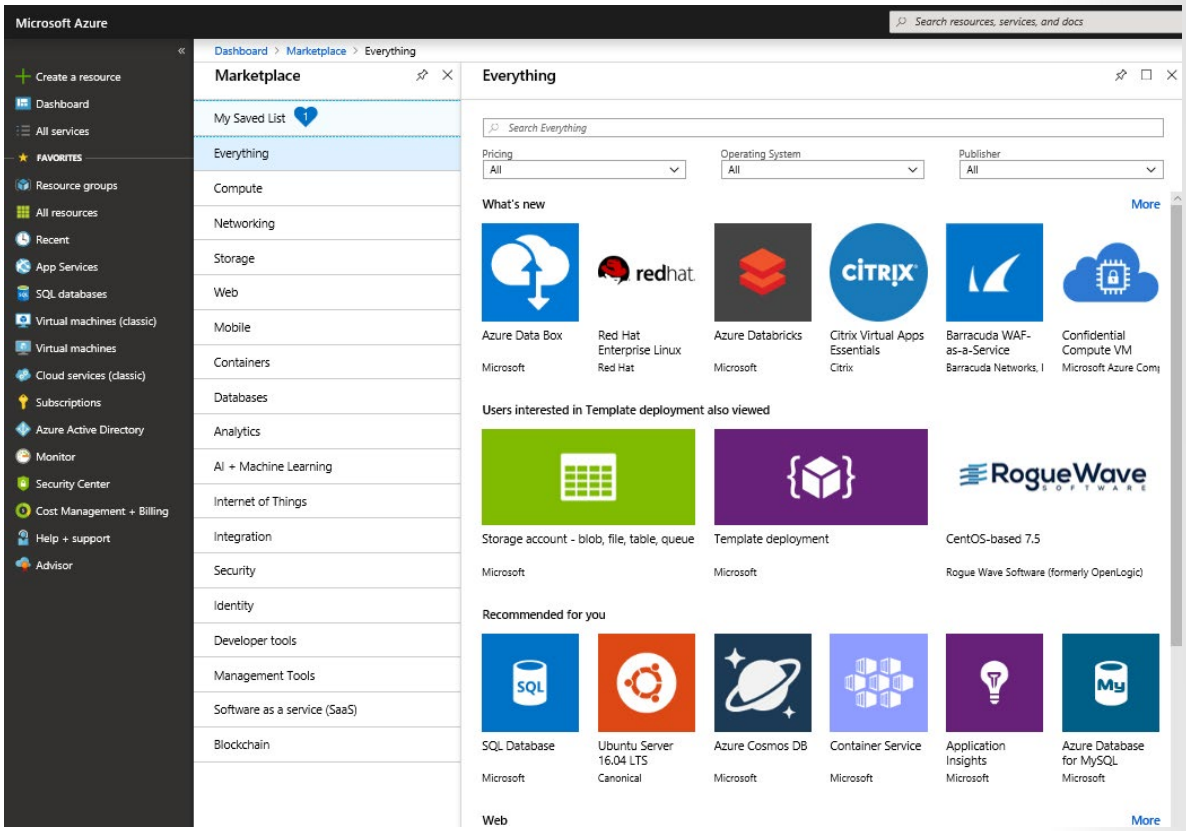
Congratulations! You have created a SQL database in Azure and successfully queried the data in that database.

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.

24 https://azure.microsoft.com/services/sql-database?azure-portal=true
25 https://azure.microsoft.com/services/database-migration?azure-portal=true
26 https://azure.microsoft.com/product-categories/databases/

Azure Marketplace

Azure Marketplace[27] 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.



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.

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

Azure Solutions

Internet of Things (IoT)

People can 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. The **Internet of Things (IoT)**[28] is the ability for devices to garner and then relay information for data analysis.

There are many services that can assist and drive end-to-end solutions for IoT on Azure. Two of the core Azure IoT service types are **Azure IoT Central**, and **Azure IoT Hub**.

IoT Central

IoT Central[29] is a fully managed global IoT software as a service (SaaS) solution that makes it easy to connect, monitor, and manage your IoT assets at scale. No cloud expertise is required to use IoT Central. As a result, you can bring your connected products to market faster while staying focused on your customers.

Azure IoT Hub

Azure IoT Hub[30] 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. IoT Hub monitoring helps you maintain the health of your solution by tracking events such as device creation, device failures, and device connections.

IoT Hub's capabilities help you build scalable, full-featured IoT solutions such as managing industrial equipment used in manufacturing, tracking valuable assets in healthcare, and monitoring office building usage.

✓ These are just two of our IoT offerings. Use the **IoT Product Selector**[31] to determine what product is best for your situation.

28 https://azure.microsoft.com/product-categories/iot/
29 https://azure.microsoft.com/services/iot-central/
30 https://azure.microsoft.com/services/iot-hub
31 https://azure.microsoft.com/overview/iot/product-selector/

Walkthrough-Implement the Azure IoT Hub

In this walkthrough, we will configure a new Azure IoT Hub in Azure Portal, and then authenticate a connection to an IoT device using the online Raspberry Pi device simulator. Sensor data and messages are passed from the Raspberry Pi simulator to your Azure IoT Hub, and you view metrics for the messaging activity in Azure Portal.

Task 1: Create an IoT hub

In this task, we will create an IoT hub.

Task 2: Add an IoT device

In this task, we will add an IoT device to the IoT hub.

Task 3: Test the device using the Raspberry Pi Simulator

In this task, we will test our device using the Raspberry Pi Simulator.

Congratulations! You have set up Azure IoT Hub to collect sensor data from an IoT device.

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.

Big Data and Analytics

Data comes in all types of forms and formats. When we talk about Big Data, we're referring to *large* volumes of data. Data from weather systems, communications systems, imaging platforms, and many other scenarios 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 SQL Data Warehouse, HDInsight, and Data Lake Analytics.

Azure Synapse Analytics

Azure Synapse Analytics[32] (formerly Azure SQL Data Warehouse) is a limitless analytics service that brings together enterprise data warehousing and Big Data analytics.

Azure HDInsight

Azure HDInsight[33] 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 run popular open-source frameworks and create cluster types such as **Apache Spark**[34], **Apache Hadoop**[35], **Apache Kafka**[36], **Apache HBase**[37], **Apache Storm**[38], **Machine Learning Services**[39]. HDInsight

32 https://docs.microsoft.com/azure/sql-data-warehouse/
33 https://azure.microsoft.com/services/hdinsight/
34 https://docs.microsoft.com/azure/hdinsight/spark/apache-spark-overview
35 https://docs.microsoft.com/azure/hdinsight/hadoop/apache-hadoop-introduction
36 https://docs.microsoft.com/azure/hdinsight/kafka/apache-kafka-introduction
37 https://docs.microsoft.com/azure/hdinsight/hbase/apache-hbase-overview
38 https://docs.microsoft.com/azure/hdinsight/storm/apache-storm-overview
39 https://docs.microsoft.com/azure/hdinsight/r-server/r-server-overview

also supports a broad range of scenarios such as extraction, transformation, and loading (ETL); data warehousing; machine learning; and IoT.

Azure Data Lake Analytics

Azure Data Lake Analytics[40] 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.

✓ For a full list of big data and analytics services available with Azure, visit the page **Analytics**[41].

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 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:

Azure Machine Learning Service

The **Azure Machine Learning service**[42] provides a cloud-based environment you can use to develop, train, test, deploy, manage, and track machine learning models. It fully supports open-source technologies, so you can use tens of thousands of open-source Python packages with machine learning components such as *TensorFlow* and *scikit-learn*. Rich tools, such as *Jupyter notebooks* or the *Visual Studio Code Tools for AI*, make it easy to interactively explore data, transform it, and then develop, and test models. Azure Machine Learning service also includes features that automate model generation and tuning to help you create models with ease, efficiency, and accuracy.

The Azure Machine Learning service 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. When you have the right model, you can easily deploy it in a container such as Docker in Azure. Use Machine Learning service if you work in a Python environment, you want more control over your machine learning algorithms, or you want to use open-source machine learning libraries.

40 https://azure.microsoft.com/services/data-lake-analytics/
41 https://azure.microsoft.com/product-categories/analytics/
42 https://azure.microsoft.com/services/machine-learning-service/

Azure Machine Learning Studio

Azure Machine Learning Studio[43] is a collaborative, drag-and-drop visual workspace where you can build, test, and deploy machine learning solutions without needing to write code. It uses pre-built and pre-configured machine learning algorithms and data-handling modules. Use Machine Learning Studio when you want to experiment with machine learning models quickly and easily, and the built-in machine learning algorithms are enough for your solutions. It does not provide as much control over machine learning algorithms as the Machine Learning Service we discussed earlier.

Note: A full list of **Artificial Intelligence and Machine Learning services**[44] is available.

Serverless computing

Serverless computing[45] is a cloud-hosted execution environment that runs your code but abstracts the underlying hosting environment. 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.

Some of the most common serverless service types in Azure are Azure Functions, Azure Logic Apps, and Azure Event Grid.

Azure Functions

Azure Functions[46] are ideal when you're only concerned with the code running your service and not the underlying platform or infrastructure. Azure Functions are 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, 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 are stateless; they behave as if they're restarted every time they respond to an event. This is ideal for processing incoming data. And if state is required, they can be connected to an Azure storage service.

43 https://azure.microsoft.com/services/machine-learning-studio/
44 https://azure.microsoft.com/services/
45 https://azure.microsoft.com/solutions/serverless/
46 https://azure.microsoft.com/services/functions/

Azure Logic Apps

Logic Apps[47] is 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.

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

Azure Event Grid

Event Grid[48] allows you to easily build applications with event-based architectures. It's a fully managed, intelligent event routing service that uses a publish-subscribe model for uniform event consumption. Event Grid has built-in support for events coming from Azure services, such as storage blobs and resource groups.
You can use Event Grid to support your own non-Azure-based events in near-real time, using custom topics. You can use filters to route specific events to different endpoints, and ensure your events are reliably delivered.

Walkthrough-Implement Azure Functions

In this walkthrough, we will create a Function App to display a Hello message when there is an HTTP request.

Task 1: Create a Function app

In this task, we will create a Function app.

Task 2: Create a HTTP triggered function and test

In this task, we will use the Webhook + API function to display a message when there is an HTTP request.

Congratulations! You have created a Function App to display a Hello message when there is an HTTP request.

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.

47 https://azure.microsoft.com/services/logic-apps/
48 https://azure.microsoft.com/services/event-grid/

Azure DevOps

DevOps[49] (Deployment 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 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.

Azure DevOps Services

DevOps Services[50] provides development collaboration tools including high-performance pipelines, free private Git repositories, configurable Kanban boards, and extensive automated and cloud-based load testing. DevOps Services was formerly known as Visual Studio Team Services (VSTS).

Azure Lab Services

Lab Services[51] is a service that helps developers and testers quickly create environments in Azure, while minimizing waste and controlling cost. Users can test their latest application versions by quickly provisioning Windows and Linux environments using reusable templates and artifacts. You can easily integrate your deployment pipeline with DevTest Labs to provision on-demand environments. With DevTest Labs you can scale up your load testing by provisioning multiple test agents and create pre-provisioned environments for training and demos. Lab Services was formally known as DevOps Test.

Azure App Service

With **Azure App Service**[52] you can quickly and easily build web and mobile apps for any platform or device. Azure App Service enables you to build and host web apps, mobile back ends, and RESTful APIs in the programming language of your choice without managing infrastructure. It offers auto-scaling and high availability, supports both Windows and Linux, and enables automated deployments from GitHub, Azure DevOps, or any Git repo.

49 https://azure.microsoft.com/solutions/devops
50 https://azure.microsoft.com/services/devops
51 https://azure.microsoft.com/services/devtest-lab/
52 https://azure.microsoft.com/services/app-service/

Key features of Azure App Service

- **Multiple languages and frameworks**. App Service has first-class support for ASP.NET, ASP.NET Core, Java, Ruby, Node.js, PHP, or Python. You can also run PowerShell and other scripts or executables as background services.
- **DevOps optimization**. Set up continuous integration and deployment with Azure DevOps, GitHub, BitBucket, Docker Hub, or Azure Container Registry. Promote updates through test and staging environments. Manage your apps in App Service by using Azure PowerShell or the cross-platform command-line interface (CLI).
- **Global scale with high availability**. Scale up or out manually or automatically. Host your apps anywhere in Microsoft's global datacenter infrastructure, and the App Service SLA promises high availability.
- **Connections to SaaS platforms and on-premises data**. Choose from more than 50 connectors for enterprise systems (such as SAP), SaaS services (such as Salesforce), and internet services (such as Facebook). Access on-premises data using Hybrid Connections and Azure Virtual Networks.
- **Security and compliance**. App Service is ISO, SOC, and PCI compliant. Authenticate users with Azure Active Directory or with social login (Google, Facebook, Twitter, and Microsoft). Create IP address restrictions and manage service identities.
- **Application templates**. Choose from an extensive list of application templates in the Azure Marketplace, such as WordPress, Joomla, and Drupal.
- **Visual Studio integration**. Dedicated tools in Visual Studio streamline the work of creating, deploying, and debugging.
- **API and mobile features**. App Service provides turn-key CORS support for RESTful API scenarios, and simplifies mobile app scenarios by enabling authentication, offline data sync, push notifications, and more.
- **Serverless code**. Run a code snippet or script on-demand without having to explicitly provision or manage infrastructure, and pay only for the compute time your code actually uses.

Walkthrough-Create a Web App

In this walkthrough, we will create a new web app that runs a Docker container. The container displays a Welcome message.

Task 1: Create a Web App that uses a Docker container.

In this task, you will create an Azure App Service Web App that uses a Docker container.

Task 2: Test the Web App

In this task, we will test the web app.

Congratulations! You have created and tested a web app.

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.

walkthrough-create-web-app

Exercise - Web App

Note - This Lab requires an Azure subscription. The sandbox you have used with other labs in the module will not function with this lab.

Lab 08 - Create a Web App

In this walkthrough, we will create a new web app that runs a Docker container. The container displays a Welcome message.

Task 1: Create a Web App

Azure App Service is actually a collection of four services, all of which are built to help you host and run web applications. The four services (Web Apps, Mobile Apps, API Apps, and Logic Apps) look different, but in the end they all operate in similar ways. Web Apps is the most commonly used of the four services (Web Apps, Mobile Apps, API Apps, and Logic Apps), and Web Apps is the service that we will be using in this lab.

In this task, you will create an Azure App Service Web App.

1. Sign in to the **Azure portal (https://portal.azure.com)**[53].
2. From the **All services** blade, search for and select **App Services**, and click **+ Add**
3. On the **Basics** tab of the **Web App** blade, specify the following settings (replace **xxxx** in the name of the web app with letters and digits such that the name is globally unique). Leave the defaults for everything else, including the App Service Plan.

Setting	Value
Subscription	**Choose your subscription**
Resource Group	**myRGWebApp1** (create new)
Name	**myDockerWebAppxxxx**
Publish	**Docker Container**
Operating System	**Linux**
Region	**East US** (ignore any service plan availability warnings)

4. Click **Next > Docker** and configure the container information. The startup command is optional and not needed in this exercise.

   [!NOTE]
   This is same container that was used in the Container Instances walkthrough to display a hello world message.

Setting	Value
Options	**Single container**
Image Source	**Docker Hub**

53 https://portal.azure.com?azure-portal=true

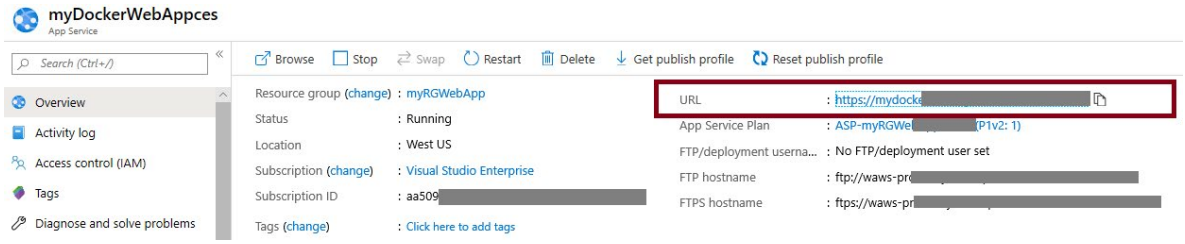
Setting	Value
Access Type	**Public**
Image and tag	**microsoft/aci-helloworld**

5. Click **Review + create**, and then click **Create**.

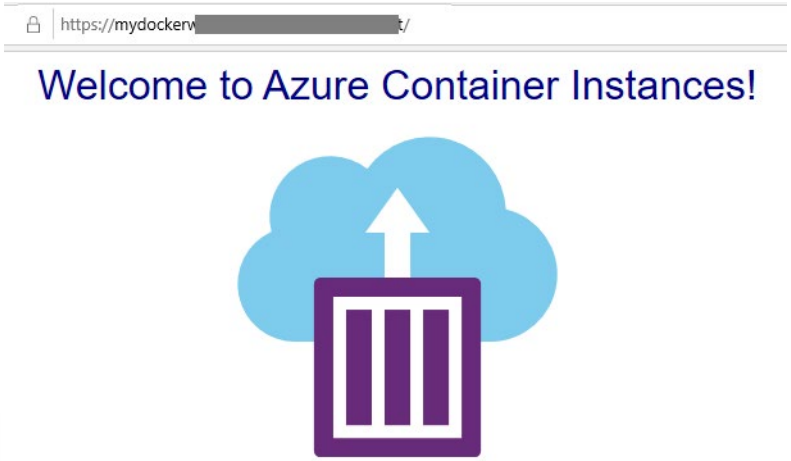
Task 2: Test the Web App

In this task, we will test the web app.

1. Wait for the Web App to deploy.
2. From **Notifications** click **Go to resource**.
3. On the **Overview** blade, locate the **URL** entry.



4. Click on the **URL** to open the new browser tab and display the Welcome to Azure Container Instances page.



5. Switch back to the **Overview** blade of your web app and note that it includes several charts. If you repeat step 4 a few times, you should be able to see corresponding telemetry being displayed in the charts. This includes number of requests and average response time.

[!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.

Azure Management Tools

Azure Management tools

You can configure and manage Azure using a broad range of tools and platforms. There are tools available for the command line, language-specific Software Development Kits (SDKs), developer tools, tools for migration, and many others.

Azure portal

The Azure portal is a public website that you can access with any web browser. After you sign in with your Azure account, you can create, manage, and monitor any available Azure services. You can identify a service you're looking for, get links for help on a topic, and deploy, manage, and delete resources. It also guides you through complex administrative tasks using wizards and tooltips.

The dashboard view provides high-level details about your Azure environment. You can customize the portal view as you need by moving and resizing tiles, displaying particular services of interest, accessing links for help and support, and providing feedback.

The portal does not provide any way to automate repetitive tasks. For example, to set up multiple VMs, you would need to create them one at a time by completing the wizard for each VM. Completing a wizard can be time-consuming and error-prone for complex tasks.

Azure PowerShell

Azure PowerShell is a module that you add to Windows PowerShell or PowerShell Core that enables you to connect to your Azure subscription and manage resources. Azure PowerShell requires Windows PowerShell to function. PowerShell provides services such as the shell window and command parsing. Azure PowerShell then adds the Azure-specific commands.

For example, Azure PowerShell provides the **New-AzVM** command that creates a virtual machine for you inside your Azure subscription. To use it, you would launch PowerShell, sign in to your Azure account using the command `Connect-AzureRMAccount`, and then issue a command such as:

```
New-AzVm `
    -ResourceGroupName "TesResourceGroup" `
    -Name "Testvm" `
    -Image "UbuntuLTS"
    ...
```

Note: PowerShell Core is a cross-platform version of PowerShell that runs on Windows Linux or macOS.

Azure Command Line Interface (CLI)

Azure CLI is a cross-platform command-line program that connects to Azure and executes administrative commands on Azure resources. *Cross platform* means that it can be run on Windows, Linux, or macOS. For example, to create a VM, you would open a command prompt window, sign in to Azure using the command `az login`, create a resource group, then use a command such as:

```
az vm create \
  --resource-group Testrg1 \
  --name Testvm \
  --image UbuntuLTS
  --generate-ssh-keys
  ...
```

Azure Cloud Shell

Azure Cloud Shell is a browser-based scripting environment in your portal. It provides the flexibility of choosing the shell experience that best suits the way you work. Linux users can opt for a Bash experience, while Windows users can opt for PowerShell.

A storage account is required to use the Cloud Shell and you will be prompted to create one when accessing the Azure Cloud Shell.

Note: You can access Azure Cloud Shell through the portal.

Azure Mobile App

The Microsoft Azure mobile app allows you to access, manage, and monitor all your Azure accounts and resources from your iOS or Android phone or tablet. Once installed, you can:

- Check the status and important metrics of your services
- Stay informed with notifications and alerts about important health issues
- Quickly diagnose and fix issues anytime, anywhere
- Review the latest Azure alerts
- Start, stop, and restart virtual machines or web apps
- Connect to your virtual machines
- Manage permissions with role-based access control (RBAC)
- Use the Azure Cloud Shell to run saved scripts or perform unplanned administrative tasks

Azure REST API

Representational State Transfer (REST) APIs are service endpoints that support sets of HTTP operations (methods), which provide create, retrieve, update, or delete access to the service's resources. A REST API defines a set of functions which developers can perform requests and receive responses via HTTP protocol such as GET and POST.

Azure Advisor

Azure Advisor[54] is a free service built into Azure that provides recommendations on high availability, security, performance, and cost. Advisor analyzes your deployed services and looks for ways to improve your environment across those four areas.

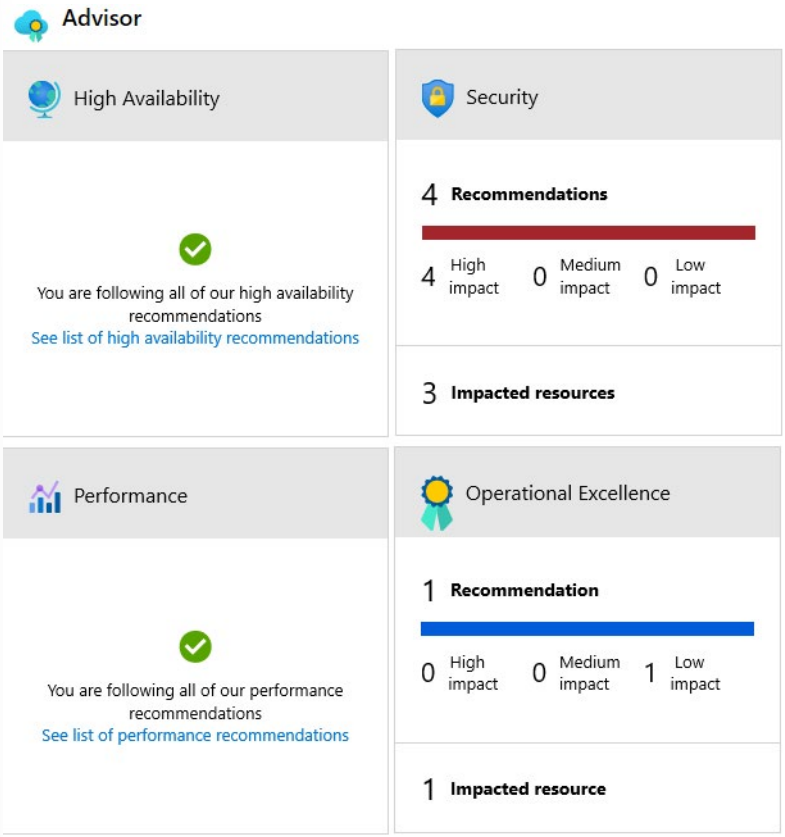
With Azure Advisor, you can:

- Get proactive, actionable, and personalized best practices recommendations.
- Improve the performance, security, and high availability of your resources as you identify opportunities to reduce your overall Azure costs.
- Get recommendations with proposed actions inline.

You can access Azure Advisor through the Azure portal. After you sign in to the portal, either select **Advisor** from the navigation menu, or search for it in the *All services* menu.

You can download recommendations from Azure Advisor in PDF or CSV format, which you can then share.

54 https://azure.microsoft.com/services/advisor/



Walkthrough-Create a VM with a Template

In this walkthrough, we will deploy a virtual machine with a QuickStart template and examine monitoring capabilities.

Task 1: Explore the gallery and deploy a template

In this task, we will browse the Azure QuickStart gallery and deploy a template to create a virtual machine.

Task 2: Verify and monitor your virtual machine deployment

In this task, we will verify the virtual machine deployed correctly.

Congratulations! You have deployed a virtual machine using a QuickStart template.

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.

Walkthrough-Create a VM with PowerShell

In this walkthrough, we will install PowerShell locally, create a resource group and virtual machine, access and use the Cloud Shell, and review Azure Advisor recommendations.

Task 1: Configure PowerShell locally

In this task, we will configure PowerShell to run from your local machine.

Task 2: Create a resource group and virtual machine

In this task, we will use PowerShell to create a resource group and a virtual machine.

Task 3: Execute commands in the Cloud Shell

In this task, we will practice executing PowerShell commands from the Cloud Shell.

Task 4: Review Azure Advisor Recommendations

Note: This same task is in the Create a VM with Azure CLI.

In this task, we will review Azure Advisor recommendations for our virtual machine.

Congratulations! You have installed PowerShell on your local machine, created a virtual machine using PowerShell, practiced with PowerShell commands, and viewed Advisor recommendations.

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.

Walkthrough-Create a VM with the CLI

In this walkthrough, we will install the Azure CLI locally, create a resource group and virtual machine, use the Cloud Shell, and review Azure Advisor recommendations.

Note: The following steps are based on a Windows installation, however they could equally be applicable to a Mac or Linux environment. However, there are **specific installation steps for each environment**[55].

Task 1: Install the CLI locally

In this task, we will install the Azure CLI on your local machine.

Task 2: Create a resource group and a virtual machine

In this task, we will create a resource group and a virtual machine using the CLI locally.

Task 3: Execute commands in the Cloud Shell

In this task, we will practice executing CLI commands from the Cloud Shell.

Task 4: Review Azure Advisor Recommendations

In this task, we will review Azure Advisor recommendations.

Note: If you have done the previous lab (Create a VM with PowerShell) then you have already completed this task.

Congratulations! You have installed PowerShell on your local machine, created a virtual machine using PowerShell, practiced with PowerShell commands, and viewed Advisor recommendations.

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.

55 https://docs.microsoft.com/cli/azure/install-azure-cli

Module 2 Review Questions

Module 02 Review Questions

Review Question 1

Which of the following ensures data-residency and compliance needs are met for customers who need to keep their data and applications close?

- ☐ Geographies
- ☐ Regions
- ☐ Zones

Review Question 2

As a best practice, all resources that are part of an application and share the same lifecycle should exist in the same?

- ☐ Availability set
- ☐ Region
- ☐ Resource group

Review Question 3

Which Azure compute resource can you use to deploy to manage a set of identical virtual machines?

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

Review Question 4

Which of the following should you use when you are concerned only about the code running your service and not the underlying platform or infrastructure?

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

Review Question 5

Azure Resource Manager templates use which format?

- ☐ HTML
- ☐ JSON
- ☐ XML

Review Question 6

Which of the following services is a distributed network of servers that can efficiently deliver web content to users?

- ☐ Azure App Services
- ☐ Azure Content Delivery Network
- ☐ Azure Cosmos DB

Review Question 7

Which of the following is optimized for storing massive amounts of unstructured data, such as videos and images?

- ☐ Blobs
- ☐ Files
- ☐ Queues

Review Question 8

Which of the following is part of the Azure Artificial Intelligence service?

- ☐ HDInsight
- ☐ Azure Machine Learning service
- ☐ Azure DevTest Labs

Review Question 9

Which of the following cloud services provides development collaboration tools including high-performance pipelines, free private Git repositories, and configurable Kanban boards?

- ☐ Azure DevOps Services
- ☐ Azure Event Grid
- ☐ HDInsight

Review Question 10

Microsoft Azure datacenters are organized and made available by?

- ☐ Geographies
- ☐ Regions
- ☐ Zones

Review Question 11

Which of the following is used to ensure availability during maintenance events?

- ☐ Availability Set
- ☐ Availability Zone
- ☐ Scale Set

Review Question 12

Which is true about Azure Load Balancer?

- ☐ Azure Load Balancer distributes traffic among similar systems, making your services more highly available.
- ☐ Azure Load Balancer works with internet-facing traffic only.
- ☐ You must use Azure Load Balancer if you want to distribute traffic among your virtual machines running in Azure.

Review Question 13

You are managing one of your Azure services remotely from your Android phone. Which management tools would best allow you to do manage remotely from your Android phone with the least amount of administrative effort?

- ☐ Azure CLI
- ☐ Azure portal
- ☐ Powershell

Review Question 14

Which of the following terms ensure that both data-residency and compliance needs are met for customers who need to keep their data and applications close?

- ☐ Geographies
- ☐ Regions
- ☐ Zones

Module 2 Summary

Module 2 Summary

In this module you've learned about core Microsoft Azure architectural components, core Azure services and solutions, and various management tools that are available to manage and configure Azure.

Core Azure architectural components

In this lesson we learned about how Azure datacenters and services are located and organized in regions and geographies. We also learned how availability is achieved using availability zones and availability sets. We gained an understanding of how to automate deployments and configuration of resources and services using declarative JSON templates that utilize the Azure Resource Manager layer to create and configure resources. And finally, we learned how to use resource groups for managing resources in Azure.

Core Azure services and products

In this lesson we learned about compute services, and the use of virtual machines and containers. We gained an understanding of some of the services that make up the compute service such as Azure VMs, VM scale sets, app services and functions, Azure Container Instances, and Azure Kubernetes Service. We also learned about networking services such as Virtual Network, Azure Load Balancer, VPN Gateway, Application Gateway, and Azure Content Delivery Network.

Azure solutions

In this lesson we learned about solutions such as IoT, and services that form part of the service offering such as Azure IoT Hub and Microsoft IoT Central. We discussed big data analytics services such as Azure SQL Data Warehouse, HDInsight, and Azure Data Lake Analytics. We also learned about AI and how it utilizes machine learning services such as Azure Machine Learning and Azure Machine Learning Studio. We also learned about serverless computing services such as Azure Functions, Azure Logic Apps, and Azure Event Grid. Finally we learned about DevOps services such as Azure DevOps and Azure DevTest Labs.

Azure management tools

In this lesson we learned about the management tools available for managing and configuring Azure, such as Azure Portal, Azure PowerShell, Azure CLI, and Azure Cloud Shell. It also includes Azure Advisor, which provides recommendations on high availability, security, performance, and cost.

Answers

Review Question 1

Which of the following ensures data-residency and compliance needs are met for customers who need to keep their data and applications close?

■ Geographies

☐ Regions

☐ Zones

Explanation
Geographies. Geographies allow customers with specific data-residency and compliance needs to keep their data and applications close. Geographies ensure that data residency, sovereignty, compliance, and resiliency requirements are honored within geographical boundaries.

Review Question 2

As a best practice, all resources that are part of an application and share the same lifecycle should exist in the same?

☐ Availability set

☐ Region

■ Resource group

Explanation
Resource group. For ease of management, resources that are part of an application and share its lifecycle should be placed in the same resource group.

Review Question 3

Which Azure compute resource can you use to deploy to manage a set of identical virtual machines?

☐ Virtual machine availability sets

☐ Virtual machine availability zones

■ Virtual machine scale sets

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

Review Question 4

Which of the following should you use when you are concerned only about the code running your service and not the underlying platform or infrastructure?

☐ Azure App Service

☐ Azure Container Instances

■ Azure Functions

Explanation
Azure Functions. Azure Functions are ideal when you're concerned only about the code running your service and not the underlying platform or infrastructure.

Review Question 5

Azure Resource Manager templates use which format?

☐ HTML

■ JSON

☐ XML

Explanation
JSON. Resource Manager templates are JSON files that define the resources you need to deploy for your solution. You can use template to easily re-create multiple versions of your infrastructure, such as staging and production.

Review Question 6

Which of the following services is a distributed network of servers that can efficiently deliver web content to users?

☐ Azure App Services

■ Azure Content Delivery Network

☐ Azure Cosmos DB

Explanation
Azure Content Delivery Network. A Content Delivery Network is a distributed network of servers that can efficiently deliver web content to users.

Review Question 7

Which of the following is optimized for storing massive amounts of unstructured data, such as videos and images?

■ Blobs

☐ Files

☐ Queues

Explanation
Blobs. 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.

Review Question 8

Which of the following is part of the Azure Artificial Intelligence service?

☐ HDInsight

■ Azure Machine Learning service

☐ Azure DevTest Labs

Explanation
Azure Machine Learning service. Machine Learning service provides a cloud-based environment that you can use to develop, train, test, deploy, manage, and track machine learning models.

Review Question 9

Which of the following cloud services provides development collaboration tools including high-performance pipelines, free private Git repositories, and configurable Kanban boards?

- ■ Azure DevOps Services
- ☐ Azure Event Grid
- ☐ HDInsight

Explanation
Azure DevOps Services. Azure DevOps Services includes development collaboration tools including high-performance pipelines, free private Git repositories, and configurable Kanban boards.

Review Question 10

Microsoft Azure datacenters are organized and made available by?

- ☐ Geographies
- ■ Regions
- ☐ Zones

Explanation
Regions. Microsoft Azure datacenters are organized and made available by region.

Review Question 11

Which of the following is used to ensure availability during maintenance events?

- ■ Availability Set
- ☐ Availability Zone
- ☐ Scale Set

Explanation
Availability sets provide VM redundancy and availability. This configuration within a datacenter (Availability Zone) ensures that during either a planned or unplanned maintenance event, at least one virtual machine is available and meets the 99.95% Azure SLA.

Review Question 12

Which is true about Azure Load Balancer?

- ■ Azure Load Balancer distributes traffic among similar systems, making your services more highly available.
- ☐ Azure Load Balancer works with internet-facing traffic only.
- ☐ You must use Azure Load Balancer if you want to distribute traffic among your virtual machines running in Azure.

Explanation
If one system is unavailable, Azure Load Balancer stops sending traffic to it. It then directs traffic to one of the responsive servers.

Review Question 13

You are managing one of your Azure services remotely from your Android phone. Which management tools would best allow you to do manage remotely from your Android phone with the least amount of administrative effort?

■ Azure CLI

☐ Azure portal

☐ Powershell

Explanation
While it's technically possible to open the Azure portal in your browser on your phone, it is not a better option than using the mobile app Azure CLI (or even Azure Cloud Shell).

Review Question 14

Which of the following terms ensure that both data-residency and compliance needs are met for customers who need to keep their data and applications close?

■ Geographies

☐ Regions

☐ Zones

Explanation
Geographies allow customers with specific data-residency and compliance needs to keep their data and applications close. Geographies ensure that data residency, sovereignty, compliance, and resiliency requirements are honored within geographical boundaries.

Module 3 Security, Privacy, Compliance and Trust

Learning Objectives

Learning Objectives

After completing this module, you will be able to:

- Understand and describe how to secure network connectivity in Microsoft Azure.
- Understand and describe core Azure identity services.
- Understand and describe security tools and features.
- Understand and describe Azure governance methodologies.
- Understand and describe monitoring and reporting in Azure.
- Understand and describe privacy, compliance, and data protection standards in Azure.

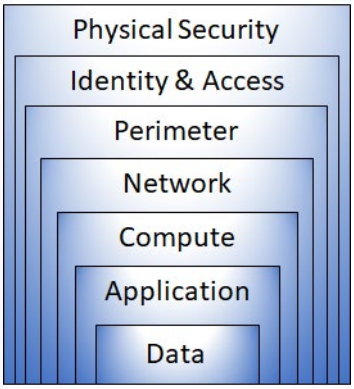
Securing network connectivity

Defense in depth

Defense in depth is a strategy that employs a series of mechanisms to slow the advance of an attack aimed at acquiring unauthorized access to data. The objective of defense in depth is to protect and prevent information from being stolen by individuals not authorized to access it. The common principles used to define a security posture are **confidentiality**, **integrity**, and **availability**, known collectively as CIA.

- **Confidentiality** - The Principle of least privilege restricts access to information only to individuals explicitly granted access. This information includes protection of user passwords, remote access certificates, and email content.
- **Integrity** - The prevention of unauthorized changes to information at rest or in transit. A common approach used in data transmission is for the sender to create a unique fingerprint of the data using a one-way hashing algorithm. The hash is sent to the receiver along with the data. The data's hash is recalculated and compared to the original by the receiver to ensure the data wasn't lost or modified in transit.
- **Availability** - Ensure services are available to authorized users. Denial of service attacks are a prevalent cause of loss of availability to users.

Defense in depth can be visualized as a set of layers, with the Data to be secured at the center. Each layer provides protection so that if one layer is breached, a subsequent layer is already in place to prevent further exposure. This approach removes reliance on any single layer of protection and acts to slow down an attack and provide alert telemetry that can be acted upon, either automatically or manually.



- **Physical security** is the first line of defense to protect computing hardware in the datacenter.
- **Identity & access** controls access to infrastructure and change control.
- **Perimeter** layer uses distributed denial-of-service (DDoS) protection to filter large-scale attacks before they can cause a denial of service for end users.
- **Networking** layer limits communication between resources through segmentation and access controls.
- **Compute** layer secures access to virtual machines.
- **Application** layer ensures applications are secure and free of vulnerabilities.

Data

In almost all cases, attackers are after data:

- Stored in a database
- Stored on disk inside virtual machines
- Stored on a SaaS application such as Office 365
- Stored in cloud storage

It's the responsibility of those storing and controlling access to data to ensure that it's properly secured. Often, there are regulatory requirements that dictate the controls and processes that must be in place to ensure the confidentiality, integrity, and availability of the data.

Application

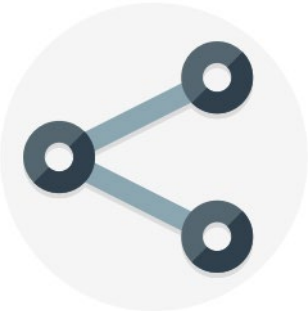
- Ensure applications are secure and free of vulnerabilities.
- Store sensitive application secrets in a secure storage medium.
- Make security a design requirement for all application development.

Integrating security into the application development life cycle will help reduce the number of vulnerabilities introduced in code. We encourage all development teams to ensure their applications are secure by default, and that they're making security requirements non-negotiable.

Compute

- Secure access to virtual machines.
- Implement endpoint protection and keep systems patched and current.

Malware, unpatched systems, and improperly secured systems open your environment to attacks. The focus in this layer is on making sure your compute resources are secure, and that you have the proper controls in place to minimize security issues.



Networking

- Limit communication between resources.
- Deny by default.
- Restrict inbound internet access and limit outbound, where appropriate.
- Implement secure connectivity to on-premises networks.

At this layer, the focus is on limiting the network connectivity across all your resources to allow only what is required. By limiting this communication, you reduce the risk of lateral movement throughout your network.

Perimeter

- Use distributed denial of service (DDoS) protection to filter large-scale attacks before they can cause a denial of service for end users.
- Use perimeter firewalls to identify and alert on malicious attacks against your network.

At the network perimeter, it's about protecting from network-based attacks against your resources. Identifying these attacks, eliminating their impact, and alerting you when they happen are important ways to keep your network secure.

Identity and access

- Control access to infrastructure and change control.
- Use single sign-on and multi-factor authentication.
- Audit events and changes.

The identity and access layer is all about ensuring identities are secure, access granted is only what is needed, and changes are logged.

Physical security

- Physical building security and controlling access to computing hardware within the data center is the first line of defense.

With physical security, the intent is to provide physical safeguards against access to assets. These safeguards ensure that other layers can't be bypassed, and loss or theft is handled appropriately.

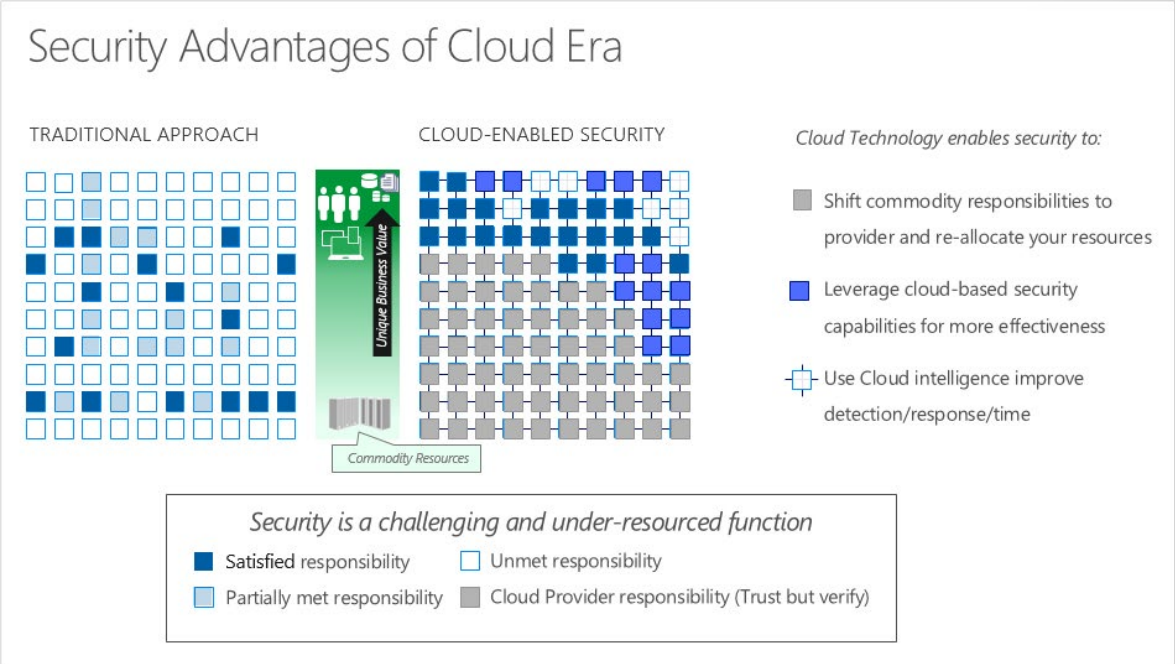
Azure helps alleviate your security concerns. But security is still a **shared responsibility**. How much of that responsibility falls on us depends on which model we use with Azure. We use the *defense in depth* rings as a guideline for considering what protections are adequate for our data and environments.

✓ Microsoft applies a layered approach to security, both in our physical datacenters and across Azure services.

define-shared-security

Shared Security

Organizations face many challenges with securing their datacenters, including recruiting and keeping security experts, using many security tools, and keeping pace with the volume and complexity of threats.



As computing environments move from customer-controlled datacenters to the cloud, the responsibility of security also shifts. Security of the operational environment is now a concern shared by both cloud providers and customers. By shifting these responsibilities to a cloud service like Azure, organizations can reduce focus on activities that aren't core business competencies. Depending on the specific technology choices, some security protections will be built into the particular service, while addressing others will remain the customer's responsibility. To ensure that the proper security controls are provided, a careful evaluation of the services and technology choices becomes necessary.

Responsibility	On-premises	IaaS	PaaS	SaaS
Data governance and Rights Management	Customer	Customer	Customer	Customer
Client endpoints	Customer	Customer	Customer	Customer
Account and access management	Customer	Customer	Customer	Customer
Identity and directory Infrastructure	Customer	Customer	Microsoft/ Customer	Microsoft/ Customer
Application	Customer	Customer	Microsoft/ Customer	Microsoft
Network controls	Customer	Customer	Microsoft/ Customer	Microsoft
Operating system	Customer	Customer	Microsoft	Microsoft
Physical hosts	Customer	Microsoft	Microsoft	Microsoft
Physical network	Customer	Microsoft	Microsoft	Microsoft
Physical datacenter	Customer	Microsoft	Microsoft	Microsoft

Contoso Shipping - Security is a shared responsibility

One of the first shifts Contoso Shipping makes is from on-premises data centers to infrastructure as a service (IaaS). With IaaS, you are leveraging the lowest-level service and asking Azure to create virtual machines (VMs) and virtual networks. At this level, it's still your responsibility to patch and secure your operating systems and software, as well as configure your network to be secure. At Contoso Shipping, you are taking advantage of IaaS when you start using Azure VMs instead of your on-premises physical servers. In addition to the operational advantages, you receive the security advantage of having out-sourced concern over protecting the physical parts of the network.

Next, it is time to build you drone app in the cloud. Moving to platform as a service (PaaS) outsources several security concerns. At this level, Azure is taking care of the operating system and of most foundational software like database management systems. Everything is updated with the latest security patches and can be integrated with Azure Active Directory for access controls. PaaS also comes with many operational advantages. Rather than building whole infrastructures and subnets for your environments by hand, you can "point and click" within the Azure portal or run automated scripts to bring complex, secured systems up and down, and scale them as needed. Contoso Shipping uses an app built on Azure for tracking telemetry data from drones and trucks — as well as a web app — which are both examples of PaaS.

With software as a service (SaaS), you outsource almost everything. SaaS is software that runs with an internet infrastructure. The code is controlled by the vendor but configured to be used by the customer. Like so many companies, Contoso Shipping uses Office 365, which is a great example of SaaS!

Azure Firewall

A **Firewall** is a service that grants server access based on the originating IP address of each request. You create firewall rules that specify ranges of IP addresses. Only clients from these granted IP addresses will be allowed to access the server. Firewall rules also include specific network protocol and port information.

Azure Firewall[1] is a managed, cloud-based, network security service that protects your Azure Virtual Network resources. It is a fully stateful firewall as a service with built-in high availability and unrestricted cloud scalability.

You can create, enforce, and log, application and network connectivity policies across subscriptions, and virtual networks, centrally. Azure Firewall uses a static public IP address for your virtual network resources, which allows outside firewalls to identify traffic originating from your virtual network. The service is fully integrated with Azure Monitor for logging and analytics.

Azure Firewall provides many features, including:

- Built-in high availability.
- Unrestricted cloud scalability.
- Inbound and outbound filtering rules.
- Azure Monitor logging.

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

Common Usage Scenarios

You typically deploy Azure Firewall on a central virtual network to control general network access. 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.

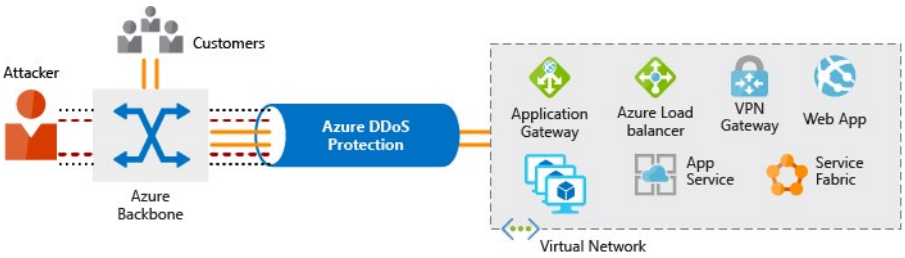
✓ **Azure Application Gateway**[2] also provides a firewall, called the **Web Application Firewall** (WAF). WAF provides centralized, inbound protection for your web applications against common exploits and vulnerabilities.

Distributed Denial of Service (DDoS)

DDoS[3] attacks attempt to overwhelm and exhaust an application's resources, making the application slow or unresponsive to legitimate users. DDoS attacks can be targeted at any endpoint that is publicly reachable through the internet. Thus, any resource exposed to the internet, such as a website, is potentially at risk from a DDoS attack.

When you combine Azure DDoS Protection with application design best practices, you help provide defense against DDoS attacks. DDoS Protection leverages the scale and elasticity of Microsoft's global network to bring DDoS mitigation capacity to every Azure region. The Azure DDoS Protection service protects your Azure applications by scrubbing 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. Azure DDoS protection identifies the attacker's attempt to overwhelm the network and blocks further traffic from reaching Azure services. Legitimate traffic from customers still flows into Azure without any interruption of service.



Azure DDoS protection service tiers

Azure DDoS Protection provides the following service tiers:

- **Basic**. The Basic service tier is automatically enabled as part of the Azure platform. Always-on traffic monitoring and real-time mitigation of common network-level attacks provide the same defenses that Microsoft's online services use. Azure's global network is used to distribute and mitigate attack traffic across regions.

2 https://azure.microsoft.com/services/application-gateway?azure-portal=true
3 https://azure.microsoft.com/services/ddos-protection?azure-portal=true

- **Standard**. The Standard service tier provides additional mitigation capabilities that are tuned specifically to Microsoft Azure Virtual Network resources. DDoS Protection Standard is simple to enable and requires no application changes. 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.

DDoS standard protection

DDoS standard protection can mitigate the following types of attacks:

- **Volumetric attacks**. The attack's goal 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**. These attacks target web application packets to disrupt the transmission of data between hosts.

Network Security Groups

Network Security Groups[4] allow you to filter network traffic to and from Azure resources in an Azure virtual network. 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.

Network security rule properties

A network security group can contain as many rules as you need, within Azure subscription limits. Each rule specifies the following properties:

Property	Explanation
Name	Unique name of 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	Individual 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	An individual port or range of ports.
Action	Allow or Deny.

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.

Application Security groups

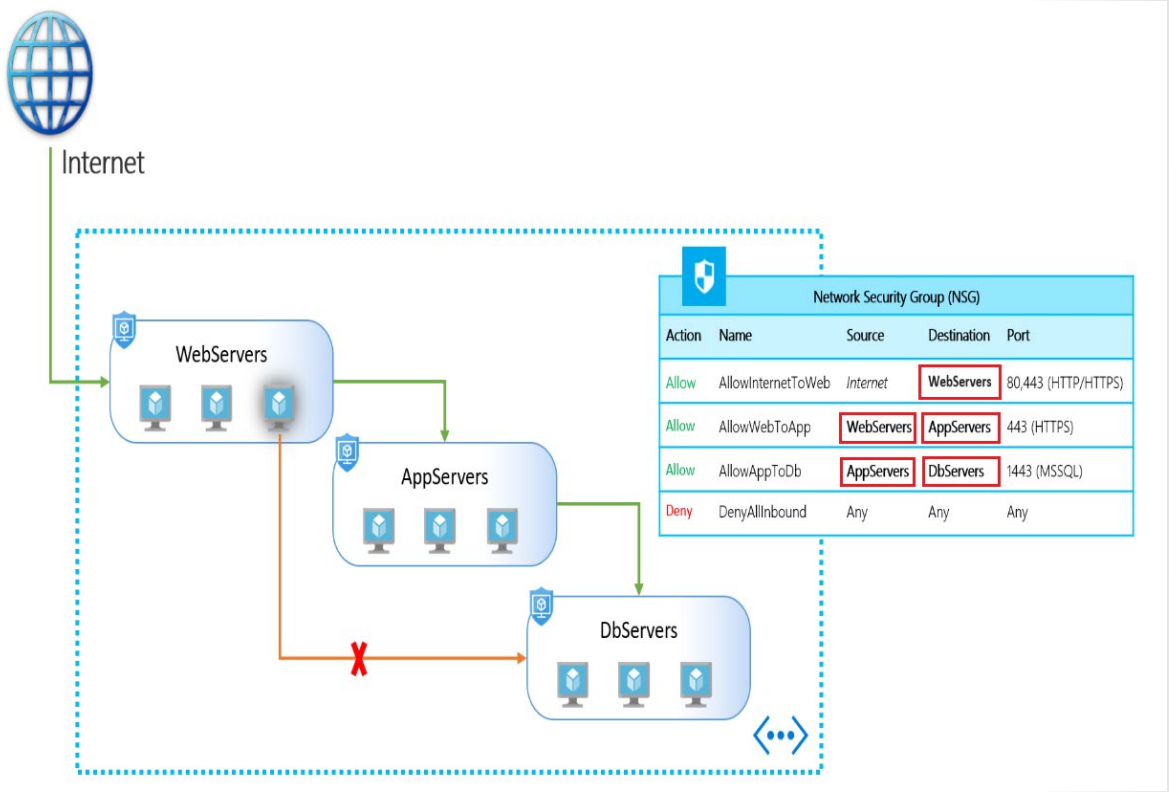
Application security groups[5] enable you to configure network security as a natural extension of an application's structure, allowing you to group virtual machines and define network security policies based on those groups.

4 https://docs.microsoft.com/azure/virtual-network/security-overview#network-security-groups?azure-portal=true
5 https://docs.microsoft.com/azure/virtual-network/security-overview#application-security-groups?azure-portal=true

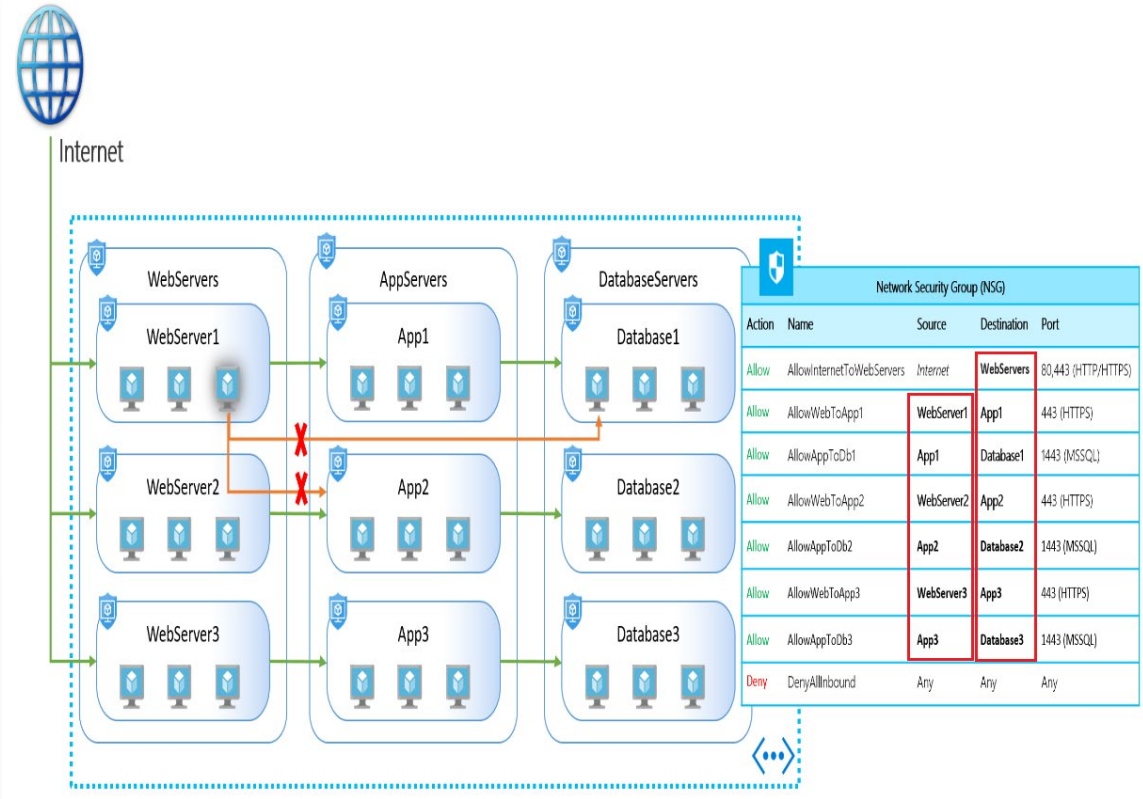
This feature allows you to reuse your security policy at scale without manual maintenance of explicit IP addresses. The platform handles the complexity of explicit IP addresses and multiple rule sets, allowing you to focus on your business logic.

Example

An ASG enables you to group servers with similar port filtering requirements, and group together servers with similar functions, such as web servers. In the below example, we have ASGs defined for Web Servers, App Servers, and DB Servers and green and red arrows indicating which network traffic paths are allowable and which are not.



In the below example, multiple applications are deployed into the same virtual network. Based on the security rules described, workloads are isolated from each other. If a VM from one of the applications is compromised, lateral exploration is limited, minimizing the potential impact of an attacker. In this example, let's assume one of the web server VMs from application1 is compromised, the rest of the application will continue to be protected, even access to critical workloads like database servers will still be unreachable. This implementation provides multiple extra layers of security to your network, making this intrusion less harmful and easy to react on such events.



ASGs help simplify how you can filter and control network traffic coming into your organization and how that network traffic is allowed to move. They allow you to isolate multiple workloads and provide additional levels of protection for your virtual network in a more easily manageable way.

Network Security Solutions

When considering your Azure security solution consider all the elements of defense in depth.

Perimeter layer

The network perimeter layer is about protecting organizations from network-based attacks against your resources. Identifying these attacks, alerting, 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.

Networking layer

At this layer, the focus is on limiting network connectivity across all your resources to only allow what is required. Segment your resources and use network-level controls to restrict communication to only what is needed. By restricting connectivity, you reduce the risk of lateral movement throughout your network

from an attack. Use NSGs to create rules about inbound and outbound communication at this layer. As best practices:

- Limit communication between resources through 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.

Combining services

You can also combine multiple Azure networking and security services to manage your network security and provide increased layered protection. The following are examples of combined services:

- **Network security groups and Azure Firewall**. Azure Firewall complements network security group functionality. 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. Azure Firewall is a fully stateful, centralized network firewall-as-a-service, which provides network and application-level protection across different subscriptions and virtual networks.
- **Application Gateway WAF and Azure Firewall**. WAF is a feature of 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, FTP), outbound network-level protection for all ports and protocols, and application-level protection for outbound HTTP/S. Combining both provides additional layers of protection.

Walkthrough-Secure network traffic

In this walkthrough, we will create and configure inbound and outbound security port rules.

Task 1: Create a virtual machine.

In this task, we will deploy a custom template to create a virtual machine.

Task 2: Create a network security group

In this task, we will create a network security group and associate the virtual machine network interface.

Task 3: Configure an inbound security port rule to allow RDP

In this task, we will allow RDP to the virtual machine by configuring an inbound security port rule.

Task 4: Configure an outbound security port rule to deny Internet access.

In this task, we will create a NSG and associate it with the virtual machine. We will then deny Internet access and test to ensure the rule is working.

Congratulations! You have created and configured inbound and outbound security port rules.

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.

Core Azure identity services

Authentication versus Authorization

Two fundamental concepts that need to be understood when talking about identity and access are authentication and authorization. They underpin everything else that happens and occur sequentially in any identity and access process:

- **Authentication**. Authentication is the process of establishing the identity of a person or service looking 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 use. It establishes if they are who they say they are.
- **Authorization**. 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.

✓ Authentication is sometimes shortened to *AuthN*, and authorization is sometimes shortened to *AuthZ*.

Azure Active Directory (Azure AD)

Azure Active Directory[6] is a Microsoft cloud-based identity and access management service. Azure AD helps employees of an organization sign in and access 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 apps developed by your own organization.

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 users to remember only one ID and one password to access multiple applications. A single identity is tied to a user, simplifying the security model. As users change roles or leave an organization, access modifications are tied to that identity, greatly reducing the effort needed to change or disable accounts.
- **Application management**. You can manage your cloud and on-premises apps using Azure AD Application Proxy, SSO, the My apps portal (also referred to as *Access panel*), and SaaS apps.
- **Business to business** (B2B) identity services. Manage your guest users and external partners while maintaining control over your own corporate data
- **Business-to-Customer** (B2C) identity services. Customize and control how users sign up, sign in, and manage their profiles when using your apps with services.
- **Device Management**. Manage how your cloud or on-premises devices access your corporate data.

6 https://azure.microsoft.com/services/active-directory?azure-portal=true

Azure AD is intended for:

- **IT administrators**. Administrators can use Azure AD to control access to apps and their resources, based on your business requirements.
- **App developers**. Developers can use Azure AD to provide a standards-based approach for adding functionality to applications that you build, such as adding Single-Sign-On functionality to an app, or allowing an app to work with a user's pre-existing credentials and other functionality.
- **Microsoft 365**, **Microsoft Office 365**, **Azure**, or **Microsoft Dynamics CRM Online** subscribers. These subscribers are already using Azure AD. Each Microsoft 365, Office 365, Azure, and Dynamics CRM Online tenant is automatically an Azure AD tenant. You can immediately start to manage access to your integrated cloud apps using Azure AD.

Let's explore a single sign-on in more detail.

Single sign-on

The more identities a user has to manage, the greater the risk of a credential-related security incident. More identities mean more passwords to remember and change. Password policies can vary between applications and, as complexity requirements increase, it becomes increasingly difficult for users to remember them.

Now, consider the logistics 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 single sign-on (SSO), users need to remember only one ID and one password. Access across applications is granted to a single identity tied to a user, simplifying the security model. As users change roles or leave an organization, access modifications are tied to the single identity, greatly reducing the effort needed to change or disable accounts. Using single sign-on for accounts will make it easier for users to manage their identities and will increase the security capabilities in your environment.

SSO with Azure Active Directory

By leveraging Azure AD for SSO you'll also have the ability to combine multiple data sources into an intelligent security graph. This security graph enables the ability to provide threat analysis and real-time identity protection to all accounts in Azure AD, including accounts that are synchronized from your on-premises AD. By using a centralized identity provider, you'll have centralized the security controls, reporting, alerting, and administration of your identity infrastructure.

As Contoso Shipping integrates its existing Active Directory instance with Azure AD, you will make controlling access consistent across the organization. Doing so will also greatly simplify the ability to sign into email and Office 365 documents without having to reauthenticate.

Azure Multi-Factor Authentication (MFA)

Azure Multi-Factor Authentication[7] provides additional security for your identities by requiring two or more elements for full authentication. These elements fall into three categories:

- **Something you know** could be a password or the answer to a security question.
- **Something you possess** might be a mobile app that receives a notification, or a token-generating device.
- **Something you are** is typically some sort of biometric property, such as a fingerprint or face scan used on many mobile devices.

Using MFA increases identity security by limiting the impact of credential exposure. To fully authenticate, an attacker who has a user's password would also need to have possession of their phone or their fingerprint, for example. Authentication with only a single factor is insufficient and, without MFA, an attacker would be unable to use those credentials to authenticate. MFA should be enabled wherever possible as MFA adds enormous benefits to security.

MFA comes as part of the following Azure service offerings:

- **Azure Active Directory Premium licenses**. These licenses provide full-featured use of Azure Multi-Factor Authentication Service (cloud) or Azure Multi-Factor Authentication Server (on-premises).
- **Multi-Factor Authentication for Office 365**. A subset of Azure Multi-Factor Authentication capabilities is available as a part of your Office 365 subscription.
- **Azure Active Directory global administrators**. Because global administrator accounts are highly sensitive, a subset of Azure Multi-Factor Authentication capabilities are available to protect these accounts.

7 https://docs.microsoft.com/azure/active-directory/authentication/concept-mfa-howitworks?azure-portal=true

Security tools and features

Azure Security Center

Azure Security Center[8] is a monitoring service that provides threat protection across all of your services both in Azure, and on-premises. Security Center can:

- Provide security recommendations based on your configurations, resources, and networks.
- Monitor security settings across on-premises and cloud workloads, and automatically apply required security to new services as they come online.
- Continuously monitor all your services and perform automatic security assessments to identify potential vulnerabilities before they can be exploited.
- Use machine learning to detect and block malware from being installed on your virtual machines and services. You can also define a list of allowed applications to ensure that only the apps you validate can execute.
- Analyze and identify potential inbound attacks and help to investigate threats and any post-breach activity that might have occurred.
- Provide just-in-time access control for ports, reducing your attack surface by ensuring the network only allows traffic that you require.

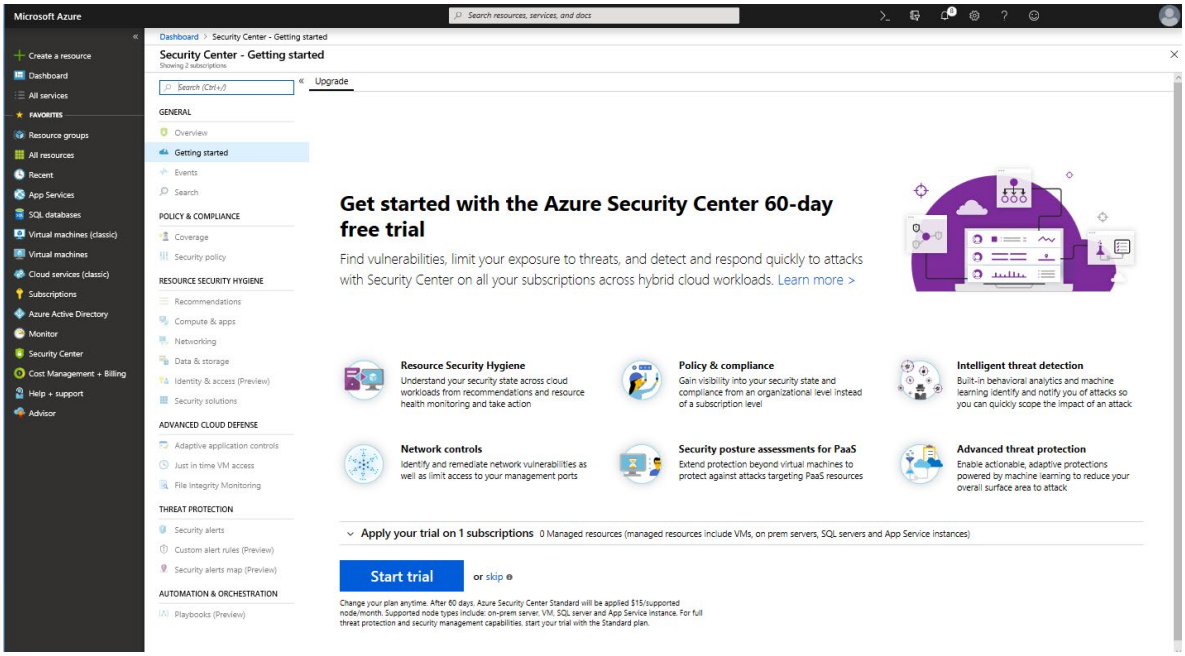
Azure Security Center Versions

Azure Security Center is available in two tiers:

- **Free**. Available as part of your Azure subscription, this tier is limited to assessments and recommendations of Azure resources only.
- **Standard**. This tier provides a full suite of security-related services including continuous monitoring, threat detection, just-in-time access control for ports, and more.

To access the full suite of Azure Security Center services you will need to upgrade to a Standard tier subscription. You can access the 30-day free trial from within the Azure Security Center dashboard in the Azure Portal.

8 https://azure.microsoft.com/services/security-center?azure-portal=true



- To upgrade a subscription to the Standard tier, you must be assigned the role of *Subscription Owner*, *Subscription Contributor*, or *Security Admin*.
- After the 30-day trial period is over, Azure Security Center is priced as per details on the https://azure.microsoft.com/pricing/details/security-center?azure-portal=true page.

Scenarios for Azure Security Center

You can integrate Security Center into your workflows and use it in many ways. Here are two examples.

Example 1 - Use Security Center for an incident response.

Many organizations learn how to respond to security incidents only after suffering an attack. To reduce costs and damage, it's important to have an incident response plan in place before an attack occurs. You can use Azure Security Center in different stages of an incident response.

You can use Security Center during the detect, assess, and diagnose stages. Here are examples of how Security Center can be useful during the three initial incident response stages:

- **Detect**. Review the first indication of an event investigation. For example, use the Security Center dashboard to review the initial verification that a high-priority security alert was raised.
- **Assess**. Perform the initial assessment to obtain more information about the suspicious activity. For example, obtain more information about the security alert.

- **Diagnose**. Conduct a technical investigation and identify containment, mitigation, and workaround strategies. For example, follow the remediation steps described by Security Center in that particular security alert.

Example 2 - Use Security Center recommendations to enhance security.

You can reduce the chances of a significant security event by configuring a security policy, and then implementing the recommendations provided by Azure Security Center.

Security policies and recommendations

A **security policy** defines the set of controls that are recommended for resources within that specified subscription or resource group. In Security Center, you define policies according to your company's security requirements.

Security Center analyzes the security state of your Azure resources. When Security Center identifies potential security vulnerabilities, it creates **recommendations** based on the controls set in the security policy. The recommendations guide you through the process of configuring the needed security controls. For example, if you have workloads that do not require the *Azure SQL Database Transparent Data Encryption* (TDE) policy, turn off the policy at the subscription level and enable it only in the resources groups where SQL TDE is required.

✓ More implementation and scenario detail is also available in the **Azure Security Center planning and operations guide**[9].

Azure Key Vault

Azure Key Vault[10] is a centralized cloud service for storing your applications' secrets. Key Vault helps you control your applications' secrets by keeping them in a single, central location and by providing secure access, permissions control, and access logging capabilities.

Usage Scenarios

- **Secrets management**. You can use Key Vault to securely store and tightly control access to tokens, passwords, certificates, *Application Programming Interface* (API) keys, and other secrets.
- **Key management**. You also can use Key Vault as a key management solution. Key Vault makes it easier to create and control the encryption keys used to encrypt your data.
- **Certificate management**. Key Vault lets you provision, manage, and deploy your public and private *Secure Sockets Layer/ Transport Layer Security* (SSL/ TLS) certificates for your Azure, and internally connected, resources more easily.
- **Store secrets backed by hardware security modules** (HSMs). The secrets and keys can be protected either by software, or by FIPS 140-2 Level 2 validated HSMs.

Key Vault benefits

The benefits of using Key Vault include:

- **Centralized application secrets**. Centralizing storage for application secrets allows you to control their distribution and reduces the chances that secrets may be accidentally leaked.

9 https://docs.microsoft.com/azure/security-center/security-center-planning-and-operations-guide?azure-portal=true
10 https://azure.microsoft.com/services/key-vault?azure-portal=true

- **Securely stored secrets and keys**. Azure uses industry-standard algorithms, key lengths, and HSMs, and access requires proper authentication and authorization.
- **Monitor access and use**. Using Key Vault, you can monitor and control access to company 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.
- **Integrate with other Azure services**. You can integrate Key Vault with storage accounts, container registries, event hubs and many more Azure services.

To go deeper on Azure Key Vault, take a look at – **Configure and Manage Secrets in Azure Key Vault**[11].

Walkthrough-Implement Azure Key Vault

In this walkthrough, we will create an Azure Key vault and then create a password secret within that key vault, providing a securely stored, centrally managed password for use with applications.

Task 1: Create an Azure Key Vault

In this task, we will create a key vault.

Task 2: Add a secret to the Key Vault

In this task, we will add a password to the key vault.

Congratulations! You have created an Azure Key vault and then created a password secret in that key vault, providing a securely stored, centrally managed password for use with applications.

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.

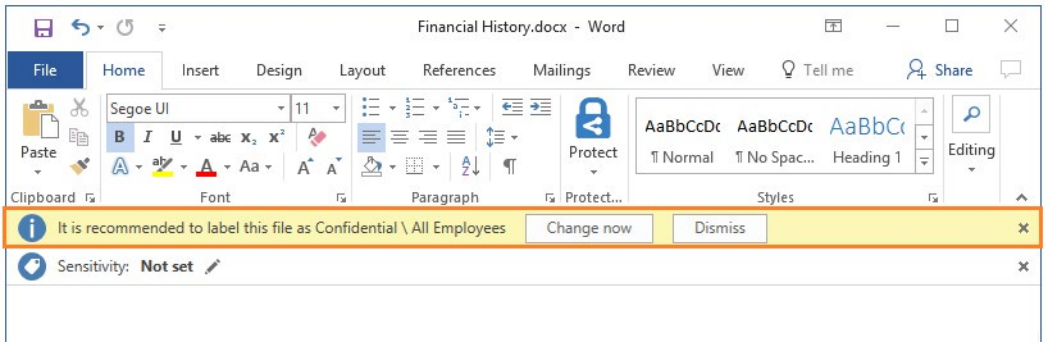
Azure Information Protection (AIP)

Azure Information Protection[12] is a cloud-based solution that helps organizations classify and (optionally) protect its documents and emails by applying labels. Labels can be applied automatically (by administrators who define rules and conditions), manually (by users), or with a combination of both (where users are guided by recommendations).

Usage scenario

The following screen capture is an example of MSIP in action on a user's computer. In this example, the administrator has configured a label with rules that detect sensitive data. When a user saves a Microsoft Word document containing a credit card number, a custom tooltip is displayed. The tooltip recommends labeling the file as *Confidential/ All Employees*, which is a label that the administrator has configured. This label classifies the document and protects it.

11 https://docs.microsoft.com/learn/modules/configure-and-manage-azure-key-vault?azure-portal=true
12 https://docs.microsoft.com/azure/information-protection/what-is-information-protection?azure-portal=true



After your content is classified (and optionally protected), you can then track and control how the content is used. For example, you can analyze data flows to gain insight into your business; detect risky behaviors and take corrective measures; track access to documents; and prevent data leakage or misuse.

✓ You can purchase MSIP either as a standalone solution, or through one of the following Microsoft licensing suites: Enterprise Mobility + Security, or Microsoft 365 Enterprise. Purchasing details are available on the https://azure.microsoft.com/pricing/details/information-protection?azure-portal=true Azure Information Protection pricing webpage.

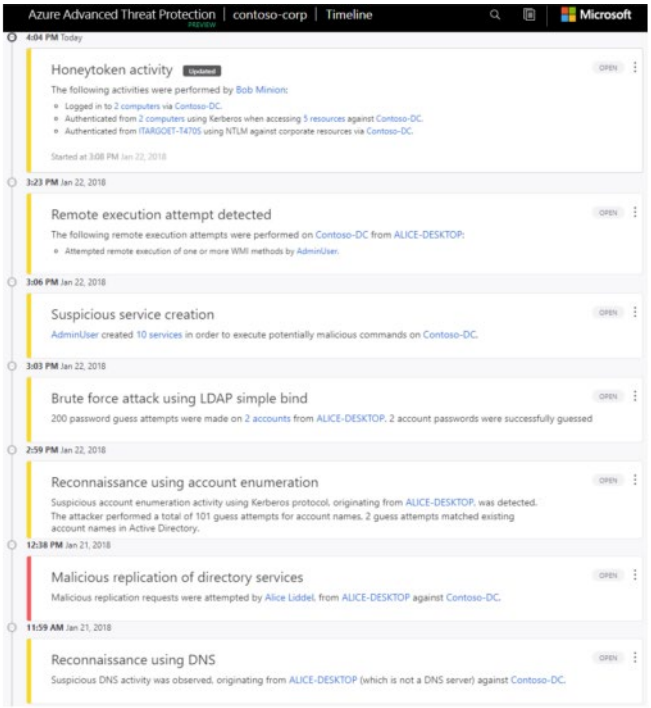
Azure Advanced Threat Protection (Azure ATP)

Azure Advanced Threat Protection[13] is a cloud-based security solution that identifies, detects, and helps you investigate advanced threats, compromised identities, and malicious insider actions directed at your organization. Azure ATP is capable of detecting known malicious attacks and techniques, security issues, and risks against your network.

Azure ATP components

- **Azure ATP portal**. Azure ATP has its own portal, through which you can monitor and respond to suspicious activity. The Azure ATP portal allows you to create your Azure ATP instance, and view the data received from Azure ATP sensors. You can also use the portal to monitor, manage, and investigate threats in your network environment.
- **Azure ATP sensor**. Azure ATP sensors are installed directly on your domain controllers. The sensor monitors domain controller traffic without requiring a dedicated server or configuring port mirroring.
- **Azure ATP cloud service**. Azure ATP cloud service runs on Azure infrastructure and is currently deployed in the United States, Europe, and Asia. Azure ATP cloud service is connected to Microsoft's intelligent security graph.

13 https://azure.microsoft.com/features/azure-advanced-threat-protection?azure-portal=true



Purchasing

Azure ATP is available as part of the Enterprise Mobility + Security 5 suite (EMS E5), and as a standalone license. You can acquire a license directly from the **Enterprise Mobility Security Pricing Options**[14] page, or through the Cloud Solution Provider (CSP) licensing model. It is not available to purchase via the Azure portal.

14 https://www.microsoft.com/cloud-platform/enterprise-mobility-security-pricing?azure-portal=true

Azure Governance methodologies

Azure Policy

Azure Policy[15] is a service in Azure that you use to create, assign, and, manage policies. These policies enforce different rules and effects over your resources, so those resources stay compliant with your corporate standards and service-level agreements (SLAs).

Azure Policy does this by using policies and initiatives. It runs evaluations of your resources and scans for those not compliant with the policies you have created. For example, you can have a policy to allow only a certain stock keeping unit (SKU) size of virtual machines (VMs) in your environment. Once you implement this policy, it will evaluate resources when you create new ones or update existing ones. It will also evaluate your existing resources.

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.

Azure Policy can also integrate with Azure DevOps, by applying any continuous integration and delivery pipeline policies that apply to the pre-deployment and post-deployment of your applications.

Azure Policy also can automatically remediate resources and configurations that are deemed non-compliant, thus ensuring the integrity of the state of the resources.

Implementing Azure Policy

There are three steps to creating an implementing an Azure policy.

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 if they are exposed to a public IP address. You also could prevent a hard disk from being used when deploying VMs to control costs.

Every policy definition has conditions under which it is enforced. And, it has an accompanying effect that takes place if the conditions are met. Here are some example policy definitions:

- **Allowed Storage Account SKUs**. This policy definition has a set of conditions/rules that determine whether a storage account that is being deployed is within a set of SKU sizes. Its effect is to deny all storage accounts that do not adhere to the set of defined SKU sizes.
- **Allowed Resource Type**. This policy definition has a set of conditions/rules to specify the resource types that your organization can deploy. Its effect is to deny all resources that are not part of the defined list.

15 https://azure.microsoft.com/services/azure-policy?azure-portal=true

- **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.
- **Allowed Virtual Machine SKUs**. This policy enables you to specify a set of VM SKUs that your organization can deploy.

More sample policies are available on the **Azure Policy Samples**[16] page.

Assign a definition to a scope of resources

To implement your policy definitions, you assign them to resources. A policy assignment is a policy definition that has been assigned to take place within a specific scope. This specific scope could range from a management group to a resource group. Policy assignments are inherited by all child resources. This means that if a policy is applied to a resource group, it is applied to all the resources within that resource group. However, you can exclude a subscope from the policy assignment.

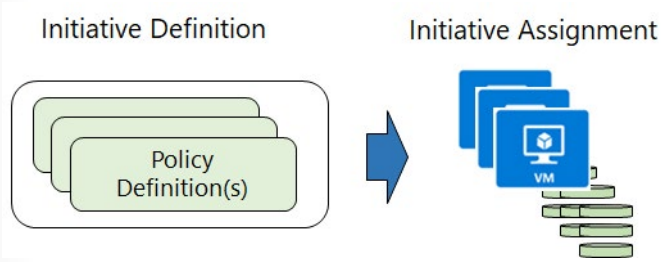
Review the policy evaluation results

When a condition is evaluated against your existing resources it is marked compliant or non-compliant. You can review the non-compliant policy results and take any action that is needed.

✓ Policy evaluation happens about once an hour, which means that if you make changes to your policy definition and create a policy assignment then it will be re-evaluated over your resources within the hour.

Policy Initiatives

Policy Initiatives work with Azure Policies.



Initiative definitions

An initiative definition is a set of policy definitions to help track your compliance state for a larger goal. Initiative assignments reduce the need to make several initiative definitions for each scope.

For example, you could create an initiative named *Enable Monitoring in Azure Security Center*, with a goal to monitor all the available security recommendations in your Azure Security Center.

Under this initiative, you would have the following policy definitions:

- *Monitor unencrypted SQL Database in Security Center* – For monitoring unencrypted SQL databases and servers.
- *Monitor OS vulnerabilities in Security Center* – For monitoring servers that do not satisfy the configured baseline.

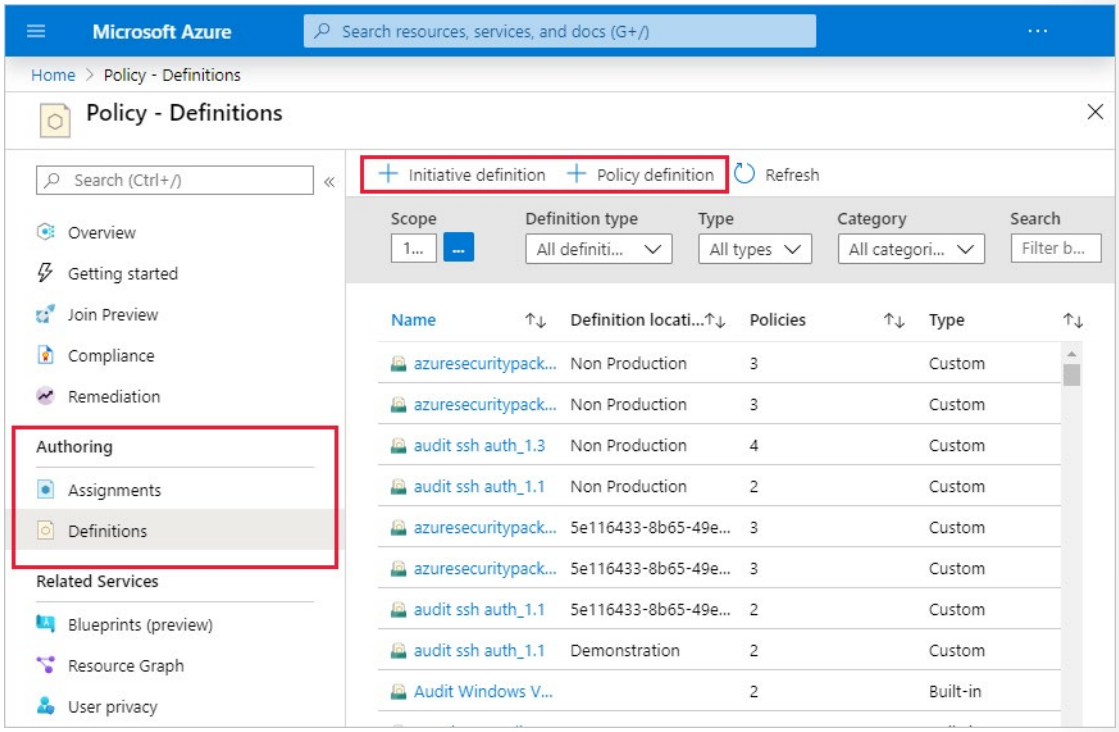
16 https://docs.microsoft.com/azure/governance/policy/samples?azure-portal=true

- *Monitor missing Endpoint Protection in Security Center* – For monitoring servers without an installed endpoint protection agent.

Initiative assignments

Like a policy assignment, an initiative assignment is an initiative definition assigned to a specific scope. Initiative assignments reduce the need to make several initiative definitions for each scope. This scope could also range from a management group to a resource group.

You can define initiatives using the Azure portal, or command-line tools. In the portal, you use the "Authoring" section.



✓ Even if you have a single policy, we recommend using initiatives if you anticipate increasing the number of policies over time.

Walkthrough-Create an Azure Policy

In this walkthrough, we will create an Azure Policy to restrict deployment of Azure resources to a specific location.

Task 1: Create a Policy assignment

In this task, we will configure the Allowed location policy and assign it to our subscription.

Task 2: Test Allowed location policy

In this task, we will test the Allowed location policy.

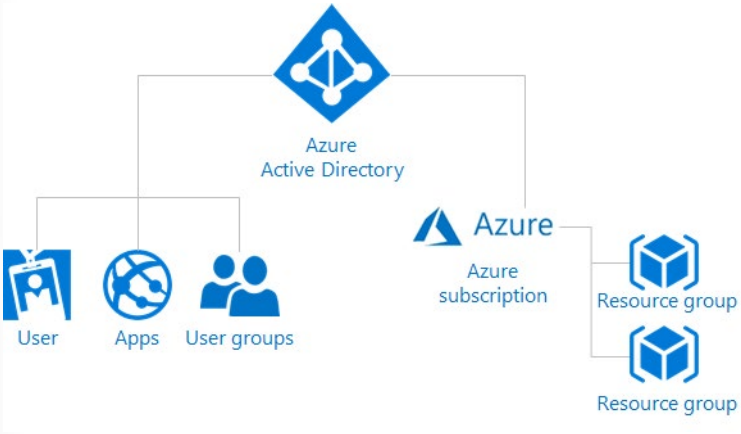
Task 3: Delete the policy assignment

In this task, we will remove the Allowed location policy assignment and test.

Congratulations! You have created an Azure Policy to restrict deployment of Azure resources to a particular datacenter.

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.

Role-based Access Control (RBAC)



Role-based access control[17] provides fine-grained access management for Azure resources, enabling you to grant users only the rights they need to perform their jobs. RBAC is provided at no additional cost to all Azure subscribers.

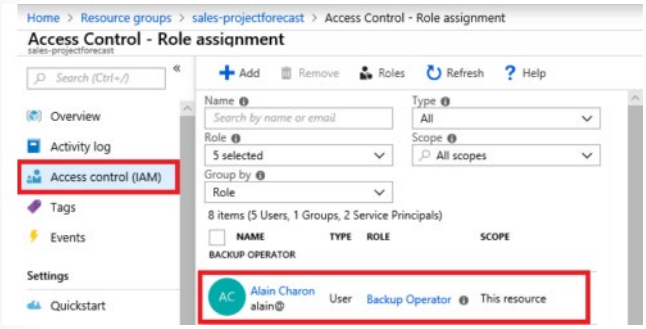
Usage Scenarios

Examples of when you might use RBAC include when you want 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.

To view access permissions, access the **Access Control** (IAM) blade in the Azure portal. This blade, shows who has access to an area and their role. Using this same blade, you can also grant or remove access.

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.



17 https://docs.microsoft.com/azure/role-based-access-control/overview?azure-portal=true

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 will have write permissions on that resource group.

Best Practices

Here are some RBAC best practices:

- Using RBAC, segregate duties within your team and grant only the amount of access to users that they need to perform their jobs. Instead of giving everybody unrestricted permissions in your Azure subscription or resources, allow only certain actions at a scope level.
- When planning your access control strategy, grant users the lowest privilege level that they need to do their work.

Walkthrough-Manage access with RBAC

In this walkthrough, we will assign roles and view activity logs.

Task 1: View and assign roles

In this task, we will assign the Virtual machine contributor role.

Task 2: View the activity log and remove a role assignment

In this task, we will view the activity log to verify the role assignment, and then remove the role.

Congratulations! You have assigned roles and viewed activity logs.

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.

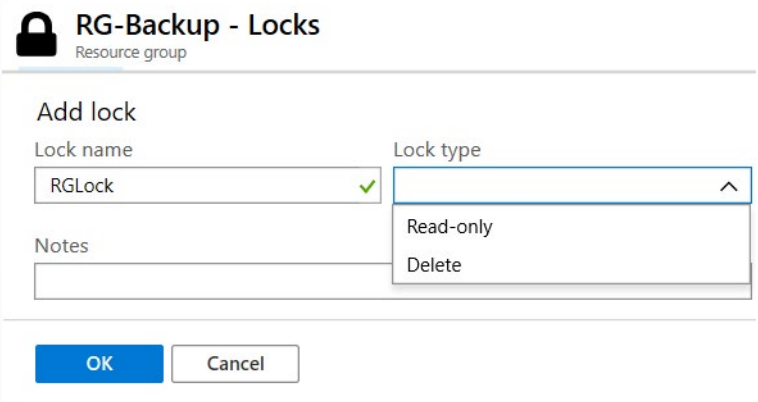
Resource Locks

Contoso, Ltd. Case Study - In a recent conversation, your manager mentioned that there had been instances where critical Azure resources were mistakenly deleted. Since there was disorganization across their Azure environment, good intentions of cleaning up unnecessary resources resulted in accidental deletions of resources critical to other systems. You've heard of resource locks on Azure. You mention to your manager that you think you can help prevent this type of incident from happening in the future. You'll take a look at how you could use resource locks to solve this problem.

What are resource locks?

Resource Locks[18] help you prevent accidental deletion or modification of your Azure resources. You can manage these locks from within the Azure portal. To view, add, or delete locks, go to the **SETTINGS** section of any resource's settings blade.

18 https://docs.microsoft.com/azure/azure-resource-manager/resource-group-lock-resources?azure-portal=true



You may need to lock a subscription, resource group, or resource to prevent other users in your organization from accidentally deleting or modifying critical resources. You can set the lock level to **CanNotDelete** or **ReadOnly**:

- **CanNotDelete** means authorized admins can still read and modify a resource, but they can't delete the resource.
- **ReadOnly** means authorized admins can read a resource, but they can't delete or update the resource. Applying this lock is like restricting all authorized users to the permissions granted by the Reader role.

When a resource lock is applied, you must first remove the lock in order to perform that activity. By putting an additional step in place before allowing the action to be taken on the resource, it helps protect resources from inadvertent actions, and 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'll actually be able to perform the blocked activity.

Walkthrough-Manage resource locks

In this walkthrough, we will create a resource group, add a lock to resource group and test deletion, test deleting a resource in the resource group, and remove the resource lock.

Task 1: Create a resource group

In this task, we will create a resource group.

Task 2: Add a Lock to the resource group and test deletion

In this task, we will add a lock to the resource group and test deletion.

Task 3: Test deleting a member of the resource group

In this task, we will add a storage account to the resource group and test deletion.

Task 4: Remove the resource lock

In this task, we will remove the resource lock.

Congratulations! You created a resource group, added a lock to resource group and tested deletion, tested deleting a resource in the resource group, and removed the resource lock.

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.

Azure Blueprints

Azure Blueprints[19] enable cloud architects to define a repeatable set of Azure resources that implement and adhere to an organization's standards, patterns, and requirements. Azure Blueprint 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 development and delivery.

Azure Blueprint is a declarative way to orchestrate the deployment of various resource templates and other artifacts, such as:

- Role assignments
- Policy assignments
- Azure Resource Manager templates
- Resource groups

Blueprint process

The process of implementing Azure Blueprint consists of the following high-level steps:

1. Create an Azure Blueprint.
2. Assign the blueprint.
3. Track the blueprint assignments.

With Azure Blueprint, the relationship between the blueprint definition (what should be deployed) and the blueprint assignment (what was deployed) is preserved. This connection supports improved deployment tracking and auditing.

Azure Blueprints are different from Azure Resource Manager Templates. When Azure Resource Manager Templates deploy resources, they have no active relationship with the deployed resources (they exist in a local environment or in source control). By contrast, with Azure Blueprint, each deployment is tied to an Azure Blueprint package. This means that the relationship with resources will be maintained, even after deployment. Maintaining relationships, in this way, improves auditing and tracking capabilities.

Usage Scenario

Adhering to security or compliance requirements, whether government or industry requirements, can be difficult and time-consuming. To help you with auditing, traceability, and compliance with your deployments, use Azure Blueprint artifacts and tools. Time-consuming paperwork is no longer needed, and your path to certification is expedited.

Azure Blueprint are also useful in Azure DevOps scenarios, where blueprints are associated with specific build artifacts and release pipelines and can be tracked more rigorously.

19 https://azure.microsoft.com/services/blueprints?azure-portal=true

Subscription governance

Azure subscriptions are discussed in many contexts. For this module, however we wish to briefly mention them here in the context of governance.

There are mainly three aspects to consider in relation to creating and managing subscriptions: **Billing**, **Access Control**, and **Subscription limits**.

- **Billing**: Reports can be generated by subscriptions, if you have multiple internal departments and need to do "chargeback", a possible scenario is to create subscriptions by department or project.
- **Access Control**: A subscription is a deployment boundary for Azure resources and every subscription is associated with an Azure AD tenant that provides administrators the ability to set up role-based access control (RBAC). When designing a subscription model, one should consider the deployment boundary factor, some customers have separate subscriptions for Development and Production, each one is isolated from each other from a resource perspective and managed using RBAC.
- **Subscription Limits**: Subscriptions are also bound to some hard limitations. For example, the maximum number of Express Route circuits per subscription is 10. Those limits should be considered during the design phase, if there is a need to go over those limits in particular scenarios, then additional subscriptions may be needed. If you hit a hard limit, there is no flexibility.

Also available to assist with managing subscriptions are management groups, which manage access, policies, and compliance across multiple Azure subscriptions. We will discuss management groups in more detail later.

✓ There is more information about **subscription limits**[20].

20 https://docs.microsoft.com/azure/azure-subscription-service-limits?azure-portal=true

Monitoring and reporting in Azure

Tags

You apply **tags**[21] to your Azure resources giving metadata to logically organize them into a taxonomy. Each tag consists of a name and a value pair. For example, you can apply the name **Environment** and the value **Production** to all the resources in production, or tag by company departments. For example, the name of **Department** with a value of **IT**.

Name	Value
Environment	Production
Department	IT

After you apply tags, you can retrieve all the resources in your subscription with that tag name and value. Tags enable you to retrieve related resources from different resource groups. This approach is helpful when you need to organize resources for billing or management.

Tag Limitations

There are some limitations with using **Tags**, such as:

- Not all resource types support tags.
- Each resource or resource group can have a maximum of 50 tag name/value pairs. Currently, storage accounts only support 15 tags, but that limit will be raised to 50 in a future release. If you need to apply more tags than the maximum allowed number, use a JSON string for the tag value. The JSON string can contain many values that are applied to a single tag name. A resource group can contain many resources that each have 50 tag name/value pairs.
- The tag name is limited to 512 characters, and the tag value is limited to 256 characters. For storage accounts, the tag name is limited to 128 characters, and the tag value is limited to 256 characters.
- Virtual Machines and Virtual Machine Scale Sets are limited to a total of 2048 characters for all tag names and values.
- Tags applied to the resource group are not inherited by the resources in that resource group.

✓ You can use Azure Policy to enforce tagging values and rules on resources.

Walkthrough-Implement resource tagging

In this walkthrough, we will create a policy assignment that requires tagging, created a storage account and test the tagging, view resources with a specified tag, and remove the tagging policy.

Task 1: Create a Policy assignment

In this task, we will configure the **Require specified tag** policy and assign it to our subscription.

Task 2: Create a storage account to test the required tagging

In this task, we will create storage accounts to test the required tagging.

Task 3: View all resources with a specific tag

In this task, we will view resources with a specific tag.

21 https://docs.microsoft.com/azure/azure-resource-manager/resource-group-using-tags?azure-portal=true

Task 4: Delete the policy assignment

In this task, we will remove the **Require specific tag** policy so it does not affect our future work.

Congratulations! In this walkthrough, we created a policy assignment that required tagging, created a storage account and tested the tagging, viewed resources with a specified tag, and removed the tagging policy.

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.

Azure Monitor

Azure Monitor[22] maximizes the availability and performance of your applications by delivering a comprehensive solution for collecting, analyzing, and acting on telemetry from your cloud and on-premises environments. It helps you understand how your applications are performing and proactively identifies issues affecting them and the resources they depend on.

What data does Azure Monitor collect?

Azure Monitor can collect data from a variety of sources. You can think of monitoring data for your applications in tiers ranging from your application, any operating system and services it relies on, down to the platform itself. Azure Monitor collects data from each of the following tiers:

- **Application monitoring data**: Data about the performance and functionality of the code you have written, regardless of its platform.
- **Guest OS monitoring data**: Data about the operating system on which your application is running. This could be running in Azure, another cloud, or on-premises.
- **Azure resource monitoring data**: Data about the operation of an Azure resource.
- **Azure subscription monitoring data**: Data about the operation and management of an Azure subscription, as well as data about the health and operation of Azure itself.
- **Azure tenant monitoring data**: Data about the operation of tenant-level Azure services, such as Azure Active Directory.

Diagnostic settings

As soon as you create an Azure subscription and start adding resources such as virtual machines and web apps, Azure Monitor starts collecting data.

- **Activity Logs** record when resources are created or modified.
- **Metrics** tell you how the resource is performing and the resources that it's consuming.

22 https://azure.microsoft.com/services/monitor?azure-portal=true

Enabling diagnostics

You can extend the data you're collecting into the actual operation of the resources by enabling **diagnostics** and adding an agent to compute resources. Under the resource settings you can enable Diagnostics

- **Enable guest-level monitoring**
- **Performance counters**: collect performance data
- **Event Logs**: enable various event logs
- **Crash Dumps**: enable or disable
- **Sinks**: send your diagnostic data to other services for more analysis
- **Agent**: configure agent settings

Azure Health Service

Azure Service Health[23] is a suite of experiences that provide personalized guidance and support when issues with Azure services affect you. It can notify you, help you understand the impact of issues, and keep you updated as the issue is resolved. Azure Service Health can also help you prepare for planned maintenance and changes that could affect the availability of your resources.

Azure Service Health is composed of the following:

- **Azure Status** provides a global view of the health state of Azure services. With Azure Status, you can get up-to-the-minute information on service availability. Everyone has access to Azure Status and can view all services that report their health state.
- **Service Health** provides you with a customizable dashboard that tracks the state of your Azure services in the regions where you use them. In this dashboard, you can track active events such as ongoing service issues, upcoming planned maintenance, or relevant *Health advisories*. When events become inactive, they are placed in your *Health history* for up to 90 days. Finally, you can use the **Service Health** dashboard to create and manage service *Health alerts*, which notify you whenever there are service issues that affect you.
- **Resource Health** helps you diagnose and obtain support when an Azure service issue affects your resources. It provides you details with about the current and past state of your resources. It also provides technical support to help you mitigate problems. In contrast to Azure Status, which informs you about service problems that affect a broad set of Azure customers, Resource Health gives you a personalized dashboard of your resources' health. Resource Health shows you times, in the past, when your resources were unavailable because of Azure service problems. It's then easier for you to understand if an SLA was violated.

Together, the Azure Service Health components provide you with a comprehensive view of the health status of Azure, at the level of granularity that is most relevant to you.

Monitoring applications and services

Data monitoring is only useful if it improves your visibility of the operations in your computing environment. **Azure Monitor** includes several features and tools that provide valuable insights into your applica-

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

tions, and the other resources they may depend on. Monitoring solutions and features, such as **Application Insights** and **Container Insights**, provide you with a deeper look into different aspects of your application and Azure services.

Azure Monitor features can be organized into four categories, these categories are: **Analyze**, **Respond**, **Visualize** and **Integrate**.

Analyze

- **Application Insights** is a service that monitors the availability, performance, and usage of your web applications, whether they're hosted in the cloud or on-premises. It leverages the powerful data analysis platform in Log Analytics to provide you with deeper insights into your application's operations. Application Insights can diagnose errors, without waiting for a user to report them. Application Insights includes connection points to a variety of development tools and integrates with Microsoft Visual Studio to support your DevOps processes.
- **Azure Monitor for containers** is a service that is designed to monitor the performance of container workloads, which are deployed to managed Kubernetes clusters hosted on Azure Kubernetes Service (AKS). It gives you performance visibility by collecting memory and processor metrics from controllers, nodes, and containers, which are available in Kubernetes through the metrics API. Container logs are also collected.
- **Azure Monitor for VMs** is a service that monitors your Azure VMs at scale, by analyzing the performance and health of your Windows and Linux VMs (including their different processes and interconnected dependencies on other resources, and external processes). Azure Monitor for VMs includes support for monitoring performance and application dependencies for VMs hosted on-premises, and for VMs hosted with other cloud providers.

Integrating any, or all, of these monitoring services with Azure Service Health has additional benefits. Staying informed of the health status of Azure services will help you understand if, and when, an issue affecting an Azure service is impacting your environment. What may seem like a localized problem could be the result of a more widespread issue, and Azure Service Health provides this kind of insight. Azure Service Health identifies any issues with Azure services that might affect your application. Azure Service Health also helps you to plan for scheduled maintenance.

Respond

In addition to allowing you to analyze your monitoring data interactively, an effective monitoring solution must respond proactively to any critical conditions that are identified within the data it collects. This might involve, for example, sending a text or email to an administrator who is responsible for investigating an issue, or launching an automated process that attempts to correct an error condition.

- **Alerts**. Azure Monitor proactively notifies you of critical conditions using Alerts and can potentially attempt to take corrective actions. Alert rules based on metrics can provide alerts in almost real-time, based on numeric values. Alert rules based on logs allow for complex logic across data, from multiple sources.
- **Autoscale**. Azure Monitor uses Autoscale to ensure that you have the right amount of resources running to manage the load on your application effectively. Autoscale enables you to create rules that use metrics, collected by Azure Monitor, to determine when to automatically add resources to handle increases in load. Autoscale can also help reduce your Azure costs by removing resources that are not being used. You can specify a minimum and maximum number of instances and provide the logic that determines when Autoscale should increase or decrease resources.

Visualize

Visualizations, such as charts and tables, are effective tools for summarizing monitoring data and for presenting data to different audiences. Azure Monitor has its own features for visualizing monitoring data, and it leverages other Azure services for publishing data for different audiences. Other tools you may use for visualizing data, for specific audiences and scenarios, include:

- **Dashboards**
- **Views**
- **Power BI**

Integrate

You'll often need to integrate Azure Monitor with other systems, and build customized solutions that use your monitoring data. Other Azure services can work with Azure Monitor to provide this integration.

Privacy, Compliance and Data Protection standards

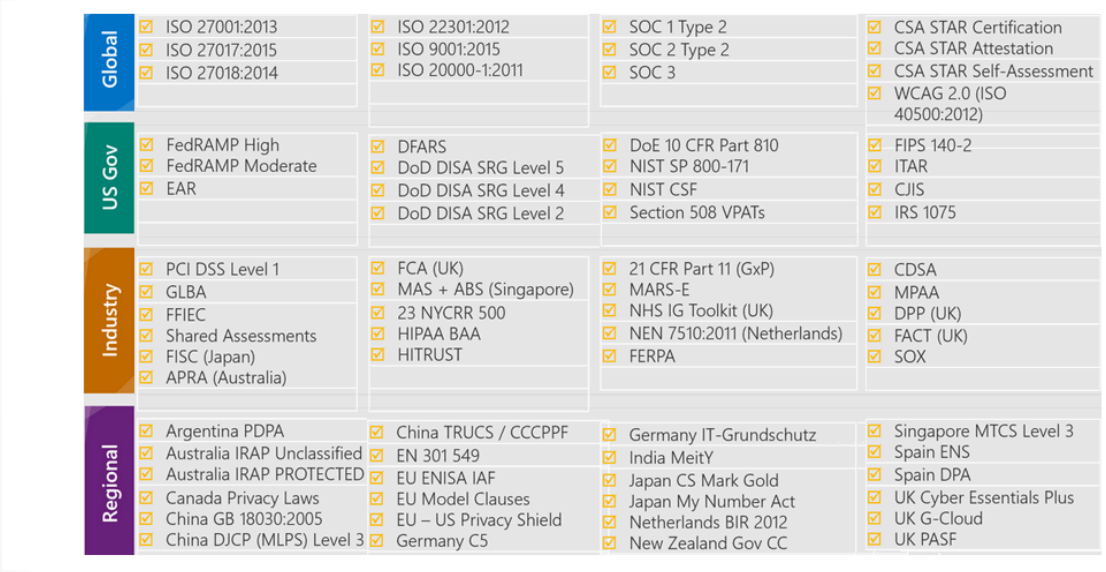
Compliance Terms

When selecting a cloud provider to host your solutions, you should understand how that provider can help you comply with regulations and standards. Some questions to ask about a potential provider include:

- How compliant is the cloud provider when it comes to handling sensitive data?
- How compliant are the services offered by the cloud provider?
- How can I deploy my own cloud-based solutions to scenarios that have accreditation or compliance requirements?

Microsoft invests heavily in the development of robust and innovative compliance processes. The Microsoft compliance framework for online services maps their controls to multiple regulatory standards, which enables Microsoft to design and build services using a common set of controls. These controls streamline compliance across a range of today's regulations as they continue to evolve in the future.

While the following image is not a full list of compliance offerings, it will provide you with an idea of the level of compliance offerings that are available with Azure.



Compliance Offerings:

The following list provides details about *some* of the compliance offerings available on Azure:

- **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.
- **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 CCM. It 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.

- **General Data Protection Regulation** (GDPR). As of May 25, 2018, a European privacy law—GDPR—is in effect. The GDPR imposes new rules on companies, government agencies, non-profits, and other organizations that offer goods and services to people in the European Union (EU), or that collect and analyze data tied to EU residents. The GDPR applies no matter where you are located.
- **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.
- **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.
- **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 SaaS. Microsoft was the first global cloud solution provider (CSP) 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)**. NSIT 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.
- **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 Pan Government Accreditor.

✓ Microsoft provides the most comprehensive set of compliance offerings (including certifications and attestations) of any cloud service provider.

✓ You can view all the Microsoft compliance offerings on the https://www.microsoft.com/trustcenter/compliance/complianceofferings?azure-portal=true Compliance Offerings webpage.

Microsoft Privacy statement

The **Microsoft privacy statement**[24] explains what personal data Microsoft processes, how Microsoft processes it, and for what purposes.

This privacy statement explains the personal data Microsoft processes, how Microsoft processes it, and for what purposes.

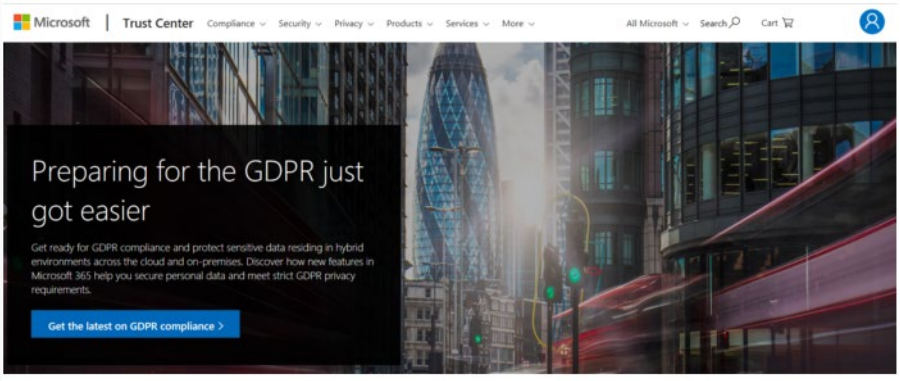
Microsoft offers a wide range of products, including server products used to help operate enterprises worldwide, devices you use in your home, software that students use at school, and services developers use to create and host what's next. References to Microsoft products in this statement include Microsoft services, websites, apps, software, servers, and devices.

Please read the product-specific details in this privacy statement, which provide additional relevant information. This statement applies to the interactions Microsoft has with you and the Microsoft products listed below, as well as other Microsoft products that display this statement.

Your privacy is important to us.

Trust Center

The **Trust Center**[25] is a website resource containing information and details about 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.



The Trust Center site provides:

- In-depth information about security, privacy, compliance offerings, policies, features, and practices across Microsoft cloud products.
- Recommended resources in the form of a curated list of the most applicable and widely used resources for each topic.
- Information specific to key organizational roles, including business managers, tenant admins or data security teams, risk assessment and privacy officers, and legal compliance teams.
- Cross-company document search, which is coming soon and will enable existing cloud service customers to search the Service Trust Portal.
- Direct guidance and support for when you can't find what you're looking for.

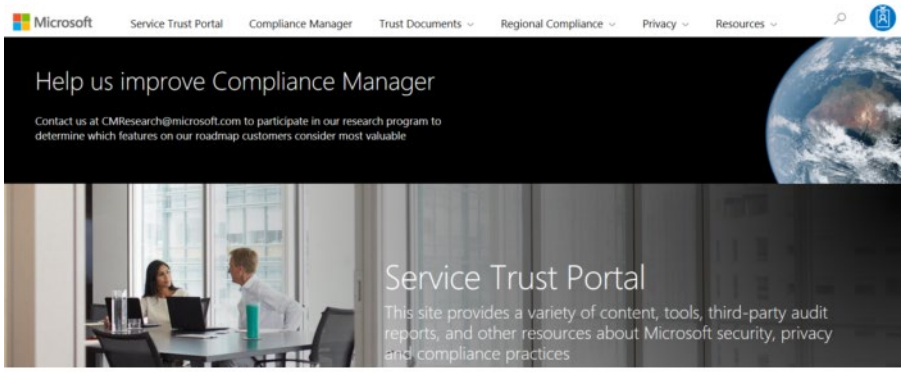
24 https://privacy.microsoft.com/privacystatement?azure-portal=true
25 https://www.microsoft.com/trustcenter?azure-portal=true

Service Trust Portal

The **Service Trust Portal** (STP) hosts the Compliance Manager service, and is the Microsoft public site for publishing audit reports and other compliance-related information relevant to Microsoft's cloud services. STP users can download audit reports produced by external auditors and gain insight from Microsoft-authored reports that provide details on how Microsoft builds and operates its cloud services.

STP also includes information about how Microsoft online services can help your organization maintain and track compliance with standards, laws, and regulations, such as:

- ISO
- SOC
- NIST
- FedRAMP
- GDPR



STP is a companion feature to the Trust Center, and allows you to:

- Access audit reports across Microsoft cloud services on a single page.
- Access compliance guides to help you understand how can you use Microsoft cloud service features to manage compliance with various regulations.
- Access trust documents to help you understand how Microsoft cloud services help protect your data.

Accessing the STP

To access some STP materials, you must sign in as an authenticated user with your Microsoft cloud services account (either an Azure AD organization account or a Microsoft account), and then review and accept the Microsoft Non-Disclosure Agreement for Compliance Materials.

Existing customers can access the STP at the https://aka.ms/STP?azure-portal=true Service Trust Portal webpage, with one of the following online subscriptions (trial or paid):

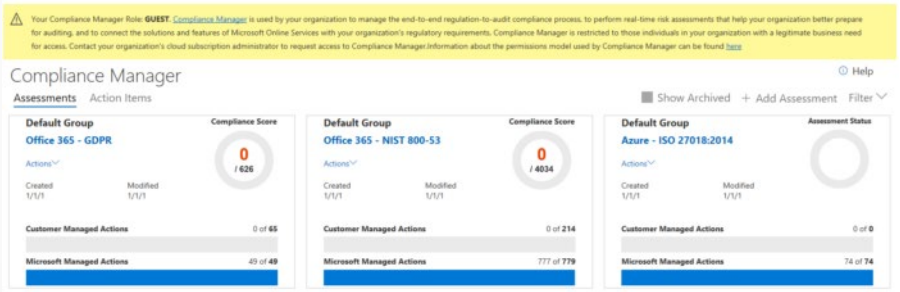
- Office 365
- Dynamics 365
- Azure

Compliance Manager

Compliance Manager[26] is a workflow-based risk assessment dashboard within the Trust Portal that enables you to track, assign, and verify your organization's regulatory compliance activities related to Microsoft professional services and Microsoft cloud services such as Office 365, Dynamics 365, and Azure.

Compliance Manager provides the following features:

- Detailed information provided by Microsoft to auditors and regulators, as part of various third-party audits of Microsoft 's cloud services against various standards (for example, ISO 27001, ISO 27018, and NIST).
- Information that Microsoft compiles internally for its compliance with regulations (such as HIPAA and the EU GDPR).
- An organization's self-assessment of their own compliance with these standards and regulations.
- Enables you to assign, track, and record compliance and assessment-related activities, which can help your organization cross team barriers to achieve your organization's compliance goals.
- Provides a Compliance Score to help you track your progress and prioritize auditing controls that will help reduce your organization's exposure to risk.
- Provides a secure repository in which to upload and manage evidence and other artifacts related to compliance activities.
- Produces richly detailed reports in Microsoft Excel that document the compliance activities performed by Microsoft and your organization, which can be provided to auditors, regulators, and other compliance stakeholders.



Compliance Manager provides ongoing risk assessments with a risk-based scores reference displayed in a dashboard view for regulations and standards. Alternatively, you can create assessments for the regulations or standards that matter more to your organization.

As part of the risk assessment, Compliance Manager also provides recommended actions you can take to improve your regulatory compliance. You can view all action items or select the action items that correspond with a specific certification.

✓ Compliance Manager is a dashboard that provides a summary of your data protection and compliance stature, and recommendations to improve data protection and compliance. The Customer Actions provided in Compliance Manager are recommendations only; it is up to each organization to evaluate the effectiveness of these recommendations in their respective regulatory environment prior to implementa-

26 https://docs.microsoft.com/microsoft-365/compliance/meet-data-protection-and-regulatory-reqs-using-microsoft-cloud?azure-portal=true

tion. Recommendations found in Compliance Manager should not be interpreted as a guarantee of compliance.

Walkthrough-Exploring the Trust Center

In this walkthrough, we will access the Trust Center, Service Trust Portal (STP), and Compliance Manager.

Task 1: Access the Trust Center

In this task, we will review the Trust Center.

Task 2: Access the Service Trust Portal (STP)

In this task, we will review the Service Trust Portal.

Task 3: Access the Compliance Manager

In this task, we will review the Compliance Manager.

Congratulations! In this walkthrough, you accessed the Trust Center, Service Trust Portal (STP), and Compliance Manager.

Microsoft Azure Government

Azure Government[27] 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, such as FedRAMP, NIST 800.171 (DIB), ITAR, IRS 1075, DoD L4, and 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 (US federal, state, and local government or their partners) are subject to validation of eligibility.

Azure Government provides the broadest compliance and Level 5 Department of Defense (DoD) approval. You can choose from six government-only datacenter regions, including two regions granted an Impact Level 5 Provisional Authorization. Azure Government also offers the most compliance certifications of any cloud provider.

✓ Most services are the same on both Azure Government and Public Azure. However, there are some differences that you should be aware of. Details are available at **Compare Azure Government and global Azure.**[28]

Azure China 21Vianet

Azure China 21Vianet[29] 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.

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.

27 https://azure.microsoft.com/global-infrastructure/government?azure-portal=true
28 https://docs.microsoft.com/azure/azure-government/compare-azure-government-global-azure?azure-portal=true
29 https://docs.microsoft.com/azure/china?azure-portal=true

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, as required by Chinese regulations for all systems and applications built on its architecture.

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.

According to the China Telecommunication Regulation (in Chinese), 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.

Module 3 Review Questions

Module 03 Review Questions

Review Question 1

Which of the following could grant or deny access based on the originating IP address?

- ☐ Azure Active Directory
- ☐ Azure Firewall
- ☐ VPN Gateway

Review Question 2

Which of the following could require both a password and a security question for full authentication?

- ☐ Azure Firewall
- ☐ Application Gateway
- ☐ Multi-Factor Authentication

Review Question 3

Which of the following services would you use to filter internet traffic in your Azure virtual network?

- ☐ Azure Firewall
- ☐ Network Security Group
- ☐ VPN Gateway

Review Question 4

Which of the following lets you store passwords in Azure so you can centrally manage them for your services and applications?

- ☐ Azure Advanced Threat Protection
- ☐ Azure Key Vault
- ☐ Azure Security Center

Review Question 5

Which of the following should you use to download published audit reports and how Microsoft builds and operates its cloud services?

- ☐ Azure Policy
- ☐ Azure Service Health
- ☐ Service Trust Portal

Review Question 6

Which of the following provides information about planned maintenance and changes that could affect the availability of your resources?

- ☐ Azure Monitor
- ☐ Azure Security Center
- ☐ Azure Service Health

Review Question 7

Where can you obtain details about the personal data Microsoft processes, how Microsoft processes it, and for what purposes?

- ☐ Microsoft Privacy Statement
- ☐ Compliance Manager
- ☐ Azure Service Health

Review Question 8

Which of the following can be used to help you enforce resource tagging so you can manage billing?

- ☐ Azure Policy
- ☐ Azure Service Health
- ☐ Compliance Manager

Review Question 9

Which of the following can be used to define a repeatable set of Azure resources that implement organizational requirements?

- ☐ Azure Blueprint
- ☐ Azure Policy
- ☐ Azure Resource Groups

Review Question 10

Which of the following lets you grant users only the rights they need to perform their jobs?

- ☐ Azure Policy
- ☐ Compliance Manager
- ☐ Role-Based Access Control

Review Question 11

Which of these options helps you most easily disable an account when an employee leaves your company?

- ☐ Enforce multi-factor authentication (MFA)
- ☐ Monitor sign-on attempts
- ☐ Use single sign-on (SSO)

Review Question 12

What is Azure Information Protection?

- ☐ AIP is a cloud-based solution that helps organizations classify and (optionally) protect its documents and emails by applying labels. Labels can be applied automatically (by administrators who define rules and conditions), manually (by users), or with a combination of both (where users are guided by recommendations).
- ☐ AIP is a cloud-based security solution that identifies, detects, and helps you investigate advanced threats, compromised identities, and malicious insider actions directed at your organization.
- ☐ AIP is a monitoring service that provides threat protection across all of your services both in Azure, and on-premises.

Review Question 13

Which of the following items would be good use of a resource lock?

- ☐ An ExpressRoute circuit with connectivity back to your on-premises network
- ☐ A non-production virtual machine used to test occasional application builds
- ☐ A storage account used to temporarily store images processed in a development environment

Review Question 14

Which of the following approaches would be the most efficient way to ensure a naming convention was followed across your subscription?

- ☐ Send out an email with the details of your naming conventions and hope it is followed.
- ☐ Create a policy with your naming requirements and assign it to the scope of your subscription
- ☐ Give all other users except for yourself read-only access to the subscription. Have all requests to create resources sent to you so you can review the names being assigned to resources, and then create them.

Module 3 Summary

Module 3 Summary

In this module you've learned about securing network connectivity in Azure, core identity services, security tools and features, Azure governance methodologies, monitoring and reporting in Azure, and privacy, compliance, and data protection standards in Azure.

Securing network connectivity in Azure

In this lesson you learned about Azure Firewalls, Azure DDos protection, NSGs, and choosing Azure network security solutions.

Core Azure identity services

In this lesson you learned about authentication and authorization, Azure AD, and MFA.

Security tools and features

In this lesson you learned about Azure Security Center and some usage scenarios for it, Key Vault, MSIP, and Azure ATP.

Azure governance methodologies

In this lesson you learned about Azure Policy, policies, initiatives, RBAC, locks, Azure Advisor, security assistance, and Azure Blueprint.

Monitoring and reporting in Azure

In this lesson you learned about Azure Monitor and Azure Service Health.

Privacy, compliance and data protection standards in Azure

In this lesson you learned about compliance terms and requirements, the Microsoft Privacy statement, Trust Center, the Service Trust Portal, Compliance Manager, Azure Government, Azure Germany, and Azure China.

Answers

Review Question 1

Which of the following could grant or deny access based on the originating IP address?

☐ Azure Active Directory

■ Azure Firewall

☐ VPN Gateway

Explanation
Azure Firewall. The Azure Firewall grants server access based on the originating IP address of each request. You create firewall rules that specify ranges of IP addresses. Only clients from these granted IP addresses will be allowed to access the server. Firewall rules also include specific network protocol and port information.

Review Question 2

Which of the following could require both a password and a security question for full authentication?

☐ Azure Firewall

☐ Application Gateway

■ Multi-Factor Authentication

Explanation
Multi-Factor Authentication (MFA). MFA can require two or more elements for full authentication.

Review Question 3

Which of the following services would you use to filter internet traffic in your Azure virtual network?

☐ Azure Firewall

■ Network Security Group

☐ VPN Gateway

Explanation
Network Security Group (NSG). NSGs allow you to filter network traffic to and from Azure resources in an Azure virtual network. 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.

Review Question 4

Which of the following lets you store passwords in Azure so you can centrally manage them for your services and applications?

☐ Azure Advanced Threat Protection

■ Azure Key Vault

☐ Azure Security Center

Explanation
Azure Key Vault. Azure Key Vault is a centralized cloud service for storing your applications' secrets. Key Vault helps you control your applications' secrets by keeping them in a single, central location and by providing secure access, permissions control, and access logging capabilities.

Review Question 5

Which of the following should you use to download published audit reports and how Microsoft builds and operates its cloud services?

☐ Azure Policy

☐ Azure Service Health

■ Service Trust Portal

Explanation
Service Trust Portal (STP). Service Trust Portal is the Microsoft public site for publishing audit reports and other compliance-related information relevant to Microsoft's cloud services. STP users can download audit reports produced by external auditors and gain insight from Microsoft-authored reports that provide details on how Microsoft builds and operates its cloud services.

Review Question 6

Which of the following provides information about planned maintenance and changes that could affect the availability of your resources?

☐ Azure Monitor

☐ Azure Security Center

■ Azure Service Health

Explanation
Azure Service Health. Azure Service Health is a suite of experiences that provide personalized guidance and support when issues with Azure services affect you. It can notify you, help you understand the impact of issues, and keep you updated as the issue is resolved. Azure Service Health can also help you prepare for planned maintenance and changes that could affect the availability of your resources.

Review Question 7

Where can you obtain details about the personal data Microsoft processes, how Microsoft processes it, and for what purposes?

■ Microsoft Privacy Statement

☐ Compliance Manager

☐ Azure Service Health

Explanation
Microsoft Privacy Statement. The Microsoft Privacy Statement explains what personal data Microsoft processes, how Microsoft processes it, and for what purposes.

Review Question 8

Which of the following can be used to help you enforce resource tagging so you can manage billing?

■ Azure Policy

☐ Azure Service Health

☐ Compliance Manager

Explanation
Azure Policy. Azure Policy can be used to enforce tagging values and rules on resources.

Review Question 9

Which of the following can be used to define a repeatable set of Azure resources that implement organizational requirements?

■ Azure Blueprint

☐ Azure Policy

☐ Azure Resource Groups

Explanation
Azure Blueprints. Azure Blueprints enable cloud architects to define a repeatable set of Azure resources that implement and adhere to an organization's standards, patterns, and requirements. Azure Blueprint 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 development and delivery.

Review Question 10

Which of the following lets you grant users only the rights they need to perform their jobs?

☐ Azure Policy

☐ Compliance Manager

■ Role-Based Access Control

Explanation
Role-Based Access Control (RBAC). RBAC lets you to grant users only the rights they need to perform their jobs.

Review Question 11

Which of these options helps you most easily disable an account when an employee leaves your company?

☐ Enforce multi-factor authentication (MFA)

☐ Monitor sign-on attempts

■ Use single sign-on (SSO)

Explanation
SSO centralizes user identity, so you can disable an inactive account in a single step.

Review Question 12

What is Azure Information Protection?

■ AIP is a cloud-based solution that helps organizations classify and (optionally) protect its documents and emails by applying labels. Labels can be applied automatically (by administrators who define rules and conditions), manually (by users), or with a combination of both (where users are guided by recommendations).

☐ AIP is a cloud-based security solution that identifies, detects, and helps you investigate advanced threats, compromised identities, and malicious insider actions directed at your organization.

☐ AIP is a monitoring service that provides threat protection across all of your services both in Azure, and on-premises.

Explanation
AIP helps you to track and secure the usage of your company's intellectual property.

Review Question 13

Which of the following items would be good use of a resource lock?

■ An ExpressRoute circuit with connectivity back to your on-premises network

☐ A non-production virtual machine used to test occasional application builds

☐ A storage account used to temporarily store images processed in a development environment

Explanation
Protection this mission critical resource from accidental deletion is a great idea.

Review Question 14

Which of the following approaches would be the most efficient way to ensure a naming convention was followed across your subscription?

☐ Send out an email with the details of your naming conventions and hope it is followed.

■ Create a policy with your naming requirements and assign it to the scope of your subscription

☐ Give all other users except for yourself read-only access to the subscription. Have all requests to create resources sent to you so you can review the names being assigned to resources, and then create them.

Explanation
Using Azure Policy ensures that you can not only recommend a naming standard but report on its adoption.

Module 4 Azure Pricing, Service Level Agreements, and Lifecycle

Learning Objectives

Learning Objectives

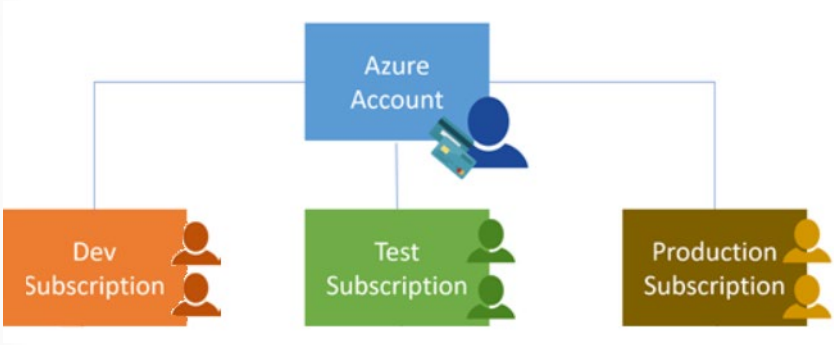
After completing this module, you will be able to:

- Understand and describe Microsoft Azure subscriptions and management groups.
- Recognize ways to plan and manage Azure costs.
- Understand and describe features of Azure service-level agreements (SLAs).
- Understand and describe the service lifecycle in Azure.

Azure Subscriptions

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.



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.

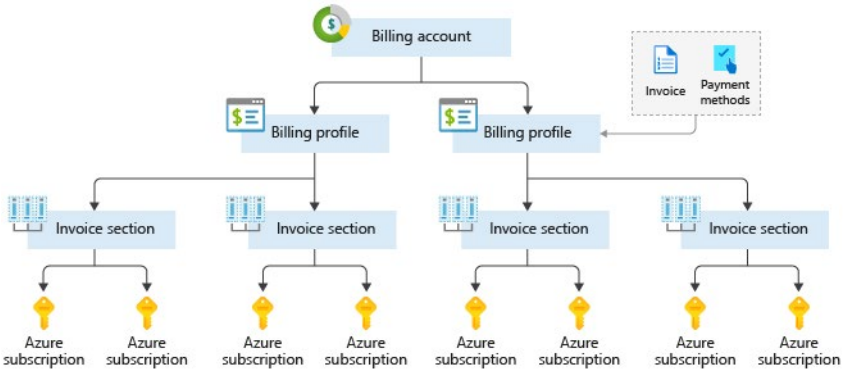
- **Billing:** You might want to also create additional subscriptions for billing purposes. Because costs are first aggregated at the subscription level, you might want to create subscriptions to manage and track costs based on your needs. For instance, you might want to create a subscription for your 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.

Customize billing to meet your needs

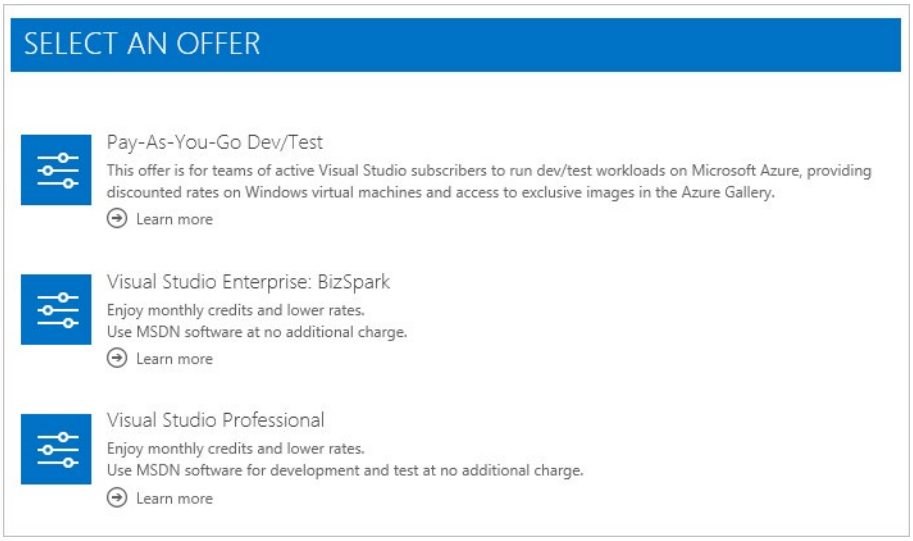
If you have multiple subscriptions, you can organize them into invoice sections. Each invoice section is a line item on the invoice that shows the charges incurred that month. For example, you might need a single invoice for your organization but want to organize charges by department, team, or project.

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.



Subscription options

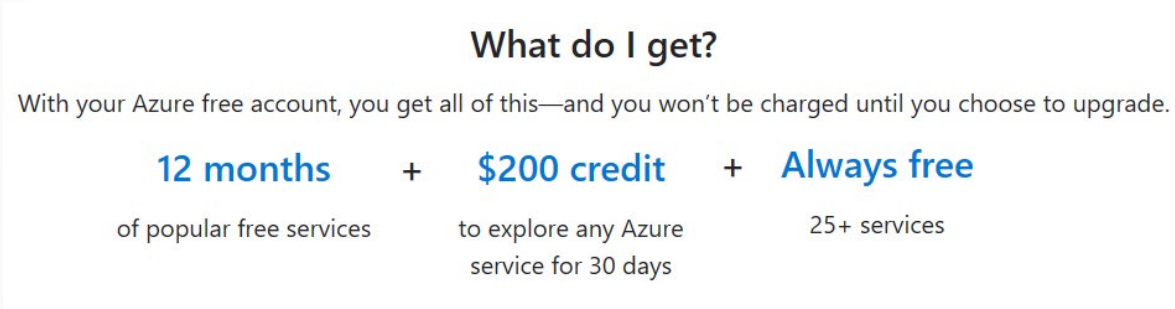


Azure offers free and paid subscription options to suit different needs and requirements.

- **A free account**. Get started with 12 months of popular free services, $200 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**. This subscription allows you to pay for what you use by attaching a credit or debit card to your account. Organizations can apply to Microsoft for invoicing privileges.
- **Member offers**. Your existing membership to certain Microsoft products and services affords you 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 BizSpark members, and Microsoft Imagine members.

✓ For more information on Azure subscription offers, refer to **Current Offers**[1].

Azure Free Accounts



An Azure **free account**[2] provides subscribers with 12 months of our most popular services, a $200 credit to explore any Azure service for 30 days, and over 25 services are free.

1 https://azure.microsoft.com/support/legal/offer-details?azure-portal=true
2 https://azure.microsoft.com/free?azure-portal=true

Do you pay anything to start with the Azure free account?
No. Starting is free, plus you get a $200 credit you can spend during the first 30 days.

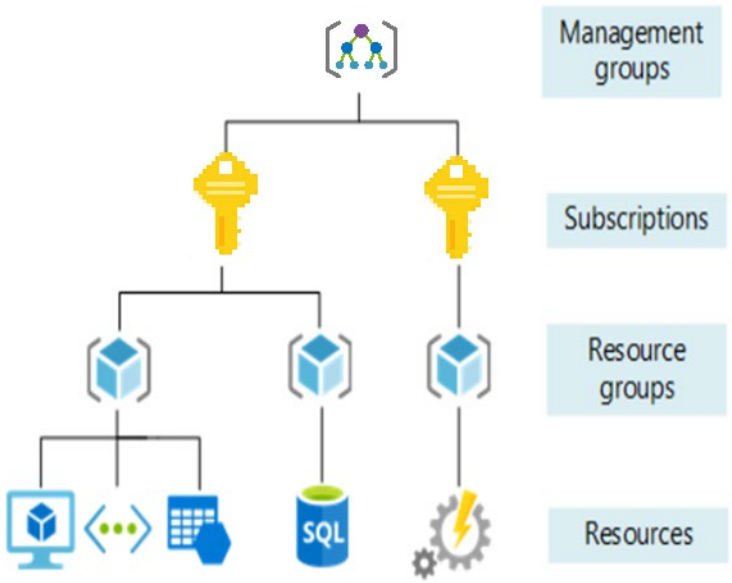
What do you need to sign up for a free account?
All you need is a phone number, a credit or debit card, and a GitHub account or Microsoft account username (formerly Windows Live ID).

What happens once you use my $200 free credit or I'm at the end of 30 days?
We'll notify you so you can decide if you want to upgrade to pay-as-you-go pricing and remove the spending limit. If you do, you'll have access to all the free products. If you don't, your account and products will be disabled, and you'll need to upgrade to resume usage.

What happens at the end of the 12 months of free products?
For 12 months after you upgrade your account, certain amounts of popular products for compute, networking, storage, and databases are free. After 12 months, any of these products you may be using will continue to run, and you'll be billed at the standard pay-as-you-go rates.

Management Groups

The organizing structure for resources in Azure has four levels: **Management groups**, **subscriptions**, **resource groups**, and **resources**. The following image shows the relationship of these levels i.e. the hierarchy of organization for the various objects



- **Management groups**: These are containers that 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.
  - 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.

- **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 you can create and use. Organizations can use subscriptions to manage costs and the resources that are created by users, teams, or projects.
- **Resource groups**: A resource group is a logical container into which Azure resources like web apps, databases, and storage accounts are deployed and managed.
- **Resources**: Resources are instances of services that you create, like virtual machines, storage, or SQL databases.

✓ Read more about **Management Groups**[3].

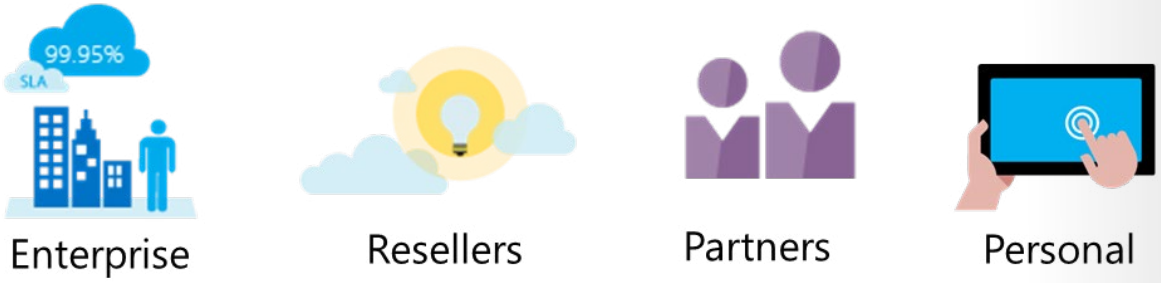
3 https://docs.microsoft.com/azure/governance/management-groups/overview?azure-portal=true

Planning and managing costs

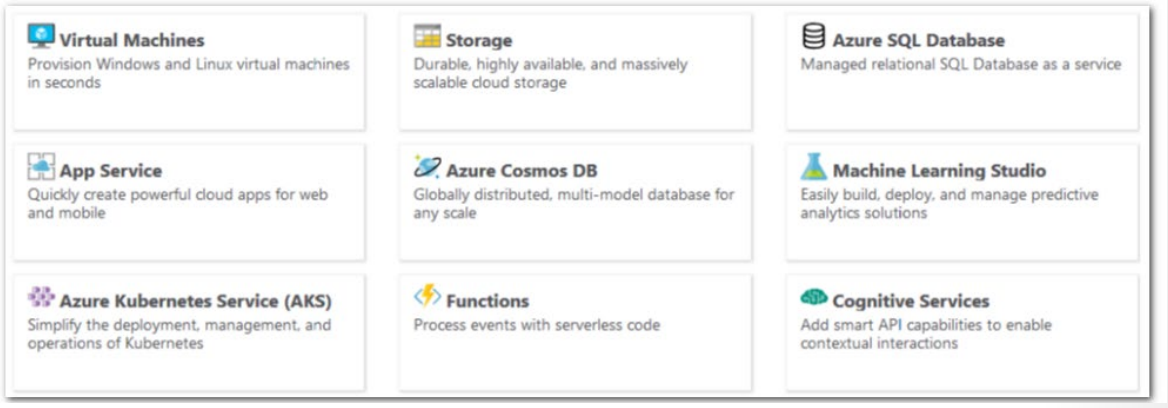
Purchasing Azure products and services

There are three main customer types on which the available purchasing options for Azure products and services is contingent, including:

- **Enterprise**. Enterprise customers sign an Enterprise Agreement with Azure that commits them to spending a negotiated amount on Azure services, which they typically pay annually. Enterprise customers also have access to customized Azure pricing.
- **Web direct**. Web direct customers pay public prices for Azure resources, and their monthly billing and payments occur through the Azure website.
- **Cloud Solution Provider**. Cloud Solution Provider (CSP) typically are Microsoft partner companies that a customer hires to build solutions on top of Azure. Payment and billing for Azure usage occurs through the customer's CSP.



Products and services in Azure are arranged by category, which have various resources that you can provision. You select the Azure products and services that fit your requirements, and your account is billed according to Azure's pay-for-what-you-use model.



✓ For more information about purchasing Azure products and services, refer to **Explore flexible purchasing options for Azure**[4].

4 https://azure.microsoft.com/pricing/purchase-options?azure-portal=true

At the end of each monthly billing cycle, the usage values will be charged to your payment method and the meters are reset. You can check the billing page in the Azure portal at any time to get a quick summary of your current usage and see any invoices from past billing cycles.

The key takeaway is that resources are always charged based on usage. For example, if you de-allocate a VM then you will not be billed for compute hours, I/O reads or writes or the private IP address since the VM is not running and has no allocated compute resources. However you will incur storage costs for the disks.

Note - De-allocating a VM is not the same as deleting a VM. De-allocation means the VM is not assigned to a CPU or network in a datacenter. However, your persistent disks remain, and the resource is present in your subscription. It's similar to turning off your physical computer.

Usage meters

When you provision an Azure resource, Azure creates one or more meter instances for that resource. The meters track the resources' usage, and each meter generates a usage record that is used to calculate your bill.

For example, a single virtual machine that you provision in Azure might have the following meters tracking its usage:

- Compute Hours
- IP Address Hours
- Data Transfer In
- Data Transfer Out
- Standard Managed Disk
- Standard Managed Disk Operations
- Standard IO-Disk
- Standard IO-Block Blob Read
- Standard IO-Block Blob Write
- Standard IO-Block Blob Delete

The following sections describe the main factors that affect Azure costs, including resource type, services, and the user's location.

Resource type

Costs are resource-specific, so the usage that a meter tracks and the number of meters associated with a resource depend on the resource type.

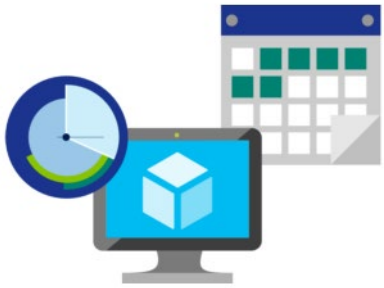
Note: Each meter tracks a specific type of usage. For example, a meter might track bandwidth usage (ingress or egress network traffic in bits-per-second), number of operations, size (storage capacity in bytes), or similar items.

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.

Services

Azure usage rates and billing periods can differ between Enterprise, Web Direct, and Cloud Solution Provider (CSP) customers. Some subscription types also include usage allowances, which affect costs.

The Azure team develops and offers first-party products and services, while products and services from third-party vendors are available in the Azure marketplace. Different billing structures apply to each of these categories.



Location

The Azure infrastructure is globally distributed, and usage costs might vary between locations that offer Azure products, services, and resources.

For example, you might want to build your Azure solution by provisioning resources in locations that offer the lowest prices, but this would require transferring data between locations, if dependent resources and their users are located in different parts of the world. If there are meters tracking the volume of data that transfers between the resources you provision, any potential savings you make from choosing the cheapest location could be offset by the additional cost of transferring data between those resources.

Note: For more information about Azure usage charges, refer to **Understand terms on your Microsoft Azure invoice**[5].

Billing Zones

Bandwidth[6] refers to data moving in and out of Azure datacenters. Some inbound data transfers, such as data going into Azure datacenters, are free. For outbound data transfers, such as data going out of Azure datacenters, data transfer pricing is based on **Zones**.

A Zone is a geographical grouping of Azure Regions for billing purposes. the following Zones exist and include the sample regions as listed below:

- **Zone 1** – West US, East US, Canada West, West Europe, France Central and others
- **Zone 2** – Australia Central, Japan West, Central India, Korea South and others

5 https://docs.microsoft.com/azure/billing/billing-understand-your-invoice?azure-portal=true
6 https://azure.microsoft.com/pricing/details/bandwidth?azure-portal=true

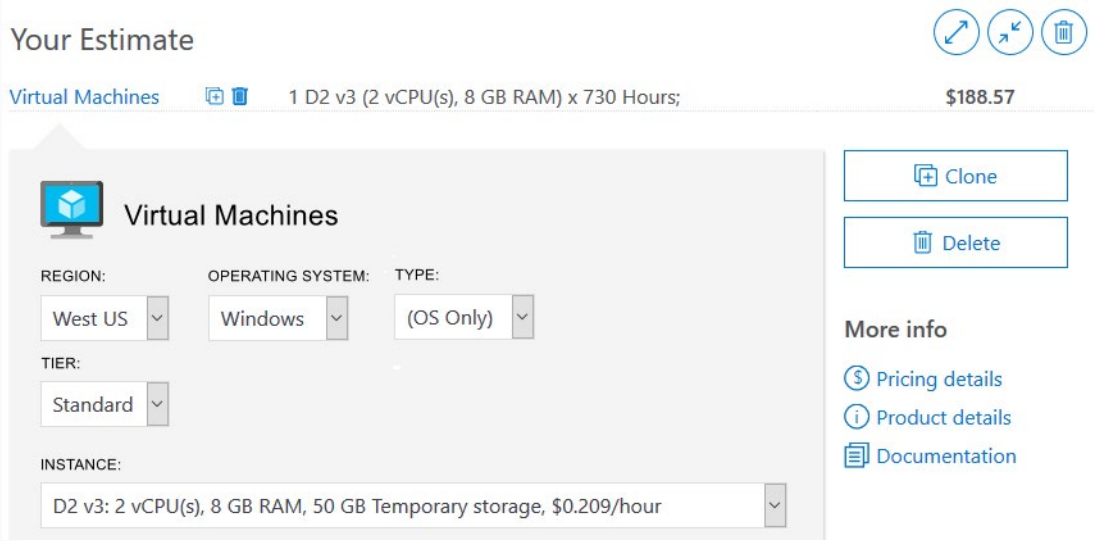
- **Zone 3** - Brazil South
- **DE Zone 1** - Germany Central, Germany Northeast

✓ To avoid confusion, be aware that a *Zone for billing purposes* is not the same as an *Availability Zone*. In Azure, the term *Zone* is for billing purposes only, and the full-term *Availability Zone* refers to the failure protection that Azure provides for datacenters.

Pricing Calculator

The **Pricing Calculator**[7] is a tool that helps you estimate the cost of Azure products. It displays Azure products in categories, and you choose the Azure products you need and configure them according to your specific requirements. Azure then provides a detailed estimate of the costs associated with your selections and configurations.

Get a new estimate from the pricing calculator by adding, removing, or reconfiguring your selected products. You also can access pricing details, product details, and documentation for each product from the pricing calculator.



The options that you can configure in the pricing calculator vary between products, but basic configuration options include:

- **Region**. Lists the regions from which you can provision a product. Southeast Asia, central Canada, the western United States, and Northern Europe are among the possible regions available for some resources.
- **Tier**. Sets the type of tier you wish to allocate to a selected resource, such as Free Tier, Basic Tier, etc.
- **Billing Options**. Highlights the billing options available to different types of customer and subscriptions for a chosen product.
- **Support Options**: Allows you to pick from included or paid support pricing options for a selected product.
- **Programs and Offers**. Allows you to choose from available price offerings according to your customer or subscription type.

7 https://azure.microsoft.com/pricing/calculator?azure-portal=true

- **Azure Dev/Test Pricing**. Lists the available development and test prices for a product. Dev/Test pricing applies only when you run resources within an Azure subscription that is based on a Dev/Test offer.

✓ The pricing calculator provides estimates, *not* actual price quotes. Actual prices may vary depending upon the date of purchase, the payment currency you are using, and the type of Azure customer you are.

Walkthrough-Use the Azure Pricing Calculator

In this walkthrough, we will use the Azure Pricing Calculator to generate a cost estimate for an Azure virtual machine and related network resources.

Task 1: Configure the pricing calculator

In this task, we will configure a simple infrastructure in the Azure Pricing Calculator.

Task 2: Review the pricing estimate

In this task, we will review the results of the Azure Pricing Calculator.

Congratulations! You downloaded an estimate from the Azure Pricing Calculator.

Total Cost of Ownership (TCO)

The **Total Cost of Ownership Calculator**[8] is a tool that you use to estimate cost savings you can realize by migrating to Azure. To use the TCO calculator, complete the three steps that the following sections explain.

Step 1: Define your workloads

Enter details about your on-premises infrastructure into the TCO calculator according to four groups:

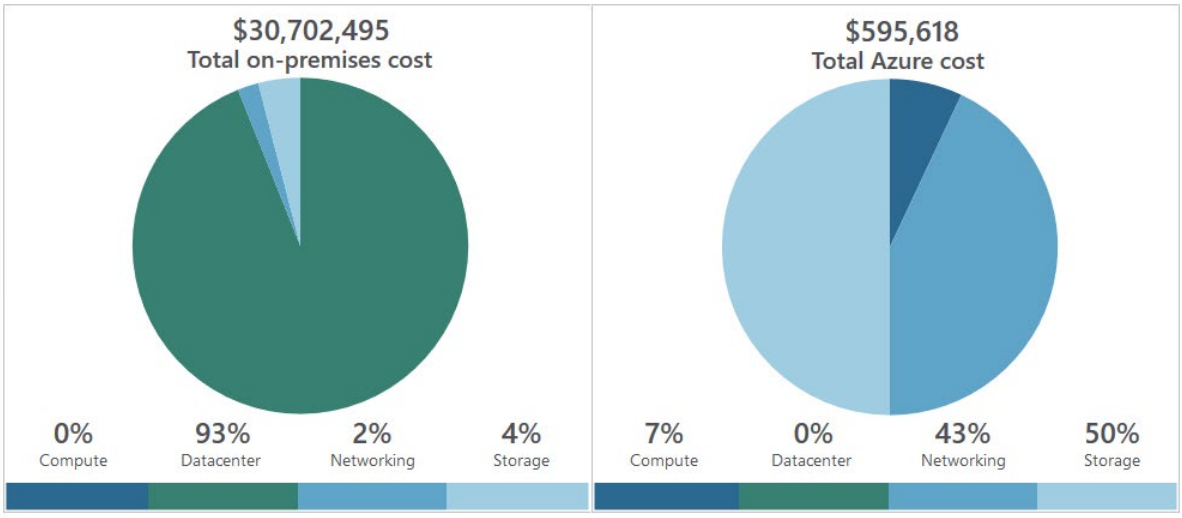
- **Servers**. Enter details of your current on-premises server infrastructure.
- **Databases**. Enter details of your on-premises database infrastructure in the **Source** section. In the **Destination** section, select the corresponding Azure service you would like to use.
- **Storage**. Enter the details of your on-premises storage infrastructure.
- **Networking**. Enter the amount of network bandwidth you currently consume in your on-premises environment.

Step 2: Adjust assumptions

Adjust the values of key assumptions that the TCO calculator makes, which might vary between customers. To improve the accuracy of the TCO calculator, you should adjust the values so they match the costs of your current on-premises infrastructure. The assumption values you can adjust include storage costs, IT labor costs, hardware costs, software costs, electricity costs, virtualization costs, datacenter costs, networking costs, and database costs.

8 https://azure.microsoft.com/pricing/tco?azure-portal=true

Step 3: View the report



The TCO calculator generates a detailed report based on the details you enter and the adjustments you make. The report allows you to compare the costs of your on-premises infrastructure with the costs using Azure products and services to host your infrastructure in the cloud.

Walkthrough-Use the Azure TCO Calculator

In this walkthrough, you will use the Total Cost of Ownership (TCO) Calculator to generate cost comparison report for an on-premises environment.

Task 1: Configure the TCO calculator

In this task, we will add infrastructure information to the calculator.

Task 2: Review the results and save a copy

In this task, we will review cost saving recommendations and download a report.

Congratulations! You have used the TCO Calculator to generate a cost comparison report for an on-premises environment.

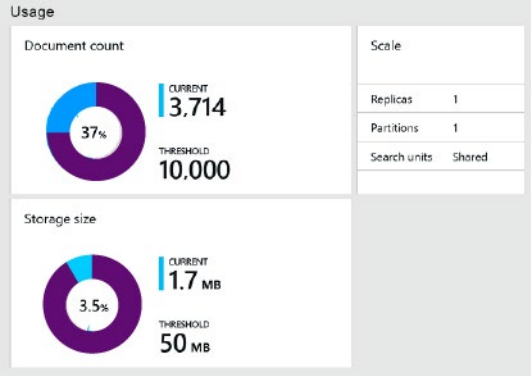
explore-minimizing-costs

The following best practice guidelines can help minimize your Azure costs.

Perform cost analyses

Plan your Azure solution wisely. 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. Additionally, you should calculate your projected costs by using the Azure Pricing and Total Cost of Ownership (TCO) calculators, only adding the products, services, and resources you need.

Monitor usage with Azure Advisor



In an efficient architecture, provisioned resources match the demand for those resources. The *Azure Advisor* feature identifies unused or under-utilized resources, and you can implement its recommendations by removing unused resources and configuring your resources to match your actual demand.

Use spending limits

Free trial customers and some credit-based Azure subscriptions can use the Spending Limits feature. Azure provides the Spending Limits feature to help prevent you from exhausting the credit on your account within each billing period. If you have a credit-based subscription and you reach your configured spending limit, Azure suspends your subscription until a new billing period begins.

The spending limit feature is not available for customers who aren't using credit-based subscriptions, such as Pay-As-You-Go subscribers.

Note: For more information on Azure spending limits, refer to **Understand Azure spending limit and how to remove it**[9]

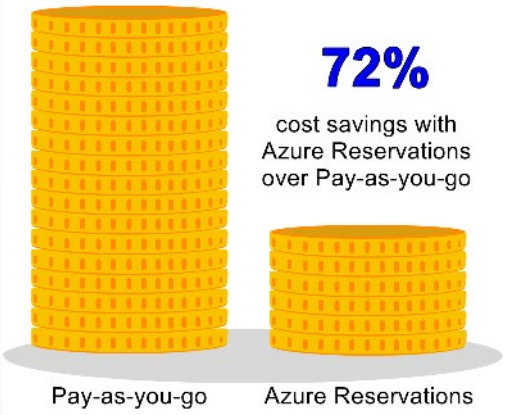
Note: Azure spending limits are not the same as Subscription, Service, or Resource Group limits and quotas. For more information, refer to **Azure subscription and service limits, quotas, and constraints.**[10]

Use Azure Reservations

Azure Reservations[11] offer discounted prices on certain Azure products and resources. To get a discount, you reserve products and resources by paying in advance. You can pre-pay for one year or three years of use of Virtual Machines, SQL Database Compute Capacity, Azure Cosmos Database Throughput, and other Azure resources.

Azure Reservations are only available to Enterprise or CSP customers and for Pay-As-You-Go subscriptions.

9 https://docs.microsoft.com/azure/billing/billing-spending-limit?azure-portal=true
10 https://docs.microsoft.com/azure/azure-subscription-service-limits?azure-portal=true
11 https://docs.microsoft.com/azure/billing/billing-save-compute-costs-reservations?azure-portal=true



Choose low-cost locations and regions

The cost of Azure products, services, and resources can vary across locations and regions, and if possible, you should use them in those locations and regions where they cost less.

Note: Some resources are metered and billed according to how much outgoing network bandwidth they consume (egress). *You should provision connected resources that are bandwidth metered in the same 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.

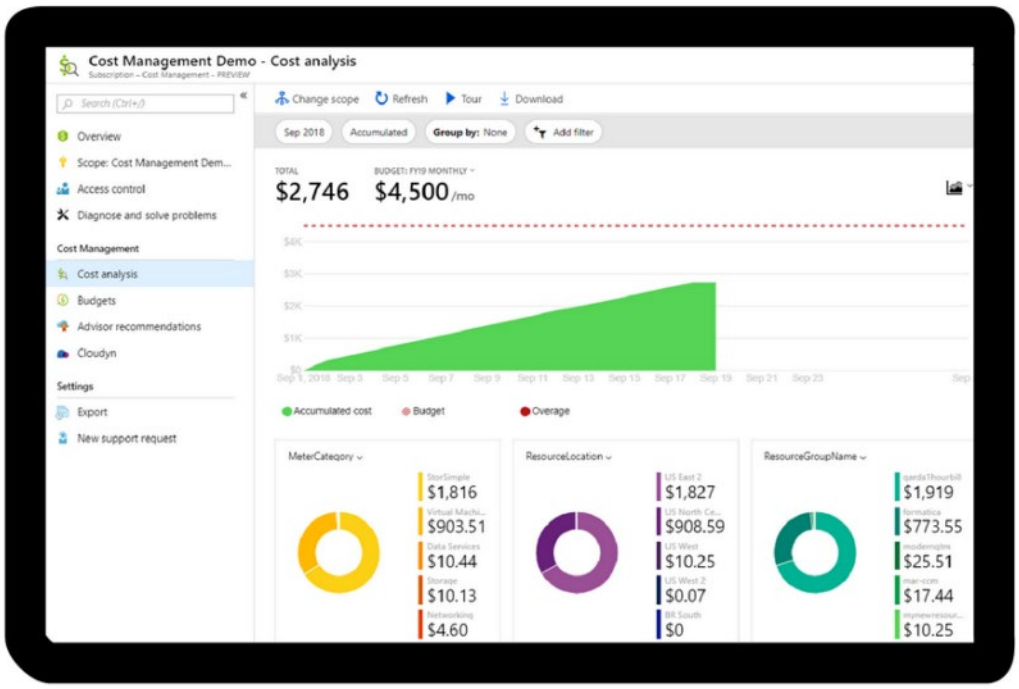
Apply tags to identify cost owners

Tags help you manage costs associated with the different groups of Azure products and resources. You can apply tags to groups of Azure products and 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 Production or Test. Tags make it easy to identify groups that generate the biggest Azure costs, so you can adjust your spending accordingly.

Cost Management

Cost Management[12] is an Azure product that provides a set of tools for monitoring, allocating, and optimizing your Azure costs.

12 https://azure.microsoft.com/services/cost-management?azure-portal=true



The main features of the Azure Cost Management toolset include:

- **Reporting**. Generate reports using historical data to 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.
- **Price**. Free to Azure customers.

Azure Service Level Agreements (SLAs)

Services Level Agreements

Microsoft maintains its commitment to providing customers with high-quality products and services by adhering to comprehensive operational policies, standards, and practices. Formal documents known as **Service-Level Agreements** (SLAs) capture the specific terms that define the performance standards that apply to Azure.

- SLAs describe Microsoft's commitment to providing Azure customers with certain performance standards.
- There are SLAs for individual Azure products and services.
- SLAs also specify what happens if a service or product fails to perform to a governing SLA's specification.

Performance Targets, Uptime and Connectivity Guarantees

A **SLA**[13] defines performance targets for an Azure product or service. The performance targets that a SLA defines are specific to each Azure product and service.

For example, performance targets for some Azure services are expressed in terms of uptime or connectivity rates.

Performance targets range from 99.9 percent to 99.99 percent

A typical SLA specifics performance-target commitments that range from 99.9 percent (“three nines”) to 99.99 percent ("four nines"), for each corresponding Azure product or service. These targets can apply to such performance criteria as uptime, or response times for services.

For example, the SLA for the Azure Database for MySQL service guarantees 99.99 percent uptime. The Azure Cosmos DB (Database) service SLA offers 99.99 percent uptime, which includes low-latency commitments of less than 10 milliseconds on DB read operations and less than 15 milliseconds on DB write operations.

13 https://azure.microsoft.com/support/legal/sla/summary?azure-portal=true

SLA downtime estimates

The following table lists the potential cumulative downtime for various SLA levels over different durations:

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

Service Credits

SLAs also describe how Microsoft will respond if an Azure product or service fails to perform to its governing SLA's specification.

For example, customers may have a discount applied to their Azure bill, as compensation for an under-performing Azure product or service. The table below explains this example in more detail.

The first column in the table below shows monthly uptime percentage SLA targets for a single instance Azure Virtual Machine. The second column shows the corresponding service credit amount you receive, if the *actual* uptime is less than the specified SLA target for that month.

Monthly Uptime Percentage	Service Credit Percentage
< 99.9	10
< 99	25
< 95	100

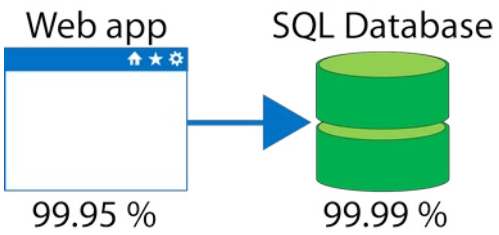
✓ Azure does not provide SLAs for many services under the *Free* or *Shared* tiers. Also, free products such as Azure Advisor do not typically have a SLA.

Composite SLA

When combining SLAs across different service offerings, the resultant SLA is a called a *Composite SLA*. The resulting composite SLA can provide higher or lower uptime values, depending on your application architecture.

Consider an App Service web app that writes to Azure SQL Database. At the time of this writing, these Azure services have the following SLAs:

- App Service Web Apps is 99.95 percent.
- SQL Database is 99.99 percent.



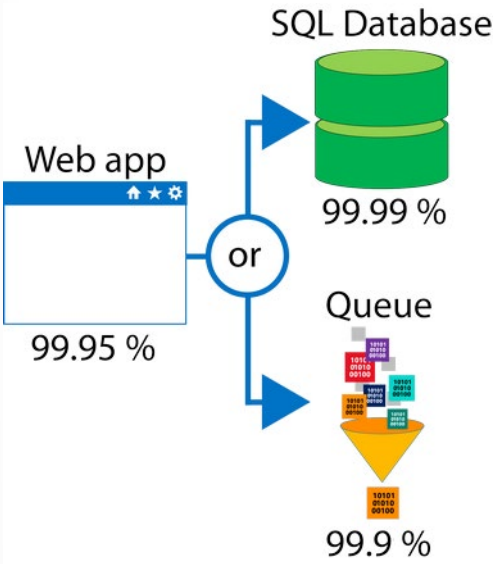
Maximum downtime you would expect for this example application

In the example above, if either service fails the whole application will fail. In general, the individual probability values for each service are independent. However, the composite SLA value for this application is:

```
99.95 percent × 99.99 percent = approx 99.94 percent
```

This means the combined probability of failure value is lower than the individual SLA values. This isn't surprising, because an application that relies on multiple services has more potential failure points.

Conversely, you can improve the composite SLA by creating independent fallback paths. For example, if **SQL Database** is unavailable, you can put transactions into a **Queue** for processing at a later time.



With the design shown in the image above, the application is still available even if it can't connect to the database. However, it fails if both the SQL Database **and** the Queue fail simultaneously. If the expected percentage of time for a simultaneous failure is `0.0001 × 0.001`, i.e. `(1.0 - 0.9999) x (1.0 - 0.999)`, the composite SLA for this combined path would be:

```
Database *OR* Queue = 1.0 - (0.0001 × 0.001) = 99.99999 percent
```

Therefore, the total composite SLA is:

```
Web app *AND* (Database *OR* Queue) = 99.95 percent × 99.99999 percent = ~
99.95 percent
```

However, there are tradeoffs to using this approach such as, the application logic is more complex, you are paying for the queue, and there may be data-consistency issues which you need to consider.

Application SLA

Azure customers can use SLAs to evaluate how their Azure solutions meet their business requirements and the needs of their clients and users. By creating your own SLAs, you can set performance targets to suit your specific Azure application. When creating an **Application SLA** consider the following:

- **Identify workloads**. A workload is a distinct capability or task that is logically separated from other tasks, in terms of business logic and data storage requirements. Each workload has different requirements for availability, scalability, data consistency, and disaster recovery. To ensure that application architecture meets your business requirements, define target SLAs for each workload. Account for the cost and complexity of meeting availability requirements, in addition to application dependencies.
- **Plan for usage patterns**. Usage patterns also play a role in requirements. Identify differences in requirements during critical and non-critical periods. For example, a tax-filing application can't fail during a filing deadline. To ensure uptime, plan redundancy across several regions in case one fails. Conversely, to minimize costs during non-critical periods, you can run your application in a single region.
- **Establish availability metrics** — mean time to recovery (MTTR) and mean time between failures (MTBF). MTTR is the average time it takes to restore a component after a failure. MTBF is how long a component can reasonably expect to last between outages. Use these measures to determine where to add redundancy and to determine service-level agreements (SLAs) for customers.
- **Establish recovery metrics** — recovery time objective and recovery point objective (RPO). RTO is the maximum acceptable time an application can be unavailable after an incident. RPO is the maximum duration of data loss that is acceptable during a disaster. To derive these values, conduct a risk assessment and make sure you understand the cost and risk of downtime or data loss in your organization.
- **Implement resiliency strategies**. Resiliency is the ability of a system to recover from failures and continue to function. Implement resiliency design patterns, such as isolating critical resources, using compensating transactions, and performing asynchronous operations whenever possible.
- **Build availability requirements into your design**. Availability is the proportion of time your system is functional and working. Take steps to ensure that application availability conforms to your service-level agreement. For example, avoid single points of failure, decompose workloads by service-level objective, and throttle high-volume users.

Understand your app requirements

Building an efficient and reliable Azure solution requires knowing your workload requirements. You can then select Azure products and services, and provision resources according to those requirements. It's important to understand the Azure SLAs that define performance targets for the Azure products and services within your solution. This understanding will help you create achievable Application SLAs.

In a distributed system, failures will happen. Hardware can fail. The network can have transient failures. It's rare for an entire service or region to experience a disruption, but even this must be planned for.

Resiliency

Resiliency is the ability of a system to recover from failures and continue to function. It's not about avoiding failures, but responding to failures in a way that avoids downtime or data loss. The goal of

resiliency is to return the application to a fully functioning state following a failure. High availability and disaster recovery are two crucial components of resiliency.

When designing your architecture you need to design for resiliency, and you should perform a Failure Mode Analysis (FMA). The goal of an FMA is to identify possible points of failure and to define how the application will respond to those failures.

Cost and complexity vs. high availability

Availability refers to the time that a system is functional and working. Maximizing availability requires implementing measures to prevent possible service failures. However, devising preventative measures can be difficult and expensive, and often results in complex solutions.

As your solution grows in complexity, you will have more services depending on each other. Therefore, you might overlook possible failure points in your solution if you have several interdependent services.

Tip - For example: A workload that requires 99.99 percent uptime shouldn't depend upon a service with a 99.9 percent SLA.

Most providers prefer to maximize the availability of their Azure solutions by minimizing downtime. However, as you increase availability, you also increase the cost and complexity of your solution.

Tip - For example: An SLA that defines an uptime of 99.999% only allows for about 5 minutes of total downtime per year.

The risk of potential downtime is cumulative across various SLA levels, which means that complex solutions can face greater availability challenges. Therefore, how critical high-availability is to your requirements will determine how you handle the addition of complexity and cost to your application SLAs.

Considerations for defining application SLAs

If your application SLA defines four 9's (99.99%) performance targets, recovering from failures by manual intervention may not be enough to fulfill your SLA. Your Azure solution must be self-diagnosing and self-healing instead.
It is difficult to respond to failures quickly enough to meet SLA performance targets above four 9's. Carefully consider the time window against which your application SLA performance targets are measured. The smaller the time window, the tighter the tolerances. If you define your application SLA as hourly or daily uptime, you need to understand these tighter tolerances might not allow for achievable performance targets.

- ✓ Performance targets about 99.99% are going to be very difficult to achieve.

Walkthrough-Calculate Composite SLAs

In this walkthrough, we will determine services SLA uptime percentages and then calculate the application composite SLA uptime percentage.

Task 1: Determine the SLA uptime percentage values for an application

In this task, we will determine the SLA uptime percentage values for an example appliation.

Task 2: Calculate the Application Composite SLA percentage uptime

In this task, we will calculate the application composite SLA percentage uptime.

Congratulations! You have determined the SLA uptime percentages for each of the services in our sample application and then calculated the composite SLA uptime percentage for the application.

Service Lifecycle in Azure

Public and private preview features

Microsoft offers previews of Azure services, features, and functionality for evaluation purposes. With *Azure Previews*, you can test pre-release features, products, services, software, and even regions. Previews allow users early access to functionality. Additionally, users providing feedback on the preview features helps Microsoft improve the Azure service.

Categories

There are two categories of preview that are available:

- **Private preview** - An Azure feature is available to *certain* Azure customers for evaluation purposes.
- **Public preview** - An Azure feature is available to *all* Azure customers for evaluation purposes.

Azure Preview Terms and Conditions

Azure feature previews are available with their own terms and conditions. The terms and conditions are specific to each Azure preview. All preview-specific terms and conditions supplement your existing Azure service agreement.

✓ Some previews aren't covered by customer support.

Note: There's a **Supplemental Terms of Use for Microsoft Azure Previews**[14] page.

Try This - Access preview features

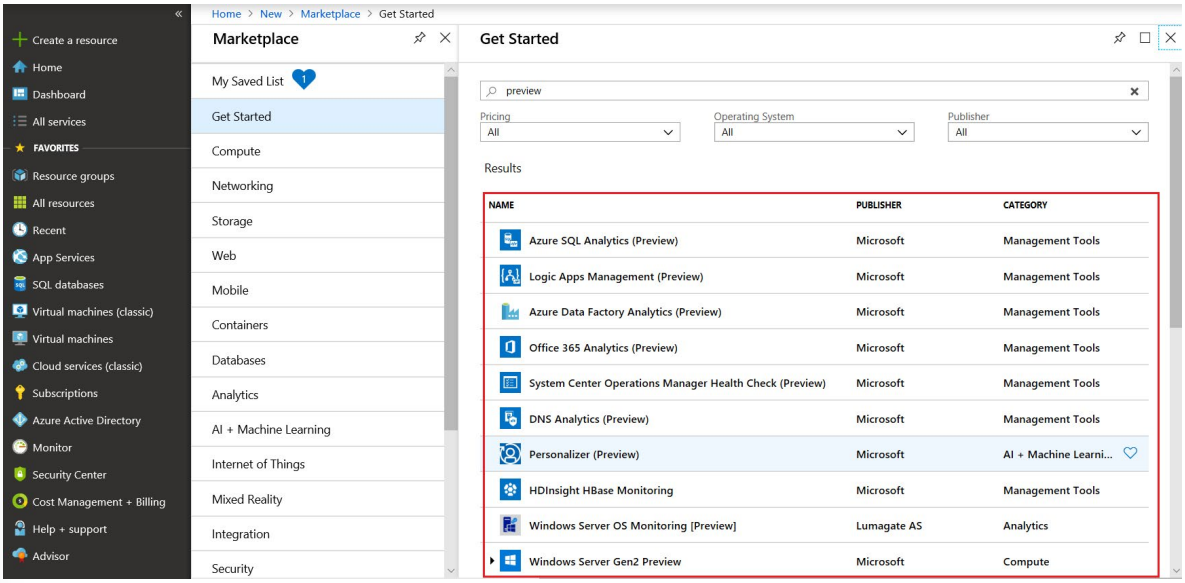
You can access publicly available Preview features directly via the Azure portal.

Preview - New Services

You can view preview services by doing the following

- Sign into the **Azure portal**
- Click **Create a resource**
- Type **preview** in the search box and press **Enter**
- A list of services is returned and displayed for you to browse through. You can select one to learn more about it, and also create an instance of the service, then try it out.

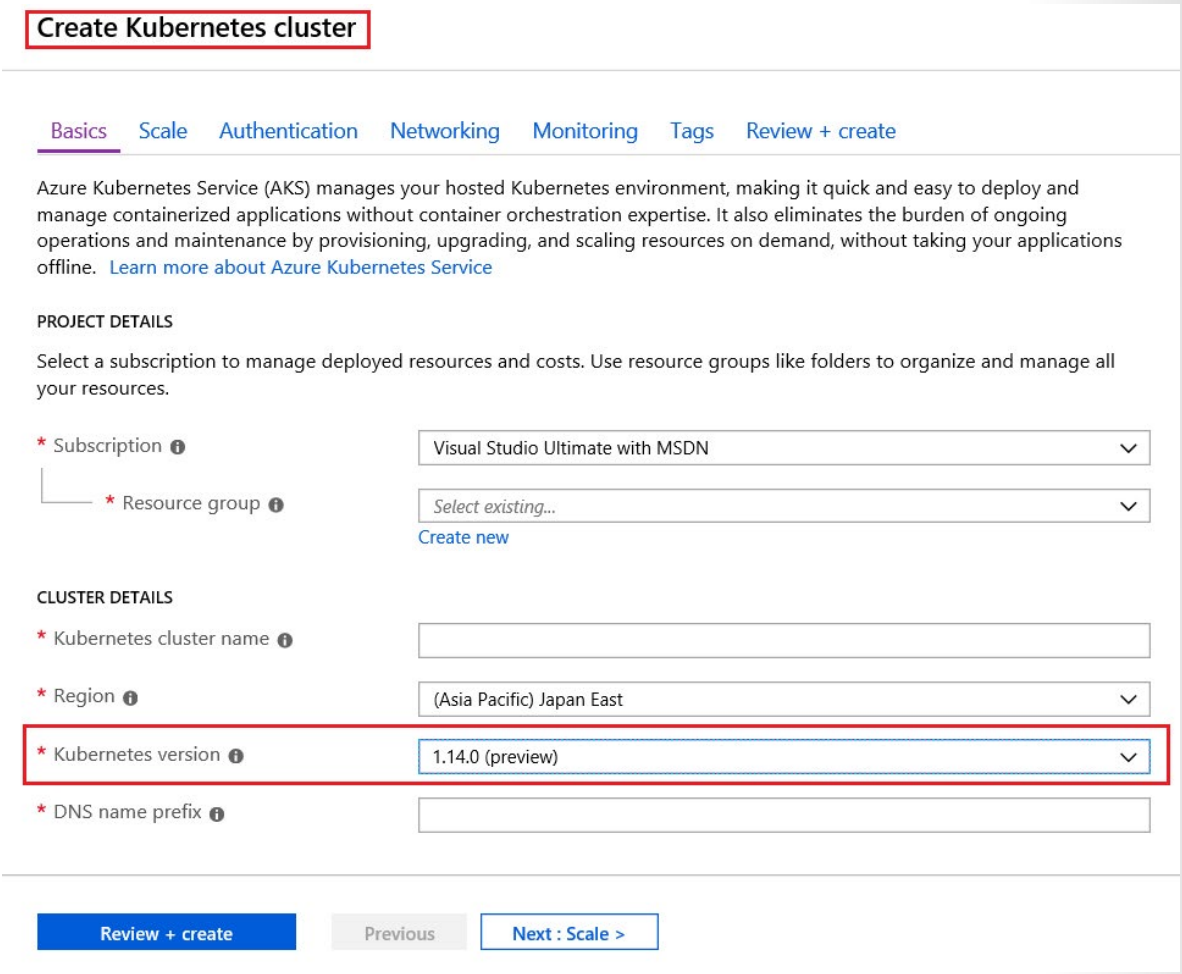
14 https://azure.microsoft.com/support/legal/preview-supplemental-terms?azure-portal=true



Preview - New Functionality/Features within an existing service

Some preview features relate to a specific area of an existing Azure Service. These preview features are accessible as you deploy, configure and manage the service. One such example is **Azure Kubernetes Service (AKS)**, where you can view preview functionality available within AKS by doing the following.

- Sign into **Azure portal**
- Open, **Azure Kubernetes Services (AKS)** then click **Create Kubernetes service** button
- Under, **Cluster Details** > **Kubernetes version** section expand the drop-down list to display the versions.
- The latest version **1.14.0** is listed as currently in preview **1.14.0 (preview)**. It's being made available to provide new functionality in AKS and allow testing.

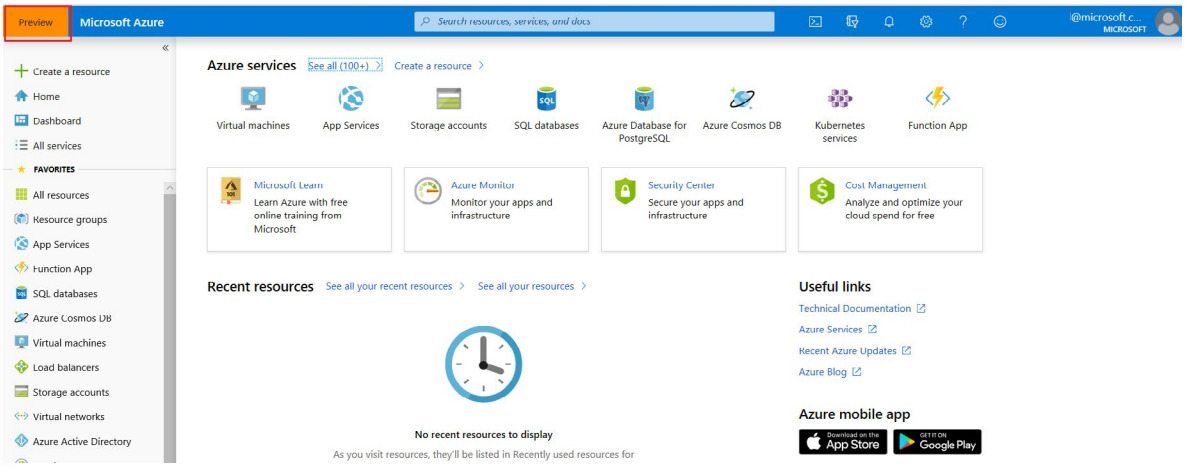


✓ You may choose to use an Azure preview service in production. Remember, the preview feature or functionality may not yet be ready for production deployments. Make sure you're aware of any limitations around its use before deploying to production.

Access Azure portal preview

You can access preview features that are specific to the Azure portal from the **https://preview.portal.azure.com**[15] page. Typical portal preview features provide performance, navigation, and accessibility improvements to the Azure portal interface.

15 https://preview.portal.azure.com?azure-portal=true



Providing Feedback

Azure customers can provide feedback on the preview features they've tested by *sending a smile* in the portal. Or customers can post ideas and suggestions on the *Azure portal feedback forum*. You can revert to the default Azure portal by going to the **https://portal.azure.com**[16] page.

✓ There is a **Azure portal feedback forum**[17].

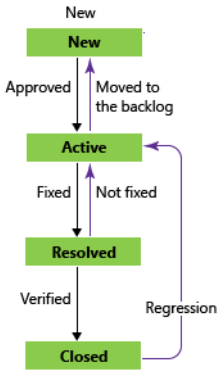
✓ For more information about Azure portal preview features, see **Get early access to the newest Azure portal features**[18].

General Availability

Once a feature is evaluated and tested successfully, it may release to customers as part of Azure.

In other words, the feature may be made available for all Azure customers. A feature released to all Azure customers typically goes to *General Availability* or *GA*.

16 https://portal.azure.com?azure-portal=true
17 https://feedback.azure.com/forums/223579-azure-portal?azure-portal=true
18 https://azure.microsoft.com/updates/get-early-access-to-new-portal-features-2?azure-portal=true

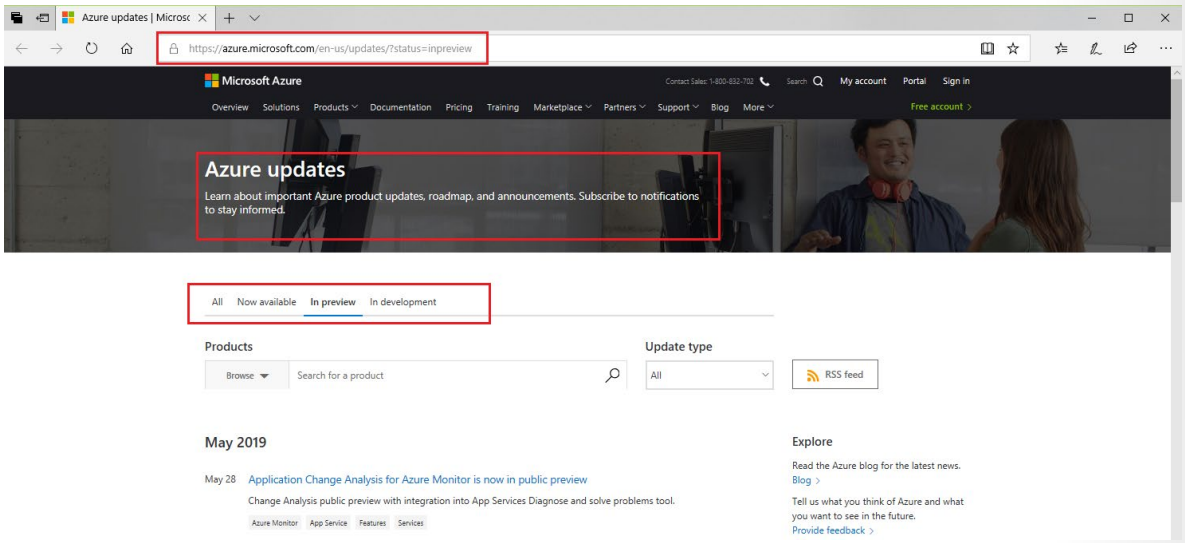


The above image outlines the general process for features and bugs during the development lifecycle. It's common for features to move from Azure preview features to GA, based on customer evaluation and feedback.

✓ Learn about updates and new product features on the **Azure announcements blog**[19].

Try This - Monitoring Service and Feature Updates

Go to the **Azure updates**[20] page for 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, by using the provided dropdown lists.
- Search for updates by keyword by entering search terms into a text-entry field.

19 https://azure.microsoft.com/blog/topics/announcements?azure-portal=true
20 https://azure.microsoft.com/updates?azure-portal=true

- Subscribe to get Azure update notifications by RSS.
- Access the Microsoft Connect page to read Azure product news and announcements.

Walkthrough-Access Azure Preview features

In this walkthrough, we will access and identify Azure preview services and features, and view the latest Azure updates information.

Task 1: Access preview services and features

In this task, we will review Marketplace Preview features.

Task 2: Review the Azure Updates page

In this task, we will review the Azure Updates page.

Congratulations! You have accessed and identified Azure preview services and features, and viewed the latest Azure updates information.

Module 4 Review Questions

Module 04 Review Questions

Review Question 1

Which of the following provides a set of tools for monitoring, allocating, and optimizing your Azure costs?

- ☐ Azure Cost Management
- ☐ Azure Pricing Calculator
- ☐ Total Cost of Ownership Calculator

Review Question 2

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

- ☐ Azure Initiatives
- ☐ Management Groups
- ☐ Resource Groups

Review Question 3

Which of the following defines performance targets, like uptime, for an Azure product or service?

- ☐ Service Level Agreements
- ☐ Support Plans
- ☐ Usage Meters

Review Question 4

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

- ☐ Azure Subscription
- ☐ Management Group
- ☐ Resource Group

Review Question 5

Which Azure support plan is best for business-critical workloads?

- ☐ Azure Developer
- ☐ Azure Professional Direct
- ☐ Azure Standard

Review Question 6

An Azure Reservations offers discounted prices if you?

- ☐ pay in advance.
- ☐ provision a certain number of resources.
- ☐ use spending limits.

Review Question 7

Which of the following give all Azure customers a chance to test beta and other pre-release features?

- ☐ General Availability
- ☐ Private Preview
- ☐ Public Preview

Review Question 8

You have two services with different SLAs. The composite SLA is determined by?

- ☐ Adding the SLAs percentages together
- ☐ Multiplying the SLAs percentages together
- ☐ Taking the lowest SLA percentage

Review Question 9

Releasing a feature to all Azure customers is called?

- ☐ General Availability
- ☐ General Preview
- ☐ Public Preview

Review Question 10

Which of the following can be used to estimate cost savings when migrating to Azure?

- ☐ Pricing calculator
- ☐ Total Cost of Ownership calculator
- ☐ Usage meter

Review Question 11

Your billing is based on your usage of Azure resources and is invoiced _____

- ☐ Annually
- ☐ Monthly
- ☐ Daily

Review Question 12

Azure Advisor provides recommendations for _____.

- ☐ Costs only
- ☐ High availability, security, performance, operational excellence, and cost
- ☐ High availability, performance, and cost

Review Question 13

To use Azure datacenters that are made available with power, cooling, and networking capabilities independent from other datacenters in a region, choose a region that supports _____?

- ☐ Geography distribution
- ☐ Service-Level Agreements (SLAs)
- ☐ Availability Zones

Review Question 14

Application availability refers to what?

- ☐ The service level agreement of the associated resource.
- ☐ Application support for an availability zone.
- ☐ The overall time that a system is functional and working.

Module 4 Summary

Module 4 Summary

##Module 4 Summary

In this module, you learned about Azure Pricing and Support. We defined Azure subscriptions and detailed the various Azure subscription options and uses; explored purchasing Azure Products and Services; and examined factors that affect Azure costs and how you can minimize them. Additionally, we detailed Azure support plans and channels, and outlined Azure SLAs and how you can improve their application. Finally, we followed the service lifecycle in Azure from the preview phase through general availability to update.

Azure subscriptions

In this lesson, we defined an Azure subscription as a logical unit of services, and we detailed the free and paid subscriptions that suit different customer requirements. Additionally, you learned that using Azure requires a subscription and that billing and management policies apply on a per-subscription basis for accounts with multiple subscriptions. We defined management groups as containers for collections of Azure resources, arranged hierarchically. Lastly, we discussed how you can apply governance and access polices to each management group.

Planning and managing costs

In this lesson, we discussed the four Azure customer types, which include Free Account, Enterprise, Web Direct, and Cloud Solution Providers (CSP), and how those customer types determine purchasing and billing options for products and services. We introduced Azures pay-for-what-you-use model and discussed how usage meters determine costs. We also examined the factors that affect costs including resource type, first-party and third-party service categories, and location. Lastly, we discussed how you can minimize your Azure costs by using tools such as Azure's Pricing and Cost of Ownership (TCO) calculators, and products such as Azure Advisor recommendations and Azure Reservations.

Azure SLAs

In this lesson, you learned how SLAs set performance targets specific to each Azure product and service. You saw how SLA performance targets typically range from 99.9 percent (three nines) to 99.99 percent (four nines), and you learned that SLAs define how Microsoft responds if an Azure product or service under-performs. You also learned how to create your own Application SLAs and how increasing availability can also raise the cost and complexity of your Azure solution.

Service lifecycle in Azure

In this lesson, you learned about the components of the Azure service lifecycle, and how Microsoft offers public and private previews of Azure features for evaluation purposes. You also learned how you can access the Azure Preview Features page and that successfully tested features are made available to Azure customers through GA releases. Finally, you learned how to get details of the latest updates to Azure products, services, and features from the Azure Updates web page.

Answers

Review Question 1

Which of the following provides a set of tools for monitoring, allocating, and optimizing your Azure costs?

- ■ Azure Cost Management
- ☐ Azure Pricing Calculator
- ☐ Total Cost of Ownership Calculator

Explanation
Azure Cost Management. Azure Cost Management is an Azure product that provides a set of tools for monitoring, allocating, and optimizing your Azure costs.

Review Question 2

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

- ☐ Azure Initiatives
- ■ Management Groups
- ☐ Resource Groups

Explanation
Management Groups. 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 RBACs, 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 3

Which of the following defines performance targets, like uptime, for an Azure product or service?

- ■ Service Level Agreements
- ☐ Support Plans
- ☐ Usage Meters

Explanation
Service Level Agreement (SLA). The SLA defines performance targets for an Azure product or service.

Review Question 4

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

- ■ Azure Subscription
- ☐ Management Group
- ☐ Resource Group

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

Review Question 5

Which Azure support plan is best for business-critical workloads?

☐ Azure Developer

■ Azure Professional Direct

☐ Azure Standard

Explanation
Azure Professional Direct is the best way to ensure your solutions are running nearly all the time.

Review Question 6

An Azure Reservations offers discounted prices if you?

■ pay in advance.

☐ provision a certain number of resources.

☐ use spending limits.

Explanation
Pay in advance. Azure Reservations offers discounted prices if you pay in advance. To get a discount, you reserve products and resources by paying in advance. You can prepay for one or three year's use of certain Azure resources.

Review Question 7

Which of the following give all Azure customers a chance to test beta and other pre-release features?

☐ General Availability

☐ Private Preview

■ Public Preview

Explanation
Public Preview. Public Preview means that an Azure feature is available to all Azure customers for evaluation purposes.

Review Question 8

You have two services with different SLAs. The composite SLA is determined by?

☐ Adding the SLAs percentages together

■ Multiplying the SLAs percentages together

☐ Taking the lowest SLA percentage

Explanation
Multiply the SLAs together. To determine a composite SLA you multiply the individual SLAs together.

Review Question 9

Releasing a feature to all Azure customers is called?

■ General Availability

☐ General Preview

☐ Public Preview

Explanation
General Availability (GA). GA is a feature released to all Azure customers.

Review Question 10

Which of the following can be used to estimate cost savings when migrating to Azure?

☐ Pricing calculator

■ Total Cost of Ownership calculator

☐ Usage meter

Explanation
Total Cost of Ownership (TCO) calculator. The TCO calculator is a tool that you use to estimate cost savings you can realize by migrating to Azure.

Review Question 11

Your billing is based on your usage of Azure resources and is invoiced _____

☐ Annually

■ Monthly

☐ Daily

Explanation
You will be billed monthly.

Review Question 12

Azure Advisor provides recommendations for _____.

☐ Costs only

■ High availability, security, performance, operational excellence, and cost

☐ High availability, performance, and cost

Explanation
Azure Advisor provides recommendations on many different capabilities for your solutions.

Review Question 13

To use Azure datacenters that are made available with power, cooling, and networking capabilities independent from other datacenters in a region, choose a region that supports _____?

☐ Geography distribution

☐ Service-Level Agreements (SLAs)

■ Availability Zones

Explanation
Availability Zones are datacenters set up to be an isolation boundary from others in the region, with their own power, cooling, and networking. If one zone in a region goes down, other Availability Zones in the region continue to work.

Review Question 14

Application availability refers to what?

☐ The service level agreement of the associated resource.

☐ Application support for an availability zone.

■ The overall time that a system is functional and working.

Explanation
The time that a system is working is referred to as the application availability.

Module 5 Course Conclusion

Summary

Summary

In this course, you have learned about:

- General cloud computing concepts.
- Core services available with Microsoft Azure.
- Security, privacy, compliance and trust with Microsoft Azure.
- Pricing and support models available with Microsoft.