

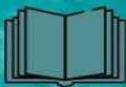


Microsoft Azure Fundamentals

2021
Updated

EXAM PREP AZ 900

The complete guide to get Microsoft Azure Fundamentals
AZ-900 certified



Course Outline

Aligned with the Latest AZ-900 Syllabus
Prepared by Azure Solutions Architect Experts



Practice Tests

250+ realistic Q&As including 3 practice test,
pre-assessment and chapter tests



Azure Roadmap

Professional guidance on growing your Azure
career from fundamentals to an Architect

Microsoft AZURE® Fundamentals

Exam Prep AZ 900

Complete guide to get Microsoft Azure Fundamentals AZ900 certified on your 1st attempt

iCertify Training NYC

Amazon Edition

This work is subject to copyright © 2021 iCertify Training. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

Trademarked names, logos, and images may appear in this book. Rather than use a trademark symbol with every occurrence of a trademarked name, logo, or image we use the names, logos, and images only in an editorial fashion and to the benefit of the trademark owner, with no intention of infringement of the trademark.

The use in this publication of trade names, trademarks, service marks, and similar terms, even if they are not identified as such, is not to be taken as an expression of opinion as to whether or not they are subject to proprietary rights.

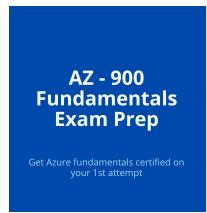
While the advice and information in this book are believed to be true and accurate at the date of publication, neither the authors nor the editors nor the publisher can accept any legal responsibility for any errors or omissions that may be made. The publisher makes no warranty, express or implied, with respect to the material contained herein.

For information on translations, contact our email helpdesk
info@icertifytraining.com, or visit www.icertifytraining.com

\$400 worth Azure Fundamentals Training



We believe in you !! and we want to ensure you get AZ-900 certified on your 1st attempt. That's why iCertify Training has launched multiple #1 Rated training materials to enable professionals to get AZ-900 certified on their 1st attempt and for a limited time you can access them for FREE!!

 <p>AZ - 900 Fundamentals Exam Prep</p> <p>Get Azure fundamentals certified on your 1st attempt</p>	<p>AZ-900 Fundamentals Exam Prep Video course</p> <p>With over 20+ videos, this covers the logistics of the AZ-900 exam: who it's for, what objectives exam takers should focus on, and which resources can be used to prepare. She then covers the concepts and skills included in the exam. Strengthen your grasp of general cloud concepts, explore core Azure services, and review key options and resources to enhance your ability to effectively plan and manage Azure costs</p>
 <p>AZ - 900 Practice Tests</p> <p>9 Realistic Practice Tests to make you Azure AZ-900 certified on your 1st attempt</p>	<p>AZ-900 Practice Tests</p> <p>With over 6 realistic practice tests, our AZ-900 exam simulator will provide you access to over 250+ questions and answers to enable you to get AZ-900 certified on your 1st attempt</p>

For a limited time, you can access these for FREE, by following instructions

below

Simply give us your Honest feedback; send us a screenshot of your Rating of our #1 Amazon Book to info@icertifytraining.com

Note: These additional training materials are NOT included in your book purchase but being provided additionally for FREE as a professional courtesy.

We believe in your Honesty, and with over \$400 worth Azure Training for FREE, we believe that it sure is worth your 5* Rating. However, if you do not believe our course deserves a 5* rating; kindly email us at info@icertifytraining.com with your reasons. For valid and constructive feedback we offer our participants \$10 Amazon gift card.

Be Kind, Be Awesome! Each of your 5* Rating enables us to keep improving our products

You shall not be disappointed, check out what our students say



Before I took the course, I was worried if I should get Azure certified. Thank goodness I took this course. I passed Az-900 on my first attempt. Not only did their course provide me with videos, but they also gave me access to their exam simulator (Saved me \$400).

Go ahead for this course... you will not regret it



Not many people offer Azure Training. This is the best I have taken and helped me get certified on my first attempt. I believe this course is awesome because it is just not course videos but also providing the 6 tests free and the eBook. This will definitely help practitioners especially like me to review and refer in my career. A great asset when going to take the certification! The course and book are perfect to get the details you need to ensure you get AZ-900 certified. GET YOUR IT CAREER OFF THE FLOOR NOW!!!!

FAQs:

- Click on “Write a Customer Review“ and leave your positive review
- We shall be sending you access to all training materials via email
- If you are not comfortable providing a feedback, simply send us a receipt of your purchase to info@icertifytraining.com and we will provide you access to your companion content

Bug report: Find any issues or typos, email us for a \$10 Amazon gift card to info@icertifytraining.com

Table of Contents

[\\$400 worth Azure Fundamentals Training](#)

[Table of Contents](#)

[Pre-assessment Quiz](#)

[Answers](#)

[Chapter 1 : Introduction](#)

[1.1 About the Author](#)

[1.2 About this book](#)

[Who should read this book](#)

[This book might not be for you if...](#)

[Assumptions](#)

[Chapter 2 : Azure Fundamentals Certification](#)

[2.1 Learning objectives](#)

[2.2 Azure Fundamentals AZ 900 Certification](#)

[2.3 Why should I take Azure fundamentals?](#)

[2.4 Skills gained](#)

[2.5 AZ-900 Certification Examination Syllabus](#)

[2.6 Prerequisites](#)

[2.7 How to take the Exam](#)

[2.8 Azure Fundamentals certification Roadmap](#)

[Chapter 3 : Cloud Concepts](#)

[3.1 Learning Objectives](#)

[3.2 Case study introduction](#)

[3.3 Cloud computing](#)

[Why is cloud computing typically cheaper to use?](#)

[Why should I move to the cloud?](#)

[What are some cloud computing advantages?](#)

[Cloud computing is a consumption-based model](#)

Capital expenses vs. Operating expenses

3.4 What are cloud service models?

3.4.1 IaaS (Infrastructure as a Service)

3.4.2 PaaS (Platform as a Service)

3.4.3 SaaS (Software as a Service)

3.5 Serverless computing

3.6 Types of cloud computing

3.7 Azure and Cloud

3.7.1 High Availability

Power:

Cooling:

Networking:

Region:

3.7.2 Fault Tolerance

Proactive Measures:

Reactive approaches

3.7.3 Disaster Recovery

3.7.4 Scalability and Elasticity

Scalability:

Elasticity:

3.7.5 Business Agility

Focus on Time to Value

Innovation

Low Latency

Economic Effectiveness

Rapid Adaptation

Flexibility

3.8 Knowledge check

Answers

3.9 Summary

Chapter 4 : Azure Fundamental Concepts

4.1 Learning objectives

4.2 Overview of Azure subscriptions, management groups, and resources

4.2.1 Get started with Azure accounts

Create an Azure account

What is the Azure free account?

4.2.2 Azure subscriptions and management groups

Azure subscriptions

Additional Azure subscriptions

Customize billing to meet your needs

4.2.3 Azure management groups

Hierarchy of management groups and subscriptions

Important facts about management groups

4.3 Azure resources and Azure Resource Manager

4.3.1 Azure resource groups

Logical grouping

Life cycle

Authorization

4.3.2 Azure Resource Manager

4.3.3 The benefits of using Resource Manager

4.4 Azure regions, availability zones, and region pairs

4.4.1 Azure regions

Why are regions important?

Special Azure regions

4.4.2 Azure availability zones

What is an availability zone?

Supported regions

Use availability zones in your apps

Azure region pairs

4.5 Knowledge Check

[Answers](#)

[4.6 Summary](#)

[Chapter 5 Azure Core Services](#)

[5.1 Learning Objectives](#)

[5.2 Azure services](#)

[5.2.1 Compute](#)

[5.2.2 Networking](#)

[5.2.3 Storage](#)

[5.2.4 Mobile](#)

[5.2.5 Databases](#)

[5.2.6 Web](#)

[5.2.7 IoT](#)

[5.2.8 Big data](#)

[5.2.9 Artificial Intelligence](#)

[5.2.10 DevOps](#)

[5.4 Azure Database Services](#)

[5.4.1 Azure Cosmos DB](#)

[5.4.2 Azure SQL Database](#)

[Exercise - Create a SQL database](#)

[Task 1: Create the database](#)

[Task 2: Test the database](#)

[5.4.3 Azure SQL Managed Instance](#)

[Features](#)

[5.4.4 Azure database for MySQL](#)

[5.4.5 Azure Database for PostgreSQL](#)

[Single Server](#)

[Hyperscale \(Citus\)](#)

[5.5 Azure Big data and analytics services](#)

[5.5.1 Azure Synapse Analytics](#)

[5.5.2 Azure HDInsight](#)

[5.5.3 Azure Databricks](#)

[5.5.4 Azure Data Lake Analytics](#)

[5.5.5 Knowledge check](#)

[Answer:](#)

[Summary](#)

[5.6 Azure Artificial Intelligence services](#)

[5.6.1 Azure Machine Learning](#)

[5.6.2 Azure Cognitive Services](#)

[5.6.3 Azure Bot Service](#)

[5.6.4 Knowledge check](#)

[Answers:](#)

[Summary](#)

[5.7 Azure Serverless Computing Services](#)

[5.7.1 Azure Functions](#)

[5.7.2 Azure Logic Apps](#)

[What are the differences between these services?](#)

[5.7.3 Knowledge Check](#)

[Answers](#)

[5.8 IOT Services](#)

[5.8.1 Azure IoT Hub](#)

[5.8.2 Azure IoT Central](#)

[5.8.3 Azure Sphere](#)

[5.8.4 Knowledge Check](#)

[Answers](#)

[Chapter 6 : Azure Management tools](#)

[6.1 Learning Objectives](#)

[6.2 The Azure portal](#)

[What is the Azure portal?](#)

[6.3 The Azure mobile app](#)

[6.4 Azure PowerShell](#)

- [6.5 The Azure CLI](#)
- [6.6 ARM templates](#)
- [6.7 Azure Marketplace](#)
- [6.8 Knowledge Check](#)

[Answers :](#)

- [6.9 Azure Monitoring Services](#)

- [6.3.1 Azure Advisor](#)
- [6.3.2 Azure Monitor](#)
- [6.3.3 Azure Service Health](#)
- [6.3.4 Knowledge Check](#)

[Answers](#)

[Chapter 7: General security and network security features](#)

- [7.1 Learning objectives](#)
- [7.2 Azure Security Center](#)
- [7.3 Azure Sentinel](#)
- [7.3 Azure Key Vault](#)
 - [What can Azure Key Vault do?](#)
 - [What are the benefits of Azure Key Vault?](#)

[Exercise - Manage a password in Azure Key Vault](#)

- [Create a key vault](#)
- [Add a password to the key vault](#)
- [Show the password](#)
- [Clean up](#)

[7.4 Azure Dedicated Host](#)

- [What are the benefits of Azure Dedicated Host?](#)
- [Availability considerations for Dedicated Host](#)
- [Pricing considerations](#)
- [Knowledge check](#)

[Answer:](#)

[Summary](#)

Chapter 8 : Identity, governance, privacy, and compliance features

8.1 Authentication vs Authorization

8.1.1 What is authentication?

8.1.2 What is authorization?

8.1.3 How are authentication and authorization related?

8.2 Azure Active Directory

8.2.1 Azure AD vs. Active Directory?

Who uses Azure AD?

What services does Azure AD provide?

What kinds of resources can Azure AD help secure?

What's a single sign-on?

How can I connect Active Directory with Azure AD?

8.3 Multifactor authentication and Conditional Access

What's multifactor authentication?

What's Azure AD Multi-Factor Authentication?

What's Conditional Access?

When can I use Conditional Access?

8.4 Knowledge check

Answers:

Summary

8.5 Cloud governance strategy on Azure

8.5.1 Role Based Access Control

8.5.2 Azure Resource Locks

8.5.3 Azure Cloud tags

8.5.4 Azure Policy

8.5.5 Azure BluePrint

8.5.6 Knowledge Check

Answers :

8.6 Privacy, compliance, and data protection standards on Azure

8.6.1 Compliance terms and requirements

[Which compliance categories are available on Azure?](#)

[8.6.2 Microsoft Privacy Statement, the Online Services Terms, and the Data Protection Addendum](#)

[First, the Microsoft Privacy Statement.](#)

[Second, the Online Services Terms.](#)

[Third, the Data Protection Addendum.](#)

[8.6.4 Microsoft Trust Center](#)

[Explore the Trust Center](#)

[8.6.3 Azure compliance documentation](#)

[8.6.3 Azure Government](#)

[8.6.4 Knowledge check](#)

[Answers](#)

[Chapter 9 : Azure cost management and service level agreements](#)

[9.1 TCO Calculator](#)

[How does the TCO Calculator work?](#)

[Step 1: Define your workloads](#)

[Step 2: Adjust assumptions](#)

[Step 3: View the report](#)

[Exercise - Compare sample workload costs by using the TCO Calculator](#)

[Define your workloads](#)

[Adjust assumptions](#)

[View the report](#)

[9.2 Purchase Azure services](#)

[9.2.1 Azure subscription models](#)

[9.2.2 Purchase Azure services](#)

[9.2.3 Cost Factors](#)

[Resource type](#)

[Usage meters](#)

[Resource usage](#)

[Azure subscription types](#)

[Azure Marketplace](#)

[Does location or network traffic affect cost?](#)

[Location](#)

[Zones for billing of network traffic](#)

[How can I estimate the total cost?](#)

[Exercise - Estimate workload cost by using the Pricing calculator](#)

[Define your requirements](#)

[Explore the Pricing calculator](#)

[Estimate your solution](#)

[Add services to the estimate](#)

[Configure services to match your requirements](#)

[Review, share, and save your estimate](#)

[Manage and minimize total cost on Azure](#)

[Knowledge check](#)

[Answer:](#)

[Summary](#)

[Chapter 10 : Practice Test 1](#)

[10.1 Answers](#)

[Chapter 11 : Practice Test 2](#)

[11.1 Practice Test 2 : Answers](#)

[Chapter 12 : Practice Test 3](#)

[Practice Test 3 : Answers](#)

[Chapter 13 : Next Steps](#)

[1. Azure Fundamentals](#)

[2. Azure Administrator Associate](#)

[3. Azure Developer Associate](#)

[4. Azure Solution Architect Expert](#)

[Microsoft Azure Architect Technologies \(AZ-300\)](#)

[Microsoft Azure Architect Design \(AZ-301\)](#)

[5. Azure DevOps Engineer Expert](#)

[Microsoft Azure DevOps Solutions \(AZ-400\)](#)

[6. Azure Security Engineer Associate](#)

[7. Azure Data Engineer Associate](#)

[DP-200: Implementing an Azure Data Solution](#)

[DP-201: Designing an Azure Data Solution](#)

Pre-assessment Quiz

This pre-assessment quiz is intended to evaluate your baseline understanding of the fundamentals of Azure Cloud services. Reviewing these self-assessment questions and the answers will enable you to benchmark your existing knowledge.

- 1)** Recommended regions in Azure cloud include multiple datacenters.
 - A. Yes
 - B. No
- 2)** Data transfer between Azure services located in two different regions is always free.
 - A. Yes
 - B. No
- 3)** Azure resources inherit locks from the resource group they are part of.
 - A. Yes
 - B. No
- 4)** If your VM has a Read-only lock applied, you can add a Delete lock as well.
 - A. Yes
 - B. No
- 5)** An Azure subscription can be associated with multiple Azure Active Directory (Azure AD) tenants.
 - A. Yes
 - B. No
- 6)** You can modify the Azure Active Directory (Azure AD) tenant to which an Azure subscription is associated.
 - A. Yes
 - B. No
- 7)** The Azure Active Directory (Azure AD) tenant is deleted by default when the Azure subscription expires.

- A. Yes
- B. No

8) Your company has started migrating multiple services into Azure. You are the Azure Administrator responsible to deploy several custom applications to Azure. Some of the applications that need to be migrated will have several prerequisite applications and services installed. Which of the following cloud deployment models would you recommend?

- A. Software as a Service (SaaS)
- B. Platform as a Service (PaaS)
- C. Infrastructure as a Service (IaaS)

9) Azure Cosmos DB is one of the many Azure popular services. What type of Azure service offering does it represent?

- A. Infrastructure as a Service (IaaS)
- B. Platform as a Service (PaaS)
- C. Software as a Service (SaaS)
- D. Serverless

10) Europe is represented by a single Azure region.

- A. Yes
- B. No

11) Your company has decided to migrate all its services to Microsoft Azure. You need to deploy an Azure architecture and use only Platform as a Service (PaaS) services available in Azure.

Solution: You create an Azure App Service and Azure SQL databases.

Does this meet the goal?

- A. Yes
- B. No

12) Your company has decided to migrate all its services to Microsoft Azure. You need to deploy an Azure architecture and use only Platform as a Service (PaaS) services available in Azure.

Solution: You create an Azure App Service and add Azure virtual machines to your setup.

Does this meet the requirements?

- A. Yes
- B. No

13) Your company has decided to migrate all its services to Microsoft Azure. You need to deploy an Azure architecture and use only Platform as a Service (PaaS) services available in Azure.

Solution: You create an Azure App Service and Azure Storage accounts (Virtual Machines).

Does this solution meet the requirements?

- A. Yes
- B. No

14) Your company has decided to migrate all its services to Microsoft Azure. You need to deploy an Azure architecture and use only Platform as a Service (PaaS) services available in Azure.

Solution: You create Azure virtual machines, Azure SQL databases, and Azure Storage accounts.

Does this solution meet the goal?

- A. Yes
- B. No

15) Please select the appropriate option to complete the following sentence:
Azure Site Recovery provides _____ for virtual machines.

- A. Disaster recovery
- B. Scalability
- C. Elasticity
- D. High availability

16) You decide to use version control for your software project. Which of the following Azure services provides a set of version control tools to manage code?

- A. Azure Repos
- B. Azure DevTest Labs
- C. Azure Storage

D. Azure Cosmos DB

17) Azure Monitor can monitor both cloud and on-premises environments.

- A. Yes
- B. No

18) Azure Monitor can trigger alerts based on data in an Azure Log Analytics workspace.

- A. Yes
- B. No

19) Please select the appropriate option to complete the following sentence: _____ is an Apache Spark-based analytics service.

- A. Azure Databricks
- B. Azure Data Factory
- C. Azure DevOps
- D. Azure HDInsight

20) Azure Monitor can send alerts to Azure action groups.

- A. Yes
- B. No

Answers

1) A. Yes

Azure's approach on availability of Azure services across regions is best described by expressing services made available in recommended regions and alternate regions.

- Recommended region - A region that provides the broadest range of service capabilities and is designed to support Availability Zones now, or in the future. These are designated in the Azure portal as Recommended.
- Alternate (other) region - A region that extends Azure's footprint within a data residency boundary where a recommended region also exists. Alternate regions help to optimize latency and provide a second region for disaster recovery needs. They are not designed to support Availability Zones (although Azure conducts regular assessment of these regions to determine if they should become recommended regions). These are designated in the Azure portal as Other.

2) B.No

Outbound data transfer is charged at the normal rate and inbound data transfer is free. The pricing rule that you should keep in mind is this: outbound traffic (leaving Azure cloud or an Azure region) is NOT free, inbound traffic is free.

3) A.Yes

When you apply a lock at a parent scope, all resources within that scope inherit the same lock. Even resources you add later inherit the lock from the parent.

4) A. Yes

This is indeed possible. Read-Only Lock means authorized users can read a resource, but they can't delete or update the resource. Delete Lock means authorized users can still read and modify a resource, but they can't delete the resource.

5) B.No

An Azure AD tenant can have multiple subscriptions but an Azure subscription can only be associated with one Azure AD tenant.

6) A.Yes

Yes, the statement is true. An Azure subscription has a trust relationship with Azure Active Directory (Azure AD). A subscription trusts Azure AD to authenticate users, services, and devices. Multiple subscriptions can trust the same Azure AD directory. Each subscription can only trust a single directory.

7) B.No

If your subscription expires, you lose access to all the other resources associated with the subscription. However, the Azure AD directory remains in Azure. You can associate and manage the directory using a different Azure subscription.

8) C.Infrastructure as a Service (IaaS)

Infrastructure as a service (IaaS) is an instant computing infrastructure, provisioned and managed over the internet. The IaaS service provider manages the infrastructure, while you purchase, install, configure, and manage your own software.

Incorrect Answers:

A: Software as a service (SaaS) allows users to connect to and use cloud-based apps over the Internet. Common examples are email, calendaring, and office tools. In this scenario, you need to run your own apps, and therefore require an infrastructure.

B: Platform as a service (PaaS) is a complete development and deployment environment in the cloud. PaaS includes infrastructure—servers, storage, and networking—but also middleware, development tools, business intelligence (BI) services, database management systems, and more. PaaS is designed to support the complete web application lifecycle: building, testing, deploying, managing, and updating.

9) B.Platform as a Service (PaaS)

Azure Cosmos DB is a fully managed platform-as-a-service (PaaS). Azure Cosmos DB is a fully managed NoSQL database platform service for modern app development.

10) B.No

Europe has several Azure regions, including North Europe, West Europe, UK West, Switzerland North and some others as well.

11) A.Yes

Azure App Service and Azure SQL databases are examples of Azure PaaS solutions. Therefore, this solution does meet the goal.

Azure App Service is a PaaS service offering - managed production environment. App Service automatically patches and maintains the OS and language frameworks for you. Spend time writing great apps and let Azure worry about the platform.

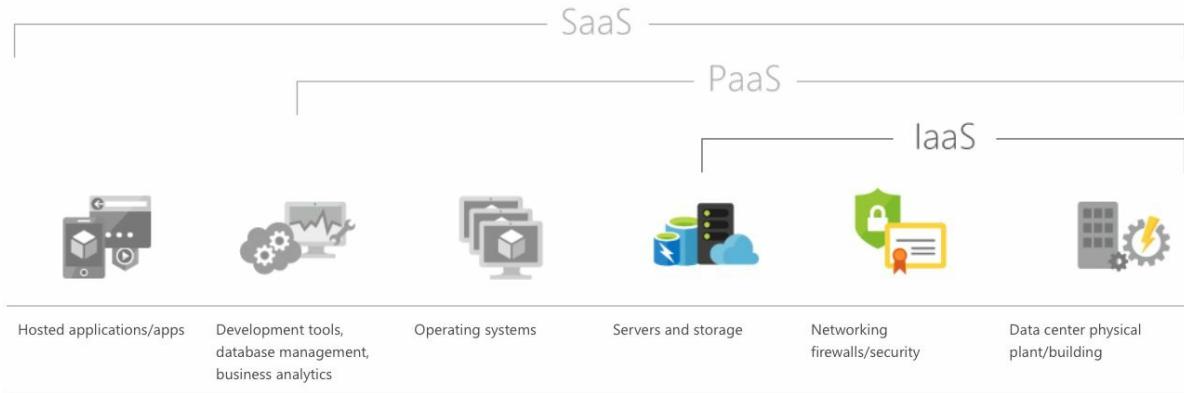
Azure SQL Database is a fully managed platform as a service (PaaS) database engine that handles most of the database management functions such as upgrading, patching, backups, and monitoring without user involvement.

12) B.No

Azure App Service is a PaaS (Platform as a Service) service. However, Azure virtual machines are an IaaS (Infrastructure as a Service) service. Therefore, this solution does not meet the goal.

13) B. No

Azure App Service is a PaaS (Platform as a Service) service. However, Azure Storage accounts are an IaaS (Infrastructure as a Service) service. Therefore, this solution does not meet the goal.



14) B.No

Azure virtual machines and Azure Storage represent Azure Infrastructure as a Service (IaaS) service offering, therefore the solution does not meet the requirements.

15) A.Disaster recovery

Azure Site Recovery helps ensure business continuity by keeping business apps and workloads running during outages. Site Recovery replicates workloads running on physical and virtual machines (VMs) from a primary site to a secondary location. You can set up disaster recovery of Azure VMs from a primary region to a secondary region.

16) A. Azure Repos

Azure Repos is a set of version control tools that you can use to manage your code. Whether your software project is large or small, using version control as soon as possible is a good idea.

17) A.Yes

Azure Monitor maximizes the availability and performance of your applications and services by delivering a comprehensive solution for collecting, analyzing, and acting on telemetry from your cloud and on-premises environments.

18) A.Yes

Azure Monitor uses Target Resource, which is the scope and signals available for alerting. A target can be any Azure resource. Example targets: a virtual machine, a storage account, a virtual machine scale set, a Log Analytics workspace, or an Application Insights resource.

19) A.Azure Databricks

Azure Databricks is an Apache Spark-based analytics platform optimized for the Microsoft Azure cloud services platform.

20) A.Yes

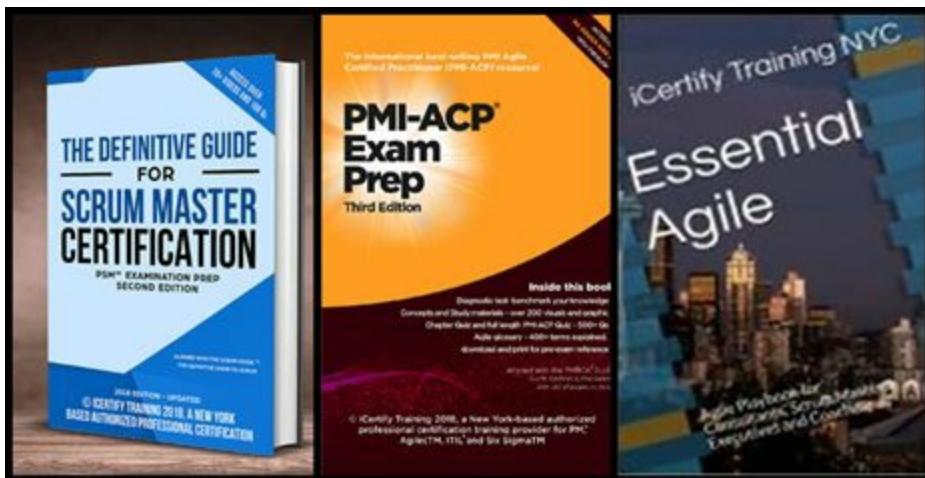
Alerts in Azure Monitor proactively notify you of critical conditions and potentially attempt to take corrective action. Alert rules in Azure Monitor use action groups, which contain unique sets of recipients and actions that can be shared across multiple rules.

Chapter 1 : Introduction

1.1 About the Author

iCertify Training is a New York-based Authorized Professional Certification Training Provider for Cloud, PMP®, Agile®, ITIL® and Six Sigma® . More than 325,000 persons have been enabled by our certification programs. More than 5,000 students are certified each month. We offer Classroom, Online and Webinars for professionals, business and government.

You can reach us at info@icertifytraining.com.



1.2 About this book

Microsoft Azure is Microsoft's cloud computing platform, providing a wide variety of services you can use without purchasing and provisioning your own hardware. Azure enables the rapid development of solutions and provides the resources to accomplish tasks that may not be feasible in an on-premises environment. Azure's compute, storage, network, and application services allow you to focus on building great solutions without the need to worry about how the physical infrastructure is assembled.

This book covers the fundamentals of Azure. It concentrates on the features of the Azure platform that you are most likely to need to know rather than on every feature and service available on the platform. This book also provides several walkthroughs you can follow to learn how to create VMs and virtual networks, websites and storage accounts, and so on. In many cases, real-world tips are included to help you get the most out of your Azure experience.

In addition to its coverage of core Azure services, the book discusses common tools useful in creating and managing Azure-based solutions. The book wraps up by providing details on a few common business scenarios where Azure can provide compelling and valuable solutions, as well as a chapter providing overviews of some of the commonly used services not covered in the book.

This book explores six foundational features of the Microsoft Azure platform, along with insights on getting started with Azure, management tools, and common business scenarios. This book also includes a chapter with overviews of some of the more commonly used services, such as HDInsight (Azure's Hadoop service) and Service Bus, but there are many services in the Azure platform that are not in the scope of this book, such as Azure Batch, Data Lake Analytics, and Azure DNS, just to mention a few.

Azure is a cloud computing platform with an ever-expanding set of services to help you build solutions to meet your business goals. Azure services range from simple web services for hosting your business presence in the cloud to running fully virtualized computers for you to run your custom software solutions. Azure provides a wealth of cloud-based services like remote

storage, database hosting, and centralized account management. Azure also offers new capabilities like AI and Internet of Things (IoT).

In this module, you'll take an entry-level, end-to-end look at Azure and its capabilities. You'll gain a solid foundation for completing the available learning paths for Azure fundamentals.

Module 1: Cloud Concepts

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

Lessons

- What is Cloud Computing
- Advantages of Cloud Computing
- Overview of different Cloud Computing Models
- Describe multiple Cloud Service Options

After completing this module, students will be able:

- 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)

Module 2: Azure Fundamental Concepts

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

Lessons

- Introduction to Azure fundamentals
- Discuss Azure fundamental concepts

- Describe core Azure architectural components

After completing this module, students will be able:

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

Module 3: Describe core Azure services

In this module, you learn about core Azure services like Azure database, Azure compute, Azure storage, and Azure Networking.

Lessons

- Explore Azure database and analytics services
- Explore Azure compute services
- Explore Azure Storage services
- Explore Azure networking services

After completing this module, students will be able:

- Understand the services available in Azure including compute, network, storage, and databases.
- Identify virtualization services such as Azure VMs, Azure Container Instances, and Azure Kubernetes.
- Compare Azure's database services such as Azure Cosmos DB, Azure SQL, and Azure Database for MySQL.
- Examine Azure networking resources such as Virtual Networks, VPN Gateways, and Azure ExpressRoute.
- Summarize Azure storage services such as Azure Blob Storage, Azure Disk Storage, and Azure File Storage.

Module 4: Describe core solutions and management tools on Azure

In this module, you'll learn about AI machine learning, Azure DevOps, monitoring fundamentals, management fundamentals, serverless computing fundamentals, and IoT fundamentals.

Lessons

- Choose the best AI service for your needs
- Choose the best tools to help organizations build better solutions
- Choose the best monitoring service for visibility, insight, and outage mitigation
- Choose the best tools for managing and configuring your Azure environment
- Choose the best Azure serverless technology for your business scenario
- Choose the best Azure IoT service for your application

After completing this module, students will be able:

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

Module 5: Describe general security and network security features

In this module, you will learn how to protect yourself against security threats, and secure your networks with Azure.

Lessons

- Protect against security threats on Azure
- Securing network connectivity in Azure
- Core Azure identity services
- Security tools and features

- Azure governance methodologies
- Monitoring and reporting in Azure
- Privacy, compliance and data protection standards in Azure

After completing this module, students will be able:

- Strengthen your security posture and protect against threats by using Azure Security Center.
- Collect and act on security data from many different sources by using Azure Sentinel.
- Manage dedicated physical servers to host your Azure VMs for Windows and Linux.
- Identify the layers that make up a defense in depth strategy.
- Explain how Azure Firewall enables you to control what traffic is allowed on the network.
- Configure network security groups to filter network traffic to and from Azure resources.
- Explain how Azure DDoS Protection helps protect your Azure resources from DDoS attacks.

Module 6: Describe identity, governance, privacy, and compliance features

In this module, you will learn about Azure identity services, how to build a cloud governance strategy, and privacy, compliance and data protection standards on Azure.

Lessons

- Secure access to your applications by using Azure identity services
- Build a cloud governance strategy on Azure
- Examine privacy, compliance, and data protection standards on Azure

After completing this module, students will be able to:

- Explain the difference between authentication and authorization.
- Describe how Azure Active Directory provides identity and access management.
- Explain the role single sign-on (SSO), multi-factor authentication, and Conditional Access play.

- Make organizational decisions about your cloud environment by using the CAF for Azure.
- Define who can access cloud resources by using Azure role-based access control.
- Apply a resource lock to prevent accidental deletion of your Azure resources.
- Apply tags to your Azure resources to help describe their purpose.
- Control and audit how your resources are created by using Azure Policy.
- Enable governance at scale across multiple Azure subscriptions by using Azure Blueprints.
- Explain the types of compliance offerings that are available on Azure.
- Gain insight into regulatory standards and compliance on Azure.
- Explain Azure capabilities that are specific to government agencies.

Module 7: Describe Azure cost management and service level agreements

In this module, you will learn how to plan and manage Azure costs, and how to choose the right Azure services through SLAs and service lifecycle.

Lessons

- Plan and manage your Azure costs
- Azure subscriptions
- Planning and managing costs
- Support options available with Azure
- Azure service level agreements (SLAs)
- Service lifecycle in Azure
- Choose the right Azure services by examining SLAs and service lifecycle

After completing this module, students will be able to:

- Use the Total Cost of Ownership Calculator.
- Describe the different ways you can purchase Azure products and services.
- Use the Pricing calculator to estimate the monthly cost of running your cloud workloads.

- Define the major factors that affect total cost and apply recommended practices to minimize cost.
- Describe what a service-level agreement (SLA) is and why SLAs are important.
- Identify factors, such as the service tier you choose, that can affect an SLA.
- Combine SLAs to compute a composite SLA.
- Describe the service lifecycle in Azure.

Who should read this book

This book focuses on providing essential information about the key services of Azure for developers and IT professionals who are new to cloud computing. Detailed, step-by-step demonstrations are included to help the reader understand how to get started with each of the key services. This material is useful not only for those who have no prior experience with Azure, but also for those who need a refresher and those who may be familiar with one area but not others. Each chapter is standalone; there is no requirement that you perform the hands-on demonstrations from previous chapters to understand any particular chapter.

This book might not be for you if...

This book might not be for you if you are looking for an in-depth developer or architecture-focused discussion on a wide range of Azure features, or if you are looking for details on other public or private cloud platforms.

Assumptions

We expect that you have at least a minimal understanding of virtualized environments and virtual machines. There are no specific skills required overall for this book, but having some knowledge of the topic of each chapter will help you gain a deeper understanding. For example, the chapter on virtual networks will make more sense if you have some understanding of networking, and the chapter on databases will be more useful if you understand what a database is and why you might use one. Web development skills will provide a good background for understanding Azure Web Apps, and some understanding of identity will be helpful when studying the chapter.

on Active Directory.

Chapter 2 : Azure Fundamentals Certification

2.1 Learning objectives

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

- Understand the need of Azure Fundamentals AZ-900 Certification Examination
- AZ 900 Examination syllabus
- How to take the examination and Costs

2.2 Azure Fundamentals AZ 900 Certification



The Azure fundamentals tests the foundational level knowledge of cloud services and how those services are provided within Microsoft Azure.

No technical background is required to take and pass this exam. This exam is also not a prerequisite to any of the Azure technical exams. This book will provide you with a good level of base knowledge.

The Microsoft Azure Fundamentals exam covers the below six areas,

Describe Cloud Concepts (20-25%)

Identify the benefits and considerations of using cloud services

- Identify the benefits of cloud computing, such as High Availability, Scalability, Elasticity, Agility, and Disaster Recovery
- Identify the differences between Capital Expenditure (CapEx) and Operational Expenditure (OpEx)
- Describe the consumption-based model

Describe the differences between categories of cloud services

- Describe the shared responsibility model

- Describe Infrastructure-as-a-Service (IaaS),
- Describe Platform-as-a-Service (PaaS)
- Describe serverless computing
- Describe Software-as-a-Service (SaaS)
- Identify a service type based on a use case

Describe the differences between types of cloud computing

- Define cloud computing
- Describe Public cloud
- Describe Private cloud
- Describe Hybrid cloud
- Compare and contrast the three types of cloud computing

Describe Core Azure Services (15-20%)

Describe the core Azure architectural components

- describe the benefits and usage of Regions and Region Pairs
- describe the benefits and usage of Availability Zones
- describe the benefits and usage of Resource Groups
- describe the benefits and usage of Subscriptions
- describe the benefits and usage of Management Groups
- describe the benefits and usage of Azure Resource Manager
- explain Azure resources

Describe core resources available in Azure

- Describe the benefits and usage of Virtual Machines, Azure App Services, Azure Container Instances (ACI), Azure Kubernetes Service (AKS), and Windows Virtual Desktop
- Describe the benefits and usage of Virtual Networks, VPN Gateway, Virtual Network peering, and ExpressRoute
- Describe the benefits and usage of Container (Blob) Storage, Disk Storage, File Storage, and storage tiers
- Describe the benefits and usage of Cosmos DB, Azure SQL Database, Azure Database for MySQL, Azure Database for PostgreSQL and SQL Managed Instance
- Describe the benefits and usage of Azure Marketplace

Core solutions and Management tools on Azure (10-15%)

Describe core solutions available in Azure

- Describe the benefits and usage of Internet of Things (IoT) Hub, IoT Central, and Azure Sphere
- Describe the benefits and usage of Azure Synapse Analytics, HDInsight, and Azure Data bricks
- Describe the benefits and usage of Azure Machine Learning, Cognitive Services and Azure Bot Service
- Describe the benefits and usage of serverless computing solutions that include Azure Functions and Logic Apps
- Describe the benefits and usage of Azure DevOps, GitHub, GitHub Actions, and Azure DevTest Labs

Describe Azure management tools

- Describe the functionality and usage of the Azure Portal, Azure PowerShell, Azure CLI, Cloud Shell, and Azure Mobile App
- Describe the functionality and usage of Azure Advisor
- Describe the functionality and usage of Azure Resource Manager (ARM) templates
- Describe the functionality and usage of Azure Monitor
- Describe the functionality and usage of Azure Service Health

Describe general security and network security features (10-15%)

Describe Azure security features

- Describe basic features of Azure Security Center, including policy compliance, security alerts, secure score, and resource hygiene
- Describe the functionality and usage of Key Vault
- Describe the functionality and usage of Azure Sentinel
- Describe the functionality and usage of Azure Dedicated Hosts

Describe Azure network security

- Describe the concept of defense in depth
- Describe the functionality and usage of Network Security Groups (NSG)
- Describe the functionality and usage of Azure Firewall
- Describe the functionality and usage of Azure DDoS protection

Describe Azure cost management and Service Level Agreements (10 - 15%)

Describe methods for planning and managing costs

- Identify factors that can affect costs (resource types, services, locations, ingress and egress traffic)
- Identify factors that can reduce costs (reserved instances, reserved capacity, hybrid use benefit, spot pricing)
- Describe the functionality and usage of the Pricing calculator and the Total Cost of Ownership (TCO) calculator
- Describe the functionality and usage of Azure Cost Management

Describe Azure Service Level Agreements (SLAs) and service life cycles

- Describe the purpose of an Azure Service Level Agreement (SLA)
- Identify actions that can impact an SLA (i.e. Availability Zones)
- Describe the service lifecycle in Azure (Public Preview and General Availability)
- Describe general Cloud Concepts

2.3 Why should I take Azure fundamentals?

Whether you're just beginning to work with the cloud or you already have cloud experience and are new to Azure, Azure fundamentals provides you with everything you need to get started.

No matter your goals, Azure fundamentals has something for you. Take Azure fundamentals if you:

- Have general interest in Azure or in the cloud.
- Want to earn official certification from Microsoft.

2.4 Skills gained

The Microsoft Azure AZ-900 certifies that the professional can

- Discuss the basics of cloud computing and Azure, and how to get started with Azure's subscriptions and accounts.
- Describe the advantages of using cloud computing services, learning to differentiate between the categories and types of cloud computing, and how to examine the various concepts, resources, and terminology that are necessary to work with Azure architecture.
- Outline the core services available with Microsoft Azure.
- Discuss the core solutions that encompass a wide array of tools and services from Microsoft Azure.
- Describe the general security and network security features, and how you can use the various Azure services to help ensure that your cloud resources are safe, secure, and trusted.
- Discuss the identity, governance, privacy, and compliance features, and how Azure can help you secure access to cloud resources, what it means to build a cloud governance strategy, and how Azure adheres to common regulatory and compliance standards.
- Discuss the factors that influence cost, tools you can use to help estimate and manage your cloud spend, and how Azure's service-level agreements (SLAs) can impact your application design decisions.

2.5 AZ-900 Certification Examination Syllabus

The contents of this book is aligned to the *latest syllabus* setup by Microsoft on skills to evaluate as part of the AZ-900 certification examination

Candidates for this exam should have foundational knowledge of cloud services and how those services are provided with Microsoft Azure. The exam is intended for candidates who are just beginning to work with cloud-based solutions and services or are new to Azure.

The Azure Fundamentals exam is an opportunity to prove knowledge of cloud concepts, Azure services, Azure workloads, security and privacy in Azure, as well as Azure pricing and support. Candidates should be familiar with the general technology concepts, including concepts of networking, storage, compute, application support, and application development.

Azure Fundamentals can be used to prepare for other Azure role-based or specialty certifications, but it is not a prerequisite for any of them

This exam includes six knowledge domain areas:

AZ-900 Domain Area	Weight
Describe cloud concepts	20-25%
Describe core Azure services	15-20%
Describe core solutions and management tools on Azure	10-15%
Describe general security and network security features	10-15%
Describe identity, governance, privacy, and compliance features	20-25%
Describe Azure cost management and Service Level Agreements	10-15%

Each domain area maps to a specific chapter/ module in this book.

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

This training helps you develop a broad understanding of Azure. Having real-world experience will help reinforce the concepts so that you're more fully prepared for the exam or to apply your skills on the job.

2.6 Prerequisites

- There are no particular prerequisites for the Microsoft Azure Fundamental exam but one should be familiar and have a basic understanding of the cloud services and the Microsoft Azure platform.

2.7 How to take the Exam

- Languages : English, Japanese, Chinese (Simplified), Korean, Spanish, German, French
- Online Proctored
- Cost : \$99

This exam is targeted at people with both technical and non-technical backgrounds. So you don't have to come from a computer science degree, or are already working as a developer or administrator if you come from a business background and you're simply interested in the cloud.

Exam AZ-900: Microsoft Azure Fundamentals

Languages: English, Japanese, Chinese (Simplified), Korean, Spanish, German, French
Retirement date: none

This exam measures your ability to describe the following concepts: cloud concepts; core Azure services; core solutions and management tools on Azure; general security and network security features; identity, governance, privacy, and compliance features; and Azure cost management and Service Level Agreements.

United States ▾

\$99 USD*

Price based on the country in which the exam is proctored.

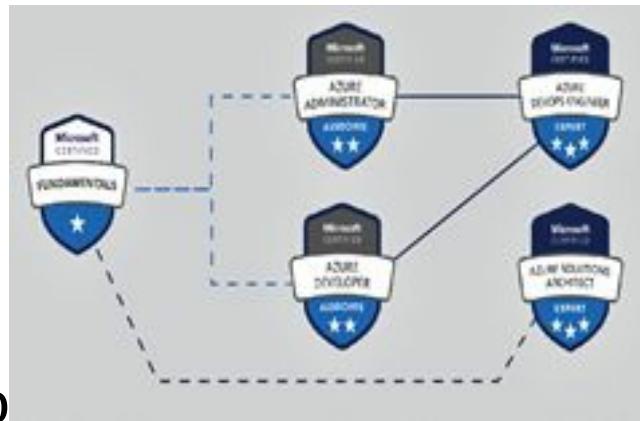
For non-students interested in technology

Schedule with Pearson VUE >

For students or instructors

Schedule with Certiport >

2.8 Azure Fundamentals certification



Roadmap

The Azure Fundamentals (AZ 900) certification is a fundamental certification on your journey to become an Azure Administrator, Developer, DEVOPS or Architect. This exam is considered as the first step in associate level and expert level Azure certifications path.

Chapter 3 : Cloud Concepts

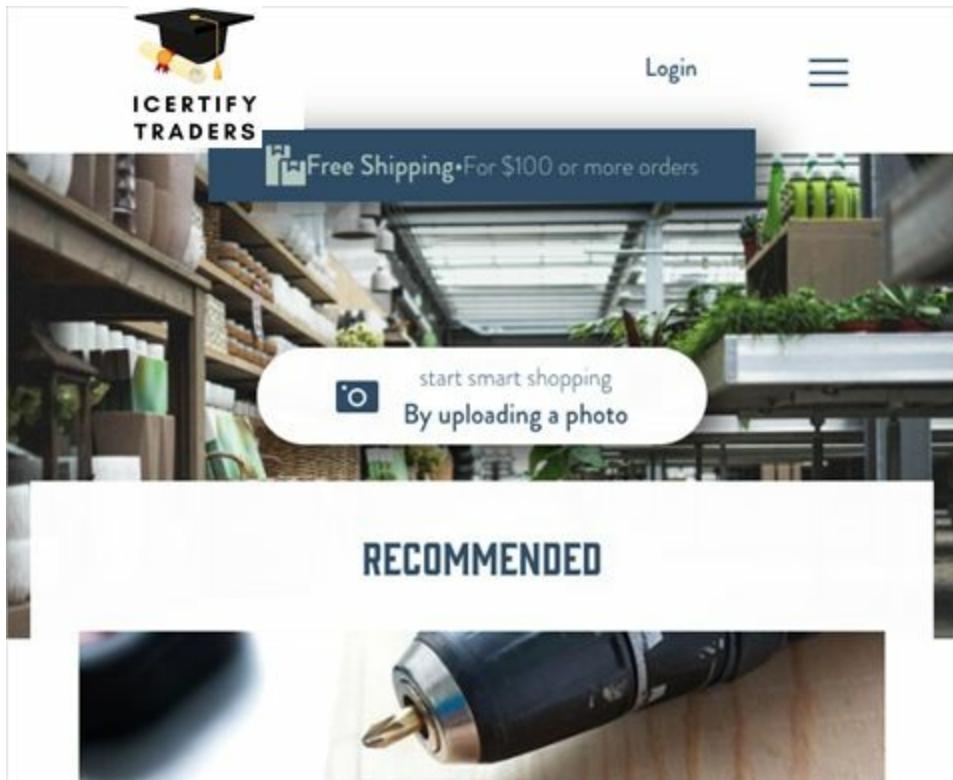
3.1 Learning Objectives

At the end of this chapter, 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)

3.2 Case study introduction

Throughout this Azure Fundamentals certification program , we'll work with iCertify Traders, a fictitious home improvement retailer. It operates retail hardware stores across the globe and online.



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

These management responsibilities create some obstacles for delivering your applications to your users in a timely fashion. As an IT pro, you realize it would be advantageous to have servers, storage, databases, and other services immediately available when you develop and deploy applications. You want to easily start a new server or add services to your solutions.

In the other units of this learning module, you've learned about some of the cloud-based services that iCertify Traders can use to address its technology challenges. With that in mind, the services that are available through Azure can help iCertify Traders conduct its business more efficiently.

As you complete the various modules in this book, we'll analyze the challenges that iCertify Traders is facing. You'll see how you can use Azure services to address each of the issues as they arise. After you've completed each of the modules, the knowledge that you gained from resolving the hypothetical challenges that the fictional iCertify Traders company encountered should benefit you in your real-world environments.

As you read through this chapter, imagine that you work in the IT department for iCertify Traders, which has decided to migrate its applications and data to Microsoft Azure. You're aware that cloud computing will save your company time and money by migrating from your existing, on-premises, physical hardware, to a cloud solution. With this new solution, you'll only need to pay for the resources and computing time that you use.



However, some of the cloud computing concepts are new to many members of your IT staff. They've been asking some specific questions about what cloud computing can do for them. For example, the team that manages iCertify Traders' website wants to know how Azure improves the site's availability and scalability. The team that handles the deployment of new hardware is curious to see how cloud computing can make their deployment processes faster.

In addition, your developer team wants to learn about the different options available to them as they are designing new applications. For example, is there a way to run their applications in a hybrid configuration, where part of their application runs on-premises and the rest of the application runs in the cloud?

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

3.3 Cloud computing

Have you ever wondered what cloud computing is? It's the delivery of computing services over the internet, which is otherwise known as the cloud. These services include servers, storage, databases, networking, software, analytics, and intelligence. Cloud computing offers faster innovation, flexible resources, and economies of scale.

Why is cloud computing typically cheaper to use?

Cloud computing is the delivery of computing services over the internet by using a pay-as-you-go pricing model. You typically pay only for the cloud services you use, which helps you:

- Lower your operating costs.
- Run your infrastructure more efficiently.
- Scale as your business needs change.

To put it another way, cloud computing is a way to rent compute power and storage from someone else's datacenter. You can treat cloud resources like you would your resources in your own datacenter. When you're done using them, you give them back. You're billed only for what you use.

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

Why should I move to the cloud?

The cloud helps you move faster and innovate in ways that were once nearly impossible. In our ever-changing digital world, two trends emerge:

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

Software releases were once scheduled in terms of months or even years. Today, teams release features in smaller batches that are often scheduled in

days or weeks. Some teams even deliver software updates continuously--sometimes with multiple releases within the same day.

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

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

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

What are some cloud computing advantages?

There are several advantages that a cloud environment has over a physical environment that your organization can use following its migration to Azure.

The Key benefits of cloud computing are as followings:

- Cost Savings - both real and Accounting
 - Agility
 - Availability
 - Security
 - Global reach
 - Range of ready on-demand services
 - Range of tools
-
- **Cost Savings** - both real and Accounting. The benefits in general can be tremendous cost savings, both real dollars per month, as well as the accountants who are changing the way that they are accounting for your expenses.

- **Agility:** There is the agility that comes with being able to respond to the marketplace, to your competitors, to new products, to customer's demand.
- **Availability :** There is an increased chance for availability. If you reboot the server for an upgrade or have a local storm knocking out the power, you are working in the cloud. A lot of these things get mitigated or can be mitigated if you design them into your application design.
- **Security :** You have the possibility of increased security of your data with cloud computing.
- **Global reach:** There is the ability for you to deploy your applications around the world in countries where you don't even have offices, but you have potential customers. You can deploy your applications into six, 10 or more regions of the world in just a button's click.
- **Range of ready on-demand services :** There is also a range of services available, not just virtual machines, Windows and Linux machines, but everything from AI and machine learning, various types of databases, analytics services, big data, etc.
- **Range of tools :** The final benefit will be various types of tools you have to manage your environment. A lot of people really like working within the cloud environment in terms of monitoring the servers and security tools. Since all of these things are now in the dashboard, it becomes very easy to work with a large range of servers and maybe even easier than a traditional virtualization environment on premise.**High availability:** Depending on the service-level agreement (SLA) that you choose, your cloud-based apps can provide a continuous user experience with no apparent downtime, even when things go wrong.
- **Scalability:** Apps in the cloud can scale vertically and horizontally:
 - Scale vertically to increase compute capacity by adding RAM or CPUs to a virtual machine.
 - Scaling horizontally increases compute capacity by adding instances of resources, such as adding VMs to the configuration.
- **Elasticity:** You can configure cloud-based apps to take advantage of autoscaling, so your apps always have the resources they need.
- **Agility:** Deploy and configure cloud-based resources quickly as your app requirements change.

- **Geo-distribution:** You can deploy apps and data to regional data centers around the globe, thereby ensuring that your customers always have the best performance in their region.
- **Disaster recovery:** By taking advantage of cloud-based backup services, data replication, and geo-distribution, you can deploy your apps with the confidence that comes from knowing that your data is safe in the event of disaster.

Cloud computing is a consumption-based model

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

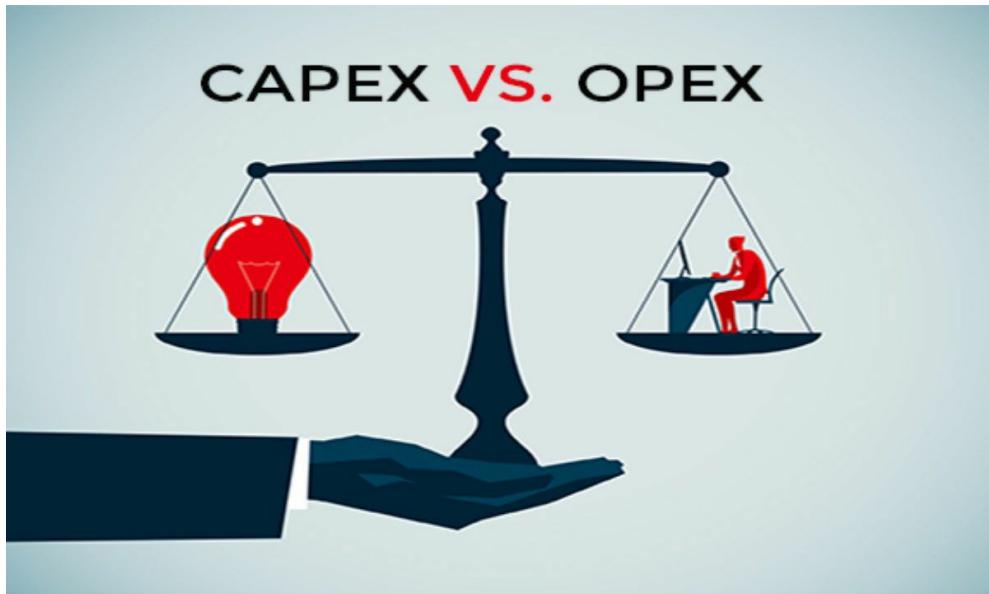
A consumption-based model has many benefits, including:

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

Capital expenses vs. Operating expenses

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

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



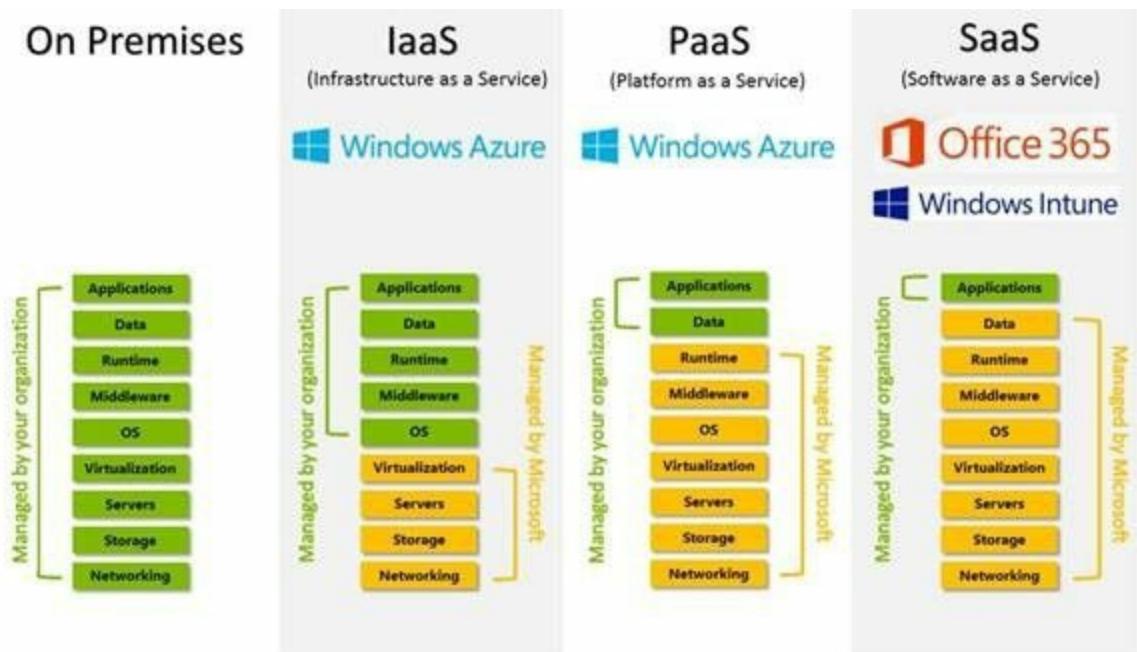
In other words, when iCertify Traders owns its infrastructure, it buys equipment that goes onto its balance sheets as assets. Because a capital investment was made, accountants categorize this transaction as a CapEx. Over time, to account for the assets' limited useful lifespan, assets are depreciated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

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

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

3.4 What are cloud service models?

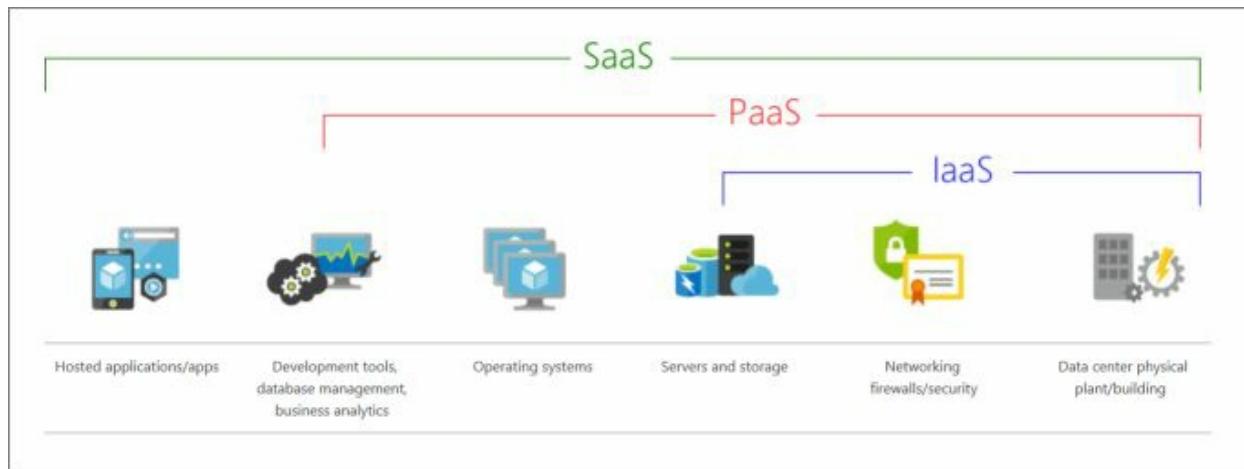
If you've been around cloud computing for a while, you've probably seen the PaaS, IaaS, and SaaS acronyms for the different cloud service models. These models define the different levels of shared responsibility that a cloud provider and cloud tenant are responsible for.



Model	Definition	Description
IaaS	Infrastructure-as-a-Service	This cloud service model is the closest to managing physical servers; a cloud provider will keep the hardware up-to-date, but operating system maintenance and network configuration is up to you as the cloud tenant. For example, Azure virtual machines are fully operational virtual computer devices running in Microsoft datacenters. An advantage of this cloud service model is rapid deployment of new compute devices. Setting up a new virtual machine is considerably faster than procuring, installing, and configuring a physical server.
PaaS	Platform-as-a-	This cloud service model is a managed hosting

	Service	environment. The cloud provider manages the virtual machines and networking resources, and the cloud tenant deploys their applications into the managed hosting environment. For example, Azure App Services provides a managed hosting environment where developers can upload their web applications, without having to worry about the physical hardware and software requirements.
SaaS	Software-as-a-Service	In this cloud service model, the cloud provider manages all aspects of the application environment, such as virtual machines, networking resources, data storage, and applications. The cloud tenant only needs to provide their data to the application managed by the cloud provider. For example, Microsoft Office 365 provides a fully working version of Microsoft Office that runs in the cloud. All you need to do is create your content, and Office 365 takes care of everything else.

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



So in this section of the course, we're going to talk about the types of cloud services that you can select, these are sort of the paradigms, if you will, of cloud services.

And then we'll talk about how that responsibility of security falls between yourself and the cloud provider.

So perhaps the most common and easy to explain type of cloud service is called infrastructure as a service. It's also commonly abbreviated as IaaS. This is when you're basically getting a Virtual Machine like Windows or Linux that you can do what you want with it. So if you take what you are running on a local physical machine and transfer that to the cloud without much changes, that is a Windows machine or Linux machine in the cloud. That's a Virtual Machine and that is infrastructure as a service.

This also includes things like networking services, load balancers, firewalls, anything that you have a physical representation in your own network, but you're using a virtualization representation in the cloud. It's sort of a one to one matching then that could be basically considered as infrastructure, as a service. Now, this isn't going to include software services like databases and things like that. But in terms of pieces of hardware that you have in your network, that you are virtualizing to run in the cloud, then that's infrastructure as a service.

So infrastructure is the most basic foundational one. You're just moving what you currently have from your own network and migrating into the cloud. And it's a pretty one to one mapping. You've got a network here, you create a network there, you've got a machine here. You create a machine there.

Now we're starting to get into what I'm calling levels of abstraction, particularly with Microsoft, but of course, all the cloud providers provide other ways of running certain code and services in the cloud that they're now more involved in.

So the first level above infrastructure is called platform as a service. So you can envision this environment where all you're doing is just compiling your code or taking your code. I'd say compile your code, putting it into a zip file and uploading it into the cloud and the cloud provider then just runs that code. So in essence, you're not picking out specific pieces of hardware. You're not setting up networks. You're not doing any of those infrastructure pieces. You're just giving them the code and you're saying, hey, here's my program, please run it. And that could be considered a platform as a service model in Microsoft, Azure. These are called Web apps.

But we'll talk about Azure specifically in a couple of sections from now. So all we need to know is any time you don't have choices over the hardware now, you do typically have tiers or, you know, you're basically choosing payment levels.

So do you want to run this as basic or standard or premium?

You're going to choose tiers, but you don't have to choose a RAM in CPU and manage the disk space and things like that. The next level of abstraction above the platform would be more of a software service now or this is abbreviated as SaaS

You may have heard this outside of the context of cloud computing. There are many famous SaaS companies that you may interact with every day. For instance, anything like Dropbox, you know, where you're putting your files in the cloud is a SaaS any of your backup services like I use back, and that's a service provider providing services to the cloud. Any of your Google Drive, Google Docs, you know, Microsoft Office 365, anything where you use a Web browser to access a service that is typically a SaaS service. You're not running the software on your own machines. It's running in the cloud.

And believe it or not, there are SaaS products within cloud providers. We talk about Office 365 running on Azure, for instance, but you could have other products. Even the Active Directory is a product that runs in the cloud as a SaaS.

So really, you're just configuring an existing product. You have no access to the code, you're not uploading code to run. You're basically using a product that's being provided to you.

So those are the three levels between infrastructure as a service platform, as a service and software as a service. Now there are others and we're going to talk about that in a second. But we do have an important point, and this is on the exam called the Shared Responsibility Model for Security.

And this is going to differentiate between software as a service platform, as a service infrastructure, as a service and running the servers on Prem, which is the on premises model, which is your hosting the machines and the networks on your own hardware.

So for SaaS percent the cloud provider has complete responsibility for physical security. They secure the data centers, the door locks, the fingerprint readers to get in the fences around it, to secure the physical networking, the switches and the wires, how they connect to the Internet through their own Internet provider. They secure the computers, the racks, the people who have access to those devices. Physically, that's a huge responsibility because all of your hacking protections mean nothing if the hacker can grab the machine and just take it. So the physical security for those three models is with Azure.

Obviously, if you're running it in your own environment, well, then that's on your shoulders. You need to have the physical security in place. You need to restrict who can have access to those machines, and so that your hacker cannot force an employee to go and do something for them. I'm going to switch to the top of the model in terms of where everything is always your own responsibility.

So the information that you pass into Azure, the data that you fill into your databases, the code that you upload, that's your own code. That's always going to be only your responsibility, any kind of connectivity that you set up your workstations and your mobile access and things like that is always going to be your responsibility. And these things are often surrounded by accounts. You know, you're going to have an Azure account, you're going to have user accounts.

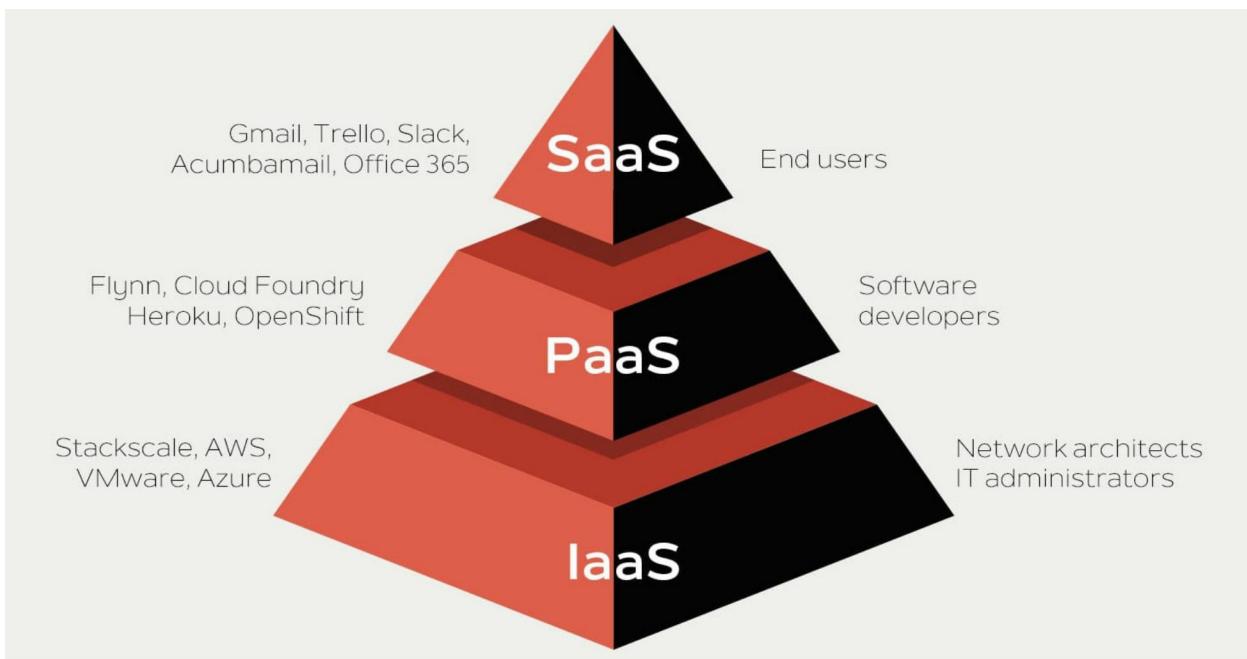
So when you're setting up accounts, managing passwords, how you do multi factor authentication, that's always going to be your responsibility. If you have a storage account and it has an access key and you somehow leave that access key on a Post-it note and that gets leaked, someone's going to steal your data and that will be entirely your responsibility.

Now, the middle layer where it says it varies by service type, that's really the finer details of this. Right. So in a SaaS model, like in the Office 365 or Azure Active Directory case, there's a shared responsibility. Microsoft has a responsibility to make sure that your accounts are not able to be hacked into to some degree. But then, of course, you still have your own responsibilities for not letting someone into your account. And the kind of applications that you upload in a SaaS model. Well, that's their responsibility. They coded it.

You're not even doing any coding in the access model, but in the infrastructure model, it's entirely your responsibility and LinkedIn passes that somewhere in between.

So I take a moment and really try to understand between those four models whose responsibility is security. And that's one of the determinations of how you're going to make a decision in terms of which model you're going to follow when you're using the cloud. We'll come back and we'll continue to talk about the different models.

Let's compare the three models in more detail in the following sections.



3.4.1 IaaS (Infrastructure as a Service)

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 up-front costs.
- **Agility.** Applications can be made accessible quickly, and deprovisioned whenever needed.
- **Management.** The shared responsibility model applies; the user manages and maintains the services they have provisioned, and the

cloud provider manages and maintains the cloud infrastructure.

- **Consumption-based model.** Organizations pay only for what they use and operate under an Operational Expenditure (OpEx) model.
- **Skills.** No deep technical skills are required to deploy, use, and gain the benefits of a public cloud. Organizations can use the skills and expertise of the cloud provider to ensure workloads are secure, safe, and highly available.
- **Cloud benefits.** Organizations can use 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 because you have control to configure and manage the hardware running your application.

3.4.2 PaaS (Platform as a Service)

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

Advantages

- **No CapEx.** Users have no up-front costs.
- **Agility.** PaaS is more agile than IaaS, and users don't need to configure servers for running applications.
- **Consumption-based model.** Users 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 PaaS.
- **Cloud benefits.** Users can take advantage of the skills and expertise of the cloud provider to ensure that their workloads are made secure and highly available. In addition, users can gain access to more cutting-edge development tools. They can then apply these tools across an application's lifecycle.
- **Productivity.** Users can focus on application development only, because the cloud provider handles all platform management. Working with distributed teams as services is easier because the platform is accessed over the internet. You can make the platform available globally more easily.

Disadvantage

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

3.4.3 SaaS (Software as a Service)

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

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

Advantages

- **No CapEx.** Users have no up-front 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.
- **Skills.** No deep technical skills are required to deploy, use, and gain the benefits of SaaS.
- **Flexibility.** Users can access the same application data from anywhere.

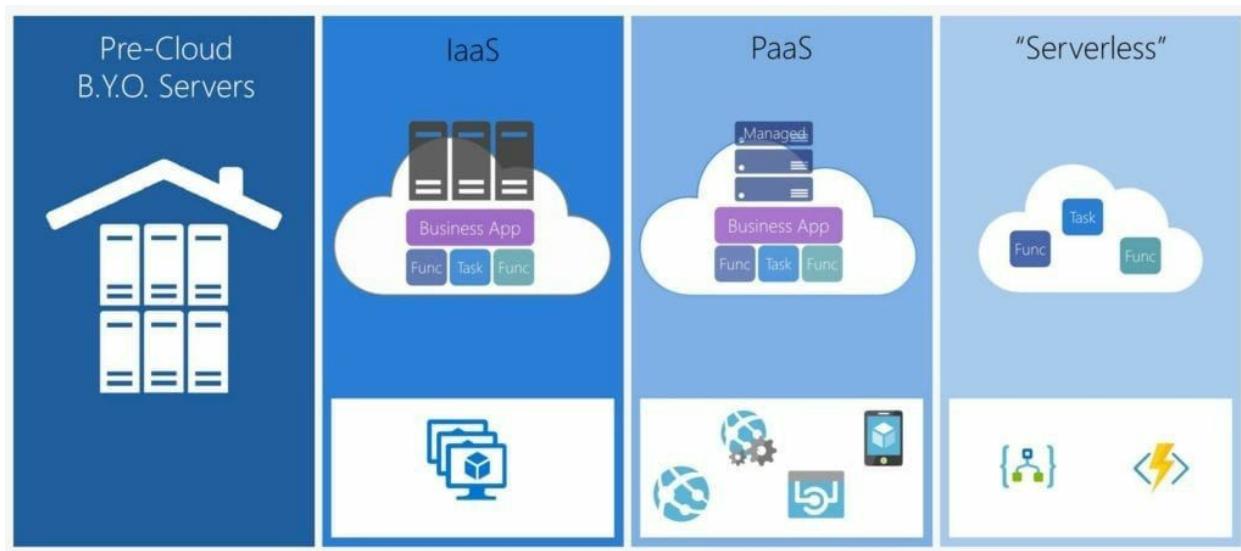
Disadvantage

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

3.5 Serverless computing

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

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



So in this lesson, we are going to review the other models. Now, the most prominent of the other models is now being called the Serverless model. The name is a little bit misleading because there are still servers. It's just even more abstracted from you. So you just have less access to the servers running a surplus model. And oftentimes you don't even know how many servers, how many processes are running your code. So at least in the platform as a service model, you do have some concept of how many instances and what

your performance expectations are. But in the Serverless model, it's just even less so. You don't have as much access to control performance in the platform as a service model.

One of the foundational elements in Azure is called the App Service Plan, and we're going to talk about that later in the course. But in the platform, as a service model, you're choosing a tier, you're choosing the basic tier, the standard tier and the premium tier, and you're also choosing plan levels within those. So standard one, standard two, standard three. And so you're going to get double the performance like two is double the performance of S1 and as three is double the performance of S2 and the features are pretty much the same between them except for the performance.

So in the past model, you do have that control over how much horsepower is running your apps. In the Serverless model, you're just handing it over and you're paying on a different level also with the pay-as-you-go model. The concept of scaling is your responsibility. So if you want your application to pay attention to the CPU utilization and then add instances when the CPU starts to get hot, that would be the past model. In the serverless model, the cloud provider takes that responsibility. So you give the code and they will add servers as they need to. OK, so there you're basically trusting them with not only the hardware but the scaling issue. So there is sort of a benefit to Serverless, which is you don't even have to worry about choosing the right plan when you're sitting in front of the computer and you're trying to set this up and you're like, oh, do I need the S2 or should I go for the S3 just in case? So Serverless is even closer to that ideal of leaving things to the cloud and only paying for what you need.

You're not worrying about scaling. You're not trying to set up the right rules in terms of is it 70 percent CPU or 75 percent?

When do you scale back another benefit to the server?

This model means there's also a chance of paying nothing.

So if you load a website into a Serverless app and no one ever visits it, your bill can come back literally as zero dollars because you're only paying for execution and you're not paying for the reservation of that.

So in an app service or platform as a service, you're paying by the hour. And

if no one ever visits your website, you're still paying. The Serverless model is you're basically paying not by the visit, but by the CPU utilization and even by data utilization. So if we look at Microsoft Azure, more specifically, there are different Serverless offerings. There is a Serverless Kubernetes offering, which is the container services, there are database serverless options and even a Cosmos DB serverless - if you have a different database and compute serverless offerings that you can go to, which again could drive your bills down to very low. But then you also could have an unexpected bill because you're not picking a plan. It's taking over for you.

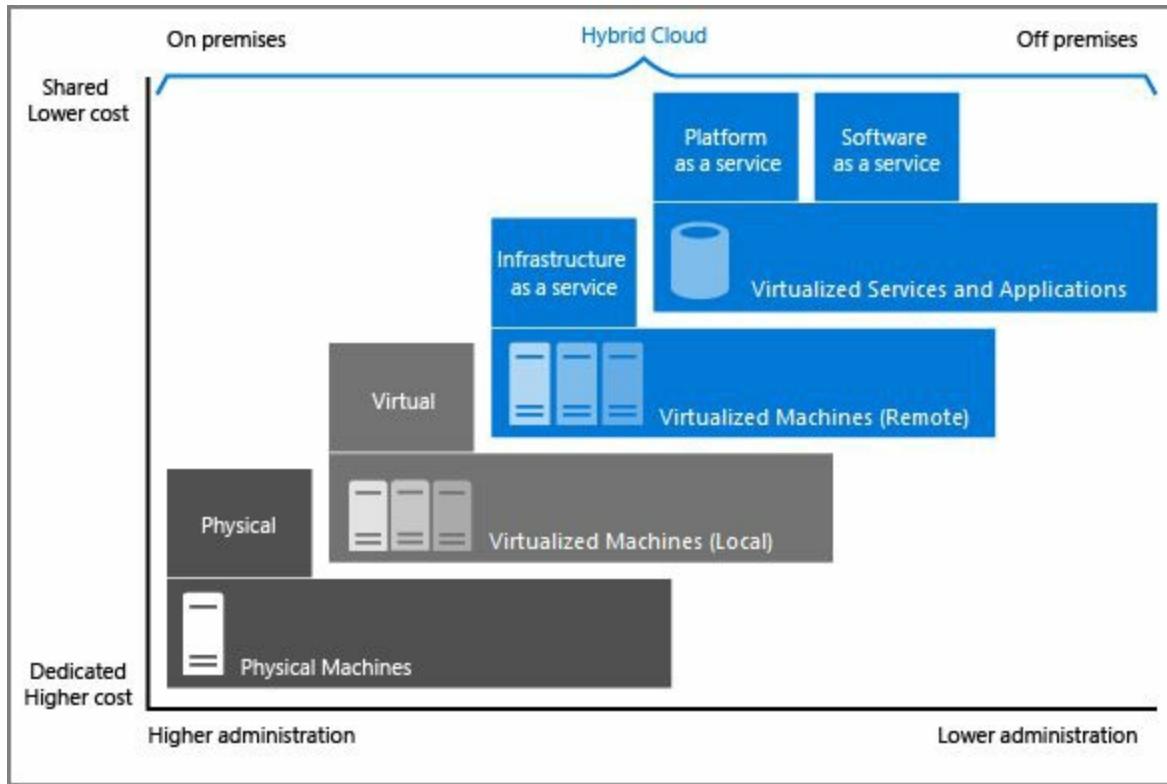
3.6 Types of cloud computing

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



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

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



So in the earlier sections, we reviewed the categories of cloud computing; In this section, we're going to talk about the types. There's a small distinction between that. Basically, you would think the cloud is just one thing, right?

When you say I'm going to run this in the cloud. Oh, OK. The cloud is just a single entity. But in actual fact, there are many different types of clouds.

The cloud that we often think about and maybe is most relevant to anyone watching this course is the public cloud. And that means that anyone can go and sign up for it. Basically, if you have a credit card, you go to Azure Dot Microsoft dot com and you sign up for an account, you give them your credit card and you can start using cloud services almost immediately. So that's the public cloud. It's just open for the public. Now, to be clear, again, Azure is the vendor. They own the hardware. They own the wires, the cables, the buildings, everything like that. It's their network, their infrastructure. And what you're doing is leasing or renting services. You're not leasing or renting hardware. You're leasing or renting services there.

But there's also this concept of the private cloud. There's something it's not often talked about, but you can actually set up a cloud environment using your own hardware. And so if you are a government or a bank or a large

enterprise, you might say, hey, we don't want to use Microsoft's hardware. We have our own data center. We are happy to pay for that, a large upfront capital expenditure. But we do love the cloud, the flexibility, the agility, the scalability, elasticity. We want some of those benefits. So that's called a private cloud. The customer owns the hardware or even leases it or has exclusive access to it. So you may work with a company like IBM or other companies to have a private cloud. But it's not just walk in with a credit card and you're using it within twenty minutes. You have to establish that relationship again. Typically you're purchasing hardware upfront, it requires long term commitments.

Microsoft has products you may have heard called Azure Stack, which is software that you can license to install on your own hardware, and you can use a portal and create VMS and stuff just like you do with the public cloud. So Azure stack is the product that's used. We're talking about private clouds with Azure, but other companies have private clouds.

The third type of cloud computing is called hybrid, and Microsoft is really bigger on this than either Google or Amazon when it comes to the cloud. And hybrid, as the name implies, is a combination of public cloud. And your private hardware doesn't have to be Azure stack running in your own environment. You could just have a typical Windows installation or Linux installation and you're just installing agents on those machines in order for the cloud to operate to the public cloud. But you're basically extending your space into the public cloud. You're extending your databases that are existing primarily on your private cloud, into the public cloud, working with servers that run some of them in the public and some of them on your own cloud, things like that. And you see that word used in the Azure world in different contexts, not just with it comes to the cloud. So let's compare and contrast the differences between public, private and hybrid.

And I think hopefully it is pretty straightforward, but public cloud, Microsoft owns the hardware and you're just temporarily using it. And again, you could set up there are things called reservations and you can put yourself in a one year or a three year contract. So there are some longer term elements and cost saving elements. The public cloud, private cloud. It is your hardware or at

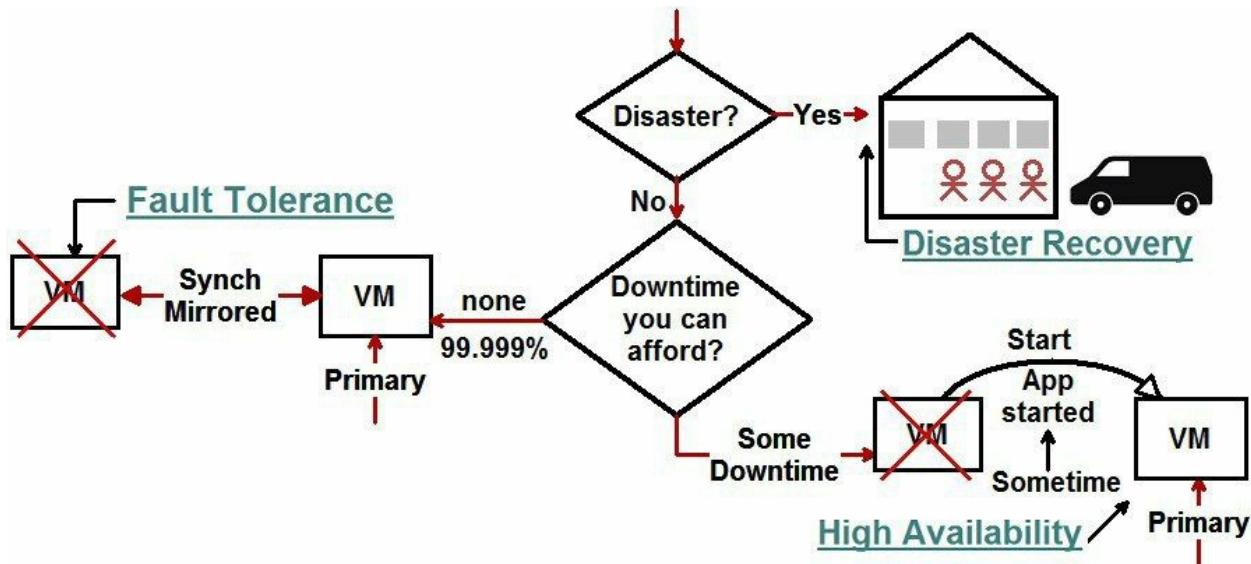
least you have an exclusive contract with someone to lease it more like a traditional on prem or hosting arrangement. But you're using the services of the public cloud and maybe get some of the benefits of the agility, flexibility and things like that. But you own the hardware, but you don't get the cost savings of being able to just stop paying for something. And finally, hybrid being the mix between some public, some private. And again, you don't even have to be running a full on private cloud, just your own hardware, your own network, your corporate network versus the Azure network, VPN and connections express things like that. So that's the difference between the three models.

3.7 Azure and Cloud

Under this topic, we will focus on cloud concepts and specifically we will be looking at the benefits and considerations of using cloud services. In this topic, we will be looking at three concepts that each tie together to provide numerous advantages to using cloud computing and those three concepts are :

1. High Availability
2. Fault Tolerance
3. Disaster recovery

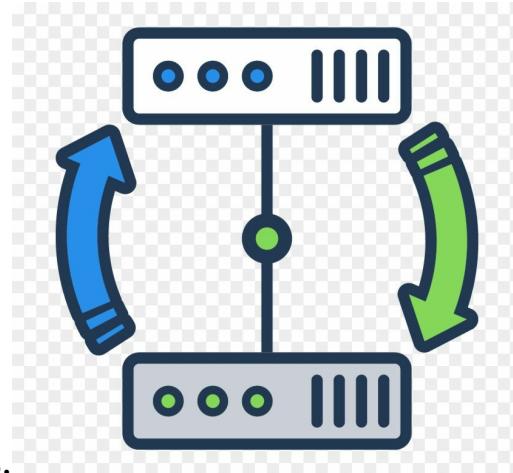
So let's start by taking a look at the interactive diagram and we'll go through each of these three concepts and make sure that we know what each one of them means and how they can each help us to achieve the best possible applications and systems.



As we go through these concepts, let us try to think about each one in terms of what it would cost us to replicate in our own data centers instead of using Azure.

3.7.1 High Availability

High Availability is the ability to maintain an acceptable, continuous performance despite temporary load fluctuations or failures in services,



hardware or data centers.

And the key point here is to maintain acceptable, continuous performance and that means that even if traffic varies to our site if it increases or decreases greatly or in fact if certain Azure services fail, some hardware fails or in fact if an entire data center fails, our applications and systems can still maintain acceptable, continuous performance.

How does Azure do that ?

It is completely based on redundancies at every level. We will start at the finest level which is a single individual data center within Azure, and we will look at the redundancies employed there to make sure that everything stays up as much as possible.

Data Center Redundancies are as follows:

- Power
- Cooling
- Networking
- Others

Power:

First off with power, the power systems in these Azure Data centers are fully redundant. It's not uncommon for a data center to be able to generate its own power and as well there might be different providers of power coming into the data center.

So if one has an interruption the other stays up. And there are also redundancies in the power generation, the power battery backups and systems like that.

Cooling:

There are also redundancies with the cooling systems. They might use a combination of different cooling approaches like water cooling, air cooling and they might have redundancies as well with the providers that they use to power and to fuel those cooling systems.

Networking:

With the networking equipment like switches, routers and other networking hardware all of those are fully redundant and their data centers as well.

As a matter of fact, there might be multiple Internet service providers coming into the data centers as well. If one is actually down or has an interruption, the other one can stay up and service the needs of the data center.

Within an Azure Data Center there's redundancies at nearly every level but in case something happens to an entire data center, we can step up a level from the data center and go to Availability Zones and reap even more redundancies there.

An Availability Zone is essentially a grouping of one or more data centers put together. In this capacity, you can deploy your apps and your systems to multiple different Availability Zones.

For example: Let us assume we deploy to two Availability Zones. If a data center and one availability goes down, we still might be deployed to a second data center in that same availability zone and our applications and systems can stay up now.

Now moving to a higher level, What happens if an entire Availability Zone somehow goes down through either a natural disaster or some sort of emergency ?

The higher level up from Availability Zones is a Region.

Region:

A Region encompasses multiple Availability Zones put together.

In fact, let us take a look at the below diagram. We can see on Microsoft's site that Azure has 54 regions worldwide at the time of writing this book and it's available in 140 countries around the world.

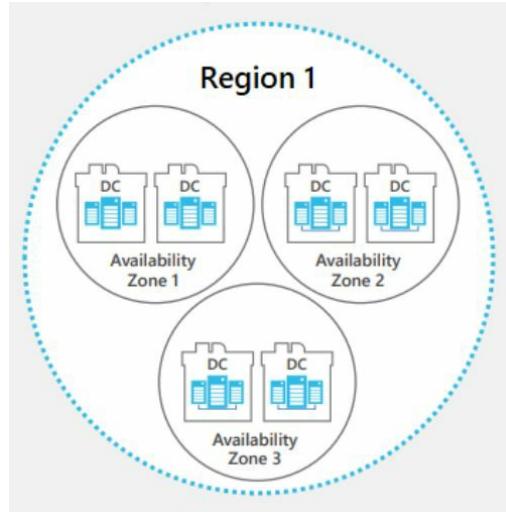
So pretty much no matter where you are in the world, you are most likely pretty close to an Azure region if not directly in one. And at the very least you should have access to the Azure cloud for your business.

It is important to note that in a region, a region groups multiple Availability Zones put together and that is reflected in the below diagram.



On the side image, we see a fictitious Region 1 which consists of 3 Availability Zones: 1,2 and 3. Within each one of those, we see 2 data centers.

You can now see how the redundancy stack together. It is starting from the data center level. There are multiple redundancies and all the utilities and the



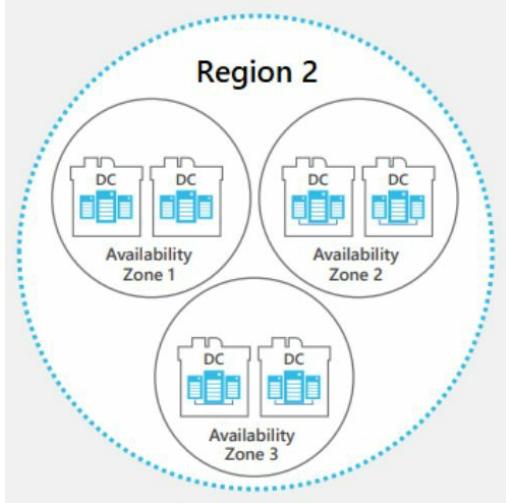
infrastructure at the data center.

Case 1:

If we have deployed two Availability Zones and then if something were to happen to a single data center, our application and system may still be in a secondary data center that is not affected and would keep up and running.

Case 2:

Likewise, if some sort of accident or disaster happens that affects an entire Availability Zone, we have the option to deploy our apps and systems across multiple Availability Zones. Even if one goes down, the data centers in the other Availability Zone can pick up the slack and continue to host our applications and systems and we will stay up and running.



Case 3:

And finally if an entire Region somehow goes down, all the Availability

Zones and all the data centers in the region can take advantage of using multiple regions within Azure.

For example: If the East U.S goes down because of some freak accident, we could also be deployed in the West U.S. and none of our applications or systems would actually go down because our second region would pick up the load.

And so it's a pretty powerful way through all these redundancies for Azure to maintain acceptable, continuous performance despite any of these fluctuations in load or failures.

3.7.2 Fault Tolerance

Fault Tolerance refers to a system's ability to continue to operate properly when one or more of its components fail. There are two ways that we can look at becoming fault tolerant.



We can use Proactive measures and we can use Reactive options.

Proactive Measures:

- Regularly backup data/apps/resources
- Deploy to multiple Availability Zones or Regions
- Load balance across multiple Availability Zones and Regions
- Monitor health of data/apps/resources.

Starting with Proactive options, some proactive ways to handle faults when they occur to make sure our systems continue operating properly are to regularly backup our data, apps and our resources and that way if something does happen we would be ready to restore them as needed and get back up and running.

We can also deploy to multiple Availability Zones or Regions to make sure that if one Availability Zone or Region goes down, our systems are in another AZ or Region and they will stay up because of that.

Now when we do that, we can also load balance across multiple Availability Zones or Regions. Even if one does go down in unlikely scenarios, our traffic will automatically be rerouted to the Availability Zone or Region that is up and it will be transparent to us. We won't see any failures because of that.

Finally, we can monitor the health of our data, apps and resources to anticipate any problems and to handle them as quickly as possible.

So these are approaches that we can take before a fault actually happens ie.. Proactive measures to make sure that we can recover from it as soon as possible and some of these options outright mitigate any errors because they spread our applications across different Regions. So there is at least one area that's not affected.

Now let's look at

Reactive approaches

They are:

- Restore data/ apps/ resources to different Availability Zones or Regions.
- Deploy to different Availability Zones or Regions.

If something does happen that takes our systems offline, we can react to that to get our apps up as quickly as possible. And one way we can do that is to restore our data apps and resources to a different environment like a different Availability Zone or a Region. That way we can get back up and running as quickly as possible.

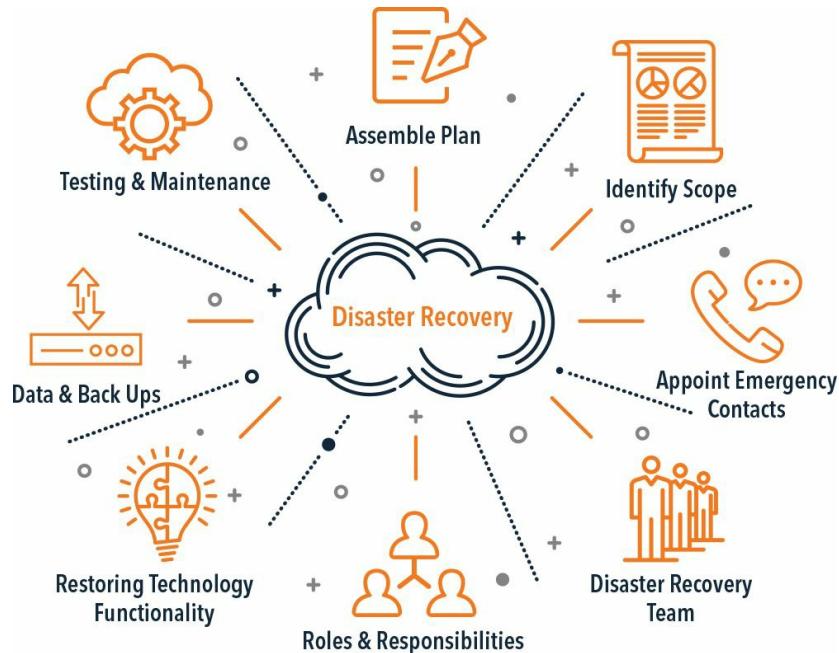
Also, if one of our Availability Zones or Regions is down, we can simply target a different Availability Zone or Region to deploy our assets there. This will help us to get back up and running as quickly as possible.

With Azure, there's a few mechanisms in place to either try to avoid failures in the first place like deploying to multiple Availability Zones or Regions. And in scenarios when a fault does happen, to be able to recover from it as quickly as possible using backups and restoring them.

And that leads us into our next topic which is Disaster Recovery.

3.7.3 Disaster Recovery

Disaster Recovery is a system's ability to backup and restore data, apps and resources when needed.

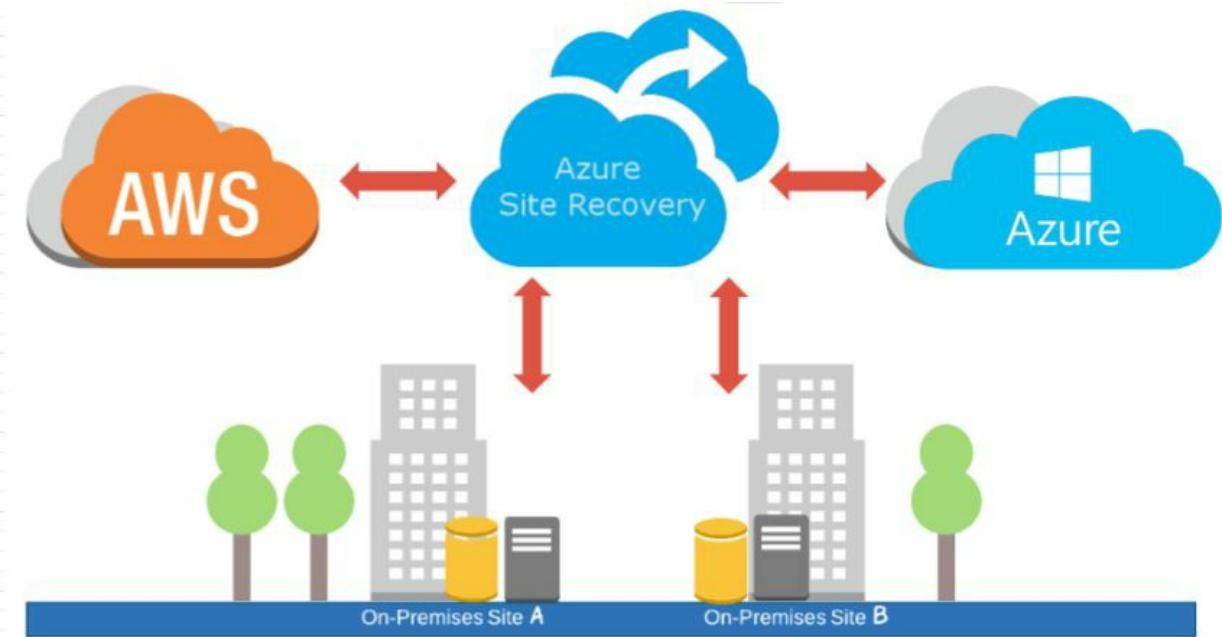


We can do this in a variety of ways. We can use Azure to restore:

- On-premises to on-premises
- On-premises to Azure
- Other cloud to Azure
- Azure to Azure

If we have on premise data centers like in the below diagram, we can assume, let's say we have Data Centers A and B. We can store all of our backups of our data, apps and resources in Azure and we can restore from our Data Center A to our Data Center B using Azure as a middleman just to store the copies of our backed up data.

This is the way we can restore from on premises to on premises Data Centers.



We can take a different approach. If our Data Center A goes out, we can store our backups in Azure and immediately restore to Azure. And in that capacity, we can be restoring from on premises Data centers to Azure Cloud Data Centers.

Additionally, if our assets are in a different cloud such as AWS, we can store backups of our data, apps and resources in Azure and we can restore to Azure. And in that capacity, we can restore from other cloud services directly to Azure.

And finally, if our applications already live in Azure, we can keep all of our backups inside of Azure as well ideally in multiple different regions for protection. In the case of an outage in one Region or Availability Zone, we can just deploy to a second Region or Availability Zone within Azure. In that way, we are restoring from Azure to Azure.

So as you can see there are a couple of different ways we can accomplish Disaster Recovery. When a disaster does strike, whether it is to our own data center, another cloud service data center or an Azure Data Center, we have the available options we need in order to restore our services and get them back up and running.

3.7.4 Scalability and Elasticity

In this topic, we will be looking at cloud concepts and specifically the

benefits and considerations of using cloud services. In this lesson, we will be looking at two concepts that tie together to provide one of the key advantages to using cloud computing and those two concepts are:

Scalability and Elasticity

We will go through each of these concepts to know what they mean and how they can help us achieve the best possible applications and systems. Let us also try to think about each one in terms of what it would cost us to replicate in our own data centers.

Scalability:

Scalability can be defined as the ability to increase the instance count or size of the existing resources. And this can be done in two different ways.

- Scaling Out
- Scaling Up

We can scale out which will increase the instance count of our existing resources. As we can check the side diagram indicating the Scale out instance count, we can increase the count of our servers.

Scale out



For Example: let's assume, we start on the left with one server and we're able to scale out and go from 1 to 4 servers and in fact even more, go from 4 to 6 servers and each server is going to share the same profile.

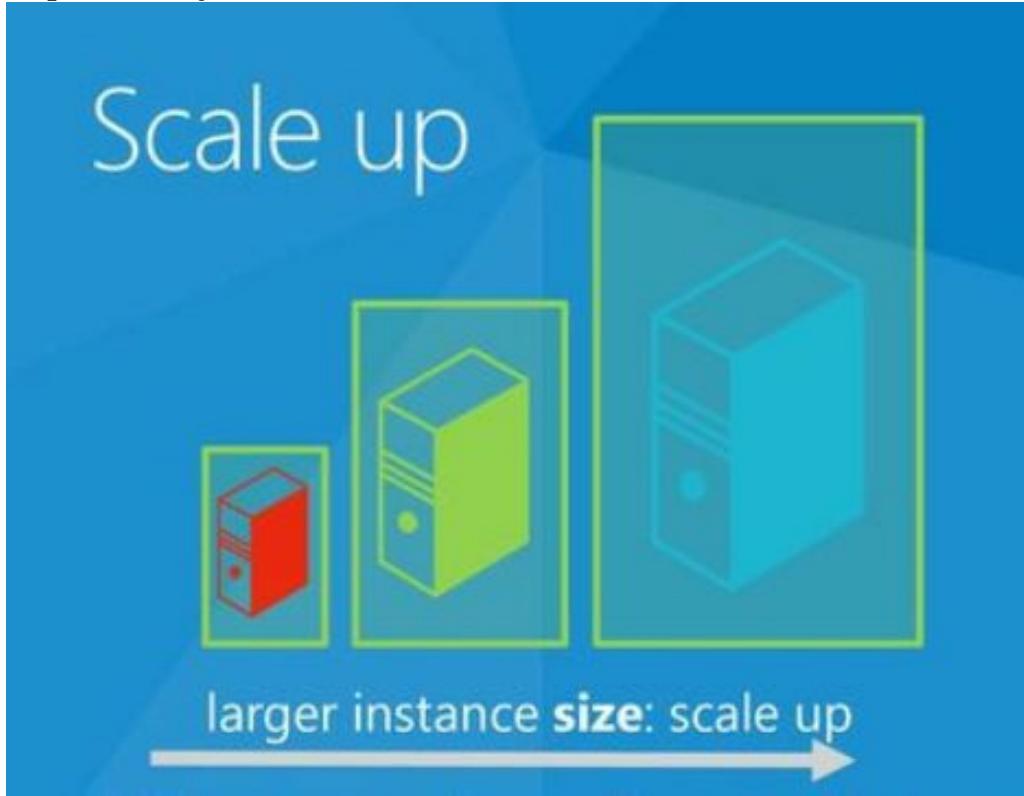
That is, they will have the same CPU, RAM and Hard Drive resources. We're just adding more of them to the pool of servers that can handle our requests. And when we do this, it is a non disruptive change. And what that means is we don't have to take any machines offline to scale out. All we have to do is add an extra server to the pool of servers that we have to handle our requests and it's automatically available to take some load off the other servers.

Basically, Scaling out is increasing the number of servers that we have to handle more requests.

There is a different type of scaling as well which is called Scaling up. Scaling up doesn't increase the count of our servers, but rather the size of our servers. And that is to say the CPU, RAM and Hard Drive profiles that the server is using.

For example: Take the image on the side. Let's say we start with a server that

has 1 CPU and 4 GB of RAM as our workload increases, not necessarily the traffic to our site but as the workload that each server has to perform increases we can scale our servers up and go from 1 CPU and 4 GB of RAM to potentially 2 CPUs and 8 GB of RAM.



If our workload increases even more, we can go to a bigger machine. We can move to 4 CPUs and 16 GB of RAM.

In this way, we can take an existing machine and add more resources to it so it can perform more work at an individual server level. But keep this in mind that Scaling up unlike Scaling out is actually

Disruptive. We have to first bring down the existing machine. Let's say our first server has 1 CPU before we can put online a second machine that will replace it with higher CPU and RAM.

So there are two ways essentially to scale whether it's Scaling out or Scaling up. Both allow us the flexibility to increase our resources as we need based on either the traffic to our site or the workload that our site's performing.

Now building on top of Scalability, we will take a look at Elasticity.

Elasticity:

In the case of Elasticity, we can think of the entire Azure cloud as a rubber band so to speak. We can pull on the rubber band and make it bigger and we can stop pulling on it and make it smaller.



Elasticity is the ability to increase or decrease the instance count or size of our existing resources based on fluctuations in traffic or load (to your site) or in the resource workload that your site has to perform.

Here are some of the abilities that Elasticity can have. They are:

- **Scale in (in/out, up/down)**

In this capacity, we can Scale in both directions. We can Scale Out and increase the number of servers as well as we can Scale In and decrease the number of servers. And likewise we can Scale Up and increase the size of our servers as well as Scale Down and decrease the size of our servers.

- **Can be Manual or Automatic**

Facilitating this elasticity can be a manual or an automatic process. In fact many services within Azure facilitate rules that allow you to auto scale based on CPU, RAM usage etc. Also, we can make it manual. If there is a business process that needs to be followed in which a certain person has to approve a change we can facilitate things like that by going with manual elasticity and manual scaling through some scripts or code of our own.

- **Changes in loads and workloads**

The important thing to remember with elasticity is that it's based on changes

in load or workload to our applications and servers. In that capacity, we have this kind of automatic ability to respond to changes in our applications and the load in our applications and adjust the amount of resources we have accordingly

- **Pay only for what you use**

One of the biggest key benefits of the cloud that has to do with this elasticity in this auto scaling is that by doing it we can eventually just pay only for what we're using. If we need to bring an extra one server or even an extra 100 servers online temporarily to handle an increase in our traffic. We are only paying for those extra 100 servers for the hour or two that they're brought online when they auto scale back down and we no longer need them, we are no longer paying for them.

And so you can see sort of the same concept in the diagram below. We may start with one single node and as our traffic and workload increases, we see on the right that we now have 7 different nodes in this example.

Likewise these are created on demand as the load to our applications dictates. And when that load drops and we no longer need seven servers we can move back the other direction and go back to 1.

Now this shows Scaling out but it could very well be scaling Up as well. For an example, we could interpret this image as 1 CPU in a single server and scale that up to 7 CPUs. Basically, the diagram works really in both directions. You can picture this as scaling out or scaling up or even both.

And again this is expanded or reduced as needed. So it's really directly tied to the load and the traffic and the workload of our applications. So keep in mind that this is really one of the core benefits of the cloud in general is the ability to pay for only what we're using and respond to changes in our applications in real time and be able to provision all the resources we need to handle that extra load.

You can imagine that doing this in our own data centers would be very very costly. Having to buy servers, set them up, manage and maintain them. And then when our load drops, what do we do?

We have to sell them to get our money back and we're not going to get very much money back for them. Maybe a quarter of what we paid. So it's a very

costly thing to constantly keep provisioning all these servers and then let them sit idle when we don't need them anymore.

3.7.5 Business Agility

In this topic, we'll be looking at cloud concepts and specifically the benefits and considerations of using cloud services. In this lesson, we will be looking at how we can gain business agility by using the Azure cloud.



Let us start by taking a look at the interactive diagram. We will go through each of the ways listed that we can gain more Business agility by using Azure and the cloud.

Business Agility is an Organization's ability to rapidly adapt to market and environmental changes in productive and cost effective ways and how we can take advantage of available resources to meet our customers demands.

Let us simplify it and say that it is our ability to rapidly adapt to any kind of

change whether it be business, political etc. and to provide our customers the best possible product by practicing the most productive and cost effective ways.

Focus on Time to Value

So the first point we will look at is a focus on time to value. It means that we want to get new products to market as soon as possible. We want shorter feedback cycles on our products whether they're with customers or internal employees and ultimately we want a faster return on our investment.

Azure helps us in all of these ways by shortening the amount of time that's needed to provision new resources or to scale our resources out and up. By being able to focus more on the business rather than IT management we are able to get our products to market as quickly as possible and to shorten those feedback cycles.

Innovation

Also there's a focus on innovation within business. We always want to look for better ways of doing things and using newer and better technologies. Azure allows us to do that by concentrating less on IT management and more on our business.

With the cheaper cost of Azure with paying only for what we use, we can instead focus our money not on data centers and servers but rather on employees and ideas to make our products better and as well we can take advantage of all of the technologies that are on Azure especially ones that are financially out of reach for us in our own data centers like Giant Clusters of servers or BlockChain servers and things like that.

And instead we can only pay for the limited resources we use and invest more money in the products of our business and the ideas of our business and our people which will lead to more innovation.

Low Latency

Also we're going to look at low latency and what this refers to is the latency in when a business makes the decision until they know if that decision was right or wrong. We are looking at that because the sooner a decision can be acted upon, the sooner the business knows whether that decision was right or

wrong and what else needs to be done.

With Azure's ability to provision even hundreds or thousands of servers immediately and have them up and running, that costs us a lot less time and money in the long run from having to purchase, configure and install those servers in our own data center. We can instead focus on immediately deploying to Azure and evaluating the business value of these decisions or applications.

It takes a complicated process of IT management away from us and instead lets us focus on just our business and by doing that, we can respond a lot quicker to the market.

Economic Effectiveness

We want to be as cost effective as possible in our processes and our use of resources. As discussed earlier, with Azure, we are able to pay for only what we use and to be able to provision hundreds or thousands of servers. Here, we are treating IT in the most cost effective way possible.

We no longer have to maintain our own data centers which potentially cost millions of dollars a year. We no longer have to maintain as much staff to manage our IT resources in our data center and we no longer have to buy extra servers and let them sit idle during the times that we don't have extra traffic.

Instead, we can rely on scaling and elasticity of the Azure cloud and paying for only what we use. We can achieve great economic effectiveness in our IT budget simply by using the cloud instead of our own data centers.

Rapid Adaptation

Rapid Adaptation means our ability as a business to quickly adapt to changes in the market. Highlighting the same points, with Azure giving us the ability to immediately deploy any number and type of resources that we need. We are able to rapidly adapt to changes in the market.

For example: if something were to happen and the business decided that there is an opportunity to capitalize upon but maybe we need 10000 servers of a certain type to do it, we no longer need an upfront investment of millions of dollars to do that we can simply go to Azure provision the servers and pay

just for what we are using. While we are using it, we are quickly able to adapt to market conditions by getting our IT resources provisioned and configured as quickly as possible, sometimes instantaneously with the Azure cloud.

Flexibility

All of this adds up to give our business more flexibility in the long run as we're able to move quickly to take advantage of new opportunities. Our business becomes more flexible. We can take advantage of new markets or new areas that the business wasn't previously involved in and it makes us more flexible to changes that might otherwise be disadvantageous to some of our competitors.

Azure as a whole with Regions around the world with redundancies to make sure that we have high availability. With the ability to recover from faults and disasters, it really gives us flexibility in our business to concentrate just on business problems and not managing an IT infrastructure.

Now, you can see how all these six items kind of play together and focus on the same themes but they all mean one thing for your business. You will be running a better business at the end of the day if you can focus less on these boiler plate IT management processes and focus more on putting your time and money into your actual business.

And with Azure, we can do that without worrying if our IT resources are online or if we have enough money to buy all the IT resources we need in our own data center instead we can quickly and simply provisioned just what we need within Azure, have it up and running immediately and pay only for what we use and more of our business time is spent on business ideas.

3.8 Knowledge check

Choose the best response for each question. Then select Check your answers.

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

- A. Platform-as-a-Service (PaaS)
- B. Networking-as-a-Service (NaaS)
- C. Infrastructure-as-a-Service (IaaS)
- D. Software-as-a-Service (SaaS)

2. Which of the following statements is true?

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

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

- A. Distributed cloud
- B. Hybrid cloud
- C. Private cloud
- D. Public cloud

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

- A. Scalability
- B. Geographic isolation
- C. Disaster recovery
- D. High availability

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

- A. IaaS, PaaS, and SaaS are examples of cloud computing service models.
- B. Cloud computing resources are usually limited to specific geographic regions.
- C. Cloud computing typically decreases your operating expenses.
- D. Three cloud computing deployment models are public cloud, private cloud, and hybrid cloud.

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

- A. True
- B. False

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

- A. True
- B. False

Answers

1. **B.** NaaS isn't a cloud computing category.
2. **B.** With Operating Expenses (OpEx), you are only responsible for the computing resources that you use.
3. **A.** A distributed cloud isn't a valid type of cloud computing.
4. **B.** You can choose to create resources in a single region; however, one of the primary advantages to cloud computing is geographic distribution.
5. **B.** Explanation: Most cloud computing resources can be distributed to global data centers.
6. **B.** Explanation: You can use a free Azure account or a Microsoft Learn sandbox to create resources.
7. **B. False.** Explanation: In an IaaS environment, the cloud provider is responsible for any hardware maintenance.

3.9 Summary

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

- Cloud services have certain characteristics and considerations, such as:
 - High availability
 - Scalability
 - Elasticity
 - Agility
 - Fault tolerance
 - Disaster recovery
 - Global reach
 - Customer latency capabilities
 - Predictive cost considerations
 - Security
- Economies of Scale : The concept of economies of scale is the ability to do things less expensively and more efficiently when operating at a larger scale in comparison to operating at a smaller scale.
- Capital Expenditure (CapEx) is the spending of money on physical infrastructure up front, and then deducting that expense from your tax bill over time. CapEx is an upfront cost which has a value that reduces over time.
- Operational Expenditure (OpEx) is spending money on services or products and being billed for them immediately. You can deduct this expense from your tax bill in the same year. There is no upfront cost, you pay for a service or product as you use it.

Chapter 4 : Azure Fundamental Concepts

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



**I C E R T I F Y
T R A D E R S**

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

4.1 Learning objectives

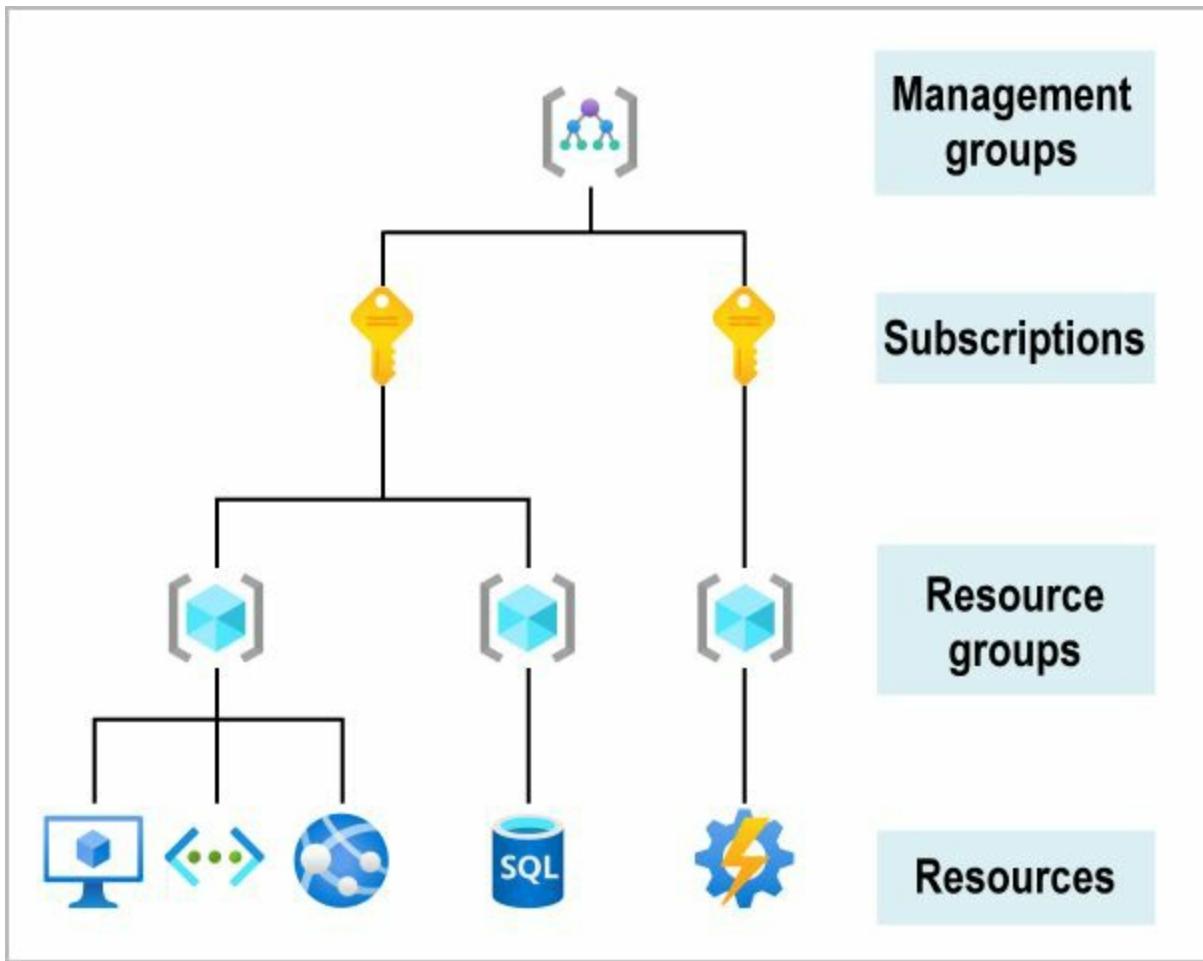
After completing this module, you'll be able to describe the benefits and usage of:

- Azure subscriptions and management groups.
- Azure resources, resource groups, and Azure Resource Manager.
- Azure regions, region pairs, and availability zones.

4.2 Overview of Azure subscriptions, management groups, and resources

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

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

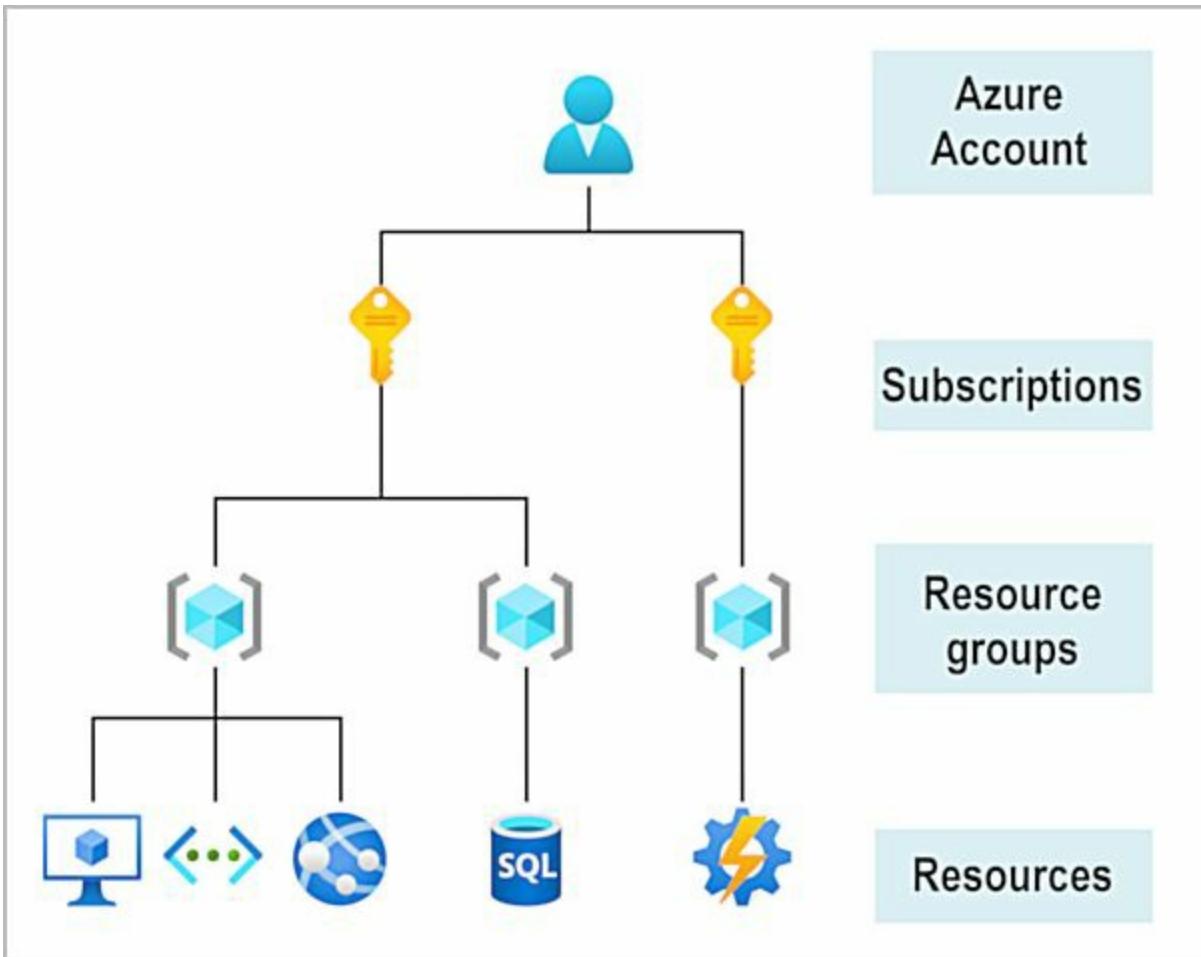


Having seen the top-down hierarchy of organization, let's describe each of those levels from the bottom up:

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

4.2.1 Get started with Azure accounts

To create and use Azure services, you need an Azure subscription. When you're working with your own applications and business needs, you need to create an Azure account, and a subscription will be created for you. After you've created an Azure account, you're free to create additional subscriptions. For example, your company might use a single Azure account for your business and separate subscriptions for development, marketing, and sales departments. After you've created an Azure subscription, you can start creating Azure resources within each subscription.



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

Create an Azure account

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

For more information on how to create an Azure account,

[What is the Azure free account?](#)

The Azure free account includes:

- Free access to popular Azure products for 12 months.
- A credit to spend for the first 30 days.
- Access to more than 25 products that are always free.

The Azure free account is an excellent way for new users to get started and explore. To sign up, you need a phone number, a credit card, and a Microsoft or GitHub account. The credit card information is used for identity verification only. You won't be charged for any services until you upgrade to a paid subscription.

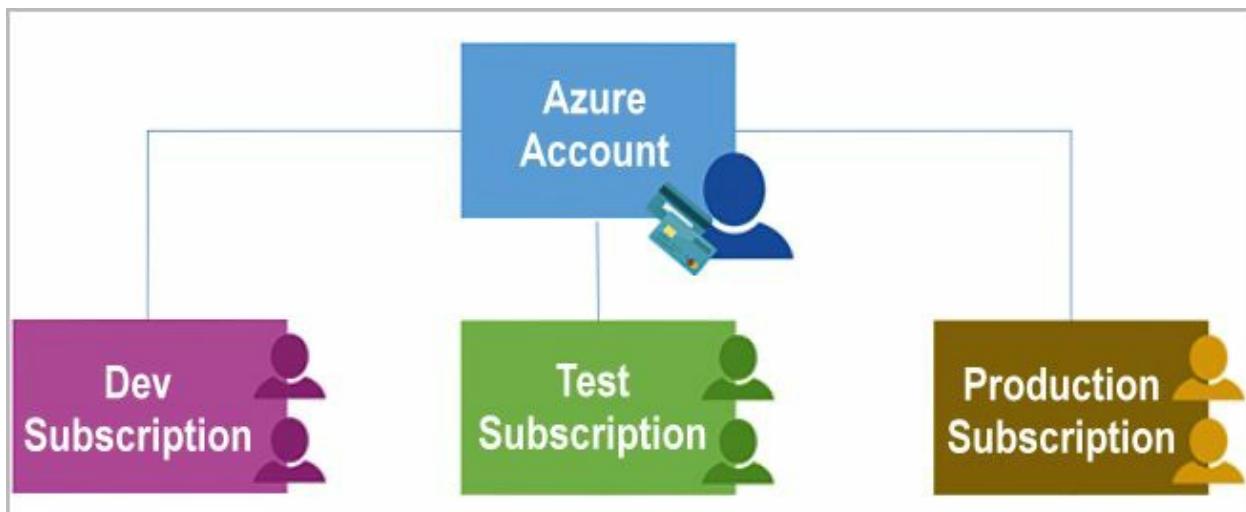
4.2.2 Azure subscriptions and management groups

As iCertify Traders gets started with Azure, one of your first steps will be to create at least one Azure subscription. You'll use it to create your cloud-based resources in Azure.

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

Azure subscriptions

Using Azure requires an Azure subscription. A subscription provides you with authenticated and authorized access to Azure products and services. It also 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 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:

- **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. Azure generates separate billing reports and invoices for each subscription so that you can organize and manage costs.
- **Access control boundary:** Azure applies 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 billing model allows you to manage and control access to the resources that users provision with specific subscriptions.

Now there's a very subtle difference between an account and a subscription, subscription is basically what they're calling a billing unit. So when you sign up for Azure, you have to give them your credit card or some other way for them to charge you, that creates a subscription. And that's the credit card to which your bills are sent. All of the resources that are created under that subscription get charged to that credit card.

You can create multiple subscriptions. So let's say you're in a situation where one customer gives you their credit card and another customer gives you their credit card and you'll want to manage the resources for both. Well, that's true. That could be done as to subscriptions. And that way it's 100 percent clear which Bill goes to which person. So subscription is the level of billing. And as an account owner, as a user, you can have access to more than one subscription. You can be the owner global administrator for one subscription, and you could only be a contributor or a user to another subscription. So you have the ability to have different levels of access to different subscriptions. So in your mind, you've got to keep separate the user ID and password that you use to log into Azure from the subscription, which is how resources get built.

When you do create a resource. If you create a Virtual Machine or a storage account, you do have to specify which subscription gets charged. So every single resource in Azure must be associated with a subscription. And like I said, it is common, if you will, to use multiple subscriptions to make sure that you're billing things separately, and even if you're going to reuse the same credit card, then you can still organize things into subscriptions. Now, Azure does give you many tools, including resource groups, including security and permissions that allow you to organize all the resources in a single subscription. But I can understand, and I'm sure obviously Azure understands that you may want to even completely firewall it off. You know, make sure that one account in one bill never, ever gets interacted with the other. And creating subscriptions for each account is one way to do that.

You can see here that there's three subscriptions in this diagram. One is for the Development Team, Testing team and finally the Production team. And so even within the same company, they're owning their own subscription.

And that way it gets built to their billing code, etc. You have your own financial way of managing resources. You can't separate them this way. And as at the top, you have an account which could be a user and they have access to all three subscriptions and they may even be the global administrator to all three subscriptions.

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 design 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 one subscription for your production workloads and another subscription for your development and testing workloads.

You might also need additional subscriptions because of:

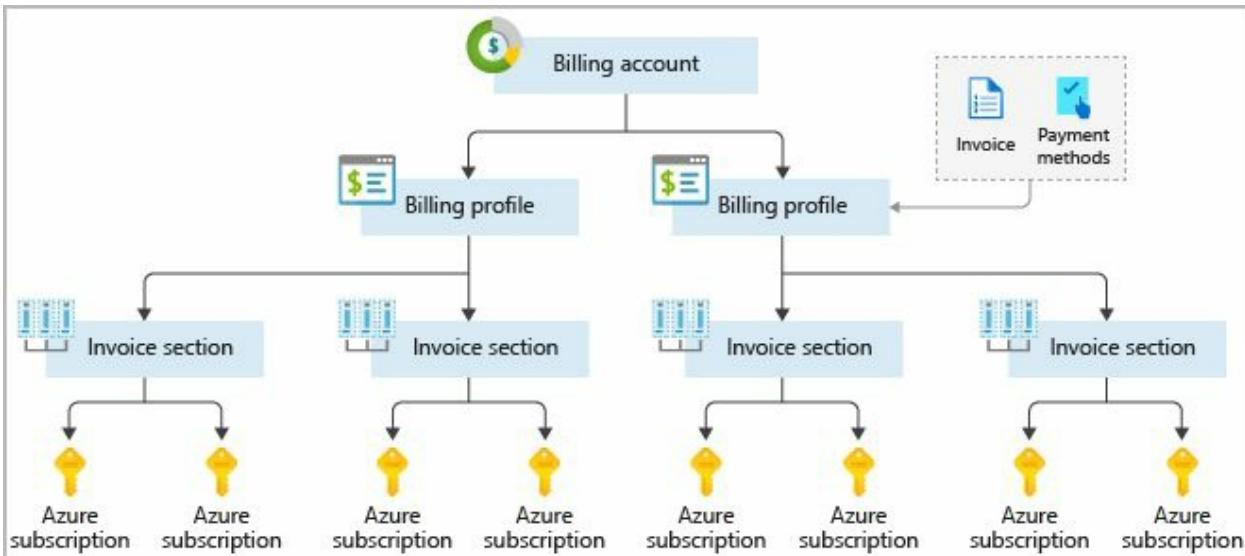
- **Subscription limits:** Subscriptions are bound to some hard limitations. For example, the maximum number of Azure ExpressRoute circuits per subscription is 10. Those limits should be considered as you create subscriptions on your account. If there's a need to go over those limits in particular scenarios,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



Flowchart-style diagram showing an example of setting up a billing structure where different groups like marketing or development have their own Azure subscription that rolls up into a larger company-paid Azure billing account.

4.2.3 Azure management groups

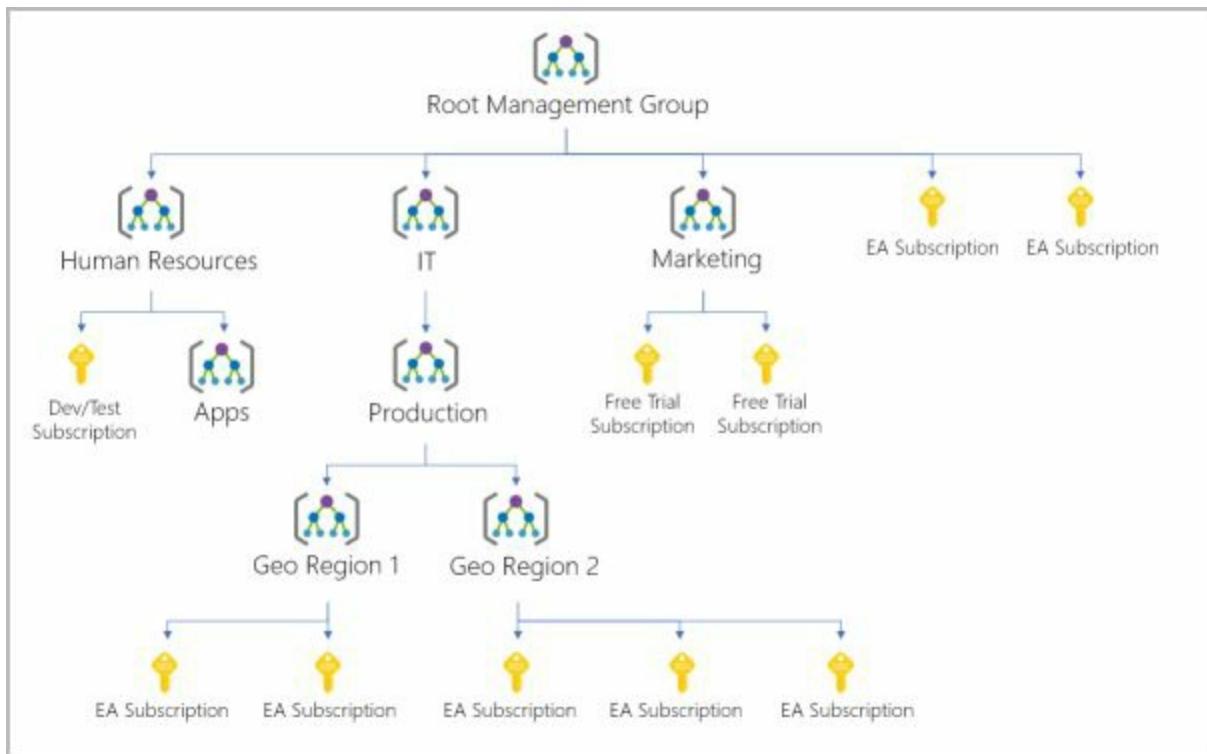
If your organization has many subscriptions, you might need a way to efficiently manage access, policies, and compliance for those subscriptions. Azure management groups provide a level of scope above subscriptions. You organize subscriptions into containers called management groups and apply your governance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

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

Hierarchy of management groups and subscriptions

You can build a flexible structure of management groups and subscriptions to organize your resources into a hierarchy for unified policy and access

management. The following diagram shows an example of creating a hierarchy for governance by using management groups.



You can create a hierarchy that applies a policy. For example, you could limit VM locations to the US West Region in a group called Production. This policy will inherit onto all the Enterprise Agreement subscriptions that are descendants of that management group and will apply to all VMs under those subscriptions. This security policy can't be altered by the resource or subscription owner, which allows for improved governance.

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

Important facts about management groups

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

4.3 Azure resources and Azure Resource Manager

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

Resource: A manageable item that's available through Azure. Virtual machines (VMs), storage accounts, web apps, databases, and virtual networks are examples of resources.

Resource group: A container that holds related resources for an Azure solution. The resource group includes resources that you want to manage as a group. You decide which resources belong in a resource group based on what makes the most sense for your organization.

4.3.1 Azure resource groups

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

Now, a resource group is basically like a folder structure or an organizational structure for resources. We have the individual resources. What we're talking about are virtual machines, storage accounts, databases and other resources that you can create in an Azure account. Like I said, there are over a thousand resources that Azure has available. You put those into resource groups, which again are logical groupings of related things. This could be by project, it could be by individual people that work on that project. Are you learning as a company to come up with logical ways to break up your resources and organize them the same way that you organize the files on your computer into

folders?

We even have above resource groups the concept of subscriptions, which we'll talk about right now. And above that you can organize your subscriptions into management groups. So important for the exam that you understand the logical groupings of subscriptions into groups, resource groups, into subscriptions and resources, into resource groups.

So I mentioned subscriptions. Now there's a very subtle difference between an account and a subscription, and we're even going to talk about Tenant in a second as well. Subscription is basically what they're calling a billing unit. So when you sign up for Azure, you have to give them your credit card or some other way for them to charge you. And that creates a subscription. And that's the credit card to which your bills are sent. All of the resources that are created under that subscription get charged to that credit card. You can create multiple subscriptions. So let's say you're in a situation where one customer gives you their credit card and another customer gives you their credit card and you'll want to manage the resources for both. Well, that's true. That could be done as to subscriptions. And that way it's 100 percent clear which Bill goes to which person. So subscription is the level of billing. And as an account owner, as a user, you can have access to more than one subscription. You can be the owner global administrator for one subscription, and you could only be a contributor or a user to another subscription. So you have the ability to have different levels of access to different subscriptions. So in your mind, you've got to keep separate the user ID and password that you use to log into Azure from the subscription, which is how resources get built. When you do create a resource. If you create a Virtual Machine or a storage account, you do have to specify which subscription gets charged. So every single resource in Azure must be associated with a subscription. And like I said, it is common, if you will, to use multiple subscriptions to make sure that you're billing things separately, and even if you're going to reuse the same credit card, then you can still organize things into subscriptions.

Now, Azure does give you many tools, including resource groups, including security and permissions that allow you to organize all the resources in a single subscription. But I can understand, and I'm sure obviously Azure understands that you may want to even completely firewall it off. You know, make sure that one account in one bill never, ever gets interacted with the

other. And creating subscriptions for each account is one way to do that.

And that way it gets built to their billing code, etc. You have your own financial way of managing resources. You can't separate them this way. And as at the top, you have an account which could be a user and they have access to all three subscriptions and they may even be the global administrator to all three subscriptions.

The next concept we briefly touched on is the concept of managing your subscriptions into management groups. And management groups can even be nested so you don't even have that single top level. You could have management groups that contain other management groups. And so here's a fictional and maybe a little excessive diagram. But you've got the talk. Santoso, which is Microsoft's fake company at the top and then the marketing and IT teams have their own groups. Marketing only needs one subscription, so they have their subscription under that. But the IT team needs multiple subscriptions and multiple groups. And you do this so that you can set policies. You can say, well, this is the rule across all our subscriptions. But this second rule only applies to these subscriptions and this third rule only applies to this one subscription. And so you can do a basically governance model on top of your subscriptions by grouping them together and then applying the rule at that group level instead of having to go into each individual subscription and reapply the rule.

Logical grouping

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



Conceptual image showing a resource group box with a function, VM, database, and app included.

Life cycle

If you delete a resource group, all resources contained within it are also deleted. Organizing resources by lifecycle can be useful in nonproduction environments, where you might try an experiment and then dispose of it. Resource groups make it easy to remove a set of resources all 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's needed.

4.3.2 Azure Resource Manager

Azure Resource Manager provides you with the tools you need to keep your resources organized and secure.

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

Azure Resource Manager has several features that you can use to organize resources, enforce standards, and protect your critical Azure resources from

accidental deletion.

Resource groups are containers for resources deployed on Azure. By placing resources of similar usage, type, or location in the same resource group, you can provide some order and organization to your Azure resources.

Tags allow you to improve the organization of your resources even further. You can use tags to associate custom details with a resource or resource group, such as a cost center or billing department. Resource groups and tags are great for helping you organize existing resources or groups.

But how do you make sure that new resources follow the same rules?

You can use Azure policies to ensure that new resources use the same tags as existing resources, keeping things organized.

How do you protect your resources once they've been deployed?

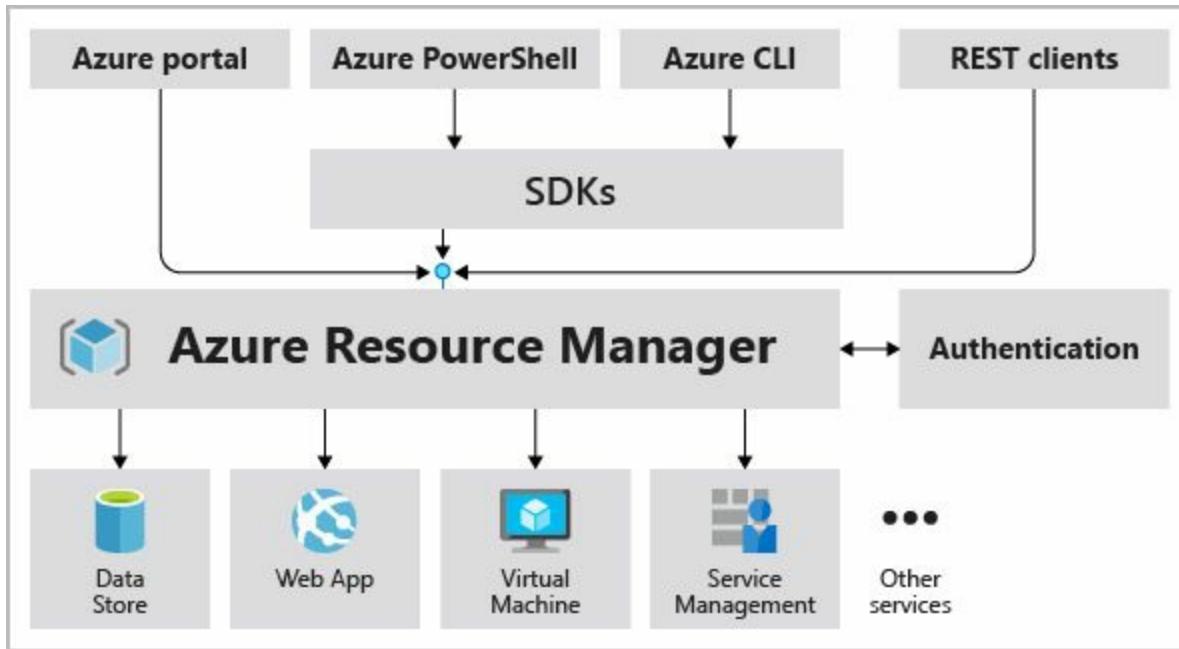
Role-based access control provides fine grained access management for your Azure resources, allowing you to grant users the specific rights they need to perform their jobs.

IT personnel can manage settings, developers can have read-only access, and administrators can have complete control all at the same time.

You can even prevent resources from being deleted accidentally - by enabling resource locks, you can block the ability to delete a resource or prevent changes to it by marking it as read-only.

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

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



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

4.3.3 The benefits of using Resource Manager

With Resource Manager, you can:

- Manage your infrastructure through declarative templates rather than scripts. A Resource Manager template is a JSON file that defines what you want to deploy to Azure.
- Deploy, manage, and monitor all the resources for your solution as a group, rather than handling these resources individually.
- Redeploy your solution throughout the development life cycle and have confidence your resources are deployed in a consistent state.
- Define the dependencies between resources so they're deployed in the correct order.
- Apply access control to all services because RBAC is natively integrated into the management platform.
- Apply tags to resources to logically organize all the resources in your

subscription.

- Clarify your organization's billing by viewing costs for a group of resources that share the same tag.

4.4 Azure regions, availability zones, and region pairs

In the previous unit, you learned about Azure resources and resource groups. Resources are created in regions, which are different geographical locations around the globe that contain Azure datacenters.

Azure is made up of data centers located around the globe. When you use a service or create a resource such as a SQL database or virtual machine (VM), you're using physical equipment in one or more of these locations. These specific data centers aren't exposed to users directly. Instead, Azure organizes them into regions. As you'll see later in this unit, some of these regions offer availability zones, which are different Azure datacenters within that region.

All right, so now it's time to get into the second major section of the exam that describes core Azure services. For the first time in this course and in the exam, obviously, we're going to be talking about the actual Azure services that exist. Our goal with this section is to learn about these services, understand their meaning, and therefore be able to answer questions about what they are and what they're good for and what they're not good for.

The two key elements on Azure, one has to do with core Azure architectural components and the other has to do with core resources.

So the first section being the elements of a set of architectural diagrams, which could be regions and subscriptions and resource manager. And then the second half of this being the actual resources that are used to build us a solution. So let's talk about that first section, first, the core Azure architectural components. The first and one of the most important concepts that you have to understand is the concepts of Azure regions. So what Microsoft has done is they've broken up the map, broken up the world into.

Now it's over 60 regions. So when you want to deploy a resource, let's say you want to deploy a virtual machine for almost every resource, you have to choose a region. And so these are the geographical locations in which those servers exist. Let's have a look at the map. And this map might even be out of date by the time that you're seeing this. But here's basically a snapshot in time of the 60 plus regions of the world.

Now, I should say that not every region is available to everyone. So we talked in the last section of the course about the public cloud and the private cloud.

We haven't yet talked about government services. Those are a version of private cloud. But we can see here we've got many of them in the United States; there is also one in Brazil.

The Western European regions have been blossoming. I can just remember a few years ago, there were only two or four. And now there are at least a dozen regions in the Western Europe. We've got South Africa coming on board, U.A.E, you know, Middle East, India, Israel is a new region that's been announced by a lot of Asian regions.

Now, the reason why when you go into Azure, you're not going to have 60 regions to choose from is that some of these regions do have certain restrictions on them. So, for instance, you can't just create a resource in China because the Chinese version of Azure is run by a Chinese company. You need to have a specific agreement with them. And so China is its own region, even though it's on the map, it's not available to the general public without a specific agreement. Then you're going to have regions such as the Department of Defense and the U.S. government regions in the United States. Obviously, you're not an employee of the U.S. government or if you're not an employee of the U.S. government, you're not going to have access to that. Conversely, if you are an employee of the U.S. government, you only have access to the U.S. government approved regions. And so there's lots of these little rules here and there. Believe in India, you can only deploy to certain regions if you are registered in India, things like that. So you'll see this map is changing every few months to introduce a new one. The next related concept to Regions is the concept that regions have pairs, so it's not just a flat map where you have the 60 regions and they're all identical to each other.

What Microsoft has done is they've taken regions and treated them as a pair. And so if you have some data that exists in one region, the paired region makes the most sense in terms of the backup that's got the fastest, lowest latency data connection between the paired regions. Microsoft keeps that in mind. When they're doing their deployments, they'll deploy to one region, but not the other, and make sure that the pair isn't as affected. And worst case,

disaster, where multiple regions go down, they're going to pick one of the regions to bring up first. And they're sort of priorities that go into it. You can go online and find out if you're, you know, into creating actual resources and you need to know all the pairs. You can go and find the full list. But here's just a sampling of the list where obviously the two regions in Canada, central and east, are a pair.

So if you deploy to Canada Central, the most logical place for you to put your backups would be in Canada East, because that's the highest speed, lowest latency prioritization in terms of bringing them back online. North Europe and West Europe per region, East U.S. and West USA, a region we should point out that Brazil only had one region. And so Brazil is one of those unique places where there is no other Brazilian region. So it's paired with the south central U.S., which means that the north central U.S. is also paired with South Central Asia. So South Korea has two paired relationships. You don't have to memorize the pairs for the exam, but you do need to understand it is beneficial to put your backups into the paired region compared to another region.

4.4.1 Azure regions

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

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

Important :

Some services or VM features are only available in certain regions, such as specific VM sizes or storage types. There are also some global Azure services that don't require you to select a particular region, such as Azure Active Directory, Azure Traffic Manager, and Azure DNS.

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

of June 2020.



Global map of available Azure regions as of June 2020.

Why are regions important?

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

Special Azure regions

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

US DoD Central, US Gov Virginia, US Gov Iowa and more: These regions are physical and logical network-isolated instances of Azure for U.S. government agencies and partners. These data centers are operated by screened U.S. personnel 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 doesn't directly maintain the data centers.

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

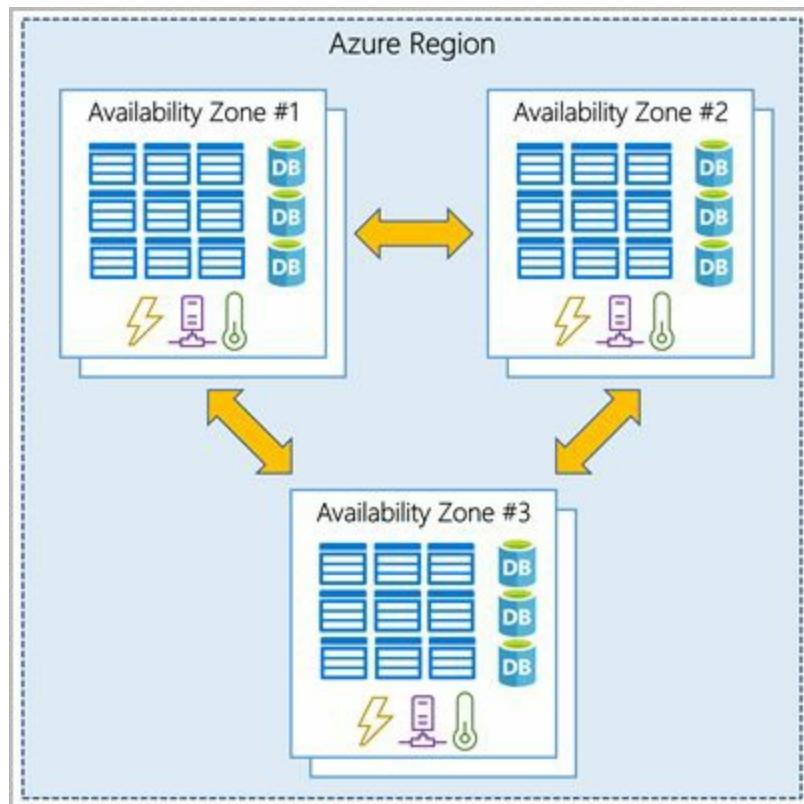
4.4.2 Azure availability zones

You want to ensure your services and data are redundant so you can protect your information in case of failure. When you host your infrastructure, setting up your own redundancy requires that you create duplicate hardware environments. Azure can help make your app highly available through availability zones.

What is an availability zone?

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

Diagram showing three datacenters connected within a single Azure region to represent an availability zone.



Supported regions

Not every region has support for availability zones. For an updated list, see Regions that support availability zones in Azure.

Use 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, VMs, managed disks, IP addresses).

Zone-redundant services: The platform replicates automatically across zones (for example, zone-redundant storage, SQL Database).

The global map of Azure regions sort of shows the concept pretty clearly where you have a region. So let's take, for example, the Canada east region. And inside that region you have three availability zones. And if you choose to, you can pick the individual availability zones within the region to deploy your resources to.

Now, they're called availability zones, primarily because when you use them, you're actually increasing the availability of your application in your solution. The reason for this is because each availability zone is physically separated from each other, running on its own power on its own heating and cooling and running on its own network. And so if there's a power outage or some breakdown, it's likely to affect one availability zone, but not the other two. So if you think about the bad things that can happen to a network, now we're drilling down to the individual building level.

Typically, availability zones are buildings on the same property, perhaps, but physically separated and running on their own individual power, Internet and cooling systems. So if you deploy your application to availability Zone one and availability zone two, even if it's in the same region, then you're increasing the likelihood of your application setting up. If only one of those

availability zones has an issue, if you don't choose to go the availability zone route, then

Azure region pairs

Availability zones are created by using one or more datacenters. There's a minimum of three zones within a single region. It's possible that a large disaster could cause an outage big enough to affect even two datacenters. That's why Azure also creates region pairs.

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

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

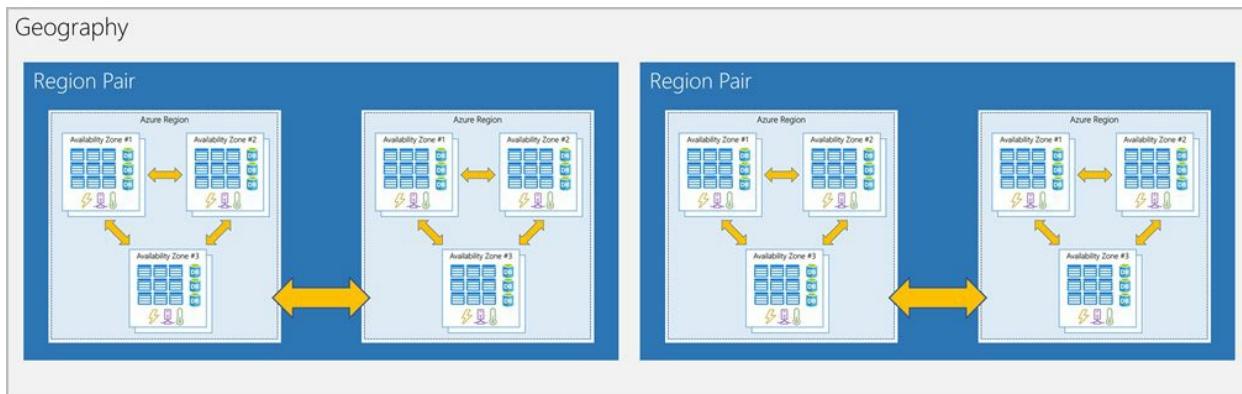


Diagram showing the relationship between geography, region pair, region, and datacenter. The geography box contains two region pairs. Each region pair contains two Azure regions. Each region contains three availability zones.

Because 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 by using region pairs.

Additional advantages of region pairs:

- If an extensive Azure outage occurs, one region out of every pair is prioritized to make sure at least one is restored as quickly 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.

4.5 Knowledge Check

1. Which of the following can be used to manage governance across multiple Azure subscriptions?
 - A. Azure initiatives
 - B. Management groups
 - C. Resource groups
2. Which of the following is a logical unit of Azure services that links to an Azure account?
 - A. Azure subscription
 - B. Management group
 - C. Resource group
3. Which of the following features doesn't apply to resource groups?
 - A. Resources can be in only one resource group.
 - B. Role-based access control can be applied to the resource group.
 - C. Resource groups can be nested.
4. Which of the following statements is a valid statement about an Azure subscription?
 - A. Using Azure doesn't require a subscription.
 - B. An Azure subscription is a logical unit of Azure services.
 - C. You can't have more than one subscription.

Answers

1. **B.** Management groups facilitate the hierarchical ordering of Azure resources into collections, at a level of scope above subscriptions. Distinct governance conditions can be applied to each management group, with Azure Policy and Azure role-based access controls, to manage Azure subscriptions effectively. The resources and subscriptions assigned to a management group automatically inherit the conditions applied to the management group.
2. **A.** An Azure subscription is a logical unit of Azure services that links to an Azure account.

3. **C.** Resource groups cannot be nested
4. **B.** A subscription is a set of Azure services bundled together for tracking and billing purposes.

4.6 Summary

In this Chapter, you learned the concepts and terminology for several of the core Azure architecture components. Now you have the basic level of understanding for Azure architecture that you'll need to make iCertify Traders successful as it migrates to the cloud.

You learned how to describe the benefits and usage of:

- Azure subscriptions and management groups.
- Azure resources, resource groups, and Azure Resource Manager.
- Azure regions, region pairs, and availability zones.

Term or concept	Description
Region	A set of datacenters deployed within a latency-defined perimeter and connected through a dedicated regional low-latency network.
Geography	An area of the world containing at least one Azure region. Geographies define a discrete market that preserves data residency and compliance boundaries. Geographies allow customers with specific data-residency and compliance needs to keep their data and applications close. Geographies are fault-tolerant to withstand complete region failure through their connection to our dedicated high-capacity networking infrastructure.
Availability Zone	Unique physical locations within a region. Each zone is made up of one or more datacenters equipped with

	independent power, cooling, and networking.
Recommended region	A region that provides the broadest range of service capabilities and is designed to support Availability Zones now, or in the future. These are designated in the Azure portal as Recommended.
Alternate (other) region	A region that extends Azure's footprint within a data residency boundary where a recommended region also exists. Alternate regions help to optimize latency and provide a second region for disaster recovery needs. They are not designed to support Availability Zones (although Azure conducts regular assessment of these regions to determine if they should become recommended regions). These are designated in the Azure portal as Other.
Foundational service	A core Azure service that is available in all regions when the region is generally available.
Mainstream service	An Azure service that is available in all recommended regions within 90 days of the region general availability or demand-driven availability in alternate regions.
Specialized service	An Azure service that is demand-driven availability across regions backed by customized/specialized hardware.
Regional service	An Azure service that is deployed regionally and enables the customer to specify the region into which the service will be deployed.

Non-regional service	An Azure service for which there is no dependency on a specific Azure region. Non-regional services are deployed to two or more regions and if there is a regional failure, the instance of the service in another region continues servicing customers.
-----------------------------	--

Chapter 5 Azure Core Services

5.1 Learning Objectives

At the end of this chapter, you will be able to

- Understand the breadth of services available in Azure including compute, network, storage, and database
- Identify virtualization services such as Azure Virtual Machines, Azure Container Instances, Azure Kubernetes Service, and Windows Virtual Desktop
- Compare Azure's database services such as Azure Cosmos DB, Azure SQL, Azure Database for MySQL, Azure Database for PostgreSQL, and Azure's big data and analysis services
- Examine Azure networking resources such as Virtual Networks, VPN Gateways, and Azure ExpressRoute
- Summarize Azure storage services such as Azure Blob Storage, Azure Disk Storage, and Azure File Storage
- Review what are the key core services available in Azure
- Different Compute services offered. Ex : Virtual Machines, Kubernetes
- Different Networking services offered. Ex : VPN, Firewall, DNS
- Different Storage services offered. Ex : Blob, File, Queue, Table
- Different Mobile services offered. Ex : mobile back-end services for iOS, Android, and Windows apps
- Different Database services offered. Ex : Cosmos, Postgres, Synapse
- Different Web services offered.
- Different Internet of Things (IoT) services offered.
- Different Big data services offered.
- Different AI services offered.
- Different DevOps services offered.

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

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

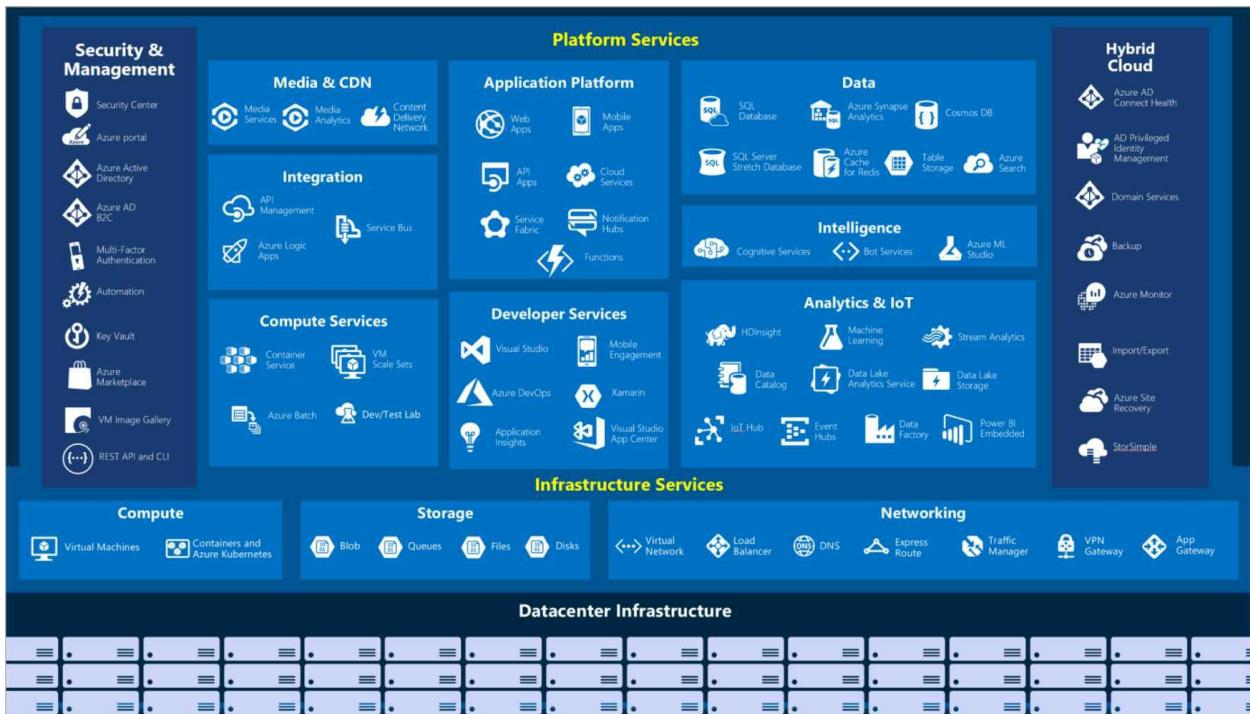
5.2 Azure services

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

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

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

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



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

- Compute
- Networking

- Storage
- Mobile
- Databases
- Web
- Internet of Things (IoT)
- Big data
- AI
- DevOps

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



Azure is Microsoft's cloud computing platform with an ever-expanding set of services to help you build solutions to meet your business goals as these supports infrastructure platform and software as a service computing which services such as virtual machines running in the cloud website and database hosting and advanced computing services like artificial intelligence machine learning and IOT. Most of these services are pay-as-you-go, so you only pay for the computing time that you use. If your business needs complete control over your computing environment as the allows you to host virtual machines in the cloud you can create virtual machines from scratch upload your own virtual hard drive to choose from and every of templates that as their provides

as the ultimate provide cloud base storage which allows you to store your application, back-up and scale safely and securely provided scalable hosting platform where developers can create web-based applications using popular development frameworks you can easily deploy operate and scale apps in a fully managed environment with as your functions you can create event-driven service applications with no coding required. Fully manage to relational and in memory databases spanning proprietary and open-source engines and microsoft's course most db provide support for several popular analyst you well api as artificial intelligence and machine learning services empowered developers and data scientists with a wide range of productive expediency is for building training and deploying machine learning models fast up as regional data-centers allow you to distribute your applications globally so you can locate your data and apps where they're needed most thereby improving your application performance feel customize the as you. Azure lets you create and control all your services and resources from a single easy-to-use web-based interface. Microsoft offers a wide array of cloud computing services where infrastructure management, scalability, availability and security are handled for-you saving you time and money.

5.2.1 Compute

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

Service name	Service function
Azure Virtual Machines	Windows or Linux virtual machines (VMs) hosted in Azure.
Azure Virtual Machine Scale Sets	Scaling for Windows or Linux VMs hosted in Azure.
Azure Kubernetes Service	Cluster management for VMs that run containerized services.
Azure Service Fabric	Distributed systems platform that runs in Azure or on-premises.
Azure Batch	Managed service for parallel and high-performance computing applications.
Azure Container Instances	Containerized apps run on Azure without provisioning servers or VMs.
Azure Functions	An event-driven, serverless computer service.

So let's move on to talk about some of the resources within Azure, so this is talking about the core resources with Azure. What we're generally talking about can be categorized into these five categories.

We can talk about compute services, all of the ways that Azure can execute programs, websites, applications, networking services, which is the way that applications can communicate with each other and the security around that storage services, which is files and data that is stored within a storage account type format. When we get into database services, which is like a storage account, except it's organized. You can have tables, columns, collections, et cetera. And finally, there is the Azure marketplace where you go to find a lot

of these services, including some that are not created by Microsoft.

We're going to talk about the following types of services, Virtual Machine, Web app, container instances, Kubernetes and added to the requirements of this exam are Windows virtual desktop. That's not necessarily a computer service, although you are storing it's a virtual desktop.

So the VM or Virtual Machine is sort of the poster child of IaaS. This is very similar. It looks, acts and behaves just like a computer that you might have at your desk, at your feet, in your server room, but it operates in the cloud. It's also virtualized, which is the virtual part of Virtual Machine, which means that to you it looks and acts like a real server. But in reality it is one server that's been divided up into many slices and you've got yourself and other customers who are taking a slice. Microsoft Azure supports both Windows and Linux operating systems.

Actually, we have a rumor that Linux is actually more popular in Microsoft Azure. So don't feel like it's a Windows only world out there. Microsoft Azure supports Linux. Microsoft loves Linux, apparently, and it is actually probably the most popular operating system running within the cloud. Like I said, it is a Virtual Machine. It looks and acts like a physical machine, but it's really just a slice. Instead of having the whole pie, you just have a slice of pie. Sometimes I like to think of it like an apartment building. When you're inside your apartment with the door locked, you think it's your home, but you're actually sharing it with your neighbors. Your upstairs neighbors are downstairs neighbors. It's that the building has been subdivided into several secure locations, but you do have full control over it.

So you can install what you like, you can modify the registry. It's got a hard disk, you can save files to, etc. So it looks and acts and in almost every way, almost every way behaves like a physical machine. There's some low level things that you don't have control over. But other than that, it's pretty much like a server. We should say when you go to Azure to create a VM, you do have a buffet selection of over 200 to choose from and you get to choose based on a number of factors, how many CPU cause the CPU speed, the amount of RAM SaaS you get, how much disk space IOPS, which stands for input output operations per second, etc.

Sometimes you'll find there are instanced families and these are often given a

letter and they are either memory optimized or storage optimized or CPU optimized. And so depending on what your particular application, you may want more CPU and not as much memory or vice versa. And there's lots of those combinations to choose from. Now, moving up the stack, we're just talking about infrastructure as a service. The ASP services our platform as a service. Basically, you take your code, packaging it up, giving it to Azure and Azure will run it.

Now, you do get to choose plan types. And so there's the basic and standard and premium plans. And you do get to choose the level standard ones, tender to tender three, etc. But you're not actually choosing CPU cores and memory. And those are not the decisions that you're making. You're choosing it from a simpler selection. And Microsoft does throw in a lot of additional benefits to being Azure services, including deployment slots and the ability to add instances very easily, etc.

So they make it a very more feature filled experience. But you do lose direct access to the system. You can't change the registry settings. You can look at some log files, but you generally can't go and access the hardware the same way you would with a Virtual Machine.

Another level of virtualization is the container paradigm; now this has become very popular in recent years. Google created a thing called Kubernetes that became open standard Kubernetes services.

And so you create a docker image and deploy that and it basically becomes easy to deploy. And so containers are very popular and Azure you get so many different options for containers. Two of them that we'll talk about covered by this exam are the Azure container instance and the Azure Kubernetes service. But Web apps also have container service barrackers, containers. There are a few other ways of running containers. You can run a container in a Virtual Machine if you wanted to. So these are the fastest, easiest ways to deploy code and you do everything on your desktop, package up the image and then deploy it.

Finally, a new addition to the exam is the Windows virtual desktop. This is just like having a Windows machine, but all your files are stored in the cloud and so you can theoretically log in from any machine and then your desktop. Is there everything, your settings are there, your desktop is there, your files

are there. So this is a relatively new paradigm of being able to not need everyone to have their own version of Windows running locally. But actually it's all set up from a cloud environment. You can also then use your cell phone, mobile phone to access it because there's iOS and Android apps or any Web browser to get through your files and to get to your emails and get whatever it is that's on your computer.

5.2.2 Networking

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

Here are some examples of networking services in Azure.

Service name	Service function
Azure Virtual Network	Connects VMs to incoming virtual private network (VPN) connections.
Azure Load Balancer	Balances inbound and outbound connections to applications or service endpoints.
Azure Application Gateway	Optimizes app server farm delivery while increasing application security.
Azure VPN Gateway	Accesses Azure Virtual Networks through high-performance VPN gateways.
Azure DNS	Provides ultra-fast DNS responses and ultra-high domain availability.
Azure Content Delivery Network	Delivers high-bandwidth content to customers globally.
Azure DDoS Protection	Protects Azure-hosted applications from distributed denial of service (DDOS) attacks.
Azure Traffic Manager	Distributes network traffic across Azure regions worldwide.

Azure ExpressRoute	Connects to Azure over high-bandwidth dedicated secure connections.
Azure Network Watcher	Monitors and diagnoses network issues by using scenario-based analysis.
Azure Firewall	Implements a high-security, high-availability firewall with unlimited scalability.
Azure Virtual WAN	Creates a unified wide area network (WAN) that connects local and remote sites.

Now, I want to further break down the concept of networking to four main categories so all of the networking services can be subdivided into one of these four categories. You have connectivity services. That is how applications connect to each other and communicate to each other protection services. This could be ensuring that only authorized people have the ability to communicate to your server, protecting attacks and denial of services and things like that. Delivery services which help you to deliver your resources and your services to the end user without another server or actually the general public. And finally, any kind of monitoring that you need to do, we're going to get into details of each of these four types of networking services.

So on screen are three examples of connectivity services. So the Virtual Network is basically the most basic level of networking. When you create a Virtual Machine, it goes onto a virtual network. It is emulating a physical network that you might have in your environment. And so I think we'll do a demonstration after the section of Virtual Machine and Virtual Network. And so you have to look at it like, you know, when you're creating a network within Azure, it's virtual. Microsoft is not actually unplugging and plugging in cables on your request. Their network already exists is called the Microsoft Global Network. So a virtual network is really just some settings in the database. And so it's pretty, quite clever, actually, if you think about it, that you're able to create all of these virtual machines and applications and apps and they know who they can communicate to and who they can't simply based on the configuration.

Now, the VPN is a virtual private network. You might be familiar with a VPN because if you are working from home, you have to use a VPN to

connect to your office in order to get access to your files that are stored on a server. And so the same type of definition here. Use a VPN when you need to connect to networks together securely so you can have two networks within Azure that are connected by VPN. You can have your office location connected to Azure by VPN and in a point to site VPN, you could even connect your desktop computer at home, your laptop or even your mobile device to Azure. Using a VPN that's encrypted can't be spied upon and you basically get access to the resources of that remote network. Our express route is a high speed private connection. It acts similar to a VPN, but you basically have to purchase it in advance. There's some hardware that gets installed and it doesn't run on the public Internet. And so those are some examples of connectivity services. Next up, we'll talk about the protection aspect of networking. You may have heard of the denial of service attack, and that is when you have thousands and hundreds of thousands of computers around the world that are directing malicious traffic at a destination with the attempt to overwhelm a much like if you go to a store and there are already 2000 people inside the store, you can't buy anything. You can't get to the checkout. It's just jammed. So the same concept with denial of service attack. And Microsoft does include a basic level of DOS protection. You can purchase an advanced level of protection for your applications. A firewall is a device that protects a network. You can set up some firewall rules and allow certain traffic and block certain traffic coming through. Network security group is a very basic type of firewall, it's what's called an access control list or ACL, and you got the rules, but they're just static rules based on IP address. There's no intelligence to them. It's just like having a list at a club. And is your name on the list? And if your names are on the list you get in, if your name isn't on the list, you don't get in. There's not any intelligence to it. That's a network security group. And finally, even the Azure private linked service is a form of protection for a network.

So these are some examples of that. Now, some of these delivery services, I think I'll point them out to you. I do want to point out that you're not going to be asked about load balancers or application gateways on the exam, but we're talking about networking and we're going to talk about three quarters of networking and we'll talk about the fourth quarter. And so the fourth quarter in this case are the delivery services. So a load balancer and an application

gateway basically allow traffic coming in to be distributed evenly to multiple servers behind. And this is how you can go to Amazon.com or Microsoft dot com and get a response. It's not a single server that is listening to traffic coming through that domain.

There are thousands of servers typically located around the world that can respond to Microsoft dotcom and they use load balancers, among other things, to make sure that you get the Web page that you're requesting.

Application Gateway is similar to a load balancer. It has a firewall. If you want to enable that content delivery network, you may have heard of this. It is a way of storing static files like images, videos, JavaScript files, CSS files closer to the end users so that the end users get their website loading a lot faster. And then the front door service is relatively new. It combines some of these things and has a load balancer, CDN and a firewall all in one. And the four types of networking service are the monitoring services. And so, again, it's important from your operations point of view that you'll be able to watch traffic traveling over your Virtual Network and make adjustments based on that log stuff, audit stuff, you know.

So these are the tools network, express route monitor and Azure matter that can be used to watch traffic coming in over the network. So those are the networking services in Azure.

5.2.3 Storage

Azure provides four main types of storage services.

Service name	Service function
Azure Blob storage	Storage service for very large objects, such as video files or bitmaps.
Azure File storage	File shares that can be accessed and managed like a file server.
Azure Queue storage	A data store for queuing and reliably delivering messages between applications.
Azure Table storage	Table storage is a service that stores non-relational structured data (also known as

structured NoSQL data) in the cloud, providing a key/attribute store with a schemaless design..

These services all share several common characteristics:

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

All right, so we've talked about computers and we talked about networking. Now it's time to talk about storage. Storage is typically considered where you're storing files into Azure. And we're not necessarily talking about database storage at the current time. We're talking about file storage. Now, I've always called stories one of the three foundational elements of any cloud computing right, you've got compute and networking and you can't have compute without some type of storage.

Now, one of those foundational elements of storage within Azure is called the Azure storage account. When you go to create an Azure storage account, you're given the choice of three different kinds. The one we're going to choose almost every time is called General-Purpose V2 or V two. General Purpose V two. It's been around for a while, but the other two that are available, General-Purpose V one and Blob Storage, are more like legacy storage accounts that are used if you already have them and you just need more of what you already have.

If you're starting out for the first time, you generally get to choose GPB (General purpose Blob storage) when you create a general purpose to be a storage account and we'll do that shortly, you're going to see that there are four types of files that can be stored within that. Now, one is called container storage or blob storage. The other would be tables, the other would be Kyuss, and the fourth would be file storage. Now you can also configure the same Azure storage account as what it's called a data lake storage. As the name implies, the data is meant to be huge. And this is where you're going to store petabytes and exabytes of data that you're using in a really large data processing operation. But you have to specifically configure your storage

account for that. Now, at Azure, storage account is typically the cheapest form of storage you're going to get. It is an unmanaged storage account like this is pay per gigabyte. And last time I looked at the prices, it's about one point eight cents per gigabyte and you pay per gigabyte. So if you're only storing five gigabytes of data in a storage account, then you're only costing you about 10 cents a month. That is extremely cheap storage. Now, that's not the only options when you're setting up a storage account or we are going to find out about access tiers. And I'll show you that when we do the demo, basically, you're able to store files for, I think, hot access tiers, basically the default. It's what you think about when you're storing files. Cool access tier is meant to save you money on the storage fees and costs you more money to do reads and writes to it. So you pretty much want to put the main files that you need for real time access in the hot storage. If you ever need files where it's kind of rare for you to access that, you put it in cold storage and archive storage is just as it sounds. It really is more of a cold storage where it actually saves you a lot of money in terms of storing files, but then it costs you ten times as much to access the file. And with archive storage, you actually have to IIS unthaw the file before you can access it. So there's probably like a one hour process to get a file out of the archive. So think of it almost like tape backup, although I don't think Microsoft's using tapes. But you have to have that mentality of you can't get access to files in the archive right away. So let's say you have a regulatory requirement to keep these files around, but you don't really expect to ever need them in an emergency like a backup from a server from six months ago. So you can put that in archives storage, save a ton of money on the storage fees, and then you can get that file back. But it does take, like I said, an hour or more. Now, there's also the performance tier. You're basically going to be able to pay extra to get a faster read and write access to a file that's called the premium tier. The location of the files. We talked about Azure being global. And so you can store files in all of these regions, the 60 plus regions of the world.

So the location is going to have different prices. If you want to store a file in South America, you're going to pay a little bit more. If you want to store it in the East US region, you'll pay a little less. And so the location of the file does impact the pricing.

You do get to choose what's called a replication or redundancy. When setting

this up, then basically you can have a backup of the file in another region by default.

Microsoft's going to keep three copies of every file that you give it, and that's the lowest level. But you can then make that globally redundant and they'll keep six copies, three in each of two regions.

And when you're signing up for storage in general, you can basically set up failover so that if one region was to go down, then your files are available in another region and then you can just switch everything over to the other region in case of emergency break glass option. That was a lot of blob storage stuff. There is a virtual distortion. This is called a managed disk. You're going to pay for a reservation. So instead of paying per gigabyte, you get a tier, maybe you get a terabyte of storage and that costs you a certain amount every month. And whether you use all of it or you use none of it, you're paying the same. So this is called managed storage and it's really optimized to become the hard disk underneath the Virtual Machine. So it's a randomized access to files.

5.2.4 Mobile

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

Other features of this service include:

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

5.2.5 Databases

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

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

So the last of the major services we'll talk about in this section is database services. Now, the database services within Microsoft Azure are Cosmos DB, Azure, SQL Database, MySQL and PostgreSQL. These are managed databases and SQL managed instant. So those are the five major database technologies within Azure. Pretty much any application that is doing

something has to have some type of database. Either it's working from a storage account or it's working from a database. So first up, we'll talk about Cosmos DB; Cosmos DB is what is called NOSQL storage. That doesn't mean that there's no skill involved, it is only not SQL, what it refers to Cosmos DB is designed to be extremely fast. And so Microsoft promises sub ten millisecond response times. That's extremely fast. So in this day and age, when you have mobile games and, you know, small uses of data, then Cosmos DB could be a good solution for that. But for big enterprise applications when you're dealing with your customer, CRM and large applications this might not be the best solution. It's great for small pieces of data that need to be extremely fast. And that could be a mobile game, would be an ideal situation for that. Also, it's very global so you can create a database and have that easily replicated around the world. And so your application, no matter where it is, can refer to the closest database and have some assurance that the data is up to date. You also get a lot of options for the way the data is stored inside the database. That's called multimodal. So unlike SQL Server, which is a traditional Microsoft database, a relational database within Cosmos DB, you have many different open source applications like Cassandre Mango and ETCD and other things. Now, the equivalent to Cosmos DB is Azure SQL database, this is a SQL Server engine running in the cloud. It is relational, it is basically a database managed by Azure. And so you're not managing CPU's and doing very low level, you know, the location of files and things like that. It's also easy to replicate in the different regions, easy to scale. If you need more power, you'll pay for more power. But to be able to switch from one plant to the other is pretty straightforward. And of course it runs on the SQL Server engine. So it's designed to be migrated from your existing application. So if you have SQL Server running on your premises, you can migrate to SQL Server running in a virtual machine, but you may want to consider trying it in a SQL database, have that flexibility and not have difficult migration.

My SQL is a popular open source database not originally designed by Microsoft, but this is supported by Microsoft Version. A website like WordPress typically uses MySQL as its database. Again, if you're already using my SQL in your website, migrating to a managed version of my SQL might be pretty straightforward. Next up is PostgreSQL, another open source

database? This one is more for the bigger databases that require clusters and more complex server setups. And so if you use this open source database in any of your apps, then migrating to the Azure database is a managed version that might be simpler. You can maintain your existing code. Your existing toolset just pointed to a different URL with a lot of benefits. And lastly, there's a type of database called a SQL managed instance. This is even more compatible with SQL Server than Azure SQL database, almost guaranteed to have a must know code changes. It is managed by Azure. And they will also keep the application up to date with the latest patches for SQL Server.

5.2.6 Web

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

5.2.7 IoT

People are able to access more information than ever before. Personal digital assistants led to smartphones, and now there are smart watches, smart thermostats, and even smart refrigerators. Personal computers used to be the norm. Now the internet allows any item that's online-capable to access valuable information. This ability for devices to garner and then relay information for data analysis is referred to as IoT.

Many services can assist and drive end-to-end solutions for IoT on Azure.

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

5.2.8 Big data

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

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

Service name	Description
Azure Synapse Analytics	Run analytics at a massive scale by using a cloud-based enterprise data warehouse that takes advantage of massively parallel processing to run complex queries quickly across petabytes of data.
Azure HDInsight	Process massive amounts of data with managed clusters of Hadoop clusters in the cloud.
Azure Databricks	Integrate this collaborative Apache Spark-based analytics service with other big data services in Azure.

5.2.9 Artificial Intelligence

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

Forecasts or predictions from machine learning can make apps and devices smarter. For example, when you shop online, machine learning helps

recommend other products you might like based on what you've purchased. Or when your credit card is swiped, machine learning compares the transaction to a database of transactions and helps detect fraud. And when your robot vacuum cleaner vacuums a room, machine learning helps it decide whether the job is done.

Here are some of the most common AI and machine learning service types in Azure.

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

A closely related set of products are the cognitive services. You can use these prebuilt APIs in your applications to solve complex problems.

Service name	Description
Vision	Use image-processing algorithms to smartly identify, caption, index, and moderate your pictures and videos.
Speech	Convert spoken audio into text, use voice for verification, or add speaker recognition to your app.
Knowledge mapping	Map complex information and data to solve tasks such as intelligent recommendations and semantic search.

Bing Search	Add Bing Search APIs to your apps and harness the ability to comb billions of web pages, images, videos, and news with a single API call.
Natural Language processing	Allow your apps to process natural language with prebuilt scripts, evaluate sentiment, and learn how to recognize what users want.

5.2.10 DevOps

DevOps brings together people, processes, and technology by automating software delivery to provide continuous value to your users. With Azure DevOps, you can 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 backlog items for tracking, automate infrastructure deployment, and integrate a range of third-party tools and services such as Jenkins and Chef. All of these functions and many more are closely integrated with Azure to allow for consistent, repeatable deployments for your applications to provide streamlined build and release processes.

Service name	Description
Azure DevOps	Use development collaboration tools such as high-performance pipelines, free private Git repositories, configurable Kanban boards, and extensive automated and cloud-based load testing. Formerly known as Visual Studio Team Services.
Azure DevTest Labs	Quickly create on-demand Windows and Linux environments to test or demo applications directly from deployment pipelines.

1. Which of the following choices would not be used to automate a CI/CD process?

- A. Azure Pipelines
 - B. GitHub Actions
 - C. Azure Boards
2. Which service could help you manage the VMs that your developers and testers need to ensure that your new app works across various operating systems?
- A. Azure DevTest Labs
 - B. Azure Test Labs
 - C. Azure Repos
3. Which service lacks features to assign individual developers tasks to work on?
- A. Azure Boards
 - B. GitHub
 - C. Azure Pipelines

Answers :

- 1. C. Azure Boards is an agile project-management tool. It would not be used to automate a CI/CD process.
- 2. B. Azure DevTest Labs is used to manage VMs for testing, including configuration, provisioning, and automatic de-provisioning.
- 3. C. Azure Pipelines is a CI/CD tool for building an automated toolchain. It lacks features to assign tasks for individual developers to work on. However, it can automate other tools to assign tasks to users.

5.4 Azure Database Services

5.4.1 Azure Cosmos DB

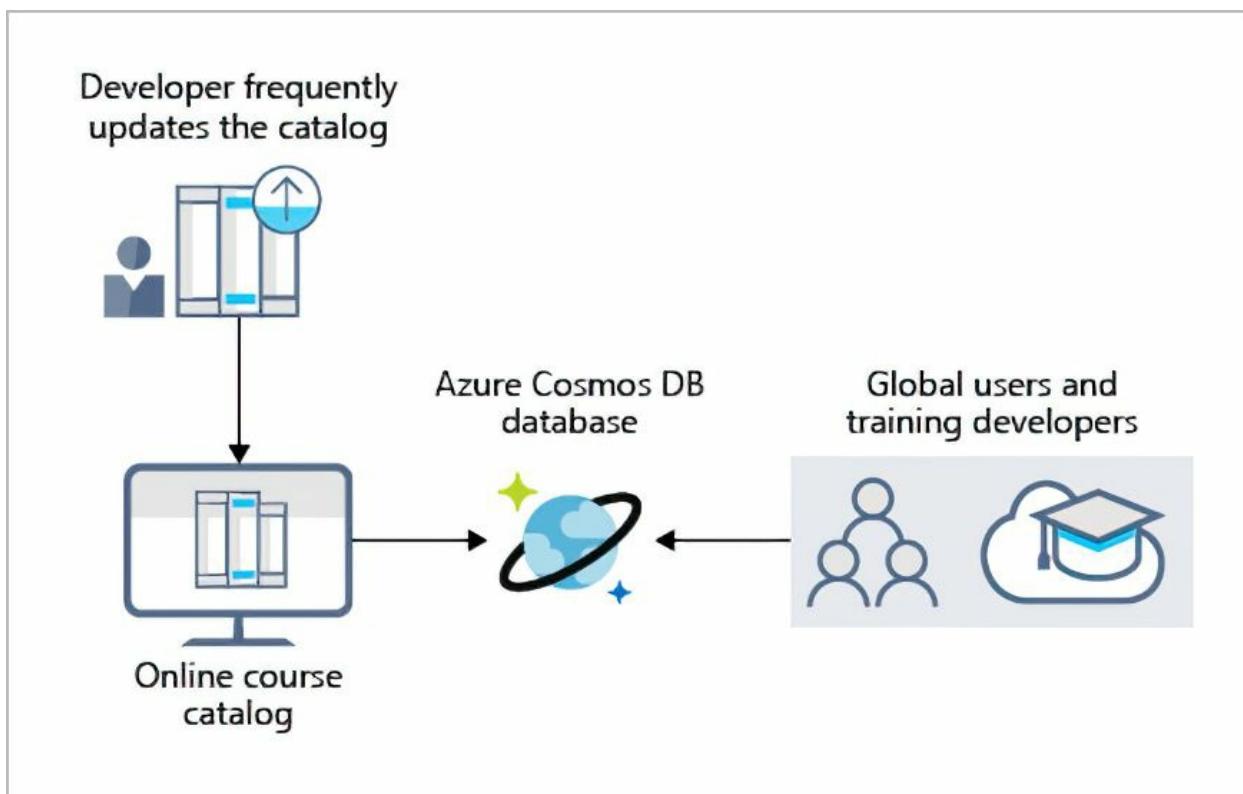
Over the years, iCertify Traders has acquired several smaller companies. Each of these companies had teams of developers who used different database services and various APIs to work with their data. A long-term plan might be to eventually move all of the disparate data to a common database service.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



Azure Cosmos DB is a globally distributed, multi-model database service. You can elastically and independently scale throughput and storage across any number of Azure regions worldwide. You can take advantage of fast, single-digit-millisecond data access by using any one of several popular APIs. Azure Cosmos DB provides comprehensive service level agreements for throughput, latency, availability, and consistency guarantees.

Azure Cosmos DB supports schema-less data, which lets you build highly responsive and "Always On" applications to support constantly changing data. You can use this feature to store data that's updated and maintained by users around the world.

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



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

5.4.2 Azure SQL Database

Azure SQL Database is a relational database based on the latest stable version of the Microsoft SQL Server database engine. SQL Database is a high-performance, reliable, fully managed, and secure database. You can use it to

build data-driven applications and websites in the programming language of your choice, without needing to manage infrastructure.



Features

Azure SQL Database is a platform as a service (PaaS) database engine. It handles most of the database management functions, such as upgrading, patching, backups, and monitoring, without user involvement. SQL Database provides 99.99 percent availability. PaaS capabilities that are built into SQL Database enable you to focus on the domain-specific database administration and optimization activities that are critical for your business. SQL Database is a fully managed service that has built-in high availability, backups, and other common maintenance operations. Microsoft handles all updates to the SQL and operating system code. You don't have to manage the underlying infrastructure.

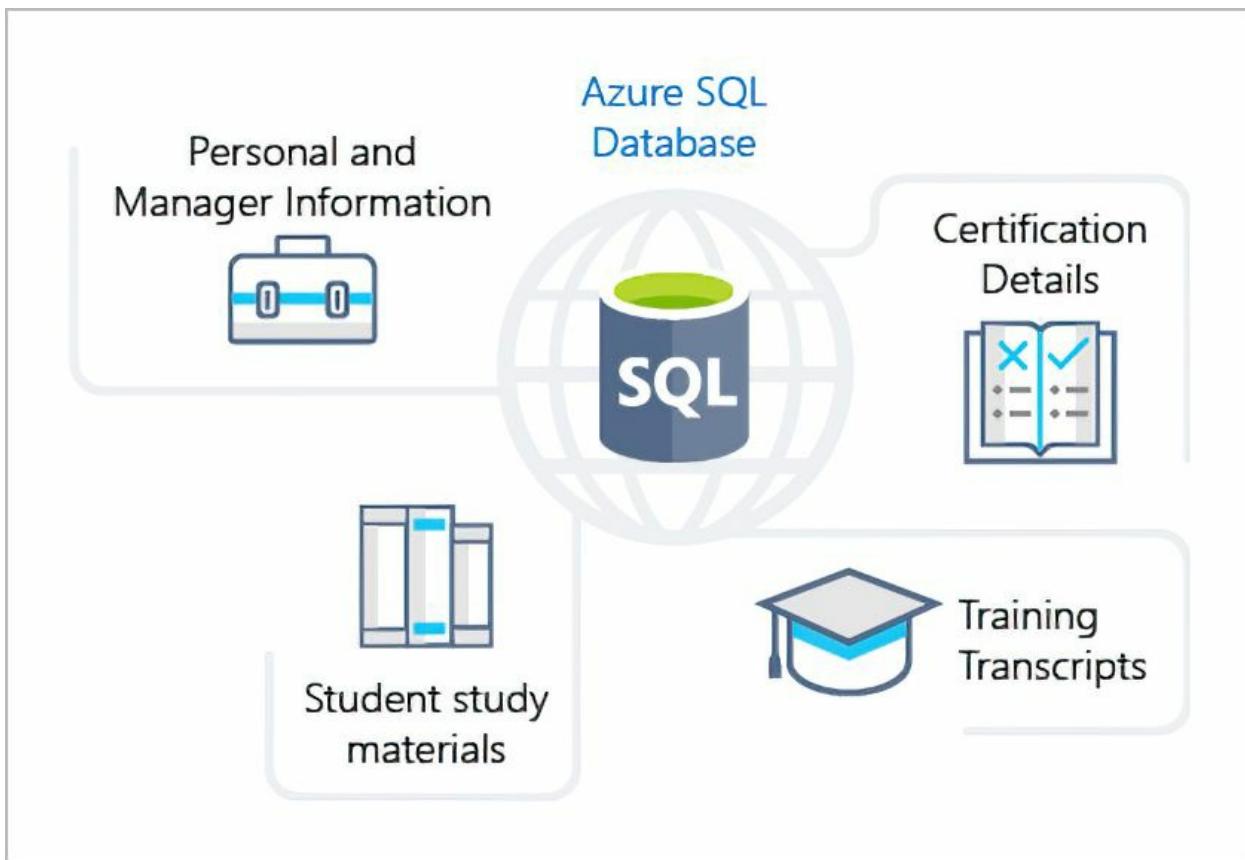
You can create a highly available and high-performance data storage layer for the applications and solutions in Azure. SQL Database can be the right choice for a variety of modern cloud applications because it enables you to process both relational data and non-relational structures, such as graphs,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

You can use advanced query processing features, such as high-performance, in-memory technologies and intelligent query processing. In fact, the newest capabilities of SQL Server are released first to SQL Database, and then to

SQL Server itself. You get the newest SQL Server capabilities, with no overhead for updates or upgrades, tested across millions of databases.

Migration

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



You can migrate your existing SQL Server databases with minimal downtime by using the Azure Database Migration Service. The Microsoft Data Migration Assistant can generate assessment reports that provide recommendations to help guide you through required changes prior to

performing a migration. After you assess and resolve any remediation required, you're ready to begin the migration process. The Azure Database Migration Service performs all of the required steps. You just change the connection string in your apps.

Exercise - Create a SQL database

iCertify Traders has chosen Azure SQL Database for part of its migration. You've been tasked with creating the database. In this exercise, you'll create a SQL database in Azure and then query the data in that database.

Task 1: Create the database

In this task, you create a SQL database based on the AdventureWorksLT sample database.

1. Sign in to the **Azure portal**.
2. Select Create a **resource** > **Databases** > **SQL database**. Fill in the following information.

Setting	Value
On the Basics tab, under Project details section:	
Subscription	Concierge Subscription
Resource group	[sandbox resource group name]
Under Database details section:	
Database name	db1
Server	Select Create new.

3. The New server panel appears. Enter the following information (replace nnnn in the name of the server with letters and digits, such that the name is globally unique).

Setting	Value
Server name	sqlservernnnn (must be unique)

Server admin login	sqluser
Password	Pa\$\$w0rd1234
Location	(US) East US

The screenshot shows the 'Create SQL Database' wizard on the 'Basics' tab. A modal window titled 'New server' is overlaid on the main form. The 'New server' dialog contains fields for 'Server name' (sqloerver4321), 'Server admin login' (sqluser), 'Password', 'Confirm password', and 'Location' (US) East US. The 'OK' button at the bottom of the dialog is highlighted with a red box.

4. Select **OK** when you have finished.
5. Select **Next : Networking**, and configure the following settings (leave defaults for remainder of fields).

Setting	Value
Under Network connectivity section:	
Connectivity method	Public endpoint

Home >

Create SQL Database ...

Microsoft

X

Basics Networking Security Additional settings Tags Review + create

Configure network access and connectivity for your server. The configuration selected below will apply to the selected server 'sqlserver' and all databases it manages. [Learn more](#)

Network connectivity

Choose an option for configuring connectivity to your server via public endpoint or private endpoint. Choosing no access creates with defaults and you can configure connection method after server creation. [Learn more](#)

Connectivity method * ⓘ

- No access
- Public endpoint
- Private endpoint

Firewall rules

Setting 'Allow Azure services and resources to access this server' to Yes allows communications from all resources inside the Azure boundary, that may or may not be part of your subscription. [Learn more](#)

Setting 'Add current client IP address' to Yes will add an entry for your client IP address to the server firewall.

Allow Azure services and resources to access this server *

No Yes

Add current client IP address *

No Yes

[Review + create](#)

< Previous

Next : Security >

6. Select **Next : Security**, and next to **Enable Azure Defender for SQL**, choose **Not now**.

Home > New >

Create SQL Database

X

Microsoft

Basics Networking **Security** Additional settings Tags Review + create

Azure Defender for SQL

Protect your data using Azure Defender for SQL, a unified security package including vulnerability assessment and advanced threat protection for your server. [Learn more](#)

Get started with a 30 day free trial period, and then 15 USD/server/month.

Enable Azure Defender for SQL * ⓘ

Start free trial

Not now

[Review + create](#)

[< Previous](#)

[Next : Additional settings >](#)

7. Select **Next : Additional settings**, and configure the following settings.

Setting	Value
Under Data source section:	
Use existing data	Sample (this will create the AdventureWorksLT sample database)
Under Database collation section:	
Collation	default

Home >

Create SQL Database

Microsoft

X

Basics Networking Security Additional settings Tags Review + create

Customize additional configuration parameters including collation & sample data.

Data source

Start with a blank database, restore from a backup or select sample data to populate your new database.

Use existing data * None Backup Sample

AdventureWorksLT will be created as the sample database.

Database collation

Database collation defines the rules that sort and compare data, and cannot be changed after database creation. The default database collation is SQL_Latin1_General_CI_AS. [Learn more](#)

Collation ⓘ SQL_Latin1_General_CI_AS

[Review + create](#) [< Previous](#) [Next : Tags >](#)

8. Select **Review + create**.
9. After validation success, on the **Create SQL Database** window, select **Create** to deploy the server and database.
10. It can take approximately 2 to 5 minutes to create the server and deploy the sample database.
11. Select **Go to resource**
12. Select **Set server firewall**, and then select **Yes** to Allow Azure services and resources to access this server.
13. Select **Save**.
14. Select **OK**.

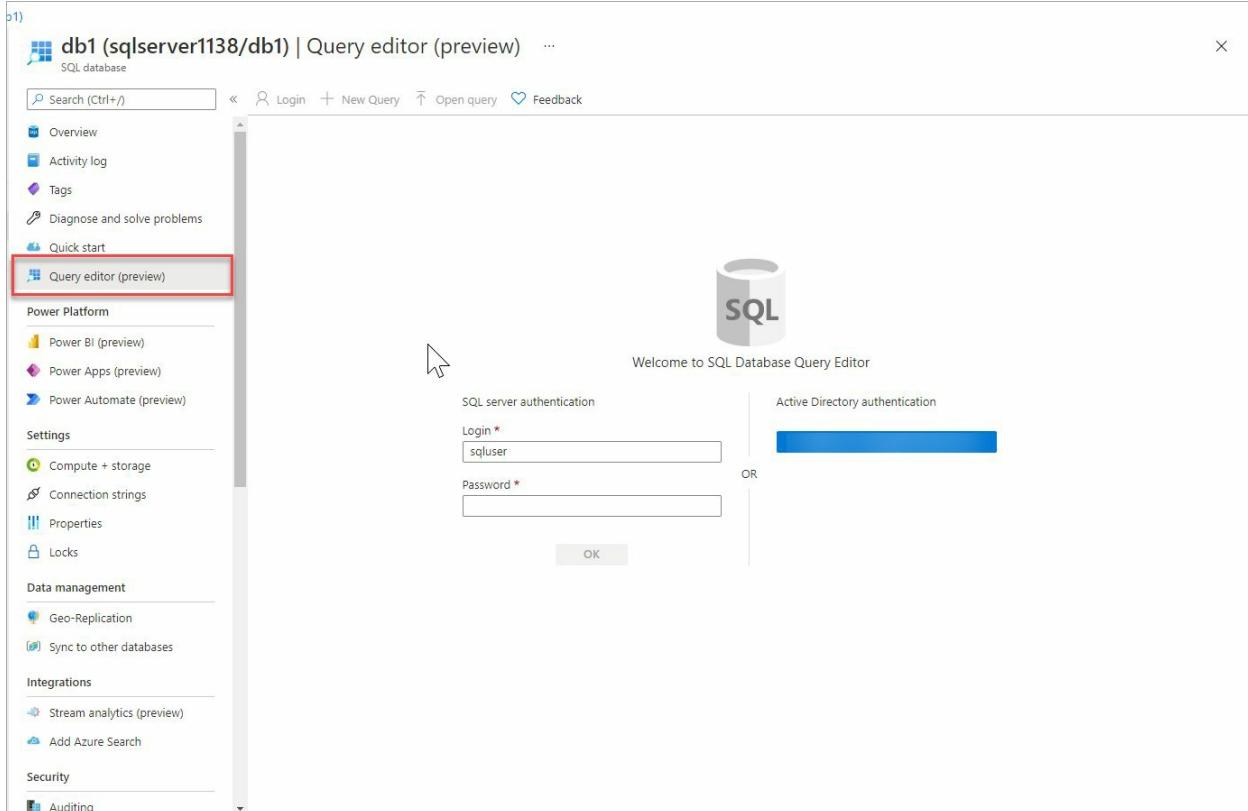
Task 2: Test the database

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

1. From the **All resources** pane, search and select **SQL databases** and ensure that your new database was created. You might need to refresh the page.

SQL databases						
Microsoft						
+ Add		Reservations	Edit columns	Refresh	Assign tags	Delete
1 items						
Name	Status	Replication role	Server	Pricing tier	Location	Subscription
 db1	Online	None	mysqlserverces	General Purpose: Gen5, 2 vCores	East US	Visual Studio Enterprise

2. Select the **db1** entry representing the SQL database you created, and then select **Query editor (preview)** in the nav bar.



The screenshot shows the Azure portal interface for managing SQL databases. On the left, a sidebar lists various management options like Overview, Activity log, Tags, Diagnose and solve problems, Quick start, and Query editor (preview). The 'Query editor (preview)' option is highlighted with a red box. The main content area displays the 'Welcome to SQL Database Query Editor'. It features two authentication methods: 'SQL server authentication' (Login: sqluser, Password: [redacted]) and 'Active Directory authentication'. A large 'OK' button is at the bottom. The top of the page shows the database name 'db1 (sqlserver1138/db1) | Query editor (preview)' and a search bar.

3. Sign in as **sqluser**, with the password **Pa\$\$w0rd1234**.
 4. You will not be able to sign in.

Note: Read the error closely and make note of the IP address that needs to be allowed through the firewall.



Welcome to SQL Database Query Editor

SQL server authentication

Login *

Password *

 ✓

Active Directory authentication

Continue as [REDACTED]

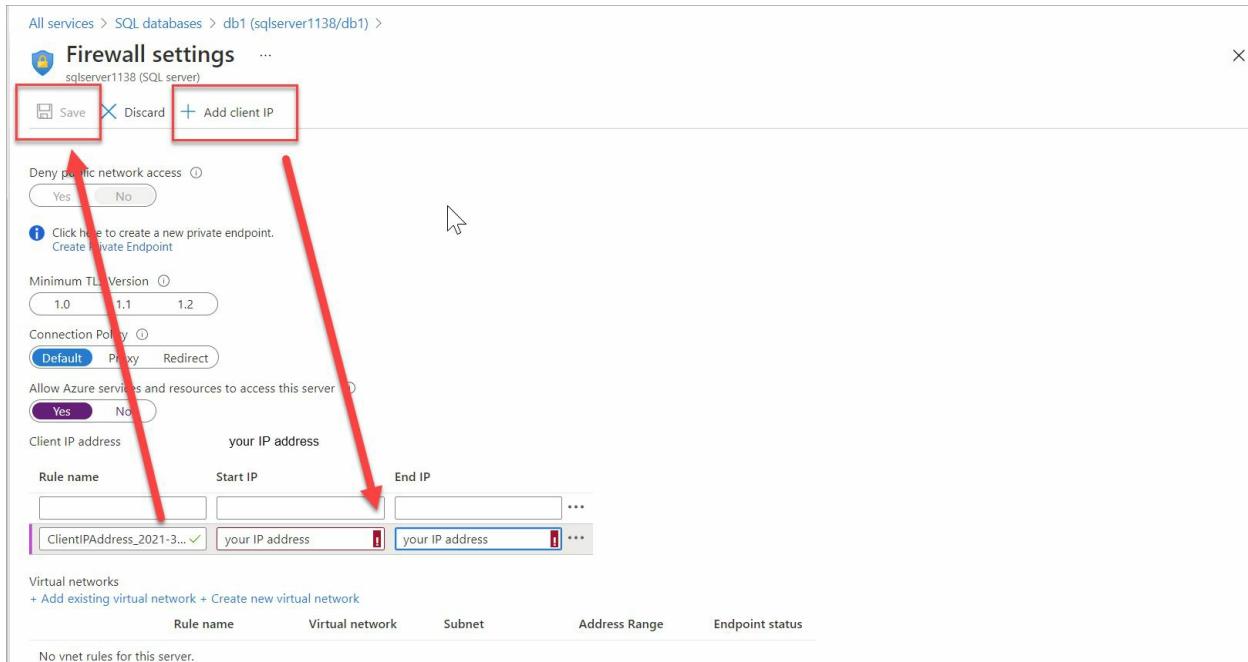
OR



✗ Cannot open server 'sqlserverxxx1' requested by the login. Client with IP address [REDACTED] is not allowed to access the server. To enable access, use the Windows Azure Management Portal or run sp_set_firewall_rule on the master database to create a firewall rule for this IP address or address range. It may take up to five minutes for this change to take effect.

[Set server firewall \(sqlserverxxx1\)](#)

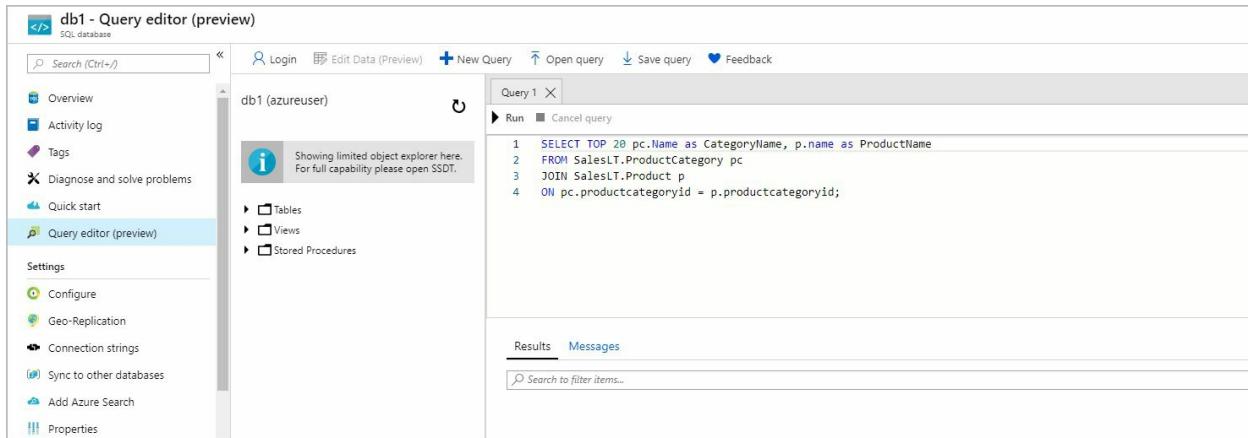
5. Select **Overview > Set server firewall**.
6. In the **Client IP address** section, your IP will be shown (verify that it is the same client IP address from the error above). Click on **+ Add client IP**, which will add a **Rule name** and put your IP in both the **Start IP** and **End IP** fields, and then select **Save**.



7. Return to your SQL database and the Query Editor sign-in page. Try to sign in again as **sqluser**, with the password **Pa\$\$w0rd1234**. This time you should succeed. It might take a couple of minutes for the new firewall rule to be deployed. If you wait and still get an error, verify the client IP address in the error, and try selecting **Firewall settings** > and adding the correct client IP address again.
8. After you sign in successfully, the query pane appears. Enter the following query into the editor pane.

```
SQL

SELECT TOP 20 pc.Name as CategoryName, p.name as ProductName
FROM SalesLT.ProductCategory pc
JOIN SalesLT.Product p
ON pc.productcategoryid = p.productcategoryid;
```



9. Select **Run**, and then review the query results in the **Results** pane. The query should run successfully.

CATEGORYNAME	PRODUCTNAME
Road Frames	HL Road Frame - Black, 58
Road Frames	HL Road Frame - Red, 58
Helmets	Sport-100 Helmet, Red
Helmets	Sport-100 Helmet, Black
Socks	Mountain Bike Socks, M

Query succeeded | 1s

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

5.4.3 Azure SQL Managed Instance

Azure SQL Managed Instance is a scalable cloud data service that provides

the broadest SQL Server database engine compatibility with all the benefits of a fully managed platform as a service. Depending on your scenario, Azure SQL Managed Instance might offer more options for your database needs.



Features

Like Azure SQL Database, Azure SQL Managed Instance is a platform as a service (PaaS) database engine, which means that your company will be able to take advantage of the best features of moving your data to the cloud in a fully-managed environment. For example, your company will no longer need to purchase and manage expensive hardware, and you won't have to maintain the additional overhead of managing your on-premises infrastructure. On the other hand, your company will benefit from the quick provisioning and service scaling features of Azure, together with automated patching and version upgrades. In addition, you'll be able to rest assured that your data will always be there when you need it through built-in high availability features and a 99.99% uptime service level agreement (SLA). You'll also be able to protect your data with automated backups and a configurable backup retention period.

Azure SQL Database and Azure SQL Managed Instance offer many of the same features; however, Azure SQL Managed Instance provides several options that might not be available to Azure SQL Database. For example, iCertify Traders currently uses several on-premises servers running SQL Server, and they would like to migrate their existing databases to a SQL database running in the cloud. However, several of their databases use

Cyrillic characters for collation. In this scenario, iCertify Traders should migrate their databases to an Azure SQL Managed Instance, since Azure SQL Database only uses the default SQL_Latin1_General_CI_AS server collation.

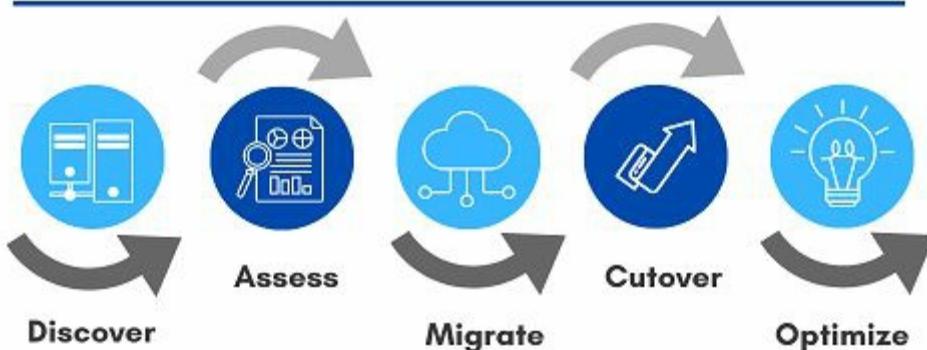
Note: For a detailed list of the differences between Azure SQL Database and Azure SQL Managed Instance, see Features comparison: Azure SQL Database and Azure SQL Managed Instance.

Migration

Azure SQL Managed Instance makes it easy to migrate your on-premises data on SQL Server to the cloud using the Azure Database Migration Service (DMS) or native backup and restore. After you have discovered all of the features that your company uses, you need to assess which on-premises SQL Server instances you can migrate to Azure SQL Managed Instance to see if you have any blocking issues. Once you have resolved any issues, you can migrate your data, then cutover from your on-premises SQL Server to your Azure SQL Managed Instance by changing the connection string in your applications.

Migration Process Flow

A step-by-step guide



Note: For a detailed description of the migration process, see Migration guide: SQL Server to SQL Managed Instance



5.4.4 Azure database for MySQL

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

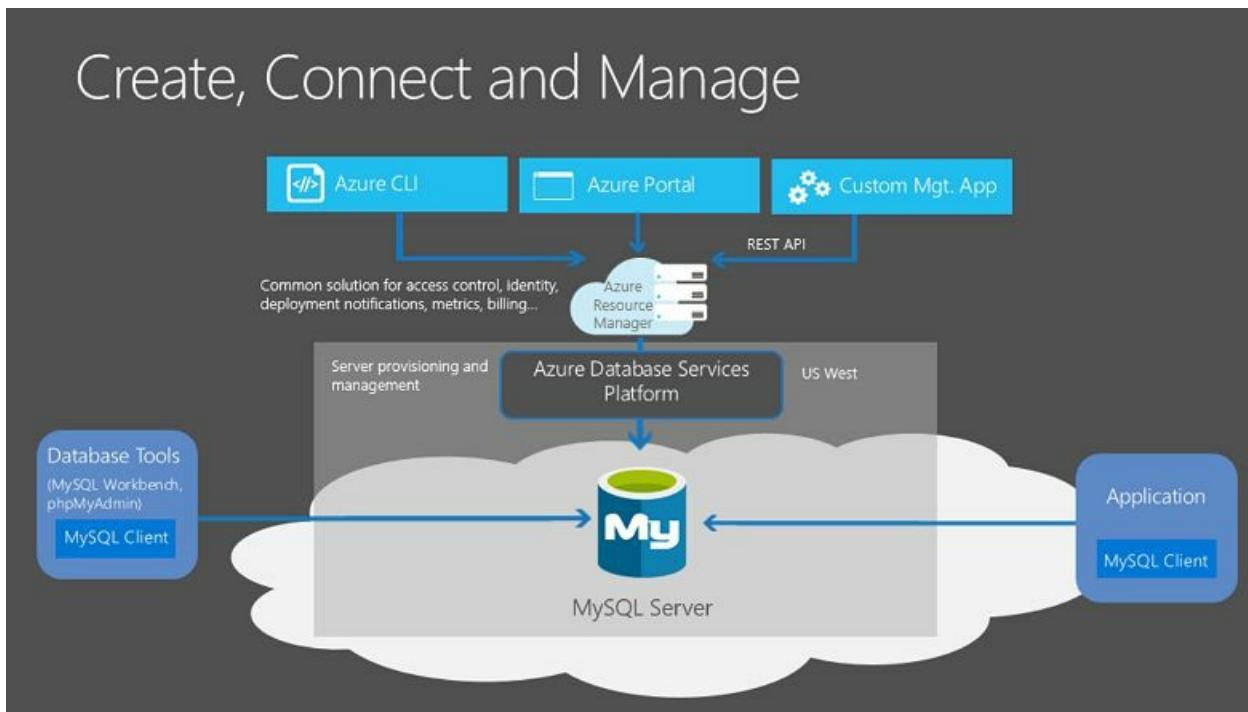
Azure Database for MySQL is a relational database service in the cloud, and it's based on the MySQL Community Edition database engine, versions 5.6, 5.7, and 8.0. With it, you have a 99.99 percent availability service level agreement from Azure, powered by a global network of Microsoft-managed datacenters.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

Azure Database for MySQL delivers:

- Built-in high availability with no additional cost.
- Predictable performance and inclusive, pay-as-you-go pricing.
- Scale as needed, within seconds.
- Ability to protect sensitive data at-rest and in-motion.

- Automatic backups.
- Enterprise-grade security and compliance.

These capabilities require almost no administration, and all are provided at no additional cost. They allow you to focus on rapid app development and accelerating your time-to-market, rather than having to manage virtual machines and infrastructure. In addition, you can migrate your existing MySQL databases with minimal downtime by using the Azure Database Migration Service. After you have completed your migration, you can continue to develop your application with the open-source tools and platform of your choice. You don't have to learn new skills.



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

5.4.5 Azure Database for PostgreSQL

As part of its overall data strategy, iCertify Traders have been using

PostgreSQL for several years. You and your team probably already know the benefits of PostgreSQL. Part of your migration is to use Azure Database for PostgreSQL, and you want to make sure that you'll have access to the same benefits as your on-premises server before moving to the cloud.



Azure Database for PostgreSQL is a relational database service in the cloud. The server software is based on the community version of the open-source PostgreSQL database engine. Your familiarity with tools and expertise with PostgreSQL is applicable when you're using Azure Database for PostgreSQL. Moreover, Azure Database for PostgreSQL delivers the following benefits:

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

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

Single Server

The Single Server deployment option delivers:

- Built-in high availability with no additional cost (99.99 percent SLA).
- Predictable performance and inclusive, pay-as-you-go pricing.
- Vertical scale as needed, within seconds.
- Monitoring and alerting to assess your server.
- Enterprise-grade security and compliance.
- Ability to protect sensitive data at-rest and in-motion.
- Automatic backups and point-in-time-restore for up to 35 days.

All those capabilities require almost no administration, and all are provided at no additional cost. You can focus on rapid application development and accelerating your time to market, rather than having to manage virtual machines and infrastructure. You can continue to develop your application with the open-source tools and platform of your choice, without having to learn new skills.

The Single Server deployment option offers three pricing tiers: Basic, General Purpose, and Memory Optimized. Each tier offers different resource capabilities to support your database workloads. You can build your first app on a small database for a few dollars a month, and then adjust the scale to meet the needs of your solution. Dynamic scalability enables your database to transparently respond to rapidly changing resource requirements. You only pay for the resources you need, and only when you need them.



Hyperscale (Citus)

The Hyperscale (Citus) option horizontally scales queries across multiple machines by using sharding. Its query engine parallelizes incoming SQL queries across these servers for faster responses on large datasets. It serves

applications that require greater scale and performance, generally workloads that are approaching, or already exceed, 100 GB of data.

The Hyperscale (Citus) deployment option supports multi-tenant applications, real-time operational analytics, and high throughput transactional workloads. Applications built for PostgreSQL can run distributed queries on Hyperscale (Citus) with standard connection libraries and minimal changes.

5.5 Azure Big data and analytics services

Several years ago, iCertify Traders rolled out a new GPS tracking system for all of its delivery vehicles. The new system provides real-time tracking data to your primary datacenter. Your CTO wants your team to look at several years of tracking data in order to determine trends. For example, an important trend might be a spike in deliveries around the holidays that would require hiring additional staff. Through an in-depth analysis of the tracking data that you've recorded, your CTO seeks to predict when changes are necessary, and then proactively take the necessary steps to appropriately manage spikes.

Data comes in all types of forms and formats. When we talk about big data, we're referring to large volumes of data. In this iCertify Traders scenario, data is collected from the GPS sensors, which includes location information, data from weather systems, and many other sources that generate large amounts of data. This amount of data becomes increasingly hard to make sense of and to base decisions on. 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 datasets. Microsoft Azure supports a broad range of technologies and services to provide big data and analytic solutions, including Azure Synapse Analytics, Azure HDInsight, Azure Databricks, and Azure Data Lake Analytics.



5.5.1 Azure Synapse Analytics

Azure Synapse Analytics (formerly Azure SQL Data Warehouse) is a limitless analytics service that brings together enterprise data warehousing and big data analytics. You can query data on your terms by using either

serverless or provisioned resources at scale. You have a unified experience to ingest, prepare, manage, and serve data for immediate BI and machine



learning needs.

5.5.2 Azure HDInsight

Azure HDInsight is a fully managed, open-source analytics service for enterprises. It's a cloud service that makes it easier, faster, and more cost-effective to process massive amounts of data. You can run popular open-source frameworks and create cluster types such as Apache Spark, Apache Hadoop, Apache Kafka, Apache HBase, Apache Storm, and Machine Learning Services. HDInsight also supports a broad range of scenarios such as extraction, transformation, and loading (ETL), data warehousing, machine learning, and IoT.

5.5.3 Azure Databricks

Azure Databricks helps you unlock insights from all your data and build artificial intelligence solutions. You can set up your Apache Spark environment in minutes, and then autoscale and collaborate on shared projects in an interactive workspace. Azure Databricks supports Python, Scala, R, Java, and SQL, as well as data science frameworks and libraries



including TensorFlow, PyTorch, and scikit-learn.

5.5.4 Azure Data Lake Analytics

Azure Data Lake Analytics 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's running,



making it more cost-effective.

5.5.5 Knowledge check

Choose the best response for each question. Then select Check your answers.

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

- A. Azure Cosmos DB
- B. Azure SQL Database

- C. Azure Databricks
- D. Azure Database for PostgreSQL

2. iCertify Traders uses the LAMP stack for several of its websites.

Which option would be ideal for migration?

- A. Azure Cosmos DB
- B. Azure Database for MySQL
- C. Azure SQL Database
- D. Azure Database for PostgreSQL

3. iCertify Traders has millions of log entries that it wants to analyze.

Which option would be ideal for analysis?

- A. Azure Cosmos DB
- B. Azure SQL Database
- C. Azure Database for PostgreSQL
- D. Azure Synapse Analytics

Answer:

1. Answer: A. Azure Cosmos DB supports SQL, MongoDB, Cassandra, Tables, and Gremlin APIs.
2. Answer: B. Azure Database for MySQL is the logical choice for existing LAMP stack applications.
3. Answer: D. Azure Synapse Analytics is the logical choice for analyzing large volumes of data.

Summary

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

In addition, you saw how Azure Cosmos DB works with a variety of popular APIs, including SQL, MongoDB, Cassandra, Tables, and Gremlin. You can use these to migrate your data to the cloud and retain or enhance your developers' skill sets. You also learned how you can use big data and analysis

services like Azure Synapse Analytics, Azure HDInsight, Azure Databricks, and Azure Data Lake Analytics to analyze large volumes of data.

5.6 Azure Artificial Intelligence services

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

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

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

Forecasts or predictions from machine learning can make apps and devices smarter. For example, when you shop online, machine learning powers product recommendation systems that offer additional products based on what you've bought and what other shoppers have bought who have purchased similar items in the past.

Machine learning is also used to detect credit card fraud by analyzing each new transaction and using what it has learned from analyzing millions of fraudulent transactions.

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

At a high level, there are three primary product offerings from Microsoft, each of which is designed for a specific audience and use case. Each option provides a diverse set of tools, services, and programmatic APIs. In this module, we'll merely scratch the surface of the options' capabilities.

5.6.1 Azure Machine Learning

Azure Machine Learning is a platform for making predictions. It consists of tools and services that allow you to connect to data to train and test models to find one that will most accurately predict a future result. After you've run

experiments to test the model, you can deploy and use it in real time via a web API endpoint.



With Azure Machine Learning, you can:

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

Choose Azure Machine Learning when your data scientists need complete control over the design and training of an algorithm using your own data. The following video discusses the basic steps required to set up a machine learning system.

Now, if you've heard that term before, great. And if you haven't, that's OK as well. Machine learning is a whole branch of computer science that involves computers being able to make decisions similar to the way that humans would and obviously, once you teach a computer to do something, it often can do it much better. And so we're seeing this in our self-driving cars and in systems all around. But we even have consumer facing devices that contain this type of technology. Your Nest thermostat, your Google home, Amazon, Alexa, your smartwatch. These are all things that you can talk about. They understand you and you can act upon your requests. Amazon, you can order me this refill of the tide pods and it will send it to your home. That technology is not limited to being Google or to being Amazon. You can use

that same technology in your own custom applications. Microsoft created a whole set of services called the Cognitive Services, which contains a bunch of APIs that you can call.

There are services around vision. This usually involves analyzing the contents of a photo. And so you can basically pass a photo to the vision service and it can either identify whether there are faces in the photo, how old they are, their gender, and if it's a celebrity, identify who they are. If it's a location, it can try to identify the place. It can identify objects such as bicycles and cars and chairs, return back a tag cloud effectively, or even just describe the picture. If it is a man swimming in blue water, all of the things that are part of the picture, the computer can analyze that. And so imagine if you have images being uploaded to your application. They even have moderation. So if you're trying to stop adult content from making its way inside or illegal content, then they have APIs that deal with adult filters and moderations, et cetera. They also have audio related API so that you can understand human speech and turn that into text or vice versa. Take it as a piece of text and turn it into speech. There's also translation APIs where you can go from one language to the other and it basically supports dozens of languages at this point. And that's just more than just taking single words and translating them one word at a time. But computer translation has really evolved over the last five or 10 years so that it understands the nature of human language. It understands the context of what you're saying. And so if you're using a word that could have several definitions in a different language, then it knows the context in which you're speaking and chooses the correct translation for that. These translator APIs are getting much, much better even in the last five years. It's a huge increase in the quality of translations. We also have various decision making APIs, you know, being able to categorize products and do predictions. And so if you've got a set of data and you want to understand which of the following people are more likely to lose weight, let's use losing weight as a predictor. Then you can feed in the data of the people, the characteristics of those people, their weights, their behaviors, and then be able to predict in advance the type of people that are more likely to achieve their goal.

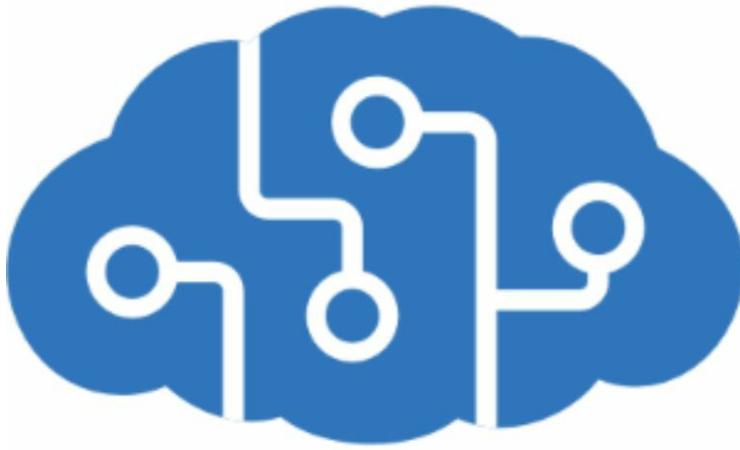
Maybe you want to know which of your customers are your best customers, which are your customers are more likely to need your service in the next

three months. And so if you have a list of customers that do need your service in the next three months, you can then train the model so that it can look at your customers where you don't know and make a prediction as to which ones do or do not need your service. So machine learning has huge growth. There's a lot of research being done and then you can act like the big guys and use that within your applications.

Another interesting advance that is also potentially helpful is what's called the bot service. So this takes natural language processing, the ability of a computer to understand human speech and even written speech and be able to respond to that in an intelligent way. So you've got an example on screen of somebody asking, do you know if my packages arrived and the computer on the other end being able to know who they are and then know that look up their history in the database to see when their packages were sent and ask them which package. So there's a context to what's being said and the computer can respond intelligently and you yourself can add it like this onto your website using the bot service. It's also good for a. Doing searches on your website so that if you know what hours are open, what's your locations, what products you store, etc. , all of that information is on your website, but a bot can answer those questions as well.

So those are the A.I. services, the umbrella categories. IIS machine learning is really the applied side of A.I. There's all sorts of cognitive services for that. And finally, a bot service where there's a chat, conversational nature, all of that stuff can be used by your applications that do not even have to be hosted in Azure. That could be hosted on your own website external to Azure that those APIs can be called from there.

5.6.2 Azure Cognitive Services

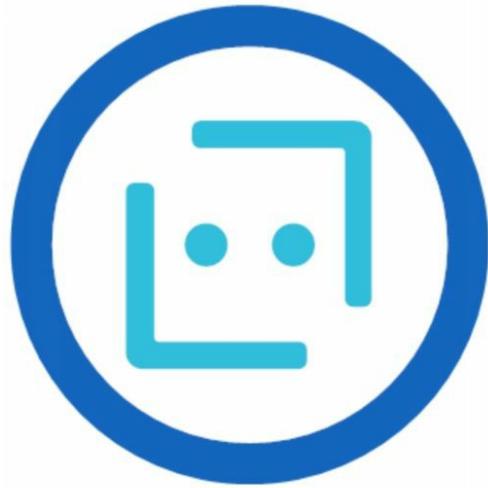


Azure Cognitive Services provides prebuilt machine learning models that enable applications to see, hear, speak, understand, and even begin to reason. Use Azure Cognitive Services to solve general problems, such as analyzing text for emotional sentiment or analyzing images to recognize objects or faces.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

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

Azure Cognitive Services can be divided into the following categories:

- Language services: Allow your apps to process natural language with prebuilt scripts, evaluate sentiment, and learn how to recognize what users want.
- Speech services: Convert speech into text and text into natural-sounding speech. Translate from one language to another and enable speaker verification and recognition.
- Vision services: Add recognition and identification capabilities when you're analyzing pictures, videos, and other visual content.
- Decision services: Add personalized recommendations for each user that automatically improve each time they're used, moderate content to monitor and remove offensive or risky content, and detect abnormalities in your time series data.



5.6.3 Azure Bot Service

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

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

5.6.4 Knowledge check

Case Study

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

1. You need to predict future behavior based on previous actions. Which product option should you select as a candidate?

- A. Azure Machine Learning
- B. Azure Bot Service
- C. Azure Cognitive Services

2. You need to create a human-computer interface that uses natural language to answer customer questions. Which product option should you select as a candidate?

- A. Azure Machine Learning
- B. Azure Cognitive Services
- C. Azure Bot Service

3. You need to identify the content of product images to automatically create alt tags for images formatted properly. Which product option is the best candidate?

- A. Azure Machine Learning
- B. Azure Cognitive Services
- C. Azure Bot Service

Answers:

1. **A.** Azure Machine Learning enables you to build models to predict the likelihood of a future result. It should not be eliminated as a candidate.
2. **C.** Azure Bot Service creates virtual agent solutions that utilize natural language. It should not be eliminated as a candidate.
3. **B.** Azure Cognitive Services includes Vision services that can identify the content of an image. Azure Cognitive Services is the best candidate.

Summary

You identified a few product options and their capabilities, including Azure Bot Service, Azure Cognitive Services, and Azure Machine Learning. You analyzed certain decision criteria to help yourself choose one option over another depending on the scenario. Then you applied those decision criteria to three iCertify Traders initiatives, helping the company find the best service option for each scenario.

Without AI services, iCertify Traders would spend more time and effort on

manual tasks, respond to customers less quickly, offer weak product recommendations, and be unable to fully support customers who speak languages other than English.

AI is one focus that could transform every area of a business. Such transformation is limited only by the creativity and imagination of the organization.

5.7 Azure Serverless Computing Services

Serverless computing is a term used to describe an execution environment that's set up and managed for you. You merely specify what you want to happen by writing code or connecting and configuring components in a visual editor, and then specify the actions that trigger your functionality, such as a timer or an HTTP request. Best of all, you never have to worry about an outage, your code can scale instantly to meet demand, and you pay based only on the actual usage of your code.

Serverless computing is a cloud-hosted execution environment that runs your code but abstracts the underlying hosting environment. The term serverless computing is a misnomer. After all, there is a server (or a group of servers) that executes your code or desired functionality.

The key idea is that you're not responsible for setting up or maintaining the server. You don't have to worry about scaling it when there's increased demand, and you don't have to worry about outages. The cloud vendor takes care of all maintenance and scaling concerns for you.

You create an instance of the service, and you then 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're billed only for the resources you use. You don't even need to reserve resources.

Serverless computing is ordinarily used to handle back-end scenarios. In other words, serverless computing is responsible for sending messages from one system to another, or processing messages that were sent from other systems. It's not used for user-facing systems but, rather, it works in the background.

In this module, we'll cover two Azure serverless computing services: Azure Functions and Azure Logic Apps.

5.7.1 Azure Functions

With the Azure Functions service, you can host a single method or function by using a popular programming language in the cloud that runs in response to an event. An example of an event might be an HTTP request, a new message on a queue, or a message on a timer.

Because of its atomic nature, Azure Functions can serve many purposes in an application's design. Functions can be written in many common programming languages, such as C#, Python, JavaScript, Typescript, Java, and PowerShell.

Azure Functions scales automatically, and charges accrue only when a function is triggered. These qualities make Azure Functions a solid choice when demand is variable. For example, you might 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.

An Azure function is a stateless environment. A function behaves as if it's restarted every time it responds to an event. This feature is ideal for processing incoming data. And if state is required, the function can be connected to an Azure storage account.

Azure Functions can perform orchestration tasks by using an extension called Durable Functions, which allow developers to chain functions together while maintaining state.

The Azure Functions solution is ideal when you're concerned only with the code that's running your service and not the underlying platform or infrastructure. You use Azure Functions most commonly when you need to perform work in response to an event. You do this often via a REST request, timer, or message from another Azure service, and when that work can be completed quickly, within seconds or less.

5.7.2 Azure Logic Apps

Logic Apps is a low-code/no-code development platform hosted as a cloud service. The service 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. This solution covers app integration, data integration, system integration, enterprise application integration (EAi), and business-to-business (B2B) integration.

Azure Logic Apps is designed in a web-based designer and can execute logic that's triggered by Azure services without writing any code. You build an app by linking triggers to actions with connectors. A trigger is an event (such as a timer) that causes an app to execute, then a new message to be sent to a queue, or an HTTP request. An action is a task or step that can be executed. There are logic actions such as those you would find in most programming languages. Examples of actions include working with variables, decision statements and loops, and tasks that parse and modify data.

To build enterprise integration solutions with Azure Logic Apps, you can choose from a growing gallery of over 200 connectors. The gallery includes services such as Salesforce, SAP, Oracle DB, and file shares.

If you can't find the action or connector you need, you can build your own by using custom code.

What are the differences between these services?

You can call Azure Functions from Azure Logic Apps, and vice versa. The primary difference between the two services is their intent. Azure Functions is a serverless compute service, and Azure Logic Apps is intended to be a serverless orchestration service. Although you can use Azure Functions to orchestrate a long-running business process that involves various connections, this was not its primary use case when it was designed.

Additionally, the two services are priced differently. Azure Functions pricing is based on the number of executions and the running time of each execution. Logic Apps pricing is based on the number of executions and the type of connectors that it utilizes.

5.7.3 Knowledge Check

1. You need to process messages from a queue, parse them by using some existing imperative logic written in Java, and then send them to a third-party

API. Which serverless option should you choose?

- A. Azure Functions
 - B. Azure Logic Apps
2. You want to orchestrate a workflow by using APIs from several well-known services. Which is the best option for this scenario?
- A. Azure Functions
 - B. Azure Logic Apps
3. Your team has limited experience with writing custom code, but it sees tremendous value in automating several important business processes. Which of the following options is your team's best option?
- A. Azure Functions
 - B. Azure Logic Apps

Answers

1. A. Azure Functions is the correct choice because you can use existing Java code with minimal modification.
2. B. Azure Logic Apps makes it easy to create a workflow across well-known services with less effort than writing code and manually orchestrating all the steps yourself.
3. B. Azure Logic Apps is best suited for users who are more comfortable in a visual environment that allows them to automate their business processes. Logic Apps is the best option in this scenario.

5.8 IOT Services

IoT enables devices to gather and then relay information for data analysis. Smart devices are equipped with sensors that collect data. A few common sensors that measure attributes of the physical world include:

- Environmental sensors that capture temperature and humidity levels.
- Barcode, QR code, or optical character recognition (OCR) scanners.
- Geo-location and proximity sensors.
- Light, color, and infrared sensors.
- Sound and ultrasonic sensors.
- Motion and touch sensors.
- Accelerometer and tilt sensors.
- Smoke, gas, and alcohol sensors.
- Error sensors to detect when there's a problem with the device.
- Mechanical sensors that detect anomalies or deformations.
- Flow, level, and pressure sensors for measuring gasses and liquids.

By using Azure IoT services, devices that are equipped with these kinds of sensors and that can connect to the internet could send their sensor readings to a specific endpoint in Azure via a message. The message's data is then collected and aggregated, and it can be converted into reports and alerts. Alternatively, all devices could be updated with new firmware to fix issues or add new functionality by sending software updates from Azure IoT services to each device.

Let's suppose your company manufactures and operates smart refrigerated vending machines. What kinds of information would you want to monitor? You might want to ensure that:

- Each machine is operating without any errors.
- The machines haven't been compromised.
- The machines' refrigeration systems are keeping their contents within a certain temperature range.
- You're notified when products reach a certain inventory level so you can restock the machines.

If the hardware of your vending machines can collect and send this information in a standard message, the messages each machine sends can be received, stored, organized, and displayed by using Azure IoT services.

The data that's collected from these devices could be combined with Azure AI services to help you predict:

- When machines need proactive maintenance.
- When inventories will need to be replenished and new products ordered from vendors.

Many services can assist and drive end-to-end solutions for IoT on Azure.

So the first thing we'll talk about are the Internet of Things type devices, including Azure Sphere. Some of the products that Azure provides are like IOT hub, IOT central and azure sphere.

Now, Internet of Things are these devices that you may have in your home, you may have on your body your watch, where it's basically communicating with the cloud to deliver you some real service. Your fridge could be like that, etc. The Iot hub and Iot central are ways to allow these devices to communicate into the cloud in the high speed, low latency way. You can't imagine if you've got a million thermostats deployed around the world that you want to really have a solution that's slow and expensive. So an Iot hub could be something where it's receiving in the communication of little small bits of data coming in from millions of devices and it's designed to handle that kind of volume. From there you can do some processing and store that data somewhere. Atmosphere is really interesting because it's both a chip as well as an operating system, and it's basically a security protocol for these devices. So you can think about these millions of thermostats and fridges and watches. Well, keeping those things secure so that hackers can't break in and install their own code and get your webcam spying on you is a big challenge. And so Azure has got this Azure sphere product which helps manufacturers to create the secure devices as well as an operating system that they can program against it.

5.8.1 Azure IoT Hub

Azure IoT Hub is a managed service that's hosted in the cloud and 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 back end. You can connect virtually any device to your IoT hub.

The IoT Hub service 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. After an IoT hub receives messages from a device, it can route that message to other Azure services.

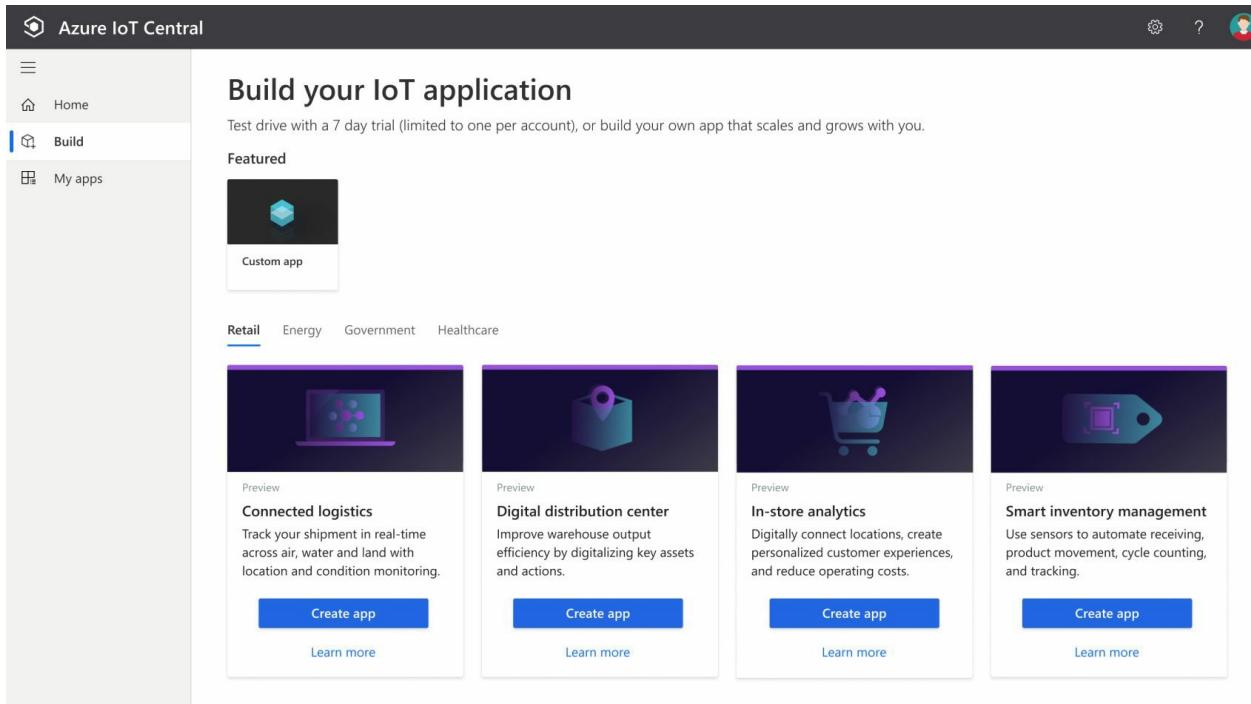
From a cloud-to-device perspective, IoT Hub allows for command and control. That is, you can have either manual or automated remote control of connected devices, so you can instruct the device to open valves, set target temperatures, restart stuck devices, and so on.

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

5.8.2 Azure IoT Central

Azure IoT Central builds on top of IoT Hub by adding a dashboard that allows you to connect, monitor, and manage your IoT devices. The visual user interface (UI) makes it easy to quickly connect new devices and watch as they begin sending telemetry or error messages. You can watch the overall performance across all devices in aggregate, and you can set up alerts that send notifications when a specific device needs maintenance. Finally, you can push firmware updates to the device.

To help you get up and running quickly, IoT Central provides starter templates for common scenarios across various industries, such as retail, energy, healthcare, and government. You then customize the design starter templates directly in the UI by choosing from existing themes or creating your own custom theme, setting the logo, and so on. With IoT Central, you can tailor the starter templates for the specific data that's sent from your devices, the reports you want to see, and the alerts you want to send.



You can use the UI to control your devices remotely. This feature allows you to push a software update or modify a property of the device. You can adjust the desired temperature for one or all of your refrigerated vending machines from directly inside of IoT Central.

A key part of IoT Central is the use of device templates. By using a device template, you can connect a device without any service-side coding. IoT Central uses the templates to construct the dashboards, alerts, and so on. Device developers still need to create code to run on the devices, and that code must match the device template specification.

5.8.3 Azure Sphere

Azure Sphere creates an end-to-end, highly secure IoT solution for customers that encompasses everything from the hardware and operating system on the device to the secure method of sending messages from the device to the message hub. Azure Sphere has built-in communication and security features for internet-connected devices.

Azure Sphere comes in three parts:

- The first part is the Azure Sphere micro-controller unit (MCU), which is responsible for processing the operating system and signals from

attached sensors. The following image displays the Seeed Azure Sphere MT3620 Development Kit MCU, one of several different starter kits that are available for prototyping and developing Azure Sphere applications.



- The second part is a customized Linux operating system (OS) that handles communication with the security service and can run the vendor's software.
- The third part is Azure Sphere Security Service, also known as AS3. Its job is to make sure that the device has not been maliciously compromised. When the device attempts to connect to Azure, it first must authenticate itself, per device, which it does by using certificate-based authentication. If it authenticates successfully, AS3 checks to ensure that the device hasn't been tampered with. After it has established a secure channel of communication, AS3 pushes any OS or approved customer-developed software updates to the device.

After the Azure Sphere system has validated the authenticity of the device and authenticated it, the device can interact with other Azure IoT services by sending telemetry and error information.

5.8.4 Knowledge Check

1. A company wants to build a new voting kiosk for sales to governments around the world. Which IoT technologies should the company choose to ensure the highest degree of security?

- A. IoT Hub
- B. IoT Central
- C. Azure Sphere

2. A company wants to quickly manage its individual IoT devices by using a web-based user interface. Which IoT technology should it choose?

- A. IoT Hub
- B. IoT Central
- C. Azure Sphere

3. You want to send messages from the IoT device to the cloud and vice versa. Which IoT technology can send and receive messages?

- A. IoT Hub
- B. IoT Central
- C. Azure Sphere

Answers

- 1) C. Azure Sphere provides the highest degree of security to ensure the device has not been tampered with.
- 2) B. IoT Central quickly creates a web-based management portal to enable reporting and communication with IoT devices.
- 3) A. An IoT hub communicates to IoT devices by sending and receiving messages.

Chapter 6 : Azure Management tools

6.1 Learning Objectives

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

- Choose the Azure management tools that best address your organization's technical needs and challenges.

Microsoft offers a variety of tools and services to manage your cloud environment, each aimed at different scenarios and users.

6.2 The Azure portal

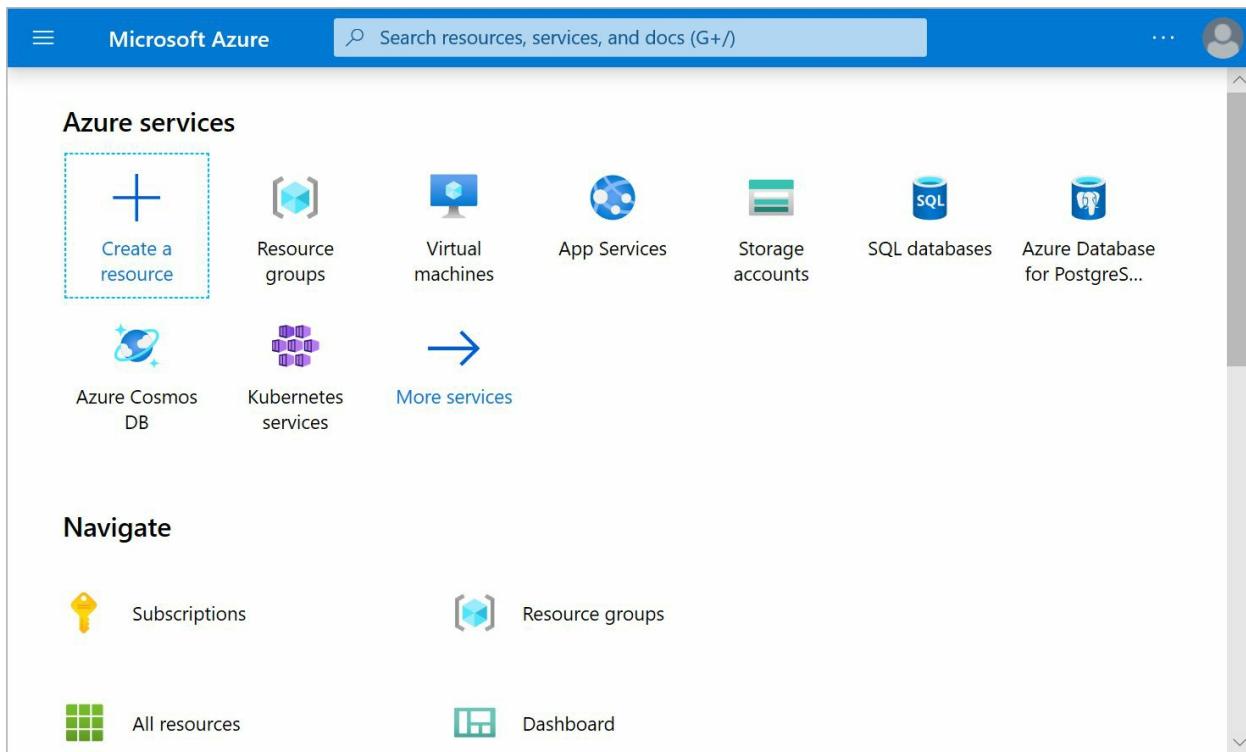
By using the Azure portal, a web-based user interface, you can access virtually every feature of Azure. The Azure portal provides a friendly, graphical UI to view all the services you're using, create new services, configure your services, and view reports. The Azure portal is how most users first experience Azure. But, as your Azure usage grows, you'll likely choose a more repeatable code-centric approach to managing your Azure resources.

What is the Azure portal?

The Azure portal is a web-based, unified console that provides an alternative to command-line tools. With the Azure portal, you can manage your Azure subscription by using a graphical user interface. You can:

- Build, manage, and monitor everything from simple web apps to complex cloud deployments.
- Create custom dashboards for an organized view of resources.
- Configure accessibility options for an optimal experience.

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



6.3 The Azure mobile app

The Azure mobile app provides iOS and Android access to your Azure resources when you're away from your computer. With it, you can:

- Monitor the health and status of your Azure resources.
- Check for alerts, quickly diagnose and fix issues, and restart a web app or virtual machine (VM).
- Run the Azure CLI or Azure PowerShell commands to manage your Azure resources.

6.4 Azure PowerShell

Azure PowerShell is a shell with which developers and DevOps and IT professionals can execute commands called cmdlets (pronounced command-lets). These commands call the Azure Rest API to perform every possible management task in Azure. Cmdlets can be executed independently or combined into a script file and executed together to orchestrate:

- The routine setup, teardown, and maintenance of a single resource or multiple connected resources.
- The deployment of an entire infrastructure, which might contain dozens or hundreds of resources, from imperative code.
- Capturing the commands in a script makes the process repeatable and automatable.

Azure PowerShell is available for Windows, Linux, and Mac, and you can access it in a web browser via Azure Cloud Shell.

Windows PowerShell has helped Windows-centric IT organizations automate many of their on-premises operations for years, and these organizations have built up a large catalog of custom scripts and cmdlets, as well as expertise.

6.5 The Azure CLI

The Azure CLI command-line interface is an executable program with which a developer, DevOps professional, or IT professional can execute commands in Bash. The commands call the Azure Rest API to perform every possible management task in Azure. You can run the commands independently or combined into a script and executed together for the routine setup, teardown, and maintenance of a single resource or an entire environment.

In many respects, the Azure CLI is almost identical to Azure PowerShell in what you can do with it. Both run on Windows, Linux, and Mac, and can be accessed in a web browser via Cloud Shell. The primary difference is the syntax you use. If you're already proficient in PowerShell or Bash, you can use the tool you prefer.

6.6 ARM templates

Although it's possible to write imperative code in Azure PowerShell or the Azure CLI to set up and tear down one Azure resource or orchestrate an infrastructure comprising hundreds of resources, there's a better way to implement this functionality.

By using Azure Resource Manager templates (ARM templates), you can describe the resources you want to use in a declarative JSON format. The benefit is that the entire ARM template is verified before any code is executed to ensure that the resources will be created and connected correctly. The template then orchestrates the creation of those resources in parallel. That is, if you need 50 instances of the same resource, all 50 instances are created at the same time.

Ultimately, the developer, DevOps professional, or IT professional needs only to define the desired state and configuration of each resource in the ARM template, and the template does the rest. Templates can even execute PowerShell and Bash scripts before or after the resource has been set up.

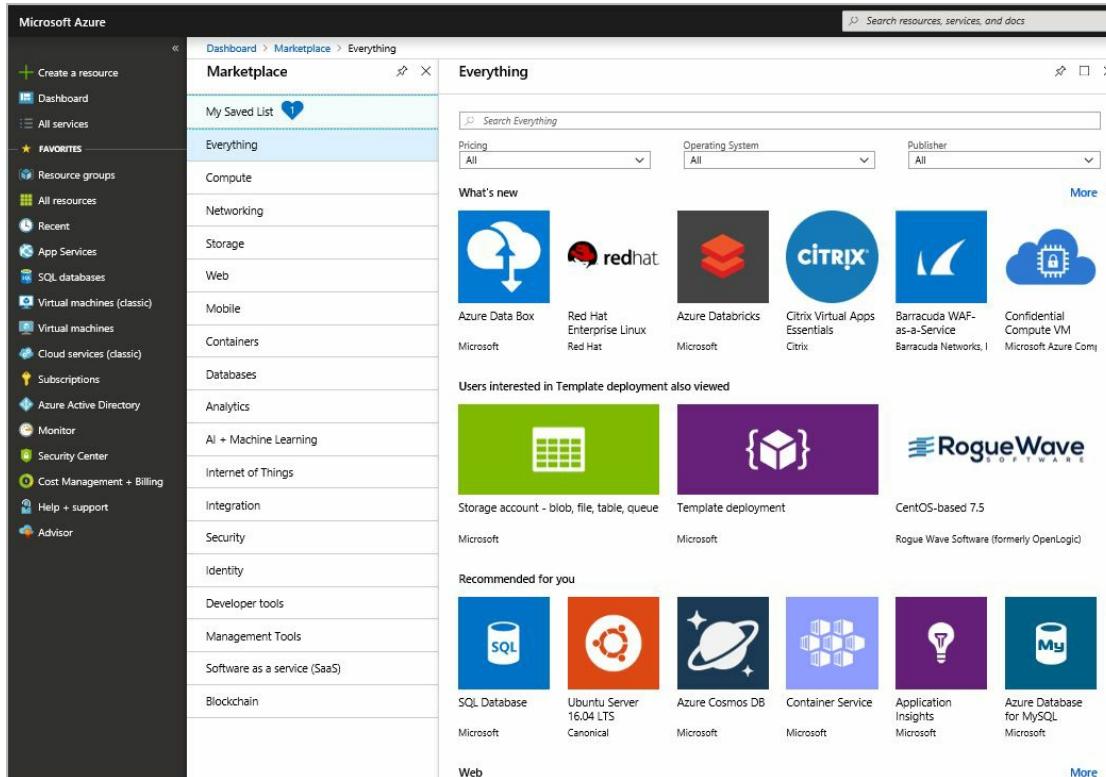
6.7 Azure Marketplace

So before we leave this section talking about Azure services, I want to mention one that a lot of people don't view as a service, but kind of is and that's called the Azure marketplace.

Azure Marketplace helps connect users with Microsoft partners, independent software vendors, and startups that are offering their solutions and services, which are optimized to run on Azure. Azure Marketplace customers can find, try, purchase, and provision applications and services from hundreds of leading service providers. All solutions and services are certified to run on Azure.

The solution catalog spans several industry categories such as 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, there are more than 8,000 listings.



Azure Marketplace is designed for IT pros 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.

The Azure marketplaces where Microsoft and its partners list the various computing services available for your use. And so this is where we say there's more than one thousand services available. You can go under here. You can see the categories on the left, and you'll be able to find hundreds of types of virtual machines, not just provided by Microsoft. So you could find a Virtual Machine that already has SQL Server database installed and that will be SQL Server in a VM. That image is available. There are also virtual machines that contain. We can see Barracuda, which is a Web application firewall, the Red Hat Enterprise. Linux is a Virtual Machine available by RedHat ET. So this is the marketplaces where companies create images and provide them. Now, you can obviously create your own image as well. There's such a thing as a custom image. So once you've set up your Virtual Machine exactly how you like with your software and your files and your permissions, you can make an image of it and that becomes the image that gets deployed. But if you want to find images created by other people, this is where you find it. Another example would be if you want a database that is not among the default Azure set, like we were just talking about databases. So if you want an Oracle database, there is an Oracle database image in here as well. So I would say if you're curious about whether Azure has native support for any of the technologies that you work with, you go to the marketplace and you do a search for those names.

So we saw earlier when creating networks, virtual machines and storage accounts that I would go into the marketplace to find those to hit the create button. And so the Azure marketplaces where Microsoft and its partners list the various computing services available for your use. And so this is where we say there's more than one thousand services available. You can go under here. You can see the categories on the left, and you'll be able to find hundreds of types of virtual machines, not just provided by Microsoft. So you could find a Virtual Machine that already has SQL Server database installed and that will be SQL Server in a VM. That image is available. There are also virtual machines that contain. We can see Barracuda, which is a Web application firewall, the Red Hat Enterprise. Linux is a Virtual Machine

available by RedHat ET. So this is the marketplaces where companies create images and provide them. Now, you can obviously create your own image as well. There's such a thing as a custom image. So once you've set up your Virtual Machine exactly how you like with your software and your files and your permissions, you can make an image of it and that becomes the image that gets deployed. But if you want to find images created by other people, this is where you find it. Another example would be if you want a database that is not among the default Azure set, like we were just talking about databases. So if you want an Oracle database, there is an Oracle database image in here as well. So I would say if you're curious about whether Azure has native support for any of the technologies that you work with, you go to the marketplace and you do a search for those names.

6.8 Knowledge Check

1. As an administrator, you need to retrieve the IP address from a particular VM by using Bash. Which of the following tools should you use?
 - A. ARM templates
 - B. Azure PowerShell
 - C. The Azure portal
 - D. The Azure CLI
2. You're a developer who needs to set up your first VM to host a process that runs nightly. Which of the following tools is your best choice?
 - A. ARM templates
 - B. Azure PowerShell
 - C. The Azure portal
 - D. The Azure CLI
3. What is the best infrastructure-as-code option for quickly and reliably setting up your entire cloud infrastructure declaratively?
 - A. ARM templates
 - B. Azure PowerShell
 - C. The Azure portal
 - D. The Azure CLI

Answers :

1. D. The Azure CLI enables you to use Bash to run one-off tasks on Azure.
2. C. The Azure portal is a great place for newcomers to learn about Azure and set up their first resources.
3. B. ARM templates are the best infrastructure-as-code option for quickly and reliably setting up your entire cloud infrastructure declaratively.

6.9 Azure Monitoring Services

Several basic questions or concerns face all companies that use the cloud.

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

Fortunately, by using a combination of monitoring solutions on Azure, you can:

- Gain answers, insights, and alerts to help ensure that you've optimized your cloud usage.
- Ascertain the root cause of unplanned issues.
- Prepare ahead of time for planned outages.

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

6.3.1 Azure Advisor

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

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

When you're in the Azure portal, the Advisor dashboard displays

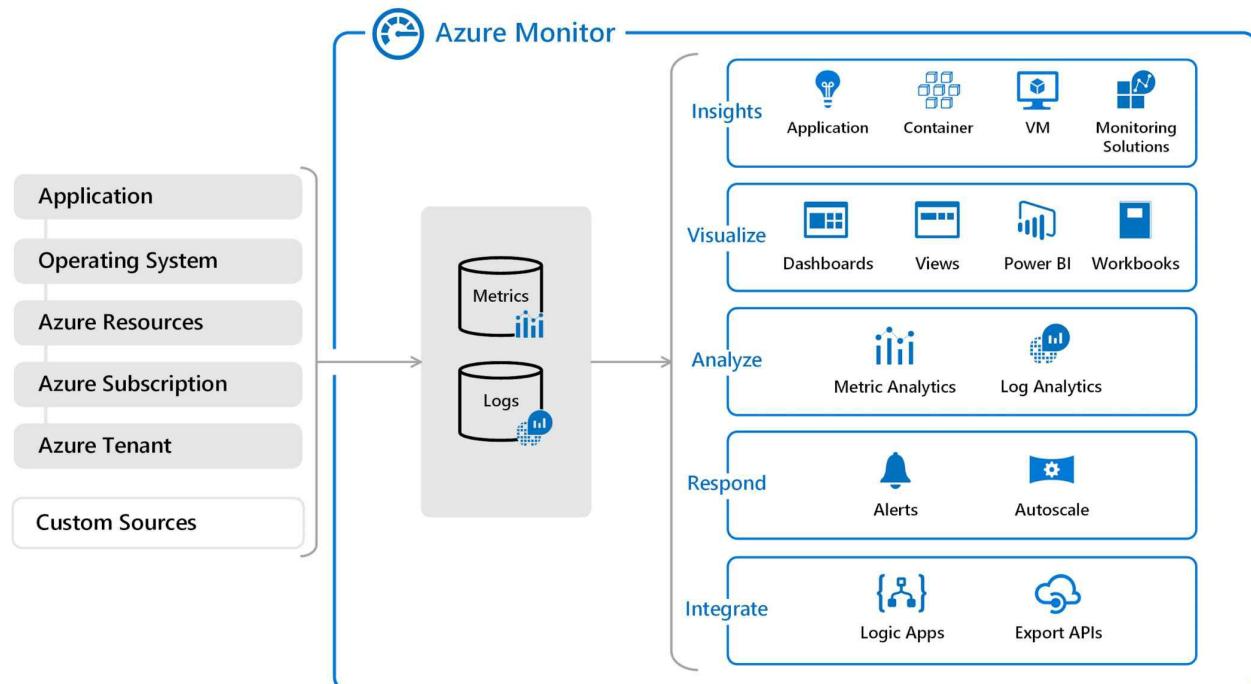
personalized recommendations for all your subscriptions, and you can use filters to select recommendations for specific subscriptions, resource groups, or services. The recommendations are divided into five categories:

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

6.3.2 Azure Monitor

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

The following diagram illustrates just how comprehensive Azure Monitor is.



- On the left is a list of the sources of logging and metric data that can be collected at every layer in your application architecture, from

application to operating system and network.

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

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

Some popular products such as Azure Application Insights, a service for sending telemetry information from application source code to Azure, uses Azure Monitor under the hood. With Application Insights, your application developers can take advantage of the powerful data-analysis platform in Azure Monitor to gain deep insights into an application's operations and diagnose errors without having to wait for users to report them.

6.3.3 Azure Service Health

Azure Service Health provides a personalized view of the health of the Azure services, regions, and resources you rely on. The status.azure.com website, which displays only major issues that broadly affect Azure customers, doesn't provide the full picture. But Azure Service Health displays both major and smaller, localized issues that affect you. Service issues are rare, but it's important to be prepared for the unexpected. You can set up alerts that help you triage outages and planned maintenance. After an outage, Service Health provides official incident reports, called root cause analyses (RCAs), which you can share with stakeholders.

Service Health helps you keep an eye on several event types:

- Service issues are problems in Azure, such as outages, that affect you right now. You can drill down to the affected services, regions, updates from your engineering teams, and find ways to share and track the

latest information.

- Planned maintenance events can affect your availability. You can drill down to the affected services, regions, and details to show how an event will affect you and what you need to do. Most of these events occur without any impact to you and aren't shown here. In the rare case that a reboot is required, Service Health allows you to choose when to perform the maintenance to minimize the downtime.
- Health advisories are issues that require you to act to avoid service interruption, including service retirements and breaking changes. Health advisories are announced far in advance to allow you to plan.

6.3.4 Knowledge Check

1. You want to be alerted when new recommendations to improve your cloud environment are available. Which service will do this?

- A. Azure Advisor
- B. Azure Monitor
- C. Azure Service Health

2. Which service provides official outage root cause analyses (RCAs) for Azure incidents?

- A. Azure Advisor
- B. Azure Monitor
- C. Azure Service Health

3. Which service is a platform that powers Application Insights, monitoring for VMs, containers, and Kubernetes?

- A. Azure Advisor
- B. Azure Monitor
- C. Azure Service Health

Answers

1. **A.** Azure Advisor can alert you when new recommendations are available.
2. **C.** Azure Service Health provides incident history and RCAs to share

with your stakeholders.

3. **B.** Azure Monitor is the platform used by Application Insights.

Chapter 7: General security and network security features

Having a good security strategy is essential in today's digital world. Every application and service, whether on-premises or in the cloud, needs to be designed with security in mind. Security needs to happen at the application level, at the data level, and at the network level.

Learn about the various Azure services you can use to help ensure that your cloud resources are safe, secure, and trusted.

Security is a small word for a significant concept. There are so many factors to consider in order to protect your applications and your data. How does Azure help you protect workloads that you run in the cloud and in your on-premises datacenter?

Meet iCertify Traders



iCertify Traders is a fictitious home improvement retailer. It operates retail hardware stores across the globe and online.

iCertify Traders specializes in competitive pricing, fast shipping, and a large range of items. It's looking at cloud technologies to improve business operations and support growth into new markets. By moving to the cloud, the company plans to enhance its shopping experience to further differentiate itself from competitors.

How will iCertify Traders run securely in the cloud and in the datacenter?

iCertify Traders runs a mix of workloads on Azure and in its datacenter.

The company needs to ensure that all of its systems meet a minimum level of

security, and that its information is protected from attacks. The company also needs a way to collect and act on security events from across its digital estate.

Let's explore how iCertify Traders can use some of the tools and features in Azure as part of its overall security strategy.

7.1 Learning objectives

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

- Strengthen your security posture and protect against threats by using Azure Security Center.
- Collect and act on security data from many different sources by using Azure Sentinel.
- Store and access sensitive information such as passwords and encryption keys securely in Azure Key Vault.
- Manage dedicated physical servers to host your Azure VMs for Windows and Linux by using Azure Dedicated Host.

iCertify Traders is broadening its use of Azure services. It still has on-premises workloads with current security-related configuration best practices and business procedures. How does the company ensure that all of its systems meet a minimum level of security and that its information is protected from attacks?

Many Azure services include built-in security features. Tools on Azure can also help iCertify Traders with this requirement. Let's start by looking at Azure Security Center.

7.2 Azure Security Center

As your technology environment grows, how do you know that your resources are configured with security in mind and that they're not under attack?

Azure Security Center gives you one place to check security settings, identify potential security weaknesses, analyze inbound attacks, and more.

You can automatically apply any required security settings to new resources when they are created, monitor both your cloud and your on-premises workloads to ensure that they retain the correct security settings.

Azure Security Center provides you with recommendations on how to improve your security posture based on your current configurations, resources, and networks. Automatic security assessments identify potential weaknesses or vulnerabilities, so you can address them before they can be exploited.

And finally with Secure Score, you can see the impact of any improvements you make.

There are also control and monitoring capabilities for networks, files and virtual machines, opening network ports only when required, alerting you when important files change, and only allowing approved applications to be installed.

This includes machine learning detecting and blocking potential malware. And finally, Azure Security Center can detect potential inbound attacks, so you can investigate them further.

This can include logons from known malicious IP addresses, changes to registry keys, or suspicious commands or applications being run. Harden your networks, secure and monitor your resources, and improve your security posture with Azure Security Center.

Azure Security Center is a monitoring service that provides visibility of your security posture across all of your services, both on Azure and on-premises. The term security posture refers to cybersecurity policies and controls, as well as how well you can predict, prevent, and respond to security threats.

Security Center can:

- Monitor security settings across on-premises and cloud workloads.
- Automatically apply required security settings to new resources as they come online.
- Provide security recommendations that are based on your current configurations, resources, and networks.
- Continuously monitor your resources and perform automatic security assessments to identify potential vulnerabilities before those vulnerabilities can be exploited.
- Use machine learning to detect and block malware from being installed on your virtual machines (VMs) and other resources. You can also use adaptive application controls to define rules that list allowed applications to ensure that only applications you allow can run.
- Detect and analyze potential inbound attacks and investigate threats and any post-breach activity that might have occurred.
- Provide just-in-time access control for network ports. Doing so reduces your attack surface by ensuring that the network only allows traffic that you require at the time that you need it to.

This short video explains how the Security Center can help harden your networks, secure and monitor your cloud resources, and improve your overall security posture.

See the following example of what you might see in Azure Security Center.

Policy & compliance

Overall Secure Score



[Review your Secure Score >](#)

Regulatory compliance

PCI DSS 3.2.1	34 of 45 passed controls
Azure CIS 1.1.0	20 of 24 passed controls
SOC TSP	12 of 13 passed controls

Subscription coverage



Let's say that iCertify Traders must comply with the Payment Card Industry's Data Security Standard (PCI DSS). This report shows that the company has resources that it needs to remediate.

In the Resource security hygiene section, iCertify Traders can see the health of its resources from a security perspective. To help prioritize remediation actions, recommendations are categorized as low, medium, and high. Here's an example.

Resource security hygiene



Secure score is a measurement of an organization's security posture.

Overall Secure Score



Secure score is based on security controls, or groups of related security recommendations. Your score is based on the percentage of security controls that you satisfy. The more security controls you satisfy, the higher the score you receive. Your score improves when you remediate all of the recommendations for a single resource within a control.

Here's an example from the Azure portal showing a score of 57 percent, or 34 out of 60 points.

Following the secure score recommendations can help protect your organization from threats. From a centralized dashboard in Azure Security Center, organizations can monitor and work on the security of their Azure resources like identities, data, apps, devices, and infrastructure.

Secure score helps you:

- Report on the current state of your organization's security posture.
- Improve your security posture by providing discoverability, visibility, guidance, and control.
- Compare with benchmarks and establish key performance indicators (KPIs).

Security Center includes advanced cloud defense capabilities for VMs, network security, and file integrity. Let's look at how some of these capabilities apply to iCertify Traders.

- **Just-in-time VM access**

iCertify Traders will configure just-in-time access to VMs. This access blocks traffic by default to specific network ports of VMs, but allows traffic for a specified time when an admin requests and approves it.

- **Adaptive application controls**

iCertify Traders can control which applications are allowed to run on its

VMs. In the background, the Security Center uses machine learning to look at the processes running on a VM. It creates exception rules for each resource group that holds the VMs and provides recommendations. This process provides alerts that inform the company about unauthorized applications that are running on its VMs.

- **Adaptive network hardening**

Security Center can monitor the internet traffic patterns of the VMs, and compare those patterns with the company's current network security group (NSG) settings. From there, the Security Center can make recommendations about whether the NSGs should be locked down further and provide remediation steps.

- **File integrity monitoring**

iCertify Traders can also configure the monitoring of changes to important files on both Windows and Linux, registry settings, applications, and other aspects that might indicate a security attack.

Workflow automation uses Azure Logic Apps and Security Center connectors. The logic app can be triggered by a threat detection alert or by a Security Center recommendation, filtered by name or by severity. You can then configure the logic app to run an action, such as sending an email, or posting a message to a Microsoft Teams channel.

7.3 Azure Sentinel

Security management on a large scale can benefit from a dedicated security information and event management (SIEM) system. A SIEM system aggregates security data from many different sources (as long as those sources support an open-standard logging format). It also provides capabilities for threat detection and response.

Azure Sentinel is Microsoft's cloud-based SIEM system. It uses intelligent security analytics and threat analysis.

Azure Sentinel enables you to:

- **Collect cloud data at scale :** Collect data across all users, devices, applications, and infrastructure, both on-premises and from multiple clouds.
- **Detect previously undetected threats :** Minimize false positives by using Microsoft's comprehensive analytics and threat intelligence.
- **Investigate threats with artificial intelligence :** Examine suspicious activities at scale, tapping into years of cybersecurity experience from Microsoft.
- **Respond to incidents rapidly :** Use built-in orchestration and automation of common tasks.

Azure Sentinel supports a number of data sources, which it can analyze for security events. These connections are handled by built-in connectors or industry-standard log formats and APIs.

- Connect Microsoft solutions

Connectors provide real-time integration for services like Microsoft Threat Protection solutions, Microsoft 365 sources (including Office 365), Azure Active Directory, and Windows Defender Firewall.

- Connect other services and solutions

Connectors are available for common non-Microsoft services and solutions, including AWS CloudTrail, Citrix Analytics (Security), Sophos XG Firewall,

VMware Carbon Black Cloud, and Okta SSO.

- Connect industry-standard data sources

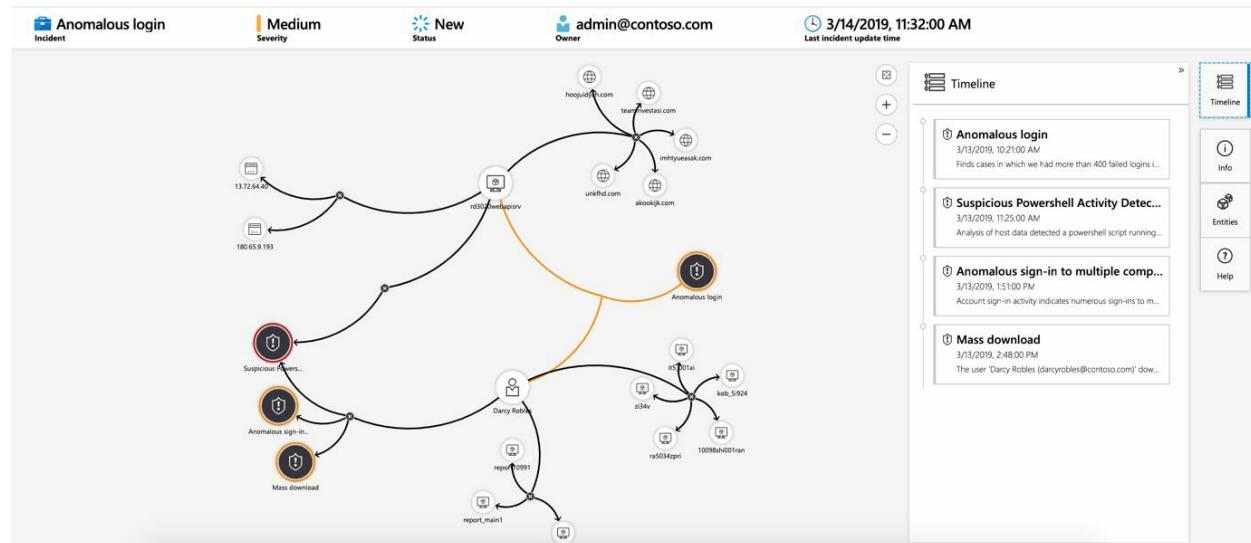
Azure Sentinel supports data from other sources that use the Common Event Format (CEF) messaging standard, Syslog, or REST API.

Built-in analytics use templates designed by Microsoft's team of security experts and analysts based on known threats, common attack vectors, and escalation chains for suspicious activity. These templates can be customized and search across the environment for any activity that looks suspicious. Some templates use machine learning behavioral analytics that are based on Microsoft proprietary algorithms.

Custom analytics are rules that you create to search for specific criteria within your environment. You can preview the number of results that the query would generate (based on past log events) and set a schedule for the query to run. You can also set an alert threshold.

When Azure Sentinel detects suspicious events, they provide an interactive graph. With the investigation graph, the company can review information from entities directly connected to the alert, and see common exploration queries to help guide the investigation.

Here's an example that shows what an investigation graph looks like in Azure Sentinel.



The company will also use Azure Monitor Workbooks to automate responses to threats. For example, it can set an alert that looks for malicious IP

addresses that access the network and create a workbook that does the following steps:

1. When the alert is triggered, open a ticket in the IT ticketing system.
2. Send a message to the security operations channel in Microsoft Teams or Slack to make sure the security analysts are aware of the incident.
3. Send all of the information in the alert to the senior network admin and to the security admin. The email message includes two user option buttons: **Block** or **Ignore**.

When an admin chooses **Block**, the IP address is blocked in the firewall, and the user is disabled in Azure Active Directory. When an admin chooses **Ignore**, the alert is closed in Azure Sentinel, and the incident is closed in the IT ticketing system.

The workbook continues to run after it receives a response from the admins. Workbooks can be run manually or automatically when a rule triggers an alert.



7.3 Azure Key Vault

As iCertify Traders builds its workloads in the cloud, it needs to carefully handle sensitive information such as passwords, encryption keys, and certificates. This information needs to be available for an application to function, but it might allow an unauthorized person access to application data.

Azure Key Vault is a centralized cloud service for storing an application's secrets in a single, central location. It provides secure access to sensitive information by providing access control and logging capabilities.

What can Azure Key Vault do?

Azure Key Vault can help you do the following:

- **Manage secrets**

You can use Key Vault to securely store and tightly control access to tokens, passwords, certificates, API keys, and other secrets.

- **Manage encryption keys**

You can use Key Vault as a key management solution. Key Vault makes it easier to create and control the encryption keys that are used to encrypt your data.

- **Manage SSL/TLS certificates**

Key Vault enables you to provision, manage, and deploy your public and private Secure Sockets Layer/Transport Layer Security (SSL/TLS) certificates for both your Azure resources and your internal resources.

- **Store secrets backed by hardware security modules (HSMs)**

These secrets and keys can be protected either by software or by FIPS 140-2 Level 2 validated HSMs.

Here's an example that shows a certificate used for testing in Key Vault.

The screenshot shows the 'Certificates' blade for a Key Vault named 'keyvaulttest6876'. The left sidebar includes links for Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, and Events (preview). The main area has a search bar and buttons for Generate/Import, Refresh, Restore Backup, and Certificate Contacts. A table lists certificates, showing one entry: 'TestCACert' with thumbprint '88D24EFCF38AE6ACDA8B...' and status 'Enabled'. A note below the table states 'In progress, failed or cancelled' and 'There are no certificates available.'

Name	Thumbprint	Status
Completed		
TestCACert	88D24EFCF38AE6ACDA8B...	✓ Enabled
In progress, failed or cancelled		
There are no certificates available.		

You'll add a secret to Key Vault later in this module.

What are the benefits of Azure Key Vault?

The benefits of using Key Vault include:

- Centralized application secrets

Centralizing the storage for your application secrets enables you to control their distribution, and reduces the chances that secrets are accidentally leaked.

- Securely stored secrets and keys

Azure uses industry-standard algorithms, key lengths, and HSMs. Access to Key Vault requires proper authentication and authorization.

- Access monitoring and access control

By using Key Vault, you can monitor and control access to your application secrets.

- Simplified administration of application secrets

Key Vault makes it easier to enroll and renew certificates from public certificate authorities (CAs). You can also scale up and replicate content within regions and use standard certificate management tools.

- Integration with other Azure services

You can integrate Key Vault with storage accounts, container registries, event hubs, and many more Azure services. These services can then securely reference the secrets stored in Key Vault.

Exercise - Manage a password in Azure Key Vault

In this exercise, you add a password to Azure Key Vault. A password is an example of sensitive information that you need to protect. You then read the password from Azure Key Vault to verify that the password is accessible.

In practice, there are several ways to add secrets to and read secrets from Key Vault. You can use the Azure portal, the Azure CLI, or Azure PowerShell. By using your favorite programming language, your applications can also securely access the secrets that they need.

Here, you create a secret in Key Vault by using the Azure portal. You then access the secret from the portal and from the Azure CLI in Azure Cloud Shell.

The Azure CLI is a way to work with Azure resources from the command line or from scripts. Cloud Shell is a browser-based shell experience to manage and develop Azure resources. Think of Cloud Shell as an interactive console that runs in the cloud.

Create a key vault

1. Go to the [Azure portal](#).
2. On the Azure portal menu, or from the Home page, select **Create a resource**.
3. From the search bar, enter **Key Vault**, and then select **Key Vault** from the results.
4. On the Key Vault pane, select **Create**. The Create key vault pane appears.
5. On the Basics tab, fill in the following values for each setting.

Note: Replace NNN with a series of numbers. This helps ensure that the name of your key vault is unique.

Setting	Value
Project details	
Subscription	Concierge Subscription
Resource group	[sandbox resource group name]
Instance details	
Key vault name	my-keyvault-NNN

Leave the other settings at their default values.

6. Select **Review + create**, and after passing validation, then select **Create**.

Wait for deployment to successfully complete.

7. Select **Go to resource**.
8. Note some of the details about your key vault.

For example, the **Vault URI field** shows the URI that your application can use to access your vault from the REST API.

Here's an example for a key vault that's named my-keyvault-321:

Resource group (change)	:	learn-dd96fca3-1b5f-462a-ae0a-0a12fc1d167a	Vault URI	:	https://my-keyvault-321.vault.azure.net/
Location	:	East US	Sku (Pricing tier)	:	Standard
Subscription (change)	:	Concierge Subscription	Directory ID	:	604c1504-c6a3-4080-81aa-b33091104187
Subscription ID	:	18974119-7a45-4077-9932-f95c83cee0e3	Directory Name	:	Microsoft Learn Sandbox
			Soft-delete	:	Enabled
			Purge protection	:	Disabled

Tags ([change](#)) : [Click here to add tags](#)

- As an optional step, on the left menu pane, under Settings, examine some of the other features.

Although they're initially empty, here you'll find places where you can store keys, secrets, and certificates.

Note: Your Azure subscription is the only one that's authorized to access this vault. Under Settings, the Access policies feature enables you to configure access to the vault.

Add a password to the key vault

1. On the left menu pane, under **Settings**, select **Secrets**. Your key vault pane appears.
2. From the top menu bar, select **Generate/Import**. The Create a secret pane appears.
3. Fill in the following values for each setting.

Setting	Value
Upload options	Manual
Name	MyPassword
Value	hVFkk96

Leave the other settings at their default values. Notice that you can specify properties such as the activation date and the expiration date. You can also disable access to the secret.

4. Select **Create**.

Show the password

Here, you access the password from Key Vault two times. First, you access it from the Azure portal. Next, you access it from the Azure CLI.

1. From your Key Vault/Secrets pane, select **MyPassword**. The MyPassword/Versions pane appears. You see that the current version is enabled.
2. Select the **current version**. The Secret Version pane appears. Under Secret Identifier, you see a URI that you can now use with applications to access the secret. Remember, only authorized applications can access this secret.
3. Select **Show Secret Value**.

A screenshot of the Azure portal interface. A modal window is open, showing the 'Secret value' for a secret named 'MyPassword'. The value 'hVFkk96' is displayed in a text input field. To the right of the input field is a blue 'Copy' button with a clipboard icon.

4. From Cloud Shell, run this command.

Note: Replace <my-keyvault-NNN> with the name you used earlier.

A screenshot of the Azure Cloud Shell. The command entered is:
az keyvault secret show \
--name MyPassword \
--vault-name <my-keyvault-NNN> \
--query value \
--output tsv

You see the password in the output.

A screenshot of the Azure Cloud Shell showing the output of the previous command. The output is:
hVFkk96

Good work! At this point, you have a key vault that contains a password secret that's securely stored for use with your applications.

Clean up

The sandbox automatically cleans up your resources when you're finished with this module.

When you're working on your own subscription, it's a good idea at the end of a project to identify whether you still need the resources you created. Resources left running can cost you money. You can delete resources individually or delete the resource group to delete the entire set of resources.

7.4 Azure Dedicated Host

On Azure, virtual machines (VMs) run on shared hardware that Microsoft manages. Although the underlying hardware is shared, your VM workloads are isolated from workloads that other Azure customers run.

Some organizations must follow regulatory compliance that requires them to be the only customer using the physical machine that hosts their virtual machines. Azure Dedicated Host provides dedicated physical servers to host your Azure VMs for Windows and Linux.

Here's a diagram that shows how VMs relate to dedicated hosts and host groups. A dedicated host is mapped to a physical server in an Azure datacenter. A host group is a collection of dedicated hosts.



What are the benefits of Azure Dedicated Host?

Azure Dedicated Host:

- Gives you visibility into, and control over, the server infrastructure that's running your Azure VMs.
- Helps address compliance requirements by deploying your workloads on an isolated server.
- Lets you choose the number of processors, server capabilities, VM series, and VM sizes within the same host.

Availability considerations for Dedicated Host

After a dedicated host is provisioned, Azure assigns it to the physical server in Microsoft's cloud datacenter.

For high availability, you can provision multiple hosts in a host group, and deploy your VMs across this group. VMs on dedicated hosts can also take

advantage of maintenance control. This feature enables you to control when regular maintenance updates occur, within a 35-day rolling window.

Pricing considerations

You're charged per dedicated host, independent of how many VMs you deploy to it. The host price is based on the VM family, type (hardware size), and region.

Software licensing, storage, and network usage are billed separately from the host and VMs. For more information, see [Azure Dedicated Host pricing](#).

Knowledge check

Consider the following scenario. Then choose the best response for each question that follows. Then, select Check your answers.

iCertify Traders is moving its online payment system from its datacenter to the cloud. The payment system consists of virtual machines (VMs) and SQL Server databases.

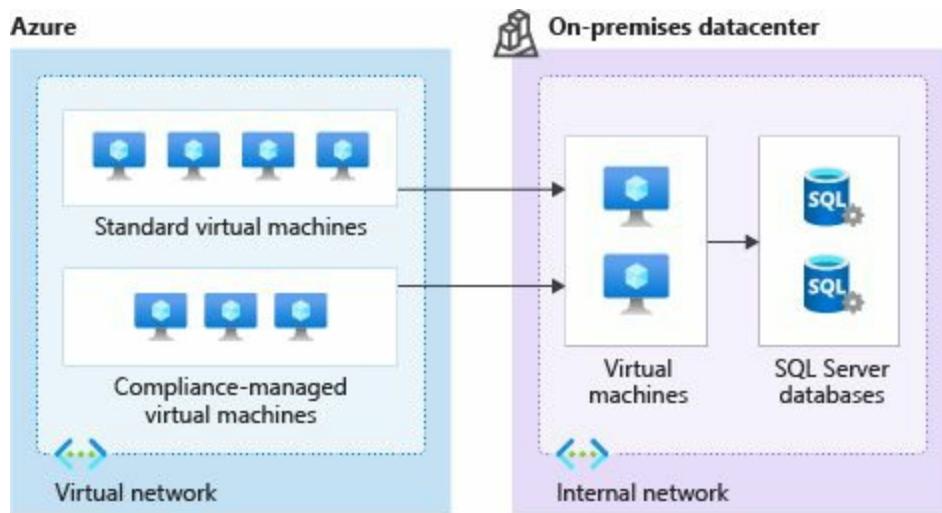
Here are a few security requirements that the company identifies as it plans the migration:

- It wants to ensure a good security posture across all of its systems, both on Azure and on-premises.
- In the datacenter, access to VMs requires a TLS certificate. The company needs a place to safely store and manage its certificates.

Here are some additional requirements that relate to regulatory compliance:

- iCertify Traders must store certain customer data on-premises, in its datacenter.
- For certain workloads, the company must be the only customer running VMs on the physical hardware.
- The company must only run approved business applications on each VM.

See the following diagram that shows the proposed architecture.



On Azure, iCertify Traders will use both standard VMs and VMs that run on dedicated physical hardware. In the datacenter, the company will run VMs that can connect to databases within its internal network.

1. How can iCertify Traders enforce having only certain applications run on its VMs?

1. Connect your VMs to Azure Sentinel.
2. Create an application control rule in Azure Security Center.
3. Periodically run a script that lists the running processes on each VM. The IT manager can then shut down any applications that shouldn't be running.

2. What's the easiest way for iCertify Traders to combine security data from all of its monitoring tools into a single report that it can take action on?

1. Collect security data in Azure Sentinel.
2. Build a custom tool that collects security data, and displays a report through a web application.
3. Look through each security log daily and email a summary to your team.

3. Which is the best way for iCertify Traders to safely store its certificates so that they're accessible to cloud VMs?

1. Place the certificates on a network share.

2. Store them on a VM that's protected by a password.
3. Store the certificates in Azure Key Vault.

4. How can iCertify Traders ensure that certain VM workloads are physically isolated from workloads being run by other Azure customers?

1. Configure the network to ensure that VMs on the same physical host are isolated.
2. This is not possible. These workloads need to be run on-premises.
3. Run the VMs on Azure Dedicated Host.

Answer:

1. **Answer: B.** With Azure Security Center, you can define a list of allowed applications to ensure that only applications you allow can run. Azure Security Center can also detect and block malware from being installed on your VMs.
2. **Answer: A.** Azure Sentinel is Microsoft's cloud-based SIEM. A SIEM aggregates security data from many different sources to provide additional capabilities for threat detection and responding to threats.
3. **Answer: C.** Azure Key Vault enables you to store your secrets in a single, central location. Key Vault also makes it easier to enroll and renew certificates from public certificate authorities (CAs).
4. **Answer: C.** Azure Dedicated Host provides dedicated physical servers to host your Azure VMs for Windows and Linux.

Summary

Azure provides tools and services that can help you detect and act on important security events. It also provides ways to help keep your data safe, which can prevent security incidents from happening to begin with.

In this module, you learned about Azure services that relate to security. Here's a brief summary:

- Azure Security Center provides visibility of your security posture across all of your services, both on Azure and on-premises.
- Azure Sentinel aggregates security data from many different sources, and provides additional capabilities for threat detection and response.
- Azure Key Vault stores your applications' secrets, such as passwords, encryption keys, and certificates, in a single, central location.
- Azure Dedicated Host provides dedicated physical servers to host your Azure VMs for Windows and Linux.

Chapter 8 : Identity, governance, privacy, and compliance features

If you're an IT pro, a risk manager, or a business decision maker the Identity, Governance, Privacy, and Compliance Features are an important aspect to understand and assimilate for your Au Fundamentals certification

With the rise of remote work, bring your own device (BYOD), mobile applications, and cloud applications, the primary security boundary has shifted from firewalls and physical access controls to identity.

Understanding who is using your systems and what they have permission to do are critical to keeping your data safe from attackers. To stay organized, manage costs, and meet your compliance goals, you need a good cloud governance strategy.

Learn how Azure can help you secure access to cloud resources, what it means to build a cloud governance strategy, and how Azure adheres to common regulatory and compliance standards.

First, we'll start with Identity, that important access plane. You'll learn about Azure Active Directory and how things like conditional access and multi-factor authentication work together to block against risky access attempts.

Then, you'll look at building a cloud Governance strategy on Azure - controlling how resources are created and configured. You'll explore resource tags, and resource locks, and learn how to enforce your corporate standards with Azure policy and Azure blueprints. Finally, we'll look at Privacy, Compliance and Data Protection Standards.

This is important for understanding how Azure adheres to industry and government regulations.

You'll learn about the online services terms, the data protection addendum and how to find the Azure compliance documentation for the Azure services that you're using.

By the end of this learning path, you'll understand your options for securing access to Azure, controlling your Azure resources and staying compliant with

your industry and government regulations.

Traditionally, protecting access to systems and data involved the on-premises network perimeter and physical access controls.

With people increasingly able to work from anywhere, plus the rise of bring your own device (BYOD) strategies, mobile applications, and cloud applications, many of those access points are now outside the company's physical networks.

Identity has become the new primary security boundary. Accurately proving that someone is a valid user of your system, with an appropriate level of access, is critical to maintaining control of your data. This identity layer is now more often the target of attack than the network is.

Meet iCertify Traders

iCertify Traders is a fictitious home improvement retailer. It operates retail hardware stores across the globe and online.



iCertify Traders specializes in competitive pricing, fast shipping, and a large range of items. It's looking at cloud technologies to improve business operations and support growth into new markets. By moving to the cloud, the company plans to enhance its shopping experience to further differentiate itself from competitors.

How will iCertify Traders secure access to its cloud applications?

The mobile workforce of iCertify Traders is increasing, as are the number of applications that the company runs in the cloud.

Retail employees located around the world are issued tablet devices from which they can create orders for customers, track delivery schedules, and plan their work schedules.

Delivery drivers can use their own mobile devices to access scheduling and logistics applications. Some delivery drivers are permanent employees of iCertify Traders. Others work on short-term contracts.

iCertify Traders uses Active Directory to secure its on-premises environment. It needs to ensure that only employees can sign in and access the company's business applications. It also needs to ensure that short-term staff can access these applications only when they're under active contract.

How can Azure Active Directory (Azure AD) help iCertify Traders consistently secure all of its applications accessed from the intranet and from public networks?

Learning objectives

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

- Explain the difference between authentication and authorization.
- Describe how Azure AD provides identity and access management.
- Explain the role that single sign-on (SSO), multifactor authentication, and Conditional Access play in managing user identity.

8.1 Authentication vs Authorization

Recall that iCertify Traders must ensure that only employees can sign in and access its business applications. iCertify Traders also needs to ensure that employees can access only authorized applications. For example, all employees can access inventory and pricing software, but only store managers can access payroll and certain accounting software. Two fundamental concepts that you need to understand when talking about identity and access are authentication (AuthN) and authorization (AuthZ). Authentication and authorization both support everything else that happens. They occur sequentially in the identity and access process.

8.1.1 What is authentication?

Authentication is the process of establishing the identity of a person or service that wants to access a resource. It involves the act of challenging a party for legitimate credentials and provides the basis for creating a security principle for identity and access control. It establishes whether the user is who they say they are.

Authentication establishes the user's identity, but authorization is the process of establishing what level of access an authenticated person or service has. It specifies what data they're allowed to access and what they can do with it.

8.1.2 What is authorization?

Authentication establishes the user's identity, but authorization is the process of establishing what level of access an authenticated person or service has. It specifies what data they're allowed to access and what they can do with it.

8.1.3 How are authentication and authorization related?

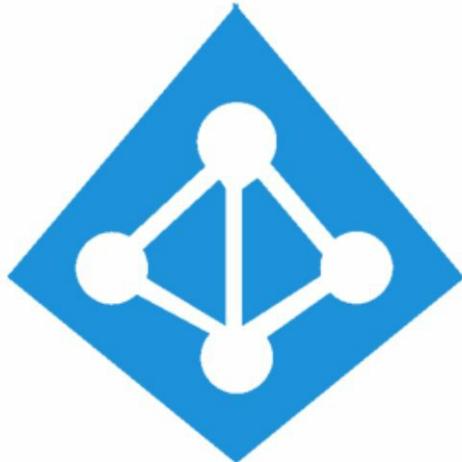
Here's a diagram that shows the relationship between authentication and authorization:



The identification card represents credentials that the user has to prove their identity (you'll learn more about the types of credentials later in this module.) Once authenticated, authorization defines what kinds of applications, resources, and data that user can access.

8.2 Azure Active Directory

In this part, you learn how Azure Active Directory (Azure AD) provides identity services that enable your users to sign in and access both Microsoft cloud applications and cloud applications that you develop. You also learn how Azure AD supports single sign-on (SSO).



iCertify Traders already uses Active Directory to secure its on-premises environments. The company doesn't want its users to have a different username and password to remember for accessing applications and data in the cloud. Can the company integrate its existing Active Directory instance with cloud identity services to create a seamless experience for its users?

Let's start with how Azure AD compares to Active Directory.

8.2.1 Azure AD vs. Active Directory?

Active Directory is related to Azure AD, but they have some key differences.

Microsoft introduced Active Directory in Windows 2000 to give organizations the ability to manage multiple on-premises infrastructure components and systems by using a single identity per user.

For on-premises environments, Active Directory running on Windows Server provides an identity and access management service that's managed by your own organization. Azure AD is Microsoft's cloud-based identity and access management service. With Azure AD, you control the identity accounts, but Microsoft ensures that the service is available globally. If you've worked with

Active Directory, Azure AD will be familiar to you.

When you secure identities on-premises with Active Directory, Microsoft doesn't monitor sign-in attempts. When you connect Active Directory with Azure AD, Microsoft can help protect you by detecting suspicious sign-in attempts at no extra cost. For example, Azure AD can detect sign-in attempts from unexpected locations or unknown devices.

Who uses Azure AD?

Azure AD is for:

- **IT administrators** : Administrators can use Azure AD to control access to applications and resources based on their business requirements.
- **App developers** : Developers can use Azure AD to provide a standards-based approach for adding functionality to applications that they build, such as adding SSO functionality to an app or enabling an app to work with a user's existing credentials.
- **Users** : Users can manage their identities. For example, self-service password reset enables users to change or reset their password with no involvement from an IT administrator or help desk.
- **Online service subscribers** : Microsoft 365, Microsoft Office 365, Azure, and Microsoft Dynamics CRM Online subscribers are already using Azure AD.

A tenant is a representation of an organization. A tenant is typically separated from other tenants and has its own identity.

Each Microsoft 365, Office 365, Azure, and Dynamics CRM Online tenant is automatically an Azure AD tenant.

Here's a screenshot of what an IT administrator might see in the Azure portal when working with Active Directory:

The screenshot shows the Azure Active Directory (Azure AD) Overview page for the tenant 'Tailwind Traders'. The left sidebar includes links for Overview, Getting started, Preview hub, Diagnose and solve problems, Manage (with sub-links for Users, Groups, External Identities, Roles and administrators, Administrative units, Enterprise applications, and Devices), and a 'Switch tenant' button. The main content area features a search bar and two large cards: 'Tenant information' (showing Your role as User, License as Azure AD Premium P2, Tenant ID as 00000000-0000-0000-0000-000000000000, and Primary domain as tailwindtraders.onmicrosoft.com) and 'Azure AD Connect' (showing Status as Enabled and Last sync as Less than 1 hour ago).

What services does Azure AD provide?

Azure AD provides services such as:

- **Authentication** : This includes verifying identity to access applications and resources. It also includes providing functionality such as self-service password reset, multi factor authentication, a custom list of banned passwords, and smart lockout services.
- **Single sign-on** : SSO enables you to remember only one username and one password to access multiple applications. A single identity is tied to a user, which simplifies the security model. As users change roles or leave an organization, access modifications are tied to that identity, which greatly reduces the effort needed to change or disable accounts.
- **Application management** : You can manage your cloud and on-premises apps by using Azure AD. Features like Application Proxy, SaaS apps, the My Apps portal (also called the access panel), and single-sign on provide a better user experience.
- **Device management** : Along with accounts for individual people, Azure AD supports the registration of devices. Registration enables devices to be managed through tools like Microsoft Intune. It also allows for device-based conditional access policies to restrict access attempts to only those coming from known devices, regardless of the

requesting user account.

What kinds of resources can Azure AD help secure?

Azure AD helps users access both external and internal resources.

External resources might include Microsoft Office 365, the Azure portal, and thousands of other software as a service (SaaS) applications.

Internal resources might include apps on your corporate network and intranet, along with any cloud applications developed within your organization.

What's a single sign-on?

Single sign-on enables a user to sign in one time and use that credential to access multiple resources and applications from different providers.

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

Consider the process of managing all those identities. Additional strain is placed on help desks as they deal with account lockouts and password reset requests. If a user leaves an organization, tracking down all those identities and ensuring they are disabled can be challenging. If an identity is overlooked, this might allow access when it should have been eliminated.

With SSO, you need to remember only one ID and one password. Access across applications is granted to a single identity that's tied to the user, which simplifies the security model. As users change roles or leave an organization, access is tied to a single identity. This change greatly reduces the effort needed to change or disable accounts. Using SSO for accounts makes it easier for users to manage their identities and increases your security capabilities.

You'll find resources at the end of this module about how to enable SSO through Azure AD.

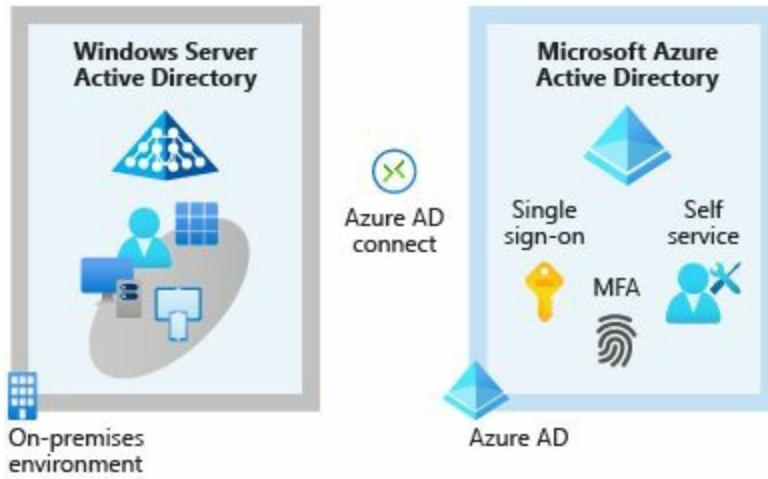
How can I connect Active Directory with Azure AD?

Connecting Active Directory with Azure AD enables you to provide a consistent identity experience to your users.

There are a few ways to connect your existing Active Directory installation with Azure AD. Perhaps the most popular method is to use Azure AD Connect.

Azure AD Connect synchronizes user identities between on-premises Active Directory and Azure AD. Azure AD Connect synchronizes changes between both identity systems, so you can use features like SSO, multi factor authentication, and self-service password reset under both systems. Self-service password reset prevents users from using known compromised passwords.

Here's a diagram that shows how Azure AD Connect fits between on-premises Active Directory and Azure AD:



As iCertify Traders integrates its existing Active Directory instance with Azure AD, it creates a consistent access model across its organization. Doing so greatly simplifies its ability to sign in to different applications, manage changes to user identities and control, and monitor and block unusual access attempts.

8.3 Multifactor authentication and Conditional Access

iCertify Traders allows delivery drivers to use their own mobile devices to access scheduling and logistics applications. Some delivery drivers are permanent employees of iCertify Traders. Others work on short-term contracts. How can the IT department ensure that an access attempt is really from a valid iCertify Traders worker?

In this part, you'll learn about two processes that enable secure authentication: Azure AD Multi-Factor Authentication and Conditional Access. Let's start with a brief look at what multifactor authentication is in general.

What's multifactor authentication?

Multifactor authentication is a process where a user is prompted during the sign-in process for an additional form of identification. Examples include a code on their mobile phone or a fingerprint scan.

Think about how you sign in to websites, email, or online gaming services. In addition to your username and password, have you ever needed to enter a code that was sent to your phone? If so, you've used multifactor authentication to sign in.

Multifactor authentication provides additional security for your identities by requiring two or more elements to fully authenticate. These elements fall into three categories:

- **Something the user knows** : This might be an email address and password.
- **Something the user has** : This might be a code that's sent to the user's mobile phone.
- **Something the user is** : This is typically some sort of biometric property, such as a fingerprint or face scan that's used on many mobile devices.



Multi Factor authentication increases identity security by limiting the impact of credential exposure (for example, stolen usernames and passwords). With multi factor authentication enabled, an attacker who has a user's password would also need to have possession of their phone or their fingerprint to fully authenticate.

Compare multi factor authentication with single-factor authentication. Under single-factor authentication, an attacker would need only a username and password to authenticate. Multifactor authentication should be enabled wherever possible because it adds enormous benefits to security.

What's Azure AD Multi-Factor Authentication?

Azure AD Multi-Factor Authentication is a Microsoft service that provides multi factor authentication capabilities. Azure AD Multi-Factor Authentication enables users to choose an additional form of authentication during sign-in, such as a phone call or mobile app notification.

These services provide Azure AD Multi-Factor Authentication capabilities:

- **Azure Active Directory** : The Azure Active Directory free edition enables Azure AD Multi-Factor Authentication for administrators with the global admin level of access, via the Microsoft Authenticator app, phone call, or SMS code. You can also enforce Azure AD Multi-Factor Authentication for all users via the Microsoft Authenticator app only, by enabling security defaults in your Azure AD tenant.

Azure Active Directory Premium (P1 or P2 licenses) allows for comprehensive and granular configuration of Azure AD Multi-Factor Authentication through Conditional Access policies (explained shortly).

- **Multi Factor authentication for Office 365** : A subset of Azure AD

Multi-Factor Authentication capabilities is part of your Office 365 subscription.

For more information on licenses and Azure AD Multi-Factor Authentication capabilities, see Available versions of Azure AD Multi-Factor Authentication.

What's Conditional Access?

Conditional Access is a tool that Azure Active Directory uses to allow (or deny) access to resources based on identity signals. These signals include who the user is, where the user is, and what device the user is requesting access from.

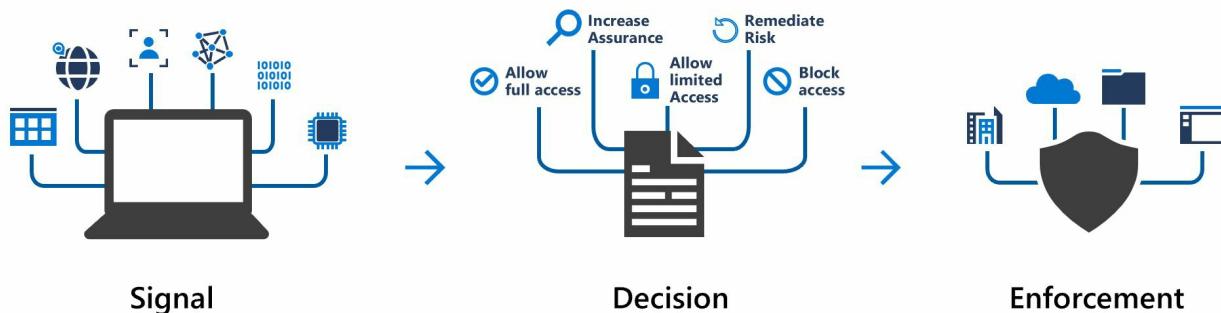
Conditional Access helps IT administrators:

- Empower users to be productive wherever and whenever.
- Protect the organization's assets.

Conditional Access also provides a more granular multifactor authentication experience for users. For example, a user might not be challenged for a second authentication factor if they're at a known location. However, they might be challenged for a second authentication factor if their sign-in signals are unusual or they're at an unexpected location.

During sign-in, Conditional Access collects signals from the user, makes decisions based on those signals, and then enforces that decision by allowing or denying the access request or challenging for a multifactor authentication response.

Here's a diagram that illustrates this flow:



Here, the signal might be the user's location, the user's device, or the application that the user is trying to access.

Based on these signals, the decision might be to allow full access if the user is signing in from their usual location. If the user is signing in from an unusual location or a location that's marked as high risk, then access might be blocked entirely or possibly granted after the user provides a second form of authentication.

Enforcement is the action that carries out the decision. For example, the action is to allow access or require the user to provide a second form of authentication.

When can I use Conditional Access?

Conditional Access is useful when you need to:

- **Require multi factor authentication to access an application :** You can configure whether all users require multi factor authentication or only certain users, such as administrators.

You can also configure whether multifactor authentication applies to access from all networks or only untrusted networks.

- **Require access to services only through approved client applications** : For example, you might want to allow users to access Office 365 services from a mobile device as long as they use approved client apps, like the Outlook mobile app.
- **Require users to access your application only from managed devices** : A managed device is a device that meets your standards for security and compliance.
- **Block access from untrusted sources, such as access from unknown or unexpected locations** : Conditional Access comes with a What If tool, which helps you plan and troubleshoot your Conditional Access policies. You can use this tool to model your proposed Conditional Access policies across recent sign-in attempts from your users to see what the impact would have been if those policies had been enabled. The What If tool enables you to test your proposed Conditional Access policies before you implement them.

8.4 Knowledge check

Consider the following scenario. Then choose the best response for each question that follows.

At iCertify Traders, recall that retail employees are issued tablet devices from which they can track orders and plan their work schedules.

iCertify Traders also allows delivery drivers to use their own mobile devices to access scheduling and logistics applications.

A stolen password might allow unauthorized access to company and customer data. iCertify Traders wants to extend its investments in Active Directory to secure all of its applications, when accessed both from the intranet and from public networks.

The company is looking into how Azure Active Directory (Azure AD), single sign-on (SSO), multi factor authentication, and Conditional Access can help it achieve those goals.

1. How can the IT department ensure that employees at the company's retail stores can access company applications only from approved tablet devices?

- A. SSO
- B. Conditional Access
- C. Multi Factor authentication

2. How can the IT department use biometric properties, such as facial recognition, to enable delivery drivers to prove their identities?

- A. SSO
- B. Conditional Access
- C. Multi Factor authentication

3. How can the IT department reduce the number of times users must authenticate to access multiple applications?

- A. SSO
- B. Conditional Access
- C. Multi Factor authentication

Answers:

1. Answer: B. Conditional Access enables you to require users to access your applications only from approved, or managed, devices.
2. Answer: C. Authenticating through multi factor authentication can include something the user knows, something the user has, and something the user is.
3. Answer: A. SSO enables a user to remember only one ID and one password to access multiple applications.

Summary

iCertify Traders needs to ensure that only its workforce can access its growing set of cloud applications, both from any location and from any device.



In building out its plan, iCertify Traders learns that:

- Authentication (AuthN) establishes the user's identity.
- Authorization (AuthZ) establishes the level of access that an authenticated user has.
- Single sign-on (SSO) enables a user to sign in one time and use that credential to access multiple resources and applications.
- Azure Active Directory (Azure AD) is a cloud-based identity and access management service. Azure AD enables an organization to control access to apps and resources based on its business requirements.
- Azure AD Multi-Factor Authentication provides additional security for identities by requiring two or more elements to fully authenticate. In general, multi factor authentication can include something the user knows, something the user has, and something the user is.
- Conditional Access is a tool that Azure AD uses to allow or deny access to resources based on identity signals such as the user's location.

With these ideas in place, the software development and IT administrator teams can begin to replace their existing authentication systems with ones that use multiple factors and allow access to multiple applications.

8.5 Cloud governance strategy on Azure

Learn how access policies, resource locks, and tags, as well as Azure services such as Azure Policy and Azure Blueprints, can help you build a comprehensive cloud governance strategy.

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

- Make organizational decisions about your cloud environment by using the Cloud Adoption Framework for Azure.
- Define who can access cloud resources by using Azure role-based access control.
- Apply a resource lock to prevent accidental deletion of your Azure resources.
- Apply tags to your Azure resources to help describe their purpose.
- Control and audit how your resources are created by using Azure Policy.
- Enable governance at scale across multiple Azure subscriptions by using Azure Blueprints.

The [Cloud Adoption Framework for Azure](#) provides you with proven guidance to help with your cloud adoption journey. The Cloud Adoption Framework helps you create and implement the business and technology strategies needed to succeed in the cloud.

iCertify Traders needs to control its cloud environment so that it complies with several industry standards, but it's not sure where to start. It has existing business requirements, and it understands how these requirements relate to its on-premises workloads. These requirements also must be met by any workloads it runs in the cloud.

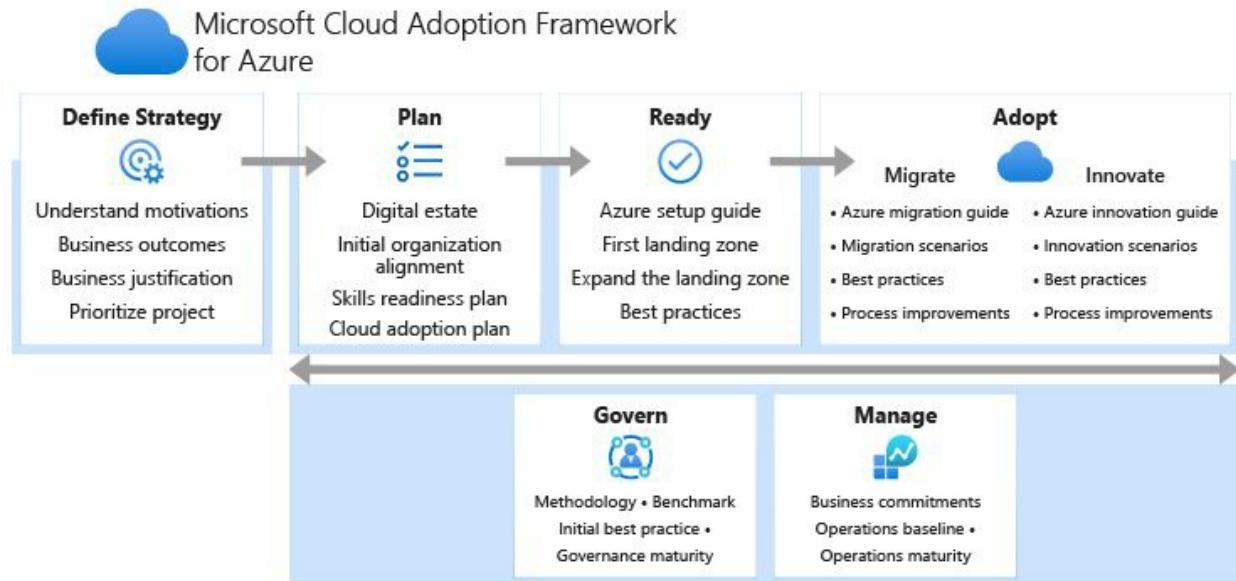
You've been tasked with investigating what's available on Azure and to define and implement the governance strategy for iCertify Traders. You decide to start with the Cloud Adoption Framework.

What's in the Cloud Adoption Framework?

The Cloud Adoption Framework consists of tools, documentation, and proven practices. The Cloud Adoption Framework includes these stages:

1. Define your strategy.
2. Make a plan.

3. Ready your organization.
4. Adopt the cloud.
5. Govern and manage your cloud environments.



The govern stage focuses on cloud governance. You can refer back to the Cloud Adoption Framework for recommended guidance as you build your cloud governance strategy.

8.5.1 Role Based Access Control

When you have multiple IT and engineering teams, how can you control what access they have to the resources in your cloud environment? It's a good security practice to grant users only the rights they need to perform their job, and only to the relevant resources.

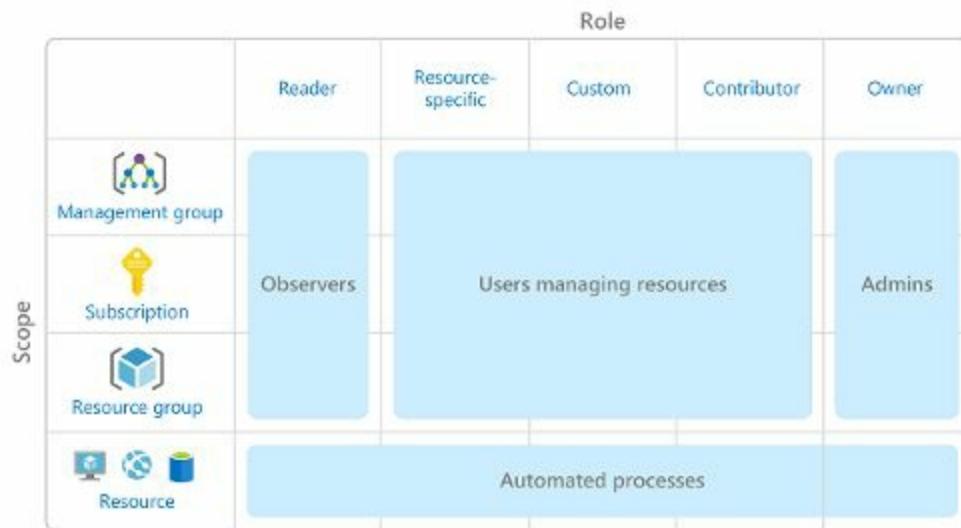
Instead of defining the detailed access requirements for each individual, and then updating access requirements when new resources are created, Azure enables you to control access through [Azure role-based access control](#) (Azure RBAC).

Azure provides built-in roles that describe common access rules for cloud resources. You can also define your own roles. Each role has an associated set of access permissions that relate to that role. When you assign individuals or groups to one or more roles, they receive all of the associated access permissions.

How is role-based access control applied to resources?

Role-based access control is applied to a scope, which is a resource or set of resources that this access applies to.

Here's a diagram that shows the relationship between roles and scopes.



Scopes include:

- A management group (a collection of multiple subscriptions).
- A single subscription.
- A resource group.
- A single resource.

Observers, Users managing resources, Admins, and Automated processes illustrate the kinds of users or accounts that would typically be assigned each of the various roles.

When you grant access at a parent scope, those permissions are inherited by all child scopes. For example:

- When you assign the [Owner](#) role to a user at the management group scope, that user can manage everything in all subscriptions within the management group.
- When you assign the [Reader](#) role to a group at the subscription scope, the members of that group can view every resource group and resource within the subscription.
- When you assign the [Contributor](#) role to an application at the resource

group scope, the application can manage resources of all types within that resource group, but not other resource groups within the subscription.

When should I use Azure RBAC?

Use Azure RBAC when you need to:

- Allow one user to manage VMs in a subscription and another user to manage virtual networks.
- Allow a database administrator group to manage SQL databases in a subscription.
- Allow a user to manage all resources in a resource group, such as virtual machines, websites, and subnets.
- Allow an application to access all resources in a resource group.

These are just a few examples. You'll find the complete list of built-in roles at the end of this module.

How is Azure RBAC enforced?

Azure RBAC is enforced on any action that's initiated against an Azure resource that passes through Azure Resource Manager. Resource Manager is a management service that provides a way to organize and secure your cloud resources.

You typically access Resource Manager from the Azure portal, Azure Cloud Shell, Azure PowerShell, and the Azure CLI. Azure RBAC doesn't enforce access permissions at the application or data level. Application security must be handled by your application.

RBAC uses an allow model. When you're assigned a role, RBAC allows you to perform certain actions, such as read, write, or delete. If one role assignment grants you read permissions to a resource group and a different role assignment grants you write permissions to the same resource group, you have both read and write permissions on that resource group.

Who does Azure RBAC apply to?

You can apply Azure RBAC to an individual person or to a group. You can also apply Azure RBAC to other special identity types, such as service principals and managed identities. These identity types are used by

applications and services to automate access to Azure resources.

iCertify Traders has the following teams with an interest in some part of their overall IT environment:

- **IT Administrators**

This team has ultimate ownership of technology assets, both on-premises and in the cloud. The team requires full control of all resources.

- **Backup and Disaster Recovery**

This team is responsible for managing the health of regular backups and invoking any data or system recoveries.

- **Cost and Billing**

People in this team track and report on technology-related spend. They also manage the organization's internal budgets.

- **Security Operations**

This team monitors and responds to any technology-related security incidents. The team requires ongoing access to log files and security alerts.

How do I manage Azure RBAC permissions?

You manage access permissions on the Access control (IAM) pane in the Azure portal. This pane shows who has access to what scope and what roles apply. You can also grant or remove access from this pane.

The following screenshot shows an example of the Access control (IAM) pane for a resource group. In this example, Alain Charon has been assigned the Backup Operator role for this resource group.

The screenshot shows the Azure portal interface for managing access control. The top navigation bar includes 'Home', 'Resource groups', 'sales-projectforecast', 'Access Control - Role assignment', 'Overview', 'Activity log', 'Access control (IAM)', 'Tags', 'Events', 'Settings', and 'Quickstart'. The 'Access control (IAM)' option is selected and highlighted with a red box. The main content area displays a search bar, role selection dropdowns ('Role: 5 selected', 'Type: All', 'Scope: All scopes'), and a table titled '8 items (5 Users, 1 Groups, 2 Service Principals)'. The table has columns for NAME, TYPE, and ROLE. One row is selected, showing 'AC Alain Charon' as a User with the Backup Operator role assigned to 'This resource'. This row is also highlighted with a red box.

8.5.2 Azure Resource Locks

A **resource lock** prevents resources from being accidentally deleted or changed.

Even with Azure role-based access control (Azure RBAC) policies in place, there's still a risk that people with the right level of access could delete critical cloud resources. Think of a resource lock as a warning system that reminds you that a resource should not be deleted or changed.

For example, at iCertify Traders, an IT administrator was performing routine cleanup of unused resources in Azure. The admin accidentally deleted resources that appeared to be unused. But these resources were critical to an application that's used for seasonal promotions. How can resource locks help prevent this kind of incident from happening in the future?

How do I manage resource locks?

You can manage resource locks from the Azure portal, PowerShell, the Azure CLI, or from an Azure Resource Manager template.

To view, add, or delete locks in the Azure portal, go to the Settings section of any resource's Settings pane in the Azure portal.

Here's an example that shows how to add a resource lock from the Azure portal. You'll apply a similar resource lock in the next part.

The screenshot shows the Azure portal interface for a resource group named 'my-test-rg'. At the top, there's a search bar labeled 'Search (Cmd+ /)' and an 'Add' button. Below the search bar, there are sections for 'Events' and 'Settings'. Under 'Settings', there are links for 'Quickstart', 'Deployments', 'Policies', 'Properties', and 'Locks'. The 'Locks' link is highlighted with a red box. At the bottom, there's an 'Export template' button.

What levels of locking are available?

You can apply locks to a subscription, a resource group, or an individual resource. You can set the lock level to CanNotDelete or ReadOnly.

- CanNotDelete means authorized people can still read and modify a resource, but they can't delete the resource without first removing the lock.
- ReadOnly means authorized people can read a resource, but they can't delete or change the resource. Applying this lock is like restricting all authorized users to the permissions granted by the Reader role in Azure RBAC.

How do I delete or change a locked resource?

Although locking helps prevent accidental changes, you can still make changes by following a two-step process.

To modify a locked resource, you must first remove the lock. After you remove the lock, you can apply any action you have permissions to perform. This additional step allows the action to be taken, but it helps protect your administrators from doing something they might not have intended to do.

Resource locks apply regardless of RBAC permissions. Even if you're an

owner of the resource, you must still remove the lock before you can perform the blocked activity.

Combine resource locks with Azure Blueprints

What if a cloud administrator accidentally deletes a resource lock? If the resource lock is removed, its associated resources can be changed or deleted.

To make the protection process more robust, you can combine resource locks with Azure Blueprints. Azure Blueprints enables you to define the set of standard Azure resources that your organization requires. For example, you can define a blueprint that specifies that a certain resource lock must exist. Azure Blueprints can automatically replace the resource lock if that lock is removed.

8.5.3 Azure Cloud tags

As your cloud usage grows, it's increasingly important to stay organized. A good organization strategy helps you understand your cloud usage and can help you manage costs.

For example, as iCertify Traders prototypes new ways to deploy its applications on Azure, it needs a way to mark its test environments so that it can easily identify and delete resources in these environments when they're no longer needed.

One way to organize related resources is to place them in their own subscriptions. You can also use resource groups to manage related resources. Resource tags are another way to organize resources. Tags provide extra information, or metadata, about your resources. This metadata is useful for:

- **Resource management**

Tags enable you to locate and act on resources that are associated with specific workloads, environments, business units, and owners.

- **Cost management and optimization**

Tags enable you to group resources so that you can report on costs, allocate internal cost centers, track budgets, and forecast estimated cost.

- **Operations management**

Tags enable you to group resources according to how critical their

availability is to your business. This grouping helps you formulate service-level agreements (SLAs). An SLA is an uptime or performance guarantee between you and your users.

- **Security**

Tags enable you to classify data by its security level, such as public or confidential.

- **Governance and regulatory compliance**

Tags enable you to identify resources that align with governance or regulatory compliance requirements, such as ISO 27001.

Tags can also be part of your standards enforcement efforts. For example, you might require that all resources be tagged with an owner or department name.

- **Workload optimization and automation**

Tags can help you visualize all of the resources that participate in complex deployments. For example, you might tag a resource with its associated workload or application name and use software such as Azure DevOps to perform automated tasks on those resources.

How do I manage resource tags?

You can add, modify, or delete resource tags through PowerShell, the Azure CLI, Azure Resource Manager templates, the REST API, or the Azure portal.

You can also manage tags by using Azure Policy. For example, you can apply tags to a resource group, but those tags aren't automatically applied to the resources within that resource group. You can use Azure Policy to ensure that a resource inherits the same tags as its parent resource group. You'll learn more about Azure Policy later in this module.

You can also use Azure Policy to enforce tagging rules and conventions. For example, you can require that certain tags be added to new resources as they're provisioned. You can also define rules that reapply tags that have been removed.

An example tagging structure

A resource tag consists of a name and a value. You can assign one or more tags to each Azure resource.

After reviewing its business requirements, iCertify Traders decides on the

following tags.

Name	Value
AppName	The name of the application that the resource is part of.
CostCenter	The internal cost center code.
Owner	The name of the business owner who's responsible for the resource.
Environment	An environment name, such as "Prod," "Dev," or "Test."
Impact	How important the resource is to business operations, such as "Mission-critical," "High-impact," or "Low-impact."

Here's an example that shows these tags as they're applied to a virtual machine during provisioning.

Name ⓘ	Value ⓘ	Resource
AppName	: SpecialOrders	Virtual machine
CostCenter	: 0224 - Infrastructure R&D	Virtual machine
Owner	: tim@tailwindtraders.com	Virtual machine
Environment	: Test	Virtual machine
Impact	: High-impact	Virtual machine

The iCertify Traders team can run queries, for example, from PowerShell or the Azure CLI, to list all resources that contain these tags.

Keep in mind that you don't need to enforce that a specific tag is present on all of your resources. For example, you might decide that only mission-critical resources have the Impact tag. All non-tagged resources would then not be considered as mission-critical.

8.5.4 Azure Policy

Now that you've identified your governance and business requirements, how do you ensure that your resources stay compliant? How can you be alerted if a resource's configuration has changed?

Azure Policy is a service in Azure that enables you to create, assign, and manage policies that control or audit your resources. These policies enforce different rules and effects over your resource configurations so that those configurations stay compliant with corporate standards.

How does Azure Policy define policies?

Azure Policy enables you to define both individual policies and groups of related policies, known as initiatives. Azure Policy evaluates your resources and highlights resources that aren't compliant with the policies you've created. Azure Policy can also prevent noncompliant resources from being created.

Azure Policy comes with a number of built-in policy and initiative definitions that you can use, under categories such as Storage, Networking, Compute, Security Center, and Monitoring.

For example, say you define a policy that allows only a certain stock-keeping unit (SKU) size of virtual machines (VMs) to be used in your environment. After you enable this policy, that policy is applied when you create new VMs or resize existing VMs. Azure Policy also evaluates any current VMs in your environment.

In some cases, Azure Policy can automatically remediate noncompliant resources and configurations to ensure the integrity of the state of the resources. For example, if all resources in a certain resource group should be tagged with the `AppName` tag and a value of "SpecialOrders," Azure Policy can automatically reapply that tag if it has been removed.

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

Azure Policy in action

Implementing a policy in Azure Policy involves these three steps:

1. Create a policy definition.

2. Assign the definition to resources.
3. Review the evaluation results.

Let's examine each step in more detail.

1. Create a policy definition

A policy definition expresses what to evaluate and what action to take. For example, you could prevent VMs from being deployed in certain Azure regions. You also could audit your storage accounts to verify that they only accept connections from allowed networks.

Every policy definition has conditions under which it's enforced. A policy definition also has an accompanying effect that takes place when the conditions are met. Here are some example policy definitions:

- Allowed virtual machine SKUs
This policy enables you to specify a set of VM SKUs that your organization can deploy.
- Allowed locations
This policy enables you to restrict the locations that your organization can specify when it deploys resources. Its effect is used to enforce your geographic compliance requirements.
- MFA should be enabled on accounts with write permissions on your subscription
This policy requires that multifactor authentication (MFA) be enabled for all subscription accounts with write privileges to prevent a breach of accounts or resources.
- CORS should not allow every resource to access your web applications
Cross-origin resource sharing (CORS) is an HTTP feature that enables a web application running under one domain to access resources in another domain. For security reasons, modern web browsers restrict cross-site scripting by default. This policy allows only required domains to interact with your web app.
- System updates should be installed on your machines
This policy enables Azure Security Center to recommend missing security system updates on your servers.

2. Assign the definition to resources

To implement your policy definitions, you assign definitions to resources. A policy assignment is a policy definition that takes place within a specific scope. This scope could be a management group (a collection of multiple subscriptions), a single subscription, or a resource group.

Policy assignments are inherited by all child resources within that scope. If a policy is applied to a resource group, that policy is applied to all resources within that resource group. You can exclude a subscope from the policy assignment if there are specific child resources you need to be exempt from the policy assignment.

3. Review the evaluation results

When a condition is evaluated against your existing resources, each resource is marked as compliant or noncompliant. You can review the noncompliant policy results and take any action that's needed.

Policy evaluation happens about once per hour. If you make changes to your policy definition and create a policy assignment, that policy is evaluated over your resources within the hour.

What are Azure Policy initiatives?

An Azure Policy initiative is a way of grouping related policies into one set. The initiative definition contains all of the policy definitions to help track your compliance state for a larger goal.

For example, Azure Policy includes an initiative named Enable Monitoring in Azure Security Center. Its goal is to monitor all of the available security recommendations for all Azure resource types in Azure Security Center.

Under this initiative, the following policy definitions are included:

- Monitor unencrypted SQL Database in Security Center
This policy monitors for unencrypted SQL databases and servers.
- Monitor OS vulnerabilities in Security Center
This policy monitors servers that don't satisfy the configured OS vulnerability baseline.
- Monitor missing Endpoint Protection in Security Center
This policy monitors for servers that don't have an installed endpoint protection agent.

In fact, the Enable Monitoring in Azure Security Center initiative contains over 100 separate policy definitions.

Azure Policy also includes initiatives that support regulatory compliance standards such as HIPAA and ISO 27001.

How do I define an initiative?

You define initiatives by using the Azure portal or by using command-line tools. From the Azure portal, you can search the list of built-in initiatives that are already provided by Azure. You also can create your own custom policy definition.

The following image shows a few example Azure Policy initiatives in the Azure portal.

The screenshot shows the Azure portal interface for managing policy definitions. The top navigation bar includes the Microsoft Azure logo, a search bar, and a 'Policy - Definitions' section. Below the navigation is a left sidebar with links like 'Overview', 'Getting started', 'Join Preview', 'Compliance', 'Remediation', 'Authoring' (which is highlighted with a red box), 'Assignments', and 'Definitions'. The main content area displays a table of policy definitions with columns for Name, Definition location, Policies, Type, and Category. The table lists several entries, mostly named 'azuresecuritypack...', which are Non Production, Custom type, and have 3 policies. One entry, 'audit ssh auth_1.3', is listed as Non Production, Custom type, and has 4 policies. Another entry, 'Audit Windows V...', is listed as Demonstration, Built-in type, and has 2 policies.

Name	Definition location	Policies	Type
azuresecuritypack...	Non Production	3	Custom
azuresecuritypack...	Non Production	3	Custom
audit ssh auth_1.3	Non Production	4	Custom
audit ssh auth_1.1	Non Production	2	Custom
azuresecuritypack...	5e116433-8b65-49e...	3	Custom
azuresecuritypack...	5e116433-8b65-49e...	3	Custom
audit ssh auth_1.1	5e116433-8b65-49e...	2	Custom
audit ssh auth_1.1	Demonstration	2	Custom
Audit Windows V...		2	Built-in

How do I assign an initiative?

Like a policy assignment, an initiative assignment is an initiative definition that's assigned to a specific scope of a management group, a subscription, or a resource group.

Even if you have only a single policy, an initiative enables you to increase the

number of policies over time. Because the associated initiative remains assigned, it's easier to add and remove policies without the need to change the policy assignment for your resources.

8.5.5 Azure BluePrint

So far, you've explored a number of Azure features that can help you implement your governance decisions, monitor the compliance of your cloud resources, and control access and protect critical resources from accidental deletion.

What happens when your cloud environment starts to grow beyond just one subscription? How can you scale the configuration of these features, knowing they need to be enforced for resources in new subscriptions?

Instead of having to configure features like Azure Policy for each new subscription, with [Azure Blueprints](#) you can define a repeatable set of governance tools and standard Azure resources that your organization requires. In this way, development teams can 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 the development and deployment phases.

Azure Blueprints orchestrates the deployment of various resource templates and other artifacts, such as:

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

Azure Blueprints in action

When you form a cloud center of excellence team or a cloud custodian team, that team can use Azure Blueprints to scale their governance practices throughout the organization.

Implementing a blueprint in Azure Blueprints involves these three steps:

1. Create an Azure blueprint.
2. Assign the blueprint.

3. Track the blueprint assignments.

With Azure Blueprints, the relationship between the blueprint definition (what should be deployed) and the blueprint assignment (what was deployed) is preserved. In other words, Azure creates a record that associates a resource with the blueprint that defines it. This connection helps you track and audit your deployments.

Blueprints are also versioned. Versioning enables you to track and comment on changes to your blueprint.

What are blueprint artifacts?

Each component in the blueprint definition is known as an artifact.

It is possible for artifacts to have no additional parameters (configurations). An example is the Deploy threat detection on SQL servers policy, which requires no additional configuration.

Artifacts can also contain one or more parameters that you can configure. The following screenshot shows the Allowed locations policy. This policy includes a parameter that specifies the allowed locations.



Allowed locations

This policy enables you to restrict the locations your organization can specify when deploying resources. Use to enforce your geo-compliance requirements. Excludes resource groups, Microsoft.AzureActiveDirectory/b2cDirectories, and resources that use the 'global' region.



You can choose to fill these parameters in now or when assigning the blueprint.

Allowed locations

0 selected



This value should be specified when the blueprint is assigned

You can specify a parameter's value when you create the blueprint definition or when you assign the blueprint definition to a scope. In this way, you can

maintain one standard blueprint but have the flexibility to specify the relevant configuration parameters at each scope where the definition is assigned.

How will iCertify Traders use Azure Blueprints for ISO 27001 compliance?

[ISO 27001](#) is a standard that applies to the security of IT systems, published by the International Organization for Standardization. As part of its quality process, iCertify Traders wants to certify that it complies with this standard. Azure Blueprints has several built-in blueprint definitions that relate to ISO 27001.

As an IT administrator, you decide to investigate the ISO 27001: Shared Services Blueprint definition. Here's an outline of your plan.

1. Define a management group that's named PROD-MG.
Recall that a management group manages access, policies, and compliance across multiple Azure subscriptions. Every new Azure subscription is added to this management group when the subscription is created.
2. Create a blueprint definition that's based on the ISO 27001: Shared Services Blueprint template. Then publish the blueprint.
3. Assign the blueprint to your PROD-MG management group.

The following image shows artifacts that are created when you run an ISO 27001 blueprint from a template.

Create blueprint

<input checked="" type="checkbox"/> Enforce encryption on Data Lake Store accounts	Policy assignment	None
<input checked="" type="checkbox"/> Require blob encryption for storage accounts	Policy assignment	None
+		
Log Analytics resource group	Resource group	2 out of 2 parameters populated
Log Analytics template	Azure Resource Manager te...	0 out of 4 parameters populated
+		
Network resource group	Resource group	2 out of 2 parameters populated
Azure Firewall template	Azure Resource Manager te...	0 out of 3 parameters populated
Virtual Network and Route Table template	Azure Resource Manager te...	0 out of 9 parameters populated

You see that the blueprint template contains policy assignments, Resource Manager templates, and resource groups. The blueprint deploys these artifacts to any existing subscriptions within the PROD-MG management

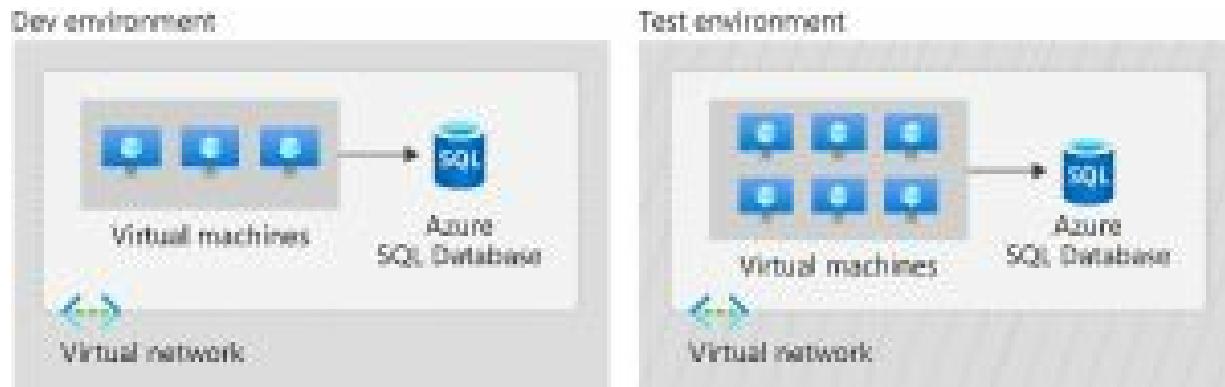
group. The blueprint also deploys these artifacts to any new subscriptions as they're created and added to the management group.

8.5.6 Knowledge Check

Consider the following scenario. Then choose the best response for each question that follows, and select Check your answers.

iCertify Traders has created environments for development and testing for its e-commerce system.

Here's a diagram that shows the basic compute, database, and networking components found in each environment.



These environments provide a way for the team to build and test new application features. If you've gone through the [Plan and manage your Azure costs](#) module, then you've already seen this layout.

Although the development and test teams report to different departments, both environments exist under the same Azure subscription.

The IT manager wants to implement governance controls to help ensure that only authorized users can access these systems. Having these controls in place will also help them track and manage operating costs.

Check your knowledge

1. How can iCertify Traders allow some users to control the virtual machines in each environment but prevent them from modifying networking and other resources in the same resource group or Azure subscription?

- A. Create a role assignment through Azure role-based access control

(Azure RBAC).

- B. Create a policy in Azure Policy that audits resource usage.
 - C. Split the environment into separate resource groups.
2. Which is the best way for iCertify Traders to ensure that the team deploys only cost-effective virtual machine SKU sizes?
- A. Create a policy in Azure Policy that specifies the allowed SKU sizes.
 - B. Periodically inspect the deployment manually to see which SKU sizes are used.
 - C. Create an Azure RBAC role that defines the allowed virtual machine SKU sizes.
3. Which is likely the best way for iCertify Traders to identify which billing department each Azure resource belongs to?
- A. Track resource usage in a spreadsheet.
 - B. Split the deployment into separate Azure subscriptions, where each subscription belongs to its own billing department.
 - C. Apply a tag to each resource that includes the associated billing department.

Answers :

1. **A.** Azure RBAC enables you to create roles that define access permissions. You might create one role that limits access only to virtual machines and a second role that provides administrators with access to everything.
2. **A.** After you enable this policy, that policy is applied when you create new virtual machines or resize existing ones. Azure Policy also evaluates any current virtual machines in your environment.
3. **C.** Tags provide extra information, or metadata, about your resources. The team might create a tag that's named BillingDept whose value would be the name of the billing department. You can use Azure Policy to ensure that the proper tags are assigned when resources are provisioned.

8.6 Privacy, compliance, and data protection standards on Azure

Learn about Microsoft's commitment to privacy and how Azure adheres to common regulatory and compliance standards.

Learning objectives

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

- Explain the types of compliance offerings that are available on Azure.
- Access the Microsoft Privacy Statement, the Online Services Terms, and the Data Protection Addendum to learn what personal data Microsoft collects, how Microsoft uses it, and for what purposes.
- Gain insight into regulatory standards and compliance on Azure from the Trust Center and from the Azure compliance documentation.
- Explain Azure capabilities that are specific to government agencies.

In this module, you'll learn about Microsoft's commitment to privacy and how Azure adheres to common regulatory and compliance standards.

If your organization is a government department or agency, or you need to deploy to regions of China, you'll also learn about some considerations that don't apply to other Azure users.

In general, compliance means to adhere to a law, standard, or set of guidelines. Regulatory compliance refers to the discipline and process of ensuring that a company follows the laws that governing bodies enforce.

Meet iCertify Traders

iCertify Traders is a fictitious home improvement retailer. It operates retail hardware stores across the globe and online.



iCertify Traders specializes in competitive pricing, fast shipping, and a large

range of items. It's looking at cloud technologies to improve business operations and support growth into new markets. By moving to the cloud, the company plans to enhance its shopping experience to further differentiate itself from competitors.

How will iCertify Traders protect its data in the cloud and stay compliant?

iCertify Traders is planning its migration to the cloud. It's used to having full control of all of its application data, which is stored on servers that it manages in its datacenter.

iCertify Traders knows that moving an application to the cloud means that data is now outside of its own walls. The company also understands that the cloud provider has access to the server hardware and infrastructure. How is the privacy of its application data protected?

iCertify Traders must also adhere to multiple regulatory and compliance frameworks. For example, it must follow certain rules to ensure that it properly handles credit card data. It will still need to ensure that its applications comply with applicable regulations and standards. How does infrastructure on Azure already adhere to these same standards?

To answer these questions, you'll start by learning about the types of compliance offerings that are available on Azure.

Learning objectives

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

- Explain the types of compliance offerings that are available on Azure.
- Access the Microsoft Privacy Statement, the Online Services Terms, and the Data Protection Addendum to learn what personal data Microsoft collects, how Microsoft uses it, and for what purposes.
- Gain insight into regulatory standards and compliance on Azure from the Trust Center and from the Azure compliance documentation.
- Explain Azure capabilities that are specific to government agencies.

8.6.1 Compliance terms and requirements

In this unit, you learn about the types of compliance offerings that are available on Azure.

As iCertify Traders moves to running its applications in the cloud, it wants to know how Azure adheres to applicable regulatory compliance frameworks. The company asks:

- How compliant is Azure when it comes to handling personal data?
- How compliant are each of Azure's individual services?

Microsoft's online services build upon a common set of regulatory and compliance controls. Think of a control as a known good standard that you can compare your solution against to ensure security. These controls address today's regulations and adapt as regulations evolve.

Which compliance categories are available on Azure?

Although there are many more, the following image shows some of the more popular compliance offerings that are available on Azure. These offerings are grouped under four categories: Global, US Government, Industry, and Regional.

Global	<input checked="" type="checkbox"/> ISO 27001:2013 <input checked="" type="checkbox"/> ISO 27017:2015 <input checked="" type="checkbox"/> ISO 27018:2014	<input checked="" type="checkbox"/> ISO 22301:2012 <input checked="" type="checkbox"/> ISO 9001:2015 <input checked="" type="checkbox"/> ISO 20000-1:2011	<input checked="" type="checkbox"/> SOC 1 Type 2 <input checked="" type="checkbox"/> SOC 2 Type 2 <input checked="" type="checkbox"/> SOC 3	<input checked="" type="checkbox"/> CSA STAR Certification <input checked="" type="checkbox"/> CSA STAR Attestation <input checked="" type="checkbox"/> CSA STAR Self-Assessment <input checked="" type="checkbox"/> WCAG 2.0 (ISO 40500:2012)
US Gov	<input checked="" type="checkbox"/> FedRAMP High <input checked="" type="checkbox"/> FedRAMP Moderate <input checked="" type="checkbox"/> EAR	<input checked="" type="checkbox"/> DFARS <input checked="" type="checkbox"/> DoD DISA SRG Level 5 <input checked="" type="checkbox"/> DoD DISA SRG Level 4 <input checked="" type="checkbox"/> DoD DISA SRG Level 2	<input checked="" type="checkbox"/> DoE 10 CFR Part 810 <input checked="" type="checkbox"/> NIST SP 800-171 <input checked="" type="checkbox"/> NIST CSF <input checked="" type="checkbox"/> Section 508 VPATs	<input checked="" type="checkbox"/> FIPS 140-2 <input checked="" type="checkbox"/> ITAR <input checked="" type="checkbox"/> CJIS <input checked="" type="checkbox"/> IRS 1075
Industry	<input checked="" type="checkbox"/> PCI DSS Level 1 <input checked="" type="checkbox"/> GLBA <input checked="" type="checkbox"/> FFIEC <input checked="" type="checkbox"/> Shared Assessments <input checked="" type="checkbox"/> FISC (Japan) <input checked="" type="checkbox"/> APRA (Australia)	<input checked="" type="checkbox"/> FCA (UK) <input checked="" type="checkbox"/> MAS + ABS (Singapore) <input checked="" type="checkbox"/> 23 NYCCR 500 <input checked="" type="checkbox"/> HIPAA BAA <input checked="" type="checkbox"/> HITRUST	<input checked="" type="checkbox"/> 21 CFR Part 11 (GxP) <input checked="" type="checkbox"/> MARS-E <input checked="" type="checkbox"/> NHS IG Toolkit (UK) <input checked="" type="checkbox"/> NEN 7510:2011 (Netherlands) <input checked="" type="checkbox"/> FERPA	<input checked="" type="checkbox"/> CDSA <input checked="" type="checkbox"/> MPAA <input checked="" type="checkbox"/> DPP (UK) <input checked="" type="checkbox"/> FACT (UK) <input checked="" type="checkbox"/> SOX
Regional	<input checked="" type="checkbox"/> Argentina PDPA <input checked="" type="checkbox"/> Australia IRAP Unclassified <input checked="" type="checkbox"/> Australia IRAP PROTECTED <input checked="" type="checkbox"/> Canada Privacy Laws <input checked="" type="checkbox"/> China GB 18030:2005 <input checked="" type="checkbox"/> China DJCP (MLPS) Level 3	<input checked="" type="checkbox"/> EN 301 549 <input checked="" type="checkbox"/> EU ENISA IAF <input checked="" type="checkbox"/> EU Model Clauses <input checked="" type="checkbox"/> EU – US Privacy Shield <input checked="" type="checkbox"/> Germany C5	<input checked="" type="checkbox"/> China TRUCS / CCCPPF <input checked="" type="checkbox"/> EU – US Privacy Shield <input checked="" type="checkbox"/> Germany IT-Grundschutz <input checked="" type="checkbox"/> India MeitY <input checked="" type="checkbox"/> Japan CS Mark Gold <input checked="" type="checkbox"/> Japan My Number Act <input checked="" type="checkbox"/> Netherlands BIR 2012 <input checked="" type="checkbox"/> New Zealand Gov CC	<input checked="" type="checkbox"/> Singapore MTCS Level 3 <input checked="" type="checkbox"/> Spain ENS <input checked="" type="checkbox"/> Spain DPA <input checked="" type="checkbox"/> UK Cyber Essentials Plus <input checked="" type="checkbox"/> UK G-Cloud <input checked="" type="checkbox"/> UK PASF

To get a sense of the variety of the compliance offerings available on Azure, let's take a closer look at a few of them.

While not all of these compliance offerings will be relevant to you or your team, they show that Microsoft's commitment to compliance is comprehensive, ongoing, and independently tested and verified.

Criminal Justice Information Service

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. Microsoft adheres to the same requirements that law enforcement and public safety entities must meet.

Cloud Security Alliance STAR Certification

Azure, Intune, and Microsoft Power BI have obtained Cloud Security Alliance (CSA) STAR Certification, which involves a rigorous independent third-party assessment of a cloud provider's security posture.

STAR Certification is based on achieving International Organization of Standards/International Electrotechnical Commission (ISO/IEC) 27001 certification and meeting criteria specified in the Cloud Controls Matrix (CCM). This certification demonstrates that a cloud service provider:

- Conforms to the applicable requirements of ISO/IEC 27001.
- Has addressed issues critical to cloud security as outlined in the CCM.
- Has been assessed against the STAR Capability Maturity Model for the management of activities in CCM control areas.

European Union Model Clauses

Microsoft offers customers European Union (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. Meeting this standard ensures that Azure customers can use Microsoft services to move data freely through Microsoft's cloud, from Europe to the rest of the world.

Health Insurance Portability and Accountability Act

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),

which stipulates adherence to certain security and privacy provisions in HIPAA and the HITECH Act. To assist customers in their individual compliance efforts, Microsoft offers a BAA to Azure customers as a contract addendum.

International Organization of Standards/International Electrotechnical Commission 27018

Microsoft is the first cloud provider to have adopted the ISO/IEC 27018 code of practice, which covers the processing of personal information by cloud service providers.

Multi-Tier Cloud Security Singapore

After rigorous assessments conducted by the Multi-Tier Cloud Security (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)
- Software as a service (SaaS)

Microsoft is the first global cloud solution provider to receive this certification across all three classifications.

Service Organization Controls 1, 2, and 3

Microsoft-covered cloud services are audited at least annually against the Service Organization Controls (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 Cybersecurity Framework

National Institute of Standards and Technology (NIST) Cybersecurity Framework (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. Microsoft cloud services certified according to the FedRAMP standards.

Additionally, through a validated assessment performed by the Health Information Trust Alliance (HITRUST), a leading security and privacy standards development and accreditation organization, Office 365 is certified to the objectives specified in the NIST CSF.

United Kingdom Government G-Cloud

The United Kingdom (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.

8.6.2 Microsoft Privacy Statement, the Online Services Terms, and the Data Protection Addendum

Microsoft runs on trust.

As you deal with an explosion of data, regulatory requirements, and cybersecurity threats, it's Microsoft's responsibility to handle your data securely and in compliance with privacy and legal requirements.

Microsoft recognizes that our customers' data is not our data.

So we give you transparent products, policies, and procedures so you can control your data as needed.

You can learn more about our approach to security, privacy, and compliance in the following three documents.

First, the Microsoft Privacy Statement.

The Microsoft Privacy Statement explains what personal data Microsoft collects from you, how we use it, and for what purposes. You'll find a Microsoft Privacy Statement for every Microsoft service, website, application, software, and device that we make.

The privacy statement covers all of Microsoft's services, websites, apps, software, servers, and devices. This list ranges from enterprise and server products to devices that you use in your home to software that students use at

school.

Microsoft's privacy statement also provides information that's relevant to specific products such as Windows and Xbox.

Second, the Online Services Terms.

The Online Services Terms is Microsoft's legal agreement with its customers. It defines the obligations we both have regarding the processing and security of data. This agreement applies specifically to services you'd use online through a subscription, like Azure, Microsoft 365, or Bing Maps.

Third, the Data Protection Addendum.

The Data Protection Addendum further defines the data processing and security terms of Microsoft's online services, including compliance with laws, disclosure of data, data security practices and policies, and data transfer, retention, and deletion. These documents detail Microsoft's commitment to protecting your data and your privacy in the Cloud.

The Data Protection Addendum (DPA) further defines the data processing and security terms for online services. These terms include:

- Compliance with laws.
- Disclosure of processed data.
- Data Security, which includes security practices and policies, data encryption, data access, customer responsibilities, and compliance with auditing.
- Data transfer, retention, and deletion.

8.6.4 Microsoft Trust Center

The [Trust Center](#) showcases Microsoft's principles for maintaining data integrity in the cloud and how Microsoft implements and supports security, privacy, compliance, and transparency in all Microsoft cloud products and services. The Trust Center is an important part of the Microsoft Trusted Cloud Initiative and provides support and resources for the legal and compliance community.

The screenshot shows a web browser window for the Microsoft Trust Center Home page at https://www.microsoft.com/trust-center. The page features a large headline 'Empowerment begins with trust' in bold black font. Below it is a sub-headline: 'To create a safer world empowered by digital transformation, we handle your data securely and in compliance with privacy and legal requirements.' A blue button labeled 'Watch video' is visible. To the right is a photograph of people working in an office environment.

“If we can’t protect people, then we don’t deserve their trust.”

—Brad Smith, President and Chief Legal Officer

The Trust Center provides:

- In-depth information about security, privacy, compliance offerings, policies, features, and practices across Microsoft cloud products.
- Additional resources for each topic.
- Links to the security, privacy, and compliance blogs and upcoming events.

The Trust Center is a great resource for other people in your organization who might play a role in security, privacy, and compliance. These people include business managers, risk assessment and privacy officers, and legal compliance teams.

Explore the Trust Center

As an optional exercise, let's take a brief look at the Trust Center's entry for ISO 27001.

Access to the Trust Center doesn't require an Azure subscription or a Microsoft account.

1. Go to the [Trust Center](#).

2. Locate the Additional resources section on the page. Under Compliance offerings, select Learn more.



Compliance offerings

Maintain compliance in the cloud with help from a comprehensive set of over 90 offerings.

[Learn more >](#)

You're taken to [Microsoft compliance offerings](#).

The offerings are grouped into four categories: Global, US Government, Industry, and Regional.

3. Under Global, select ISO 27001.

Global

[CIS Benchmark](#)
[CSA-STAR attestation](#)
[CSA-STAR certification](#)
[CSA-STAR self assessment](#)
[ISO 20000-1:2011](#)
[ISO 22301](#)
[ISO 27001](#)
[ISO 27017](#)
[ISO 27018](#)
[ISO 27701](#)
[ISO 9001](#)
[SOC](#)
[WCAG](#)

The ISO 27001 Information Security Management Standards page is typical of the type of compliance information we provide.

4. Briefly review the documentation for ISO/IEC 27001.

You see:

- An overview of the standard.
 - Which cloud services are in scope.
 - An overview of the audit cycle and links to audit reports.
 - Answers to frequently asked questions.
 - Additional resources and white papers.
5. The areas of documentation for other compliance offerings will vary, but this format is the typical one that you'll find.

8.6.3 Azure compliance documentation

The [Azure compliance documentation](#) provides you with detailed documentation about legal and regulatory standards and compliance on Azure.

Here you find compliance offerings across these categories:

- Global
- US government
- Financial services
- Health
- Media and manufacturing
- Regional

There are also additional compliance resources, such as audit reports, privacy information, compliance implementations and mappings, and white papers and analyst reports. Country and region privacy and compliance guidelines are also included. Some resources might require you to be signed in to your cloud service to access them.

Examine PCI DSS compliance

As an optional exercise, here you follow along.

1. Go to the [Azure compliance documentation](#).
2. Under Financial services, select PCI DSS.

Financial services

- ≡ GLBA (US)
- ≡ KNF (Poland)
- ≡ MAS and ABS (Singapore)
- ≡ NBB and FSMA (Belgium)
- ≡ OSFI (Canada)
- ≡ **PCI DSS**
- ≡ RBI and IRDAI (India)
- ≡ SEC 17a-4 (US)
- ≡ SEC Regulation SCI (US)
- ≡ Shared Assessments
- ≡ SOX (US)
- ≡ TruSight

There you see:

- An overview of the PCI DSS standard.
- How PCI DSS applies to Microsoft.
- Which cloud services are in scope.
- An overview of the audit cycle.
- Answers to frequently asked questions.
- Additional resources and white papers.

8.6.3 Azure Government

[Azure Government](#) is a separate instance of the Microsoft Azure service. It addresses the security and compliance needs of US federal agencies, state and local governments, and their solution providers. Azure Government offers physical isolation from non-US government deployments and provides screened US personnel.

Azure Government services handle data that is subject to certain government regulations and requirements:

- Federal Risk and Authorization Management Program (FedRAMP)
- National Institute of Standards and Technology (NIST) 800.171 Defense Industrial Base (DIB)
- International Traffic in Arms Regulations (ITAR)
- Internal Revenue Service (IRS) 1075
- Department of Defense (DoD) L4
- Criminal Justice Information Service (CJIS)

To provide the highest level of security and compliance, Azure Government uses physically isolated datacenters and networks located only in the US. Azure Government customers, such as the US federal, state, and local government or their partners, are subject to validation of eligibility.

Azure Government provides the broadest compliance and Level 5 DoD approval. Azure Government is [available in eight geographies](#) and offers the most compliance certifications of any cloud provider.

8.6.4 Knowledge check

Consider the following scenario. Then choose the best response for each question that follows, and select Check your answers.

At iCertify Traders, the legal and IT departments want to better understand how Microsoft handles personal data. They also want to better understand how Azure services can help them meet their compliance goals.

Their needs go beyond just Azure. For example, applications in their retail stores use Cortana to help store employees quickly locate items.

1. Where can the team access details about the personal data Microsoft processes and how the company processes it, including for Cortana?
 - A. Microsoft Privacy Statement
 - B. The Azure compliance documentation
 - C. Microsoft compliance offerings
2. Where can the legal team access information around how the Microsoft cloud helps them secure sensitive data and comply with applicable laws and regulations?
 - A. Microsoft Privacy Statement
 - B. Trust Center
 - C. Online Services Terms
3. Where can the IT department find reference blueprints that it can apply directly to its Azure subscriptions?
 - A. Online Services Terms
 - B. Azure compliance documentation
 - C. Microsoft Privacy Statement

Answers

1. **A.** The Microsoft Privacy Statement provides information that's relevant to specific services, including Cortana.
2. **B.** The Trust Center is a great resource for people in your organization who might play a role in security, privacy, and compliance.
3. **B.** The compliance documentation provides reference blueprints, or policy definitions, for common standards that you can apply to your Azure subscription.

In this module, you learned about Microsoft's approach to privacy, security, and compliance. You explored resources specific to online services, including Azure, and how governments can use Azure to meet their specific security and compliance needs.

The security team at iCertify Traders now has a better understanding of what resources are available to help it protect its data in the cloud and stay compliant:

- The [Microsoft Privacy Statement](#) provides trust in how Microsoft collects, protects, and uses customer data.
- The [Trust Center](#) provides you with documentation about compliance standards and how Azure can support your business.
- The [Azure compliance documentation](#) includes detailed information about legal and regulatory standards and compliance on Azure.

Keep in mind that compliance status for Azure products and services doesn't automatically translate to compliance for the service or application you build or host on Azure. You're responsible for ensuring that you achieve compliance with the legal and regulatory standards that you must follow.

Most services are the same on both Azure Government and global Azure. But there are some differences that you should be aware of. To learn more, [compare Azure Government and global Azure](#).

Chapter 9 : Azure cost management and service level agreements

Migration to the cloud presents new ways to think about your IT expenses. The cloud also removes the burden of supporting IT infrastructure.

As you move to the cloud, you might ask:

- How much will it cost?
- What guarantees does Azure provide around uptime and connectivity?
- How do preview services impact my production applications?

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

This module starts with planning and managing your Azure costs, a vital consideration for using cloud computing.

You'll examine tools that can help you plan your costs like the total cost of ownership calculator, and the pricing calculator, and some great tips for managing and minimizing your cloud costs.

Then, you'll learn how to choose the right Azure services by examining Service Level Agreements and understanding the service life cycle.

This helps you to make design decisions that reflect the needs of your business for system availability and resiliency.

You'll discover what a Service Level Agreement is, (also known as a SLA), how to define a SLA that meets your business requirements, and how to design an application to meet that SLA with the right products and service choices.

You'll also learn the different stages that a new Azure service or feature goes through and how you can get access to test new capabilities that are in preview.

Once you have completed this learning path,

you'll understand how to estimate, compare, and control your cloud costs, how to design applications to meet your business requirements for availability, and how you can incorporate new services and capabilities into your testing and development.

Learning objectives

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

- Use the Total Cost of Ownership Calculator to compare your current datacenter costs to running the same workloads on Azure.
- Describe the different ways you can purchase Azure products and services.
- Use the Pricing calculator to estimate the monthly cost of running your cloud workloads.
- Define some of the major factors that affect total cost, and apply recommended practices to minimize cost.

9.1 TCO Calculator

The TCO Calculator helps you estimate the cost savings of operating your solution on Azure over time, instead of in your on-premises datacenter.

The term total cost of ownership is commonly used in finance. It can be hard to see all the hidden costs related to operating a technology capability on-premises. Software licenses and hardware are additional costs.

With the TCO Calculator, you enter the details of your on-premises workloads. Then you review the suggested industry average cost (which you can adjust) for related operational costs. These costs include electricity, network maintenance, and IT labor. You're then presented with a side-by-side report. Using the report, you can compare those costs with the same workloads running on Azure. The following image shows one example.



Note: You don't need an Azure subscription to work with the TCO Calculator.

How does the TCO Calculator work?

Working with the TCO Calculator involves three steps:

- Define your workloads.
- Adjust assumptions.
- View the report.



Define your workloads

Adjust assumptions

View report

Let's take a closer look at each step.

Step 1: Define your workloads

First, you enter the specifications of your on-premises infrastructure into the TCO Calculator, based on these four categories:

- **Servers**

This category includes operating systems, virtualization methods, CPU cores, and memory (RAM).

- **Databases**

This category includes database types, server hardware, and the Azure service you want to use, which includes the expected maximum concurrent user sign-ins.

- **Storage**

This category includes storage type and capacity, which includes any backup or archive storage.

- **Networking**

This category includes the amount of network bandwidth you currently consume in your on-premises environment.

Step 2: Adjust assumptions

Next, you specify whether your current on-premises licenses are enrolled for Software Assurance, which can save you money by reusing those licenses on Azure. You also specify whether you need to replicate your storage to another Azure region for greater redundancy.

Then, you can see the key operating cost assumptions across several different areas, which vary among teams and organizations. These costs have been certified by Nucleus Research, an independent research company. For example, these costs include:

- Electricity price per kilowatt hour (KWh).
- Hourly pay rate for IT administration.
- Network maintenance cost as a percentage of network hardware and software costs.

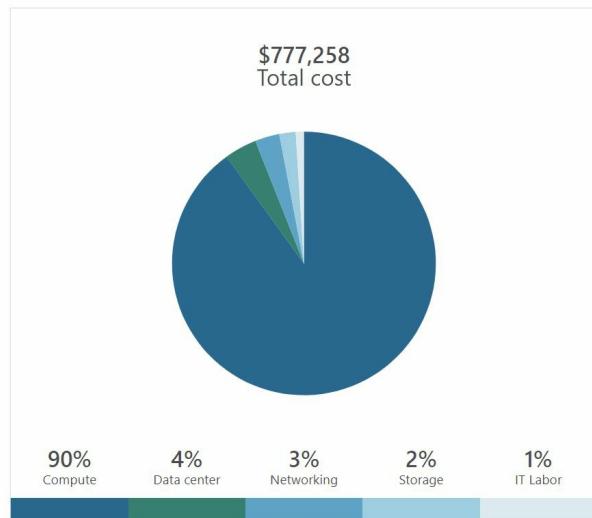
To improve the accuracy of the TCO Calculator results, you adjust the values so that they match the costs of your current on-premises infrastructure.

Step 3: View the report

Choose a time frame between one and five years. The TCO Calculator generates a report that's based on the information you've entered. Here's an example:

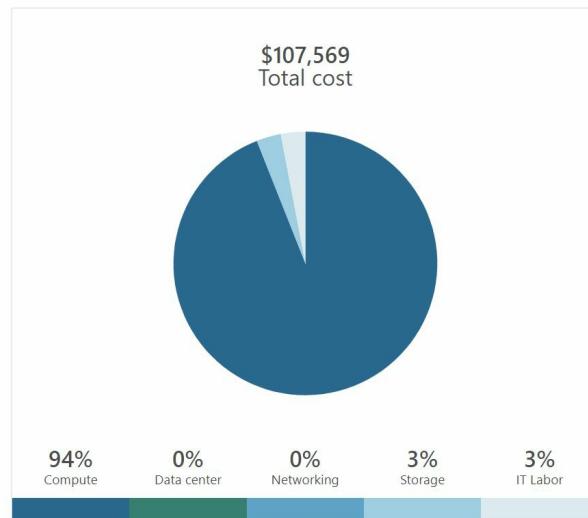
Total on-premises over 2 year(s)

TCO of on-premises environments tends to be driven by compute and data center costs.



Total Azure cost over 2 year(s)

In Azure, certain cost categories decrease or go away completely.



For each category (compute, datacenter, networking, storage, and IT labor), you can also view a side-by-side comparison of the cost breakdown of operating those workloads on-premises versus operating them on Azure.

Here's an example:

Estimated on-premises cost (2 year(s))	Estimated Azure cost (2 year(s))
Compute cost	Azure compute cost
Data center cost	Azure data center cost
Networking cost	Azure networking cost
Storage cost	Azure storage cost
Hardware	Page Blob storage
Local Disk/SAN-HDD Cost per GB Storage (RAID 10 configuration) volume in GB	Usable storage volume in GB Storage cost per GB/month Annual storage cost per usable volume
Total storage procurement cost	\$5,191.68
	1,024 \$0.045 \$552.96
	Total Page Blob LRS storage maintenance cost over two year(s)
	\$1,105.92

You can download, share, or save this report to review later.

In the next unit, you'll use the TCO Calculator to help the iCertify Traders team understand their total costs.

Exercise - Compare sample workload costs by using the TCO Calculator

In this exercise, you use the Total Cost of Ownership (TCO) Calculator to compare the cost of running a sample workload in the datacenter versus on Azure. iCertify Traders is interested in moving some of its on-premises workloads to the cloud. But first, the Chief Financial Officer wants to understand more about moving from a relatively fixed cost structure to an ongoing monthly cost structure.

You've been tasked to investigate whether there are any potential cost savings in moving your European datacenter to the cloud over the next three years. You need to take into account all of the potentially hidden costs involved with operating on-premises and in the cloud.

Instead of manually collecting everything you think might be included, you

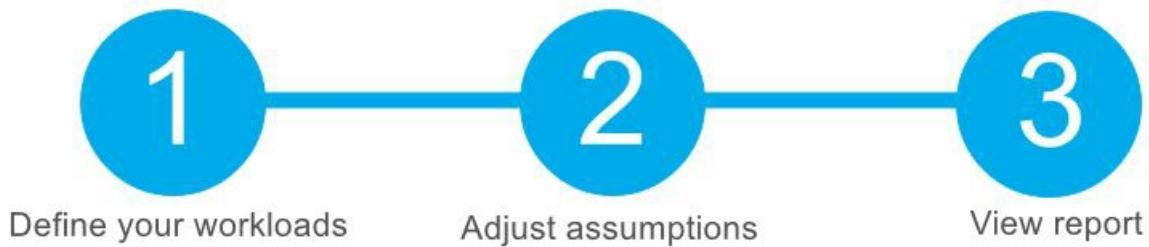
use the TCO Calculator as a starting point. You adjust the provided cost assumptions to match iCertify Traders' on-premises environment.

Note: Remember, you don't need an Azure subscription to work with the TCO Calculator.

Let's say that:

- iCertify Traders runs two sets, or banks, of 50 virtual machines (VMs) in each bank.
- The first bank of VMs runs Windows Server under Hyper-V virtualization.
- The second bank of VMs runs Linux under VMware virtualization.
- There's also a storage area network (SAN) with 60 terabytes (TB) of disk storage.
- You consume an estimated 15 TB of outbound network bandwidth each month.
- There are also a number of databases involved, but for now, you'll omit those details.

Recall that the TCO Calculator involves three steps:



Let's see how iCertify Traders' existing workloads compare in the datacenter versus on Azure.

Define your workloads

Enter the specifications of your on-premises infrastructure into the TCO Calculator.

1. Go to the **TCO Calculator**.
2. Under Define your workloads, select **Add server workload** to create a row for your bank of Windows Server VMs.
3. Under Servers, set the value for each of these settings:

Setting	Value
Name	Servers: Windows VMs
Workload	Windows/Linux Server
Environment	Virtual Machines
Operating system	Windows
VMs	50
Virtualization	Hyper-V
Core(s)	8
RAM (GB)	16
Optimize by	CPU
Windows Server 2008/2008 R2	Off

4. Select **Add server workload** to create a second row for your bank of Linux VMs. Then specify these settings:

Setting	Value
Name	Servers: Linux VMs
Workload	Windows/Linux Server
Environment	Virtual Machines

Operating system	Linux
VMs	50
Virtualization	VMware
Core(s)	8
RAM (GB)	16 GB
Optimize by	CPU

5. Under Storage, select **Add storage**. Then specify these settings:

Setting	Value
Name	Server Storage
Storage type	Local Disk/SAN
Disk type	HDD
Capacity	60 TB
Backup	120 TB
Archive	0 TB

6. Under Networking, set Outbound bandwidth to **15 TB**.

7. Select **Next**.

Adjust assumptions

Here, you specify your currency. For brevity, you leave the remaining fields at their default values.

In practice, you would adjust any cost assumptions and make any adjustments to match your current on-premises environment.

1. At the top of the page, select your currency. This example uses US Dollar (\$).
2. Select Next.

View the report

Take a moment to review the generated report.

Remember, you've been tasked to investigate cost savings for your European datacenter over the next three years. To make these adjustments:

- Set Timeframe to 3 Years.
- Set Region to North Europe.

Scroll to the summary at the bottom. You see a comparison of running your workloads in the datacenter versus on Azure. The prices you see might differ, but here's an example of the cost savings you might expect.

Total on-premises cost over three year(s)	\$23,218,059.00	Total Azure cost over three year(s)	\$7,995,256.00
A total savings of \$15,222,803.00 with Microsoft Azure			
Download	Share	Save	

Select **Download** to download or print a copy of the report in PDF format.

Great work. You now have the information that you can share with your Chief Financial Officer. If you need to make adjustments, you can revisit the TCO Calculator to generate a fresh report.

9.2 Purchase Azure services

In this unit, you learn how to purchase Azure services and get a sense for other factors that affect cost.

You meet with your Chief Financial Officer and some of the team leads. You learn about some assumptions you've missed. You were able to quickly update your total estimated spend through the Total Cost of Ownership (TCO) Calculator.

During the meeting, some new questions arose as the discussion moves toward cloud migration:

- What types of Azure subscriptions are available?
- How do we purchase Azure services?
- Does location or network traffic affect cost?
- What other factors affect the final cost?
- How can we get a more detailed estimate of the cost to run on Azure?

It's important to learn how costs are generated in Azure so that you can understand how your purchasing and solution design decisions can impact your final cost. You agree to research these questions, so let's review each one in greater detail.

9.2.1 Azure subscription models

What are the types of Azure Subscriptions I can use ?

You probably know that an Azure subscription provides you with access to Azure resources, such as virtual machines (VMs), storage, and databases. The types of resources you use impact your monthly bill.

Azure offers both free and paid subscription options to fit your needs and requirements.

They are:

- **Free trial** : A free trial subscription provides you with 12 months of popular free services, a credit to explore any Azure service for 30 days, and more than 25 services that are always free. Your Azure services are disabled when the trial ends or when your credit expires for paid products, unless you upgrade to a paid subscription.
- **Pay-as-you-go** : A pay-as-you-go subscription enables you to pay for what you use by attaching a credit or debit card to your account. Organizations can apply for volume discounts and prepaid invoicing.
- **Member offers** : Your existing membership to certain Microsoft products and services might provide you with credits for your Azure account and reduced rates on Azure services. For example, member offers are available to Visual Studio subscribers, Microsoft Partner Network members, Microsoft for Startups members, and Microsoft Imagine members.

9.2.2 Purchase Azure services

There are three main ways to purchase services on Azure.

They are:

- **Enterprise Agreement** : Larger customers, known as enterprise customers, can sign an Enterprise Agreement with Microsoft. This agreement commits them to spending a predetermined amount on Azure services over a period of three years. The service fee is typically paid annually. As an Enterprise Agreement customer, you'll receive the best customized pricing based on the kinds and amounts of services you plan on using.
- **Directly from the web** : Here, you purchase Azure services directly from the Azure portal website and pay standard prices. You're billed monthly, as a credit card payment or through an invoice. This purchasing method is known as Web Direct.
- **Through a Cloud Solution Provider** : A Cloud Solution Provider

(CSP) is a Microsoft Partner who helps you build solutions on top of Azure. Your CSP bills you for your Azure usage at a price they determine. They also answer your support questions and escalate them to Microsoft, as needed.

You can bring up, or provision, Azure resources from the Azure portal or from the command line. The Azure portal arranges products and services by category. You select the services that fit your needs. Your account is billed according to Azure's "pay for what you use" model.

Here's an example that shows the Azure portal.

The screenshot shows the Azure portal interface. On the left, there is a sidebar with categories: Overview, Categories, All, General, Compute (selected), Networking, Storage, Web, Mobile, Containers, Databases, Analytics, and Blockchain. The main area is titled 'COMPUTE (35)' and lists various services: Virtual machines, Virtual machine scale sets, App Services, Batch accounts, Mesh applications, Kubernetes services, Disks, Snapshots, Image definitions, and Shared image galleries. The 'Virtual machines' service is highlighted with a grey background.

At the end of each month, you're billed for what you've used. At any time, you can check the cost management and billing page in the Azure portal to get a summary of your current usage and review invoices from prior months.

9.2.3 Cost Factors

The way you use resources, your subscription type, and pricing from third-party vendors are common factors. Let's take a quick look at each.

Resource type

A number of factors influence the cost of Azure resources. They depend on the type of resource or how you customize it.

For example, with a storage account you specify a type (such as block blob storage or table storage), a performance tier (standard or premium), and an access tier (hot, cool, or archive). These selections present different costs.

Usage meters

When you provision a resource, Azure creates meters to track usage of that resource. Azure uses these meters to generate a usage record that's later used to help calculate your bill.

Think of usage meters similar to how you use electricity or water in your home. You might pay a base price each month for electricity or water service, but your final bill is based on the total amount that you consumed.

Let's look at a single VM as an example. The following kinds of meters are relevant to tracking its usage:

- Overall CPU time.
- Time spent with a public IP address.
- Incoming (ingress) and outgoing (egress) network traffic in and out of the VM.
- Disk size and amount of disk read and disk write operations.

Each meter tracks a specific type of usage. For example, a meter might track bandwidth usage (ingress or egress network traffic in bits per second), number of operations, or its size (storage capacity in bytes).

The usage that a meter tracks correlates to a quantity of billable units. Those units are charged to your account for each billing period. The rate per billable unit depends on the resource type you're using.

Resource usage

In Azure, you're always charged based on what you use. As an example, let's look at how this billing applies to deallocated a VM.

In Azure, you can delete or deallocate a VM. Deleting a VM means that you no longer need it. The VM is removed from your subscription, and then it's prepared for another customer.

Deallocating a VM means that the VM is no longer running. But the associated hard disks and data are still kept in Azure. The VM isn't assigned to a CPU or network in Azure's datacenter, so it doesn't generate the costs associated with compute time or the VM's IP address. Because the disks and data are still stored, and the resource is present in your Azure subscription, you're still billed for disk storage.

Deallocating a VM when you don't plan on using it for some time is just one way to minimize costs. For example, you might deallocate the VMs you use for testing purposes on weekends when your testing team isn't using them. You'll learn more about ways to minimize cost later in this module.

Azure subscription types

Some Azure subscription types also include usage allowances, which affect costs.

For example, an Azure free trial subscription provides access to a number of Azure products that are free for 12 months. It also includes credit to spend within your first 30 days of sign-up. And you get access to more than 25 products that are always free (based on resource and region availability).

Azure Marketplace

You can also purchase Azure-based solutions and services from third-party vendors through Azure Marketplace. Examples include managed network firewall appliances or connectors to third-party backup services. Billing structures are set by the vendor.

Does location or network traffic affect cost?

When you provision a resource in Azure, you need to define the location (known as the Azure region) of where it will be deployed. Let's see why this decision can have cost consequences.

Location

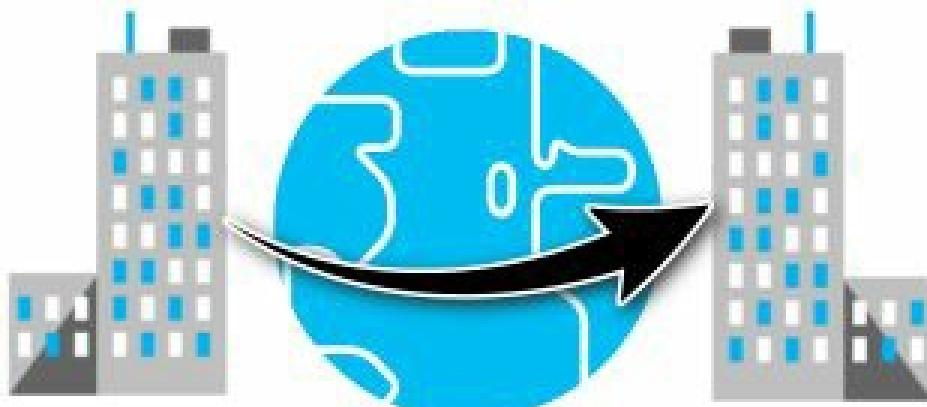
Azure infrastructure is distributed globally, which enables you to deploy your services centrally or provision your services closest to where your customers use them.

Different regions can have different associated prices. Because geographic regions can impact where your network traffic flows, network traffic is a cost influence to consider as well.

For example, say iCertify Traders decides to provision its Azure resources in the Azure regions that offer the lowest prices. That decision would save the company some money. But, if they need to transfer data between those regions, or if their users are located in different parts of the world, any potential savings could be offset by the additional network usage costs of transferring data between those resources.

Zones for billing of network traffic

Billing zones are a factor in determining the cost of some Azure services.



Bandwidth refers to data moving in and out of Azure datacenters. Some inbound data transfers (data going into Azure datacenters) are free. For outbound data transfers (data leaving Azure datacenters), data transfer pricing

is based on zones.

A zone is a geographical grouping of Azure regions for billing purposes. The following zones include some of the regions as shown here:

- **Zone 1:** Australia Central, West US, East US, Canada West, West Europe, France Central, and others
- **Zone 2:** Australia East, Japan West, Central India, Korea South, and others
- **Zone 3:** Brazil South, South Africa North, South Africa West, UAE Central, UAE North
- **DE Zone 1:** Germany Central, Germany Northeast

How can I estimate the total cost?

As you've learned, an accurate cost estimate takes all of the preceding factors into account. Fortunately, the Azure Pricing calculator helps you with that process.

The Pricing calculator displays Azure products in categories. You add these categories to your estimate and configure according to your specific requirements. You then receive a consolidated estimated price, with a detailed breakdown of the costs associated with each resource you added to your solution. You can export or share that estimate or save it for later. You can load a saved estimate and modify it to match updated requirements.

You also can access pricing details, product details, and documentation for each product from within the Pricing calculator.

The screenshot shows the Azure Pricing calculator interface. At the top, there's a summary row for a 'Virtual Machines' estimate: 'Virtual Machines' with edit and delete icons, '1 D2 v3 (2 vCPU(s), 8 GB RAM) x 730 Hours;', and a total price of '\$188.57'. Below this is a larger section for 'Virtual Machines' with the following configuration:

- Icon:** A monitor icon with a blue cube.
- Name:** Virtual Machines
- Region:** West US
- Operating System:** Windows
- Type:** (OS Only)
- Tier:** Standard
- Instance:** D2 v3: 2 vCPU(s), 8 GB RAM, 50 GB Temporary storage, \$0.209/hour

On the right side of this section, there are three buttons: 'Clone' (with a plus sign and arrow), 'Delete' (with a trash bin icon), and 'More info'. Under 'More info', there are links for 'Pricing details', 'Product details', and 'Documentation'.

The options that you can configure in the Pricing calculator vary between products, but they can include:

- **Region**

A region is the geographical location in which you can provision a service.

Southeast Asia, Central Canada, Western United States, and Northern Europe are a few examples.

- **Tier**

Tiers, such as the Free tier or Basic tier, have different levels of availability or performance and different associated costs.

- **Billing options**

Billing options highlight the different ways you can pay for a service.

Options can vary based on your customer type and subscription type and can include options to save costs.

- **Support options**

These options enable you to select additional support pricing options for certain services.

- **Programs and offers**

Your customer or subscription type might enable you to choose from specific licensing programs or other offers.

- **Azure Dev/Test pricing**

This option lists the available prices for development and test workloads.

Dev/Test pricing applies when you run resources within an Azure subscription that's based on a Dev/Test offer.

Keep in mind that the Pricing calculator provides estimates and not actual price quotes. Actual prices can vary depending upon the date of purchase, the payment currency you're using, and the type of Azure customer you are.

Exercise - Estimate workload cost by using the Pricing calculator

In this exercise, you use the Pricing calculator to estimate the cost of running a basic web application on Azure. With an understanding of the more important cost factors associated with running on Azure, iCertify Traders wants to take a typical workload and estimate how much it would cost each month to run it on Azure.

The IT Manager at iCertify Traders is faced with the decision about whether to replace some aging on-premises hardware or move the application to Azure. The company needs to know how much the ongoing monthly cost of the solution in Azure would be.

Let's start by defining which Azure services you need.

Note: The Pricing calculator is for information purposes only. The prices are only an estimate, and you won't be charged for any services you select.

Define your requirements

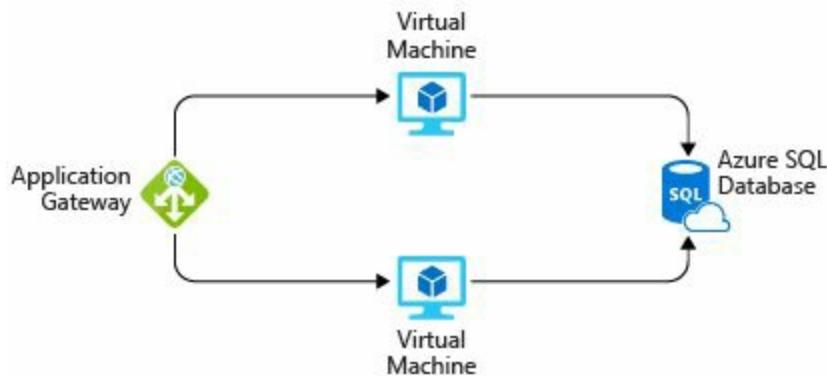
Before you run the Pricing calculator, you first need a sense of what Azure services you need. You meet with the application development team to discuss their migration project.

In their datacenter, the team has an ASP.NET web application that runs on Windows. The web application provides information about product inventory and pricing. They have two virtual machines that are connected through a central load balancer. The web application connects to a SQL Server database that holds inventory and pricing information.

The team decides to:

- Use Azure Virtual Machines instances, similar to the virtual machines they use in the datacenter.
- Use Azure Application Gateway for load balancing.
- Use Azure SQL Database to hold inventory and pricing information.

Here's a diagram that shows the basic configuration:



In practice, you would define your requirements in greater detail. But here are some basic facts and requirements that came up during the meeting:

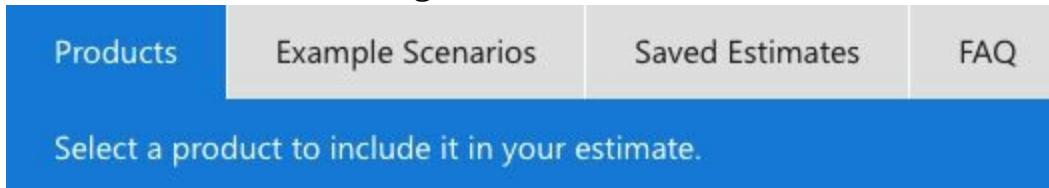
- The application is used by iCertify Traders employees at their retail stores. It's not accessible to customers.
- This application doesn't require a massive amount of computing power.

- The virtual machines and the database run all the time (730 hours per month).
- The network processes about 1 TB of data per month.
- The database doesn't need to be configured for high-performance workloads and requires no more than 32 GB of storage.

Explore the Pricing calculator

Let's start with a quick tour of the Pricing calculator.

1. Go to the Pricing calculator.
2. Notice the following tabs:



- **Products**

This is where you choose the Azure services that you want to include in your estimate. You'll likely spend most of your time here.

- **Example Scenarios**

Here you'll find several reference architectures, or common cloud-based solutions that you can use as a starting point.

- **Saved Estimates**

Here you'll find your previously saved estimates.

- **FAQ**

Here you'll discover answers to frequently asked questions about the Pricing calculator.

Estimate your solution

Here you add each Azure service that you need to the calculator. Then you configure each service to fit your needs.

Tip: Make sure you have a clean calculator with nothing listed in the estimate. You can reset the estimate by selecting the trash can icon next to each item.

Add services to the estimate

1. On the Products tab, select the service from each of these categories:

Category	Service
Compute	Virtual Machines
Databases	Azure SQL Database
Networking	Application Gateway

2. Scroll to the bottom of the page. You see that each service is listed with its default configuration.

Your Estimate

▲ Virtual Machines ⓘ 1 D2 v3 (2 vCPU(s), 8 GB RAM) x 730 ...

Virtual Machines

REGION: OPERATING SYSTEM: TYPE:

West US Windows (OS Only)

Configure services to match your requirements

1. Under **Virtual Machines**, set these values:

Setting	Value
Region	West US
Operating system	Windows
Type	(OS Only)
Tier	Standard
Instance	D2 v3
Virtual machines	2 x 730 Hours

Leave the remaining settings at their current values.

2. Under **Azure SQL Database**, set these values:

Setting	Value
Region	West US
Type	Single Database
Backup storage tier	RA-GRS
Purchase model	vCore
Service tier	General Purpose
Compute tier	Provisioned
Generation	Gen 5
Instance	8 vCore

Leave the remaining settings at their current values.

3. Under **Application Gateway**, set these values:

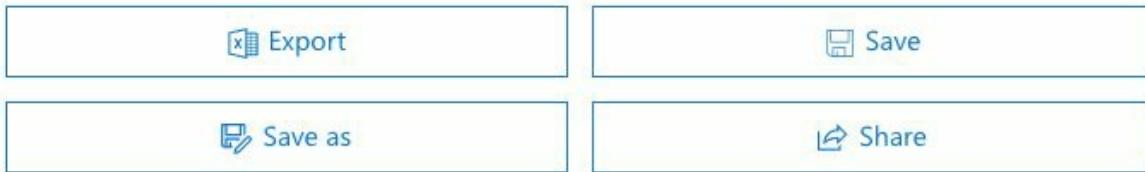
Setting	Value
Region	West US
Tier	Web Application Firewall
Size	Medium
Gateway hours	2 x 730 Hours
Data processed	1 TB
Outbound data transfer	5 GB

Leave the remaining settings at their current values.

Review, share, and save your estimate

At the bottom of the page, you see the total estimated cost of running the solution. You can change the currency type if you want.

Estimated monthly cost



\$0.00

\$1,902.64

US Dollar (\$) ▾

At this point, you have a few options:

- Select Export to save your estimate as an Excel document.
- Select Save or Save as to save your estimate to the Saved Estimates tab for later.
- Select Share to generate a URL so you can share the estimate with your team.

You now have a cost estimate that you can share with your team. You can make adjustments as you discover any changes to your requirements.

Experiment with some of the options you worked with here, or create a purchase plan for a workload you want to run on Azure.

Manage and minimize total cost on Azure

As a home improvement retailer, the proverb "measure twice, cut once" is fitting for the team at iCertify Traders. Here are some recommended practices that can help you minimize your costs.

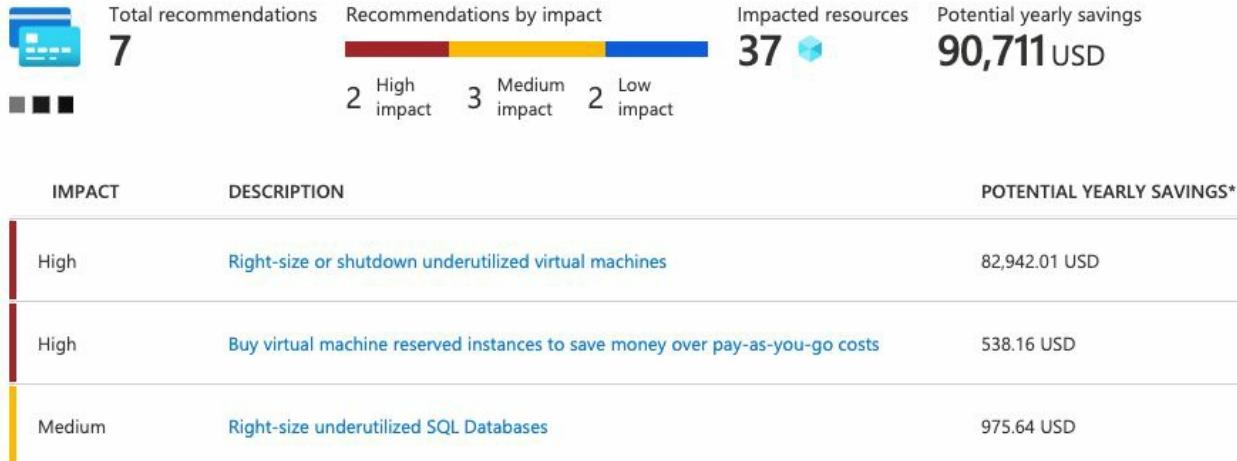
- Understand estimated costs before you deploy

To help you plan your solution on Azure, carefully consider the products, services, and resources you need. Read the relevant documentation to understand how each of your choices is metered and billed. Calculate your projected costs by using the Pricing calculator and the Total Cost of Ownership (TCO) Calculator. Only add the products, services, and resources that you need for your solution.

- Use Azure Advisor to monitor your usage

Ideally, you want your provisioned resources to match your actual usage. Azure Advisor identifies unused or underutilized resources and recommends unused resources that you can remove. This information helps you configure your resources to match your actual workload.

The following image shows some example recommendations from Azure Advisor:



Recommendations are sorted by impact: high, medium, or low. In some cases, Azure Advisor can automatically remediate, or fix, the underlying problem. Other issues, such as the two that are listed as high impact, require human intervention.

- Use spending limits to restrict your spending

If you have a free trial or a credit-based Azure subscription, you can use spending limits to prevent accidental overrun.

For example, when you spend all the credit included with your Azure free account, Azure resources that you deployed are removed from production and your Azure virtual machines (VMs) are stopped and deallocated. The data in your storage accounts is available as read-only. At this point, you can upgrade your free trial subscription to a pay-as-you-go subscription.

If you have a credit-based subscription and you reach your configured spending limit, Azure suspends your subscription until a new billing period begins.

A related concept is quotas, or limits on the number of similar resources you can provision within your subscription. For example, you can allocate up to 25,000 VMs per region. These limits mainly help Microsoft plan its datacenter capacity.

- Use Azure Reservations to prepay

Azure Reservations offers discounted prices on certain Azure services. Azure Reservations can save you up to 72 percent as compared to pay-as-you-go

prices. To receive a discount, you reserve services and resources by paying in advance.

For example, you can prepay for one year or three years of use of VMs, database compute capacity, database throughput, and other Azure resources.

The following example shows estimated savings on VMs. In this example, you save an estimated 72 percent by committing to a three-year term.

Select the product you want to purchase ×

Reserved VM Instances (RIs) provide a significant discount over pay-as-you-go VM prices by allowing you to pre-purchase the base costs of your VM usage for a period of 1 or 3 years. Reserved instance discount will automatically apply to matching VMs, you don't need to re-deploy resources to get reservation discount. The reservation applies only to hardware usage. Windows is charged separately. [Learn More](#)

Scope * Shared Billing subscription * Cost Management Research (1caa5a3-2b66-438e-8...)

[Recommended](#) [All Products](#)

[Filter by name, region, or instance flexi...](#) Region : **East US** Term : **Three Years** Billing frequency : **Monthly** [Add Filter](#) [Reset filters](#)

Showing recommendations based on your usage over the last 30 d... [Learn more](#)

Name	Region	Instance flexibility group	vCPUs	RAM (GB)	Term	Billing frequency	Recommended Quantity
Standard_DS3_v2	East US	DSv2 Series	4	14	Three Years	Monthly	9 - See details
Standard_DS2_v2	East US	DSv2 Series	2	7	Three Years	Monthly	5 - See details
Standard_DS1_v2	East US	DSv2 Series	1	3.5	Three Years	Monthly	2 - See details
Standard_D2s_V3	East US	DSv3 Series	2	8	Three Years	Monthly	2 - See details
Standard_E16s_v3	East US	ESv3 Series	16	128	Three Years	Monthly	2 - See details
Standard_F2s_v2	East US	FSv2 Series	2	4	Three Years	Monthly	2 - See details
Standard_D2_v3	East US	Dv3 Series	2	8	Three Years	Monthly	1 - See details

Not seeing what you want? [Browse all products](#).

[Add to cart](#) [Close](#) Monthly price per VM: 59.00 USD
72% Estimated savings

Azure Reservations are available to customers with an Enterprise Agreement, Cloud Solution Providers, and pay-as-you-go subscriptions.

- Choose low-cost locations and regions

The cost of Azure products, services, and resources can vary across locations and regions. If possible, you should use them in those locations and regions where they cost less.

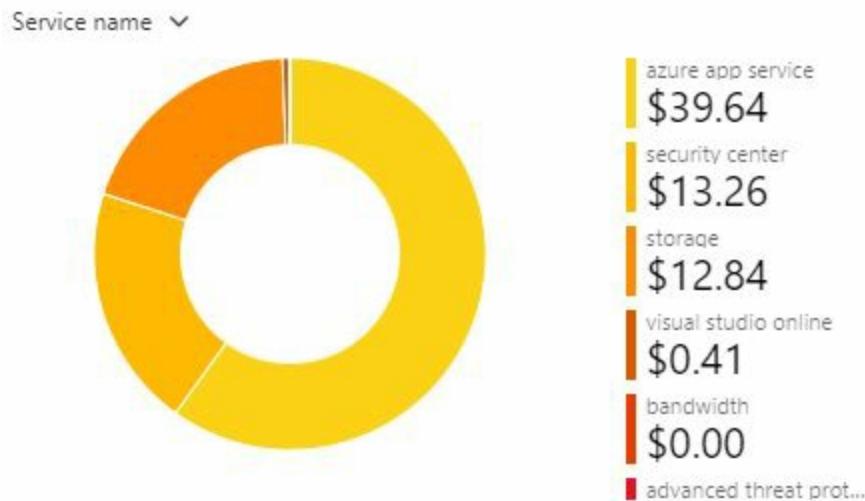
But remember, some resources are metered and billed according to how much outgoing (egress) network bandwidth they consume. You should provision connected resources that are metered by bandwidth in the same Azure region to reduce egress traffic between them.

- Research available cost-saving offers

Keep up to date with the latest Azure customer and subscription offers, and switch to offers that provide the greatest cost-saving benefit.

- Use Azure Cost Management + Billing to control spending

Azure Cost Management + Billing is a free service that helps you understand your Azure bill, manage your account and subscriptions, monitor and control Azure spending, and optimize resource use. The following image shows current usage broken down by service:



In this example, Azure App Service, a web application hosting service, generates the greatest cost.

Azure Cost Management + Billing features include:

- **Reporting** : Use historical data to generate reports and forecast future usage and expenditure.
- **Data enrichment** : Improve accountability by categorizing resources with tags that correspond to real-world business and organizational units.
- **Budgets** : Create and manage cost and usage budgets by monitoring resource demand trends, consumption rates, and cost patterns.
- **Alerting** : Get alerts based on your cost and usage budgets.
- **Recommendations** : Receive recommendations to eliminate idle resources and to optimize the Azure resources you provision.

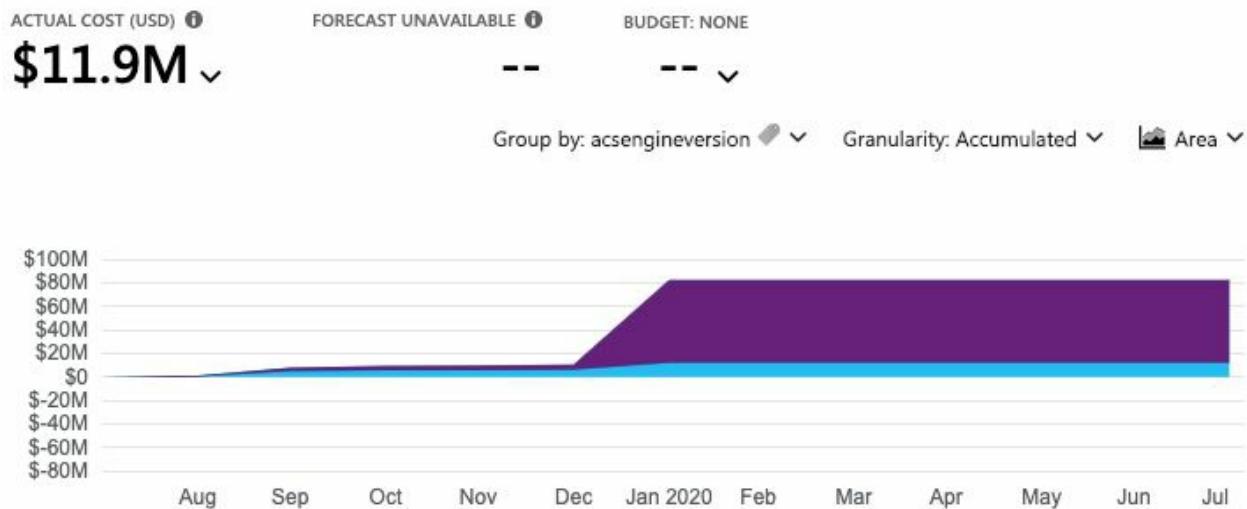
Apply tags to identify cost owners

Tags help you manage costs associated with the different groups of Azure products and resources. You can apply tags to groups of Azure resources to

organize billing data.

For example, if you run several VMs for different teams, you can use tags to categorize costs by department, such as Human Resources, Marketing, or Finance, or by environment, such as Test or Production.

Tags make it easier to identify groups that generate the biggest Azure costs, which can help you adjust your spending accordingly. The following image shows a year's worth of usage broken down by tags on the Azure Cost Management + Billing page:

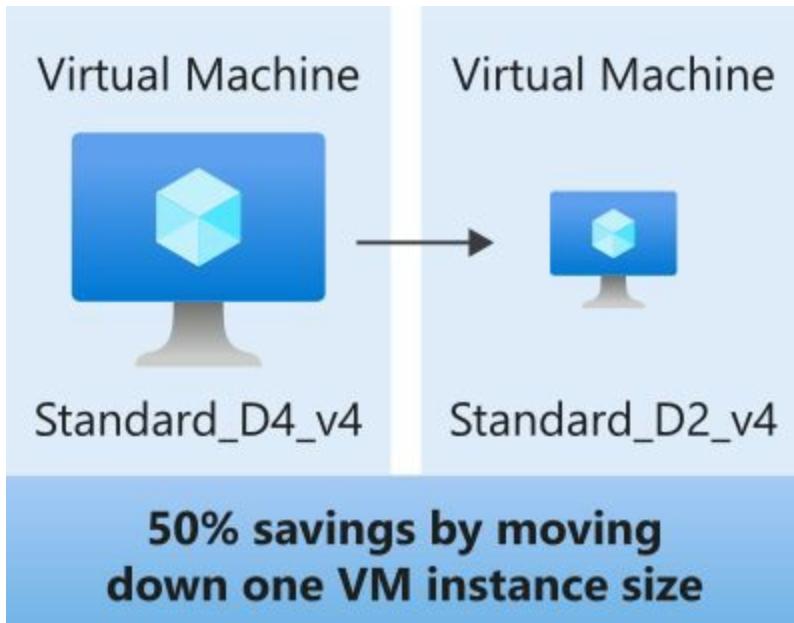


Resize underutilized virtual machines

A common recommendation that you'll find from Azure Cost Management + Billing and Azure Advisor is to resize or shut down VMs that are underutilized or idle.

As an example, say you have a VM whose size is Standard_D4_v4, a general-purpose VM type with four vCPUs and 16 GB of memory. You might discover that this VM is idle 90 percent of the time.

Virtual machine costs are linear and double for each size larger in the same series. So in this case, if you reduce the VM's size from Standard_D4_v4 to Standard_D2_v4, which is the next size lower, you reduce your compute cost by 50 percent. The following image shows this idea:



Keep in mind that resizing a VM requires it to be stopped, resized, and then restarted. This process might take a few minutes depending on how significant the size change is. Be sure to properly plan for an outage, or shift your traffic to another instance while you perform resize operations.

- Deallocate virtual machines during off hours

Recall that to deallocate a VM means to no longer run the VM, but preserve the associated hard disks and data in Azure.

If you have VM workloads that are only used during certain periods, but you're running them every hour of every day, you're wasting money. These VMs are great candidates to shut down when not in use and start back when you need them, saving you compute costs while the VM is deallocated.

This approach is an excellent strategy for development and testing environments, where the VMs are needed only during business hours. Azure even provides a way to automatically start and stop your VMs on a schedule.

- Delete unused resources

This recommendation might sound obvious, but if you aren't using a resource, you should shut it down. It's not uncommon to find nonproduction or proof-of-concept systems that are no longer needed following the completion of a project.

Regularly review your environment, and work to identify these systems. Shutting down these systems can have a dual benefit by saving you on infrastructure costs and potential savings on licensing and operating costs.

- Migrate from IaaS to PaaS services

As you move your workloads to the cloud, a natural evolution is to start with infrastructure as a service (IaaS) services because they map more directly to concepts and operations you're already familiar with.

Over time, one way to reduce costs is to gradually move IaaS workloads to run on platform as a service (PaaS) services. While you can think of IaaS as direct access to compute infrastructure, PaaS provides ready-made development and deployment environments that are managed for you.

As an example, say you run SQL Server on a VM running on Azure. This configuration requires you to manage the underlying operating system, set up a SQL Server license, manage software and security updates, and so on. You also pay for the VM whether or not the database is processing queries. One way to potentially save costs is to move your database from SQL Server on a VM to Azure SQL Database. Azure SQL Database is based on SQL Server.

Not only are PaaS services such as Azure SQL Database often less expensive to run, but because they're managed for you, you don't need to worry about software updates, security patches, or optimizing physical storage for read and write operations.

- Save on licensing costs

Licensing is another area that can dramatically impact your cloud spending. Let's look at some ways you can reduce your licensing costs.

- Choose cost-effective operating systems

Many Azure services provide a choice of running on Windows or Linux. In some cases, the cost depends on which you choose. When you have a choice, and your application doesn't depend on the underlying operating system, it's useful to compare pricing to see whether you can save money.

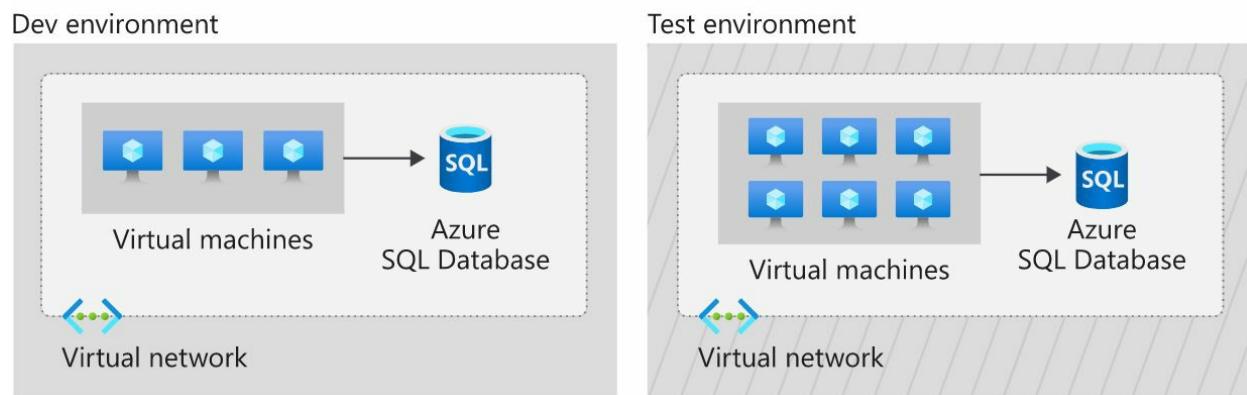
- Use Azure Hybrid Benefit to repurpose software licenses on Azure

If you've purchased licenses for Windows Server or SQL Server, and your licenses are covered by Software Assurance, you might be able to repurpose those licenses on VMs on Azure. Some of the details vary between Windows Server or SQL Server. We'll provide resources at the end of this module where you can learn more.

Knowledge check

Consider the following scenario. Then choose the best response for each question that follows, and select Check your answers. Before they migrate their existing e-commerce system from their datacenter to production environments on Azure, the iCertify Traders team wants to first set up environments for development and testing.

Here's a diagram that shows the basic compute, database, and networking components found in each environment:



An e-commerce system might require a website, the products database, a payment system, and so on. Because developers can't always run the entire service from their local development environment, the Dev environment is the first place where everything the app needs comes together.

After the development team verifies changes to the Dev environment, they promote changes to the Test environment. The Test environment is where the testing team verifies new app features and also verifies that no regressions, or breaks to existing features, happen as new features are added.

The team will map each component in their existing infrastructure to the appropriate Azure service.

1. Which is the best first step the team should take to compare the cost of

running these environments on Azure versus in their datacenter?

- A. They're just test environments. Spin them up and check the bill at the end of the month.
- B. Assume that running in the cloud costs about the same as running in the datacenter.
- C. Run the Total Cost of Ownership Calculator.

2. What's the best way to ensure that the development team doesn't provision too many virtual machines at the same time?

- A. Do nothing. Let the development team use what they need.
- B. Apply spending limits to the development team's Azure subscription.
- C. Verbally give the development lead a budget and hold them accountable for overages.

3. Which is the most efficient way for the testing team to save costs on virtual machines on weekends, when testers are not at work?

- A. Delete the virtual machines before the weekend and create a new set the following week.
- B. Deallocate virtual machines when they're not in use.
- C. Just let everything run. Azure bills you only for the CPU time that you use.

4. Resources in the Dev and Test environments are each paid for by different departments. What's the best way to categorize costs by department?

- A. Apply a tag to each virtual machine that identifies the appropriate billing department.
- B. Split the cost evenly between departments.
- C. Keep a spreadsheet that lists each team's resources.

Answer:

1. **Answer: C.** Running the Total Cost of Ownership Calculator is a great first step because it can provide an accurate comparison of running workloads in the datacenter versus on Azure, certified by an independent research company.
2. **Answer: B.** If you exceed your spending limit, active resources are deallocated. You can then decide whether to increase your limit or provision fewer resources.
3. **Answer: B.** When you deallocate virtual machines, the associated hard disks and data are still kept in Azure. But you don't pay for CPU or network consumption, which can help save costs.
4. **Answer: A.** You can apply tags to groups of Azure resources to organize billing data.

Summary

iCertify Traders is taking a methodical approach toward cloud migration. While proof-of-concept projects can help demonstrate technical feasibility, having a clear picture of the total cost of running in the cloud will further help the team validate its approach.

To start, the iCertify Traders team used the Total Cost of Ownership Calculator to estimate the cost savings of operating its solution on Azure instead of in its on-premises datacenter.

From there, the team used the Pricing calculator to get a more detailed estimate for running a typical workload on Azure each month. The team also created a checklist of cost-saving measures that it can use to help keep down costs. This list includes:

- Perform cost analysis before you deploy.
- Use Azure Advisor to monitor your usage.
- Use spending limits to prevent accidental spending.
- Use Azure Reservations to prepay.
- Choose low-cost locations and regions.
- Research available cost-saving offers.
- Apply tags to identify cost owners.

Chapter 10 : Practice Test 1

1) You are migrating your on-premises Microsoft Exchange email system to Office 365. What kind of cloud service would this be considered?

- A. Infrastructure-as-a-Service (IaaS)
- B. Serverless
- C. Platform-as-a-Service (PaaS)
- D. Software-as-a-Service (SaaS)

2) Which of the following are considered capital expenditures (CapEx)?

- A. Storage area network
- B. Office 365 licenses
- C. Hyper-V host server
- D. Cloud-based virtual machine

3) Define the concept of "dynamic elasticity."

- A. A cloud service that responds quickly when demand increases and scales down when demand decreases.
- B. A cloud service that responds quickly when demand increases and needs to be manually scaled-down when demand decreases.
- C. The ability of a cloud service to be accessed quickly from any location via the internet.
- D. A cloud service that remains available after a failure occurs.

4) Which of the following statements are true for IaaS cloud services?

- A. The client is responsible for all guest VM OS and application updates.
- B. The client is responsible for purchasing all Operating System (OS) host licensing.
- C. The client has complete control over the hardware hosting the VM.
- D. Services can be scaled automatically to support system load.

5) Your company is migrating an internal web application to the cloud. The application requires specific configuration changes within the Operating System. Which of the following cloud deployment solutions would be most suitable?

- A. Infrastructure as a Service (IaaS)

- B. Platform as a Service (PaaS)
 - C. Software as a Service (SaaS)
 - D. Function as a Service (FaaS)
- 6) A cloud architecture consisting of both on-premise and public cloud networks is joined to allow applications to operate across the two. What is this known as?
- A. Stretched Cloud
 - B. Public Cloud
 - C. Hybrid Cloud

7) Which of the following are characteristic of private clouds?

- A. Lower costs
- B. Limited flexibility
- C. High scalability
- D. Improved security

8) Which of the following statements about Azure availability zones are true?

- A. Availability zones are used to replicate data and applications to multiple datacenters within an Azure region. Zone-redundant services replicate your applications and data across Availability Zones.
- B. An Availability Zone in an Azure region combines a fault domain and an update domain
- C. Availability zones are used to ensure that the VM resources are isolated from each other when they are deployed within an Azure datacenter.
- D. Only virtual machines that run Windows Server can be created in availability zones.

9) What is the name of the logical container used to group together and manage resources in Azure?

- A. Cloud Folders.
- B. Cloud Groups.
- C. Resource Groups.

10) For each of the following statements, select Yes if the statement is true. Otherwise, select No.

Statements	Yes	No
Availability zones can be implemented in all Azure regions.	<input type="checkbox"/>	<input type="checkbox"/>
Only virtual machines that run Windows Server can be created in availability zones.	<input type="checkbox"/>	<input type="checkbox"/>
Availability zones are used to replicate data and applications to multiple regions.	<input type="checkbox"/>	<input type="checkbox"/>

11) Your company has an Azure Kubernetes Service AKS cluster and a Windows 10 workstation with Azure CLI installed. You plan to use the Kubectl client on Windows 10. Which of the following commands should you run?

- A. az aks install-cli
- B. az aks nodepool
- C. az aks create
- D. az aks browse

12) This question requires that you evaluate the italicized text in double quotes to determine if it is correct.

When you need to delegate permissions to several Azure virtual machines simultaneously, you must deploy the Azure virtual machines "*to the same Azure region*".

Instructions: Review the italicized text in double quotes. If it makes this statement correct, select “No change is needed”. If this statement is incorrect, select the answer choice that makes the statement correct.

- A. No Change is needed
- B. By using the same Azure resource manager template
- C. To the same resource group
- D. To the same availability Zone

13) Please evaluate the following statement and select the right answer
Azure resources inherit locks from the resource group they are part of.

- A. YES
- B. NO

14) You received a new urgent task to create several Azure virtual machines in your Azure environment. Unfortunately, you are on holiday and you only have a tablet with you, that runs Android operating system.

Solution: You use Bash in Azure Cloud Shell.

Does this meet the goal?

- A. YES

B. NO

15) Please evaluate the following statement and select Yes if the statement is true, otherwise select No.

If your VM has a Read-only lock applied, you can add a Delete lock as well.

A. YES

B. NO

10.1 Answers

- 1) D. Office 365 on Azure is a Software as a Service component which is available to migrate the on-premise Microsoft Exchange email service. (Software-as-a-Service (SaaS)) - Software as a service (SaaS) allows users to connect to and use cloud-based apps over the Internet. Common examples are email, calendaring, and office tools (such as Microsoft Office 365)
- 2) A, C. Capex refers to large costs associated with initial setup of physical infrastructure, and all other options refer to limited costs of either renting cloud inventory or product licenses.
(Storage area network) - Storage costs are typically considered CapEx and include storage hardware components and the cost of supporting them. Depending on the application and level of fault tolerance, centralized storage can be expensive. Server costs are considered CapEx and include all server hardware components and the cost of supporting them.

(Hyper-V host server) - Physical server costs are considered CapEx and include all server hardware components and the cost of supporting them. When purchasing servers, make sure to design for fault tolerance and redundancy (e.g., server clustering, redundant power supplies, and uninterruptible power supplies). When a server needs to be replaced or added to a data center, you need to pay for the computer. This can affect your immediate cash flow because you must pay for the server up front.
- 3) A. Dynamic elasticity refers to an ability of auto-scaling and also auto-resizing based on demand. (A cloud service that responds quickly when demand increases and scales down when demand decreases) - Dynamic elasticity is defined as a cloud service that both quickly scales up and also back down in order to serve your changing workload patterns for

the lowest cost.

- 4) **A, B, D.** With Infrastructure as a Service (IaaS) the clients have complete control right from hardware to software; but this also creates a challenge on requiring manual intervention to support scaling of infrastructure based on demand

Client is responsible for all guest VM OS and application updates. Operating System (OS) licensing is included in the per-use cost of the service and is owned by the client.

However, the physical management of the servers are still owned by the Datacenter provider and hence not fully owned by the client.

Services can be scaled automatically to support system load. - IaaS host services often feature the ability to scale automatically to combat increased system load and scale back during periods of inactivity.

- 5) **A.** Since this is an internal web application, you would need to have control over every aspect and security of hosting this application (Infrastructure as a Service (IaaS)) - Only Infrastructure as a Service provides the required level of access to the Operating System. Platform as a Service (PaaS) is a complete development and deployment environment in the cloud, but does not provide the same level of Operating System access as an IaaS solution. Software as a service (SaaS) allows users to connect to and use cloud-based apps over the Internet but provides no access to the Operating System. Function as a Service (FaaS) such as Azure Functions are small single-purpose applications which do not provide Operating System access.
- 6) **C.** Hybrid Cloud is the cloud architecture which allows both public and private cloud to seamlessly operate together. A Hybrid Cloud is created when on-premise and public cloud environments are joined. This is a method many companies with existing on-premise infrastructure transition through in their journey to cloud, as it gives flexibility between the two environments and enables a phased migration

approach.

- 7) **C,D.** Private clouds enable high customization and security configuration and also as a result are more expensive to maintain Improved security - Because resources are not shared with others, private clouds provide higher levels of control and security.
High scalability - Private clouds still afford the scalability and efficiency of a public cloud.
- 8) **A,B .**Azure Availability zones eliminate any single point of failure and provide high availability and scalability through a regional network design that connects at least three physically distinct strategically placed data centers in each region. <https://azure.microsoft.com/en-us/global-infrastructure/availability-zones/#features>
Availability Zones replicate data and applications to multiple datacenters, Zone-redundant services replicate your applications and data across Availability Zones - Multiple datacenters protect your applications and data across availability zones to protect from single points of failure. By using this combination, high availability can be achieved. Both Linux and Windows virtual machines are supported in availability zones.
Availability Zone in an Azure region combines a fault domain and an update domain - Multiple datacenters protect your applications and data across availability zones to protect from single points of failure. By using this combination, high availability can be achieved.
- 9) **C.** Azure resource groups are logical containers to group and manage resources in Azure. An Azure Resource Group is a container used to hold the resources deployed in your Azure account. Resource Groups can contain almost any type of resource in Azure, such as Virtual Machines, VNets, and Storage Accounts. The other options do not exist.

- 10) Box 1: **No** - Not all Azure regions support availability zones.
Box 2: **No** - Availability zones can be used with many Azure services, not just VMs.
Box 3: **No** - Availability Zones are unique physical locations within a single Azure region.
- Reference:<https://docs.microsoft.com/en-us/azure/availability-zones/az-region#azure-regions-with-availability-zones>
- 11) A. – az aks install-cli
- 12) C. A resource group is a container that holds related resources for an Azure solution. The resource group can include all the resources for the solution, or only those resources that you want to manage as a group
- 13) A. Yes When you apply a lock at a parent scope, all resources within that scope inherit the same lock. Even resources you add later inherit the lock from the parent.
- 14) A. Yes, With Azure Cloud Shell, you can create virtual machines using Bash or PowerShell. Azure Cloud Shell is an interactive, authenticated, browser-accessible shell for managing Azure resources. It provides the flexibility of choosing the shell experience that best suits the way you work, either Bash or PowerShell.
- 15) A. Yes, This is indeed possible. Read-Only Lock means authorised users can read a resource, but they can't delete or update the resource. Delete Lock means authorised users can still read and modify a resource, but they can't delete the resource.

Chapter 11 : Practice Test 2

QUESTION 1

Which of the following solutions describes Azure Cosmos DB?

- A. A powerful database service designed specifically for analytics.
- B. A scalable in-memory data store.
- C. A MySQL compatible database solution with high availability and elastic scaling.
- D. A globally distributed multi-model database service.

QUESTION 2

You plan to map a network drive from several computers that run Windows 10 to Azure Storage.

You need to create a storage solution in Azure for the planned mapped drive.

What should you create?

- A. an Azure SQL database
- B. a virtual machine data disk
- C. a Files service in a storage account
- D. a Blobs service in a storage account

QUESTION 3

To complete the sentence, select the appropriate option in the answer area.

Data that is stored in the Archive access tier of an Azure storage account:

- A. can be accessed at any time using azcopy.exe.
- B. can only be read using Azure Backup.
- C. must be restored before the data can be accessed.
- D. Must be rehydrated before the data can be accessed.

QUESTION 4

What Azure service allows you to have a DNS-based traffic load balancer?

- A. Azure Private Load Balancer

- B. Azure Network Interface
- C. Azure Public Load Balancer
- D. Azure Traffic Manager

QUESTION 5

Azure Cosmos DB is an example of a _____ offering.

- A. Platform as a service
- B. Infrastructure as a service
- C. Serverless
- D. Software as a service

QUESTION 6

You have an Azure subscription that contains a policy-based virtual network gateway named GW1 and a virtual network named VNet1.

You need to ensure that you can configure a point-to-site connection from VNet1 to an on-premises computer.

Which two actions should you perform?

- A. Reset GW1
- B. Create a route based virtual network gateway
- C. Delete GW1
- D. Add a public IP address space to VNet1
- E. Add a connection to GW1
- F. Add a service endpoint to VNet1

QUESTION 7

The company CFO is concerned about the costs the new Azure ExpressRoute connection will bring. Please evaluate the following statement and select Yes if the statement is true, otherwise select No.

You explain to the CFO that inbound data traffic from the company's on-premises data centre to Azure cloud is always free, while using Azure ExpressRoute.

- A. YES

B. NO

QUESTION 8

Please evaluate the following statement and select Yes if the statement is true, otherwise select No.

Outbound data traffic from Azure to external destinations is always free.

- A. YES
- B. NO

QUESTION 9

Please evaluate the following statement and select Yes if the statement is true, otherwise select No.

Azure Firewall encrypts network traffic sent from Azure to outside destinations.

- A. YES
- B. NO

QUESTION 10

Please evaluate the following statement and select Yes if the statement is true, otherwise select No.

Azure Network Security Groups (NSGs) encrypt traffic sent from Azure to outside destinations.

- A. YES
- B. NO

11.1 Practice Test 2 : Answers

1. **D.** globally distributed multi-model database service - Azure Cosmos DB is a globally distributed multi-model database offering designed to guarantee low latency and high availability. It is compatible with Cassandra, MongoDB and other NoSQL workloads.
2. **C.** Azure Files is Microsoft's easy-to-use cloud file system. Azure file shares can be seamlessly used in Windows and Windows Server. To use an Azure file share with Windows, you must either mount it, which means assigning it a drive letter or mount point path, or access it via its UNC path. Unlike other SMB shares you may have interacted with, such as those hosted on a Windows Server, Linux Samba server, or NAS device, Azure file shares do not currently support Kerberos authentication with your Active Directory (AD) or Azure Active Directory (AAD) identity, although this is a feature we are working on. Instead, you must access your Azure file share with the storage account key for the storage account containing your Azure file share. A storage account key is an administrator key for a storage account, including administrator permissions to all files and folders within the file share you're accessing, and for all file shares and other storage resources (blobs, queues, tables, etc) contained within your storage account.
3. **D.** Must be rehydrated before the data can be accessed. Azure storage offers different access tiers: hot, cool and archive. The archive access tier has the lowest storage cost. But it has higher data retrieval costs compared to the hot and cool tiers. Data in the archive tier can take several hours to retrieve.

While a blob is in archive storage, the blob data is offline and can't be read, overwritten, or modified. To read or download a blob in an archive, you must first rehydrate it to an online tier.

Example usage scenarios for the archive access tier include:

☞ Long-term backup, secondary backup, and archival datasets

- ☞ Original (raw) data that must be preserved, even after it has been processed into final usable form.
- ☞ Compliance and archival data that needs to be stored for a long time and is hardly ever accessed.

Reference: <https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blob-storage-tiers?tabs=azure-portal#archive-access-tier>

4. **D.** Azure Traffic Manager is a DNS-based traffic load balancer that enables you to distribute traffic optimally to services across global Azure regions while providing high availability and responsiveness. Traffic Manager uses DNS to direct client requests to the most appropriate service endpoint based on a traffic-routing method and the health of the endpoints.
5. **A.** platform as a service (PaaS)
Cosmos Database (DB) is a horizontally scalable, globally distributed, fully managed, low latency, multi-model, multi query-API database for managing data at large scale. Cosmos DB is a PaaS (Platform as a Service) offering from Microsoft Azure and is a cloud-based NoSQL database. Cosmos DB is sometimes referred to as a serverless database, and it is a highly available, highly reliable, and high throughput database. Cosmos DB is a superset of Azure Document DB and is available in all Azure regions.
6. **B,C.**
A VPN gateway is used when creating a VPN connection to your on-premises network.
Route-based VPN devices use any-to-any (wildcard) traffic selectors, and let routing/forwarding tables direct traffic to different IPsec tunnels. It is typically built on router platforms where each IPsec tunnel is modeled as a network interface or VTI (virtual tunnel interface).
Policy-based VPN devices use the combinations of prefixes from both

networks to define how traffic is encrypted/decrypted through IPsec tunnels. It is typically built on firewall devices that perform packet filtering. IPsec tunnel encryption and decryption are added to the packet filtering and processing engine.

Point-to-Site connections do not require a VPN device or a public-facing IP address; so you can delete GW1

7. **A.** Yes, With Azure ExpressRoute, all inbound data transfer is free of charge, but outbound data is charged based on your plan.
8. **B.** No, while inbound data transfer is free, outbound is not
9. **B.** No, Azure firewall does not encrypt network traffic. It is used to block or allow traffic based on source/destination IP address, source/destination ports and protocol.
10. **B.** No, A network security group does not encrypt network traffic. It works in a similar way to a firewall and is used to block or allow traffic based on source/destination IP address, source/destination ports and protocol.

Chapter 12 : Practice Test 3

QUESTION 1

Your company plans to deploy several million sensors that will upload data to Azure.

You need to identify which Azure resources must be created to support the planned solution.

Which two Azure resources should you identify?

- A. Azure Data Lake
- B. Azure Queue Storage
- C. Azure File Storage
- D. Azure IoT Hub
- E. Azure Notifications tab

QUESTION 2

Please evaluate the following statement and select Yes if the statement is true, otherwise select No.

Azure Monitor can trigger alerts based on data in an Azure Log Analytics workspace.

- A. YES
- B. NO

QUESTION 3

You are working for a multinational company that has local presence with offices in 40+ countries. As per company policy, you need to make sure that Azure resources are created in an Azure region where each office is located.

What Azure service would you use in order to meet the policy requirement ?

- A. Azure Policy
- B. Management Group
- C. Reservation

- D. Read Only lock

QUESTION 4

You have been working on a new migration project for several weeks already. The project manager has asked you to configure Azure to send email alerts when the cost of the current billing period for the Azure subscription exceeds a specified limit.

What will you use in this case?

- A. Azure Advisor
- B. Budget Alerts
- C. Azure IAM
- D. Compliance Manager

QUESTION 5

Which Azure service provides a platform for serverless code?

- A. Azure Container Instances
- B. Azure Virtual Machines
- C. Azure Functions
- D. Azure App Service

QUESTION 6

You have an on-premises application that sends email notifications automatically based on a rule. You plan to migrate the application to Azure.

You need to recommend a serverless computing solution for the application.

What should you include in the recommendation?

- A. An API App
- B. A web app
- C. A server image in Azure marketplace
- D. A logic App

QUESTION 7

Please evaluate the following statement and select Yes if the statement is true, otherwise select No.

Azure App Service hosts web applications.

- A. YES
- B. NO

QUESTION 8

Please evaluate the following statement and select Yes if the statement is true, otherwise select No.

Azure Databricks is a big data analysis Azure service used for machine learning.

- A. YES
- B. NO

QUESTION 9

Please evaluate the following statement and select Yes if the statement is true, otherwise select No.

Azure Application Insights detects and diagnoses anomalies in web applications.

- A. YES
- B. NO

QUESTION 10

Please evaluate the following statement and select Yes if the statement is true, otherwise select No.

Azure Advisor generates a list of Azure virtual machines that are protected by Azure Backup.

- A. YES
- B. NO

Practice Test 3 : Answers

1) A,D.

Azure Data lake is CORRECT here because it is used for storing different kinds of data such as structured, semi-structured, or unstructured data which is generated from a variety of applications including social networks, IoT hubs and sensors, relational data, videos, web apps, mobile or desktop devices. The data uploaded by the sensors (using azure data factory REST APIs or IoT Hub) don't need to be processed immediately and should be stored for a good period of time to allow it to be analyzed later. Hence Data Lake is the more appropriate answer.

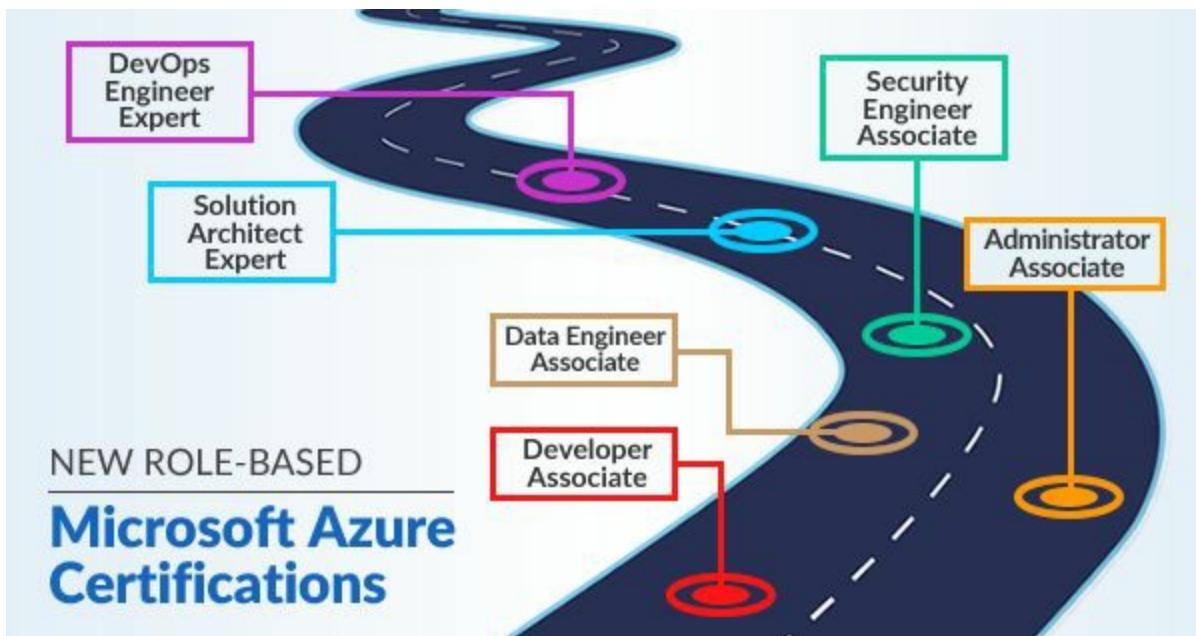
IoT Hub (Internet of things Hub) is CORRECT here because it provides data from millions of sensors and supports writing data to Azure data lake gen2 (built on top of Azure storage account) in the Apache Avro format as well as in JSON format.

- 2) **A.** Yes, Azure Monitor uses Target Resource, which is the scope and signals available for alerting. A target can be any Azure resource. Example targets: a virtual machine, a storage account, a virtual machine scale set, a Log Analytics workspace, or an Application Insights resource
- 3) **A.** Azure Policy. Azure policies can be used to define requirements for resource properties during deployment and for already existing resources. Azure Policy controls properties such as the types or locations of resources.
Azure Policy offers several built-in policies that are available by default. In this question, we would use the 'Allowed Locations' policy to define the locations where resources can be deployed.
- 4) **B.** Budget alerts notify you when spending, based on usage or cost, reaches or exceeds the amount defined in the alert condition of the budget. Cost Management budgets are created using the Azure portal or

- the Azure Consumption API.
- 5) **C.** Azure Functions. Azure provides a range of serverless execution environments, fully managed services and a comprehensive set of developer tools and services to build your applications. If we now refer to running code in Azure in a serverless manner, Azure Functions service can be used.
- 6) **D.** Logic App, Azure Logic Apps can be used and integrated with your applications to send email notifications based on conditions that you configure. You can use Logic Apps to send email notifications from your Office365 or even personal Gmail account.
- 7) **A.** Yes, Azure App service can host web applications (webapps)
- 8) **A.** Yes, Azure Databricks is an Apache Spark-based analytics platform. The platform consists of several components including 'MLib'. 'Mlib' is a Machine Learning library consisting of common learning algorithms and utilities, including classification, regression, clustering, collaborative filtering, dimensionality reduction, as well as underlying optimization primitives.
- 9) **A.** Yes, Application Insights, a feature of Azure Monitor, is an extensible Application Performance Management (APM) service for developers and DevOps professionals. Use it to monitor your live applications. It will automatically detect performance anomalies, and includes powerful analytics tools to help you diagnose issues and to understand what users actually do with your app.
- 10) **B.** No, Azure Advisor does not generate a list of virtual machines that are protected by Azure Backup. Azure Advisor does however, generate a list of virtual machines that ARE NOT protected by Azure Backup. You can view a list of virtual machines that are protected by Azure

Backup by viewing the Protected Items in the Azure Recovery Services Vault.

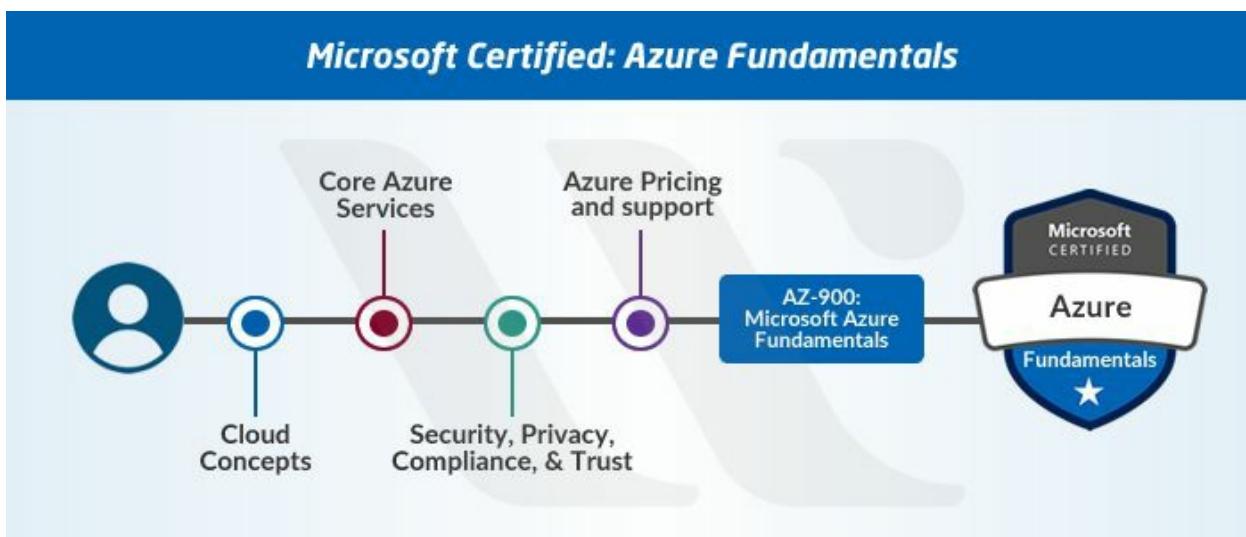
Chapter 13 : Next Steps



The new role-based Azure certifications establish a learning path from the Fundamental level to Associate level and then to the Expert level. There are five Microsoft Azure Certifications path for five different roles particularly based on Azure; the roles are –

- Azure Fundamentals
- Azure Administrator Associate
- Azure Developer Associate
- Azure Solution Architect Expert
- Azure DevOps Engineer Expert
- Azure Security Engineer Associate
- Azure Data Engineer Associate

1. Azure Fundamentals



Azure Fundamentals (AZ-900) is the foundational level exam in the new Azure certifications path. This exam is intended for those who want to demonstrate their basic knowledge of cloud services with Microsoft Azure. Even if you are non-technical (Sales, Marketing, etc) but as long as you have some basic understanding of the concepts of cloud, you can take this certification exam.

Exam AZ-900: Microsoft Azure Fundamentals

This exam is considered as the first step in associate level and expert level Azure certifications path. Although it's an optional step, validating your foundational knowledge will benefit you to some extent.

Let's have a look at the details of the Azure AZ-900 exam.

Prerequisites: There are no particular prerequisites for the Microsoft Azure Fundamental exam but one should be familiar and have a basic understanding of the cloud services and the Microsoft Azure platform.

Domains Covered in AZ-900 Exam are –

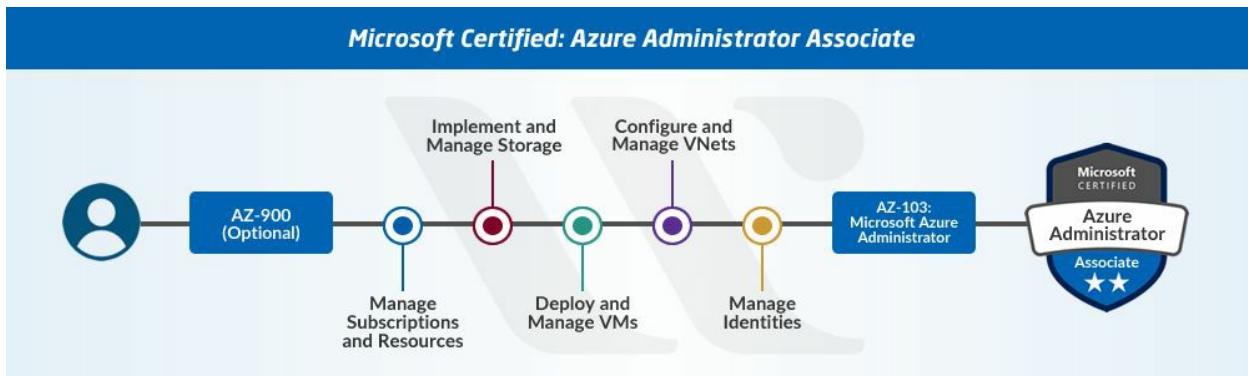
Domain	% Weight
Understand Cloud Concepts	15-20%
Understand Core Azure Services	30-35%
Understand Security, Privacy, Compliance, and Trust	25-30%

Understand Azure Pricing and Support | 25-30%

Exam Languages: English, Japanese, Simplified Chinese, and Korean

Certification Cost: USD 99

2. Azure Administrator Associate



As per the new updates, one needs to pass only one certification exam i.e. Exam AZ-103: Microsoft Azure Administrator to become Azure Administrator Associate. After passing the certification exam for AZ-103, you will become a Microsoft Certified Azure Administrator Associate and receive a badge of Azure Administrator Associate.

AZ-103: Microsoft Azure Administrator

From May 1, 2019, the aspirants will only need to pass AZ-103: Microsoft Azure Administrator exam to earn the Azure Developer Associate certification. The exam AZ-103 combines the skills and domains covered in the exams AZ-100 and AZ-101; more from the AZ-100 exam. This exam also acts as a prerequisite for the Microsoft Certified Azure DevOps Engineer Expert exam.

Prerequisites: Prerequisites for Microsoft Azure Infrastructure and Deployment are –

- You should have prior knowledge of Azure applications, Operating Systems, Cloud and Storage Infrastructure.
- You should also have a basic knowledge of networking components and

virtualization tools.

- If you know PowerShell and the Command Line Interface, then it will be an added advantage.

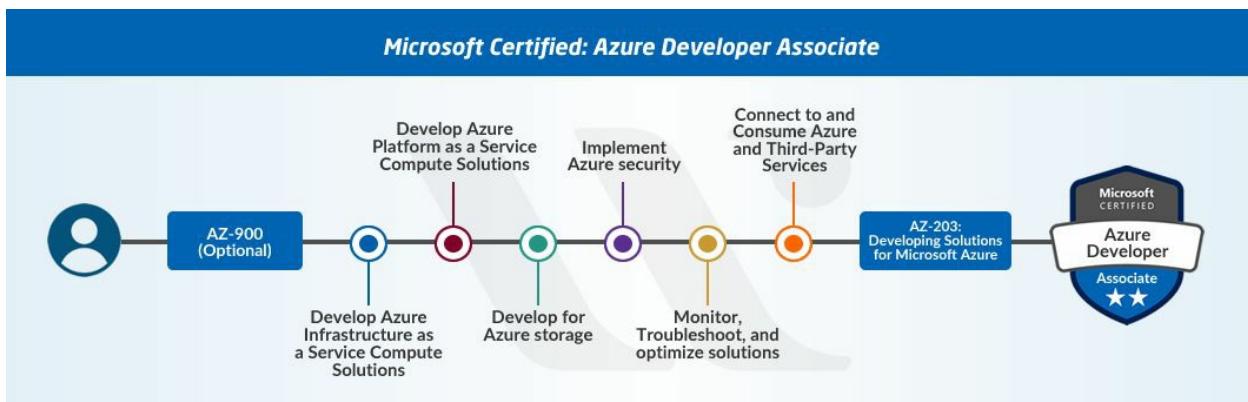
Domains Covered in the Exam are –

Domain	% Weight
Manage Azure subscriptions and resources	15-20%
Implement and manage storage	15-20%
Deploy and manage virtual machines (VMs)	15-20%
Configure and manage virtual networks	30-35%
Manage identities	15-20%

Exam Languages: English, Japanese, Simplified Chinese, and Korean

Certification Cost: USD 165

3. Azure Developer Associate



For the Azure Developer Associate role, you need to pass only one certification Exam AZ-203: Developing Solutions for Microsoft Azure. After passing the certification exam for AZ-203, you will become Microsoft Certified Azure Developer Associate and will receive a badge of Azure Developer Associate.

AZ-203: Developing Solutions for Microsoft Azure

AZ-203: Developing Solutions for Microsoft Azure exam released on September 24, 2018. Developing Solutions for Microsoft Azure exam (AZ-203) is the only exam for the Azure Developer Associate role. It also acts as a

prerequisite for the Microsoft Certified Azure DevOps Engineer Expert exam.

Whether you have already passed the 70-532 exam or not, you will receive the badge of Microsoft Certified Azure Developer Associate on passing the AZ-203 exam.

Note that, previously, Microsoft launched [Exam AZ-200](#) and [Exam AZ-201](#) for the Azure Developer Associate Role. But now Microsoft has discontinued AZ-200 and AZ-201 exams and replaced them with AZ-203 exams as per the feedback on the beta versions of AZ-200 and AZ-201 exams.

Prerequisites: AZ-203 exam is for the Azure developers who are responsible for the designing and building cloud solutions on the Azure platform.

Prerequisites for Developing Solutions for Microsoft Azure (AZ-203) are –

- The candidate should have the proficiency to develop services and apps by the implementation of Azure tools and technologies
- The candidate should have at least one year of experience in developing scalable solutions
- The candidate should be skilled in at least one cloud-supported programming language

Domains Covered in the Exam are –

Domain	% Weight
Develop Azure Infrastructure as a Service Compute Solutions	10-15%
Develop for Azure Storage	15-20%
Develop Azure Platform as a Service Compute Solutions	20-25%
Implement Azure Security	10-15%
Monitor, Troubleshoot, and Optimize Azure Solutions	15-20%
Connect and Consume Azure Services & Third-party	

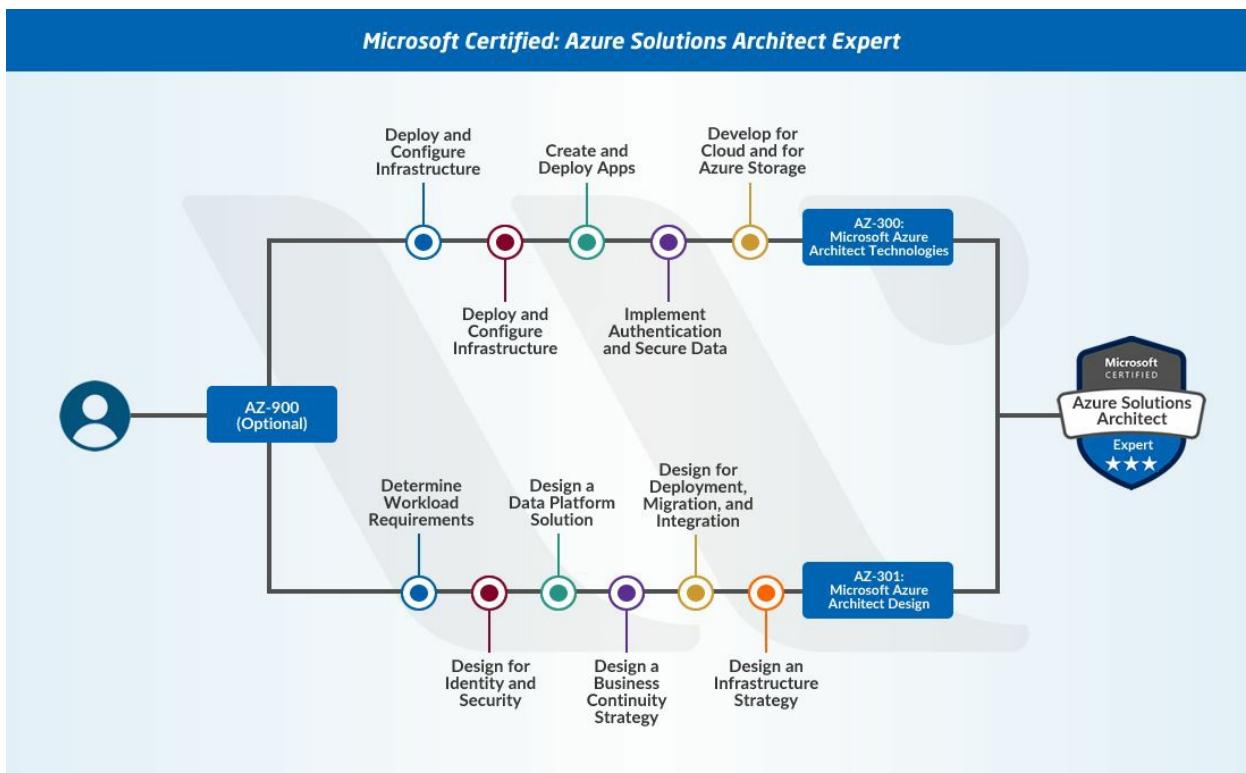
Services

20-25%

Exam Languages: English, Japanese, Simplified Chinese, and Korean

Certification Cost: USD 165

4. Azure Solution Architect Expert



As per the new role-based Azure certifications path, for Azure Solution Architect Expert role, you need to pass two certifications – Exam AZ-300: Microsoft Azure Architect Technologies and Exam AZ-301: Microsoft Azure Architect Design. After passing the certification exams for AZ-300 and AZ-301, you will become Microsoft Certified Azure Solution Architect Expert and will receive a badge of Azure Solution Architect Expert.

Microsoft Azure Architect Technologies (AZ-300)

On September 24, 2018 – Microsoft released the beta version of Microsoft Azure Architect Technologies (AZ-300). This certification comes under the Azure Solutions Architect Expert role in the new role-based Azure

certifications path. You need to pass the AZ-300 exam first to become an Azure Solutions Architect Expert. It provides knowledge in architecting solutions that are reliable and secure.

Note that the beta version for the AZ-300 exam has been retired now.

Prerequisites: Prerequisites for Microsoft released Microsoft Azure Architect Technologies (AZ-300) are –

- You should have knowledge of security, identity, data management, and IT operations.
- One year experience is also required for this certification.
- You should also have knowledge of DevOps, Azure development and Azure administration.

Domains Covered in the Exam are –

Domain	% Weight
Deploy and Configure Infrastructure	25-30%
Implement Workloads and Security	20-25%
Architect Cloud Technology Solutions	5-10%
Create and Deploy Apps	5-10%
Implement Authentication and Secure Data	5-10%
Develop for the Cloud	20-25%

Exam Languages: English, Japanese, Simplified Chinese, and Korean

Certification Cost: USD 165

Microsoft Azure Architect Design (AZ-301)

Microsoft also released Microsoft Azure Architect Design (AZ-301) in beta on September 24, 2018. This certification also comes under the Azure Solutions Architect Expert role in the new role-based Azure certifications path. After the AZ-300 exam, you need to pass the AZ-301 exam to become an Azure Solutions Architect Expert.

Prerequisites: Prerequisites for Microsoft Azure Architect Design (AZ-301) are the same as in Microsoft Azure Architect Technologies (AZ-300). But one should have passed the AZ-300 exam to take the AZ-301 exam.

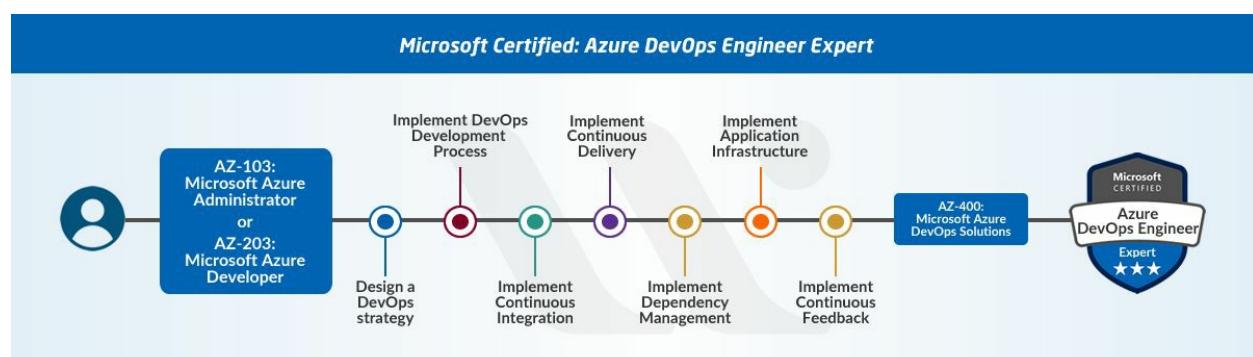
Domains covered in the exam are –

Domain	% Weight
Determine Workload Requirements	10-15%
Design for Identity and Security	20-25%
Design a Data Platform Solution	15-20%
Design a Business Continuity Strategy	15-20%
Design for Deployment, Migration, and Integration	10-15%
Design an Infrastructure Strategy	15-20%

Exam Languages: English, Japanese, Simplified Chinese, and Korean

Certification Cost: USD 165

5. Azure DevOps Engineer Expert



One who has already received the badge of Azure Administrator Associate or Azure Developer Associate can become an Azure DevOps Engineer Expert.

Whether be the Azure Administrator Associate or Azure Developer Associate, the candidate needs to pass Exam AZ-400: Microsoft Azure DevOps Solutions to become Azure DevOps Engineer.

Let's have a look at the details of the AZ-400 exam.

Microsoft Azure DevOps Solutions (AZ-400)

Microsoft also released Microsoft Azure DevOps Solutions (AZ-400) – BETA Version in beta on September 24, 2018. This certification also comes under the Azure DevOps Engineer Expert role. After receiving the badge of Azure Administrator Associate or Azure Developer Associate, one needs to pass the AZ-400 exam to become an Azure DevOps Engineer Expert.

Prerequisites: Prerequisites for Microsoft Azure DevOps Solutions (AZ-400) exam are –

- Familiarity with both the Azure development and Azure administration and expertise in at least one of these areas
- Ability to design and implement DevOps practices for infrastructure as code, version control, configuration management, compliance, release, build, and testing with the use of Azure technologies.
- Proficiency in Agile practices

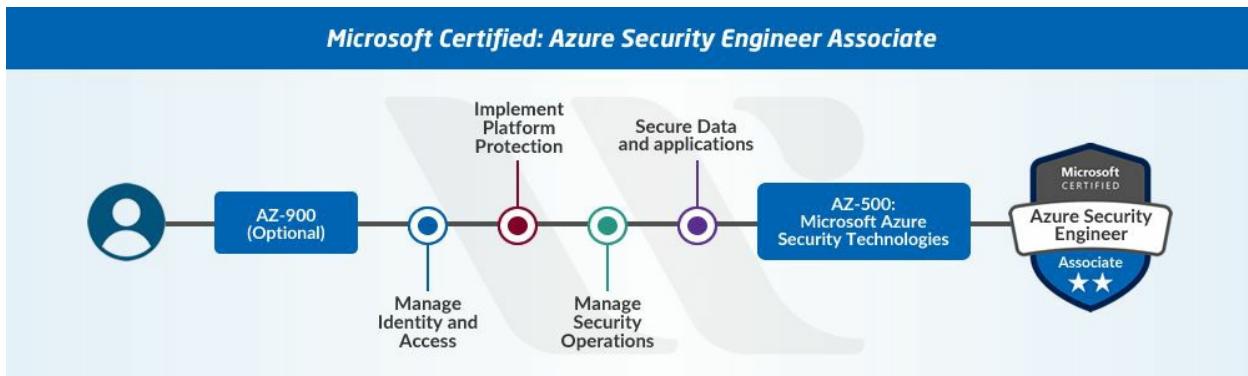
Domains Covered in the Exam are –

Domain	% Weight
Design a DevOps Strategy	20-25%
Implement DevOps Development Processes	20-25%
Implement Continuous Integration	10-15%
Implement Continuous Delivery	10-15%
Implement Dependency Management	5-10%
Implement Application Infrastructure	15-20%
Implement Continuous Feedback	10-15%

Exam Languages – English, Japanese, Simplified Chinese, and Korean

Certification Cost – USD 165

6. Azure Security Engineer Associate



Azure Security Engineer is the newest role added in the role-based Azure certification path. To become a Microsoft Certified Azure Security Engineer, you need to pass only one certification – Exam AZ-500: Microsoft Azure Security Technologies. On passing the certification exam for AZ-500, you will become a Microsoft Certified Azure Security Engineer and will receive a badge of Azure Security Engineer. Let's have a look at the details of the AZ-500 exam.

Microsoft Azure Security Technologies (AZ-500)

Microsoft has recently launched AZ-500: Azure Security Technologies exam for Azure security engineers. You don't need to pass any other certification to be eligible for the AZ-500 exam but it is recommended to pass AZ-900: Microsoft Azure Fundamentals exam.

Prerequisites: Prerequisites for Microsoft Azure Security Technologies (AZ-500) exam are –

- Familiarity with the implementation of security controls on the Microsoft Azure platform
- In-depth knowledge of virtualization, cloud N-tier architecture, Amazon Kubernetes Service, and networking
- Ability to recognize and address vulnerabilities using several security tools; implementing security solutions for the protection of networks, applications, and data
- Expertise in scripting and automation, identity and access management,

and maintaining security status

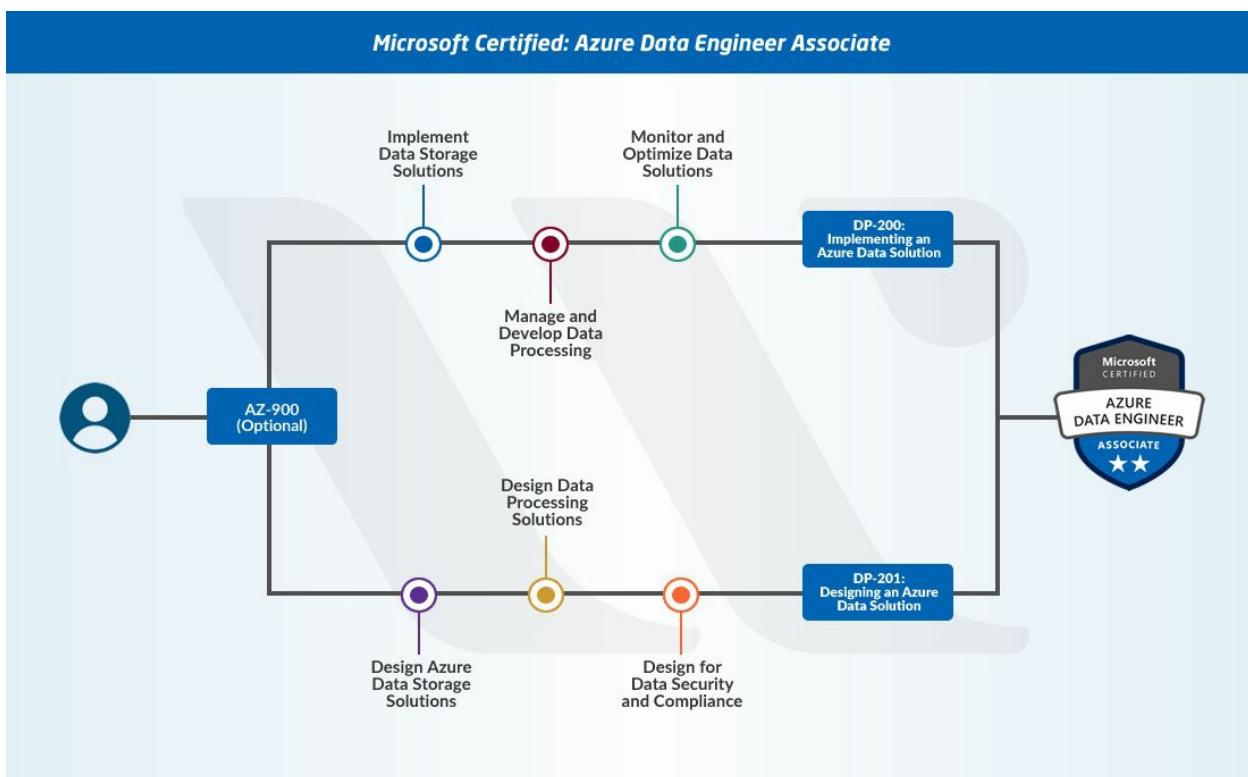
Domains Covered in the Exam are –

Domain	% Weight
Manage Identity and Access	20-25%
Implement Platform Protection	35-40%
Manage Security Operations	15-20%
Secure Data and Applications	30-35%

Exam Languages – English, Simplified Chinese, Japanese, and Korean

Certification Cost – USD 165

7. Azure Data Engineer Associate



The Microsoft Certified: Azure Data Engineer Associate is one of the latest additions to the Azure certifications path. The certification is ideal for individuals who want to pursue the role of Azure Data Engineers. Azure data engineers specialize in the design and implementation of data management, monitoring, security, and privacy.

Azure data engineers also show comprehensive fluency in the complete stack of Azure data services to address business requirements. Candidates have to clear two Azure certification exams to earn the tag of ‘Azure Data Engineer Associate.’ The two exams have the codes DP-200 and DP-201. Let us reflect further on the details of each certification exam.

DP-200: Implementing an Azure Data Solution

DP-200: Implementing an Azure Data Solution exam is suitable for Microsoft Azure data engineers. The DP-200 came into the Azure certifications path on January 31st, 2019. The DP-200 certification exam is one out of the two exams for Azure Data Engineer Associate certification. It serves as a supporting examination for the other examination, i.e., DP-201 in the Microsoft Certified: Azure Data Engineer Associate exam.

Prerequisites

DP-200 exam is for the Azure data engineers responsible for implementing data solutions on the Azure cloud platform. The prerequisites for the DP-200 Azure certification exam are as follows.

1. The ability for implementing data solutions using Azure services.
2. No previous Azure certification is needed.

Domains covered in the DP-200 exam are –

Domain	Weight
Implementing data storage solutions	40-45%
Managing and developing data processing	25-30%
Monitoring and optimization of data solutions	30-35%

Exam Languages: English, Japanese, Korean, and Simplified Chinese.

Certification Cost: \$165 USD.

DP-201: Designing an Azure Data Solution

Microsoft released the DP-201 exam in Azure certifications path on January 31st, 2019, alongside the DP-200 exam. The certification is a part of the Azure Data Engineer Associate job role in the new role-based certification path. Candidates have to clear DP-200 and DP-201 both to obtain the Azure Data Engineer Associate certification.

Prerequisites

The prerequisites for DP-201: Designing an Azure Data Solution exam are as follows.

1. The ability for designing solutions using Azure services.
2. No prior certification is needed.

One important highlight in the case of the DP-201 exam is the recommended practice of clearing the DP-200 exam before registering for DP-201.

Domains covered in the DP-201 exam are –

Domain	Weight
Designing Azure data storage solutions	40-45%
Designing Azure data processing solutions	25-30%
Designing for data security and compliance	25-30%

Exam Languages: English, Simplified Chinese, Korean and Japanese.

Certification cost: \$165 USD.