AZ-900 Azure Fundamentals

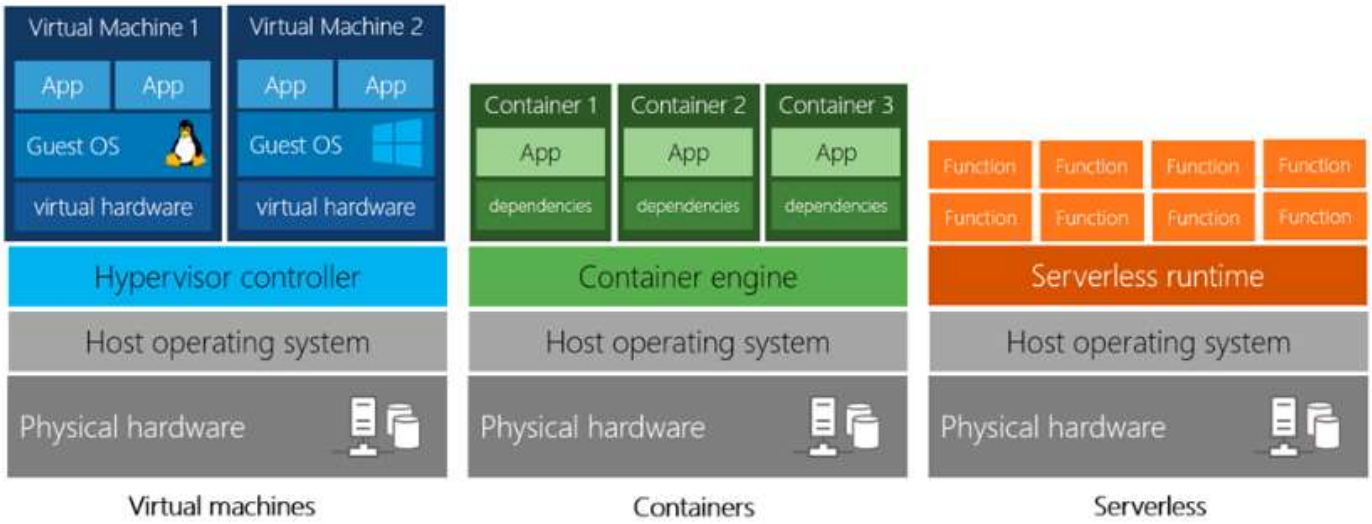
Tuesday, September 15, 2020 1:36 PM

Describe Cloud Concepts (15-20%)

Describe the benefits and considerations of using cloud services

Computing Power

VM vs. Containers vs. Serverless Computing:



• Describe terms such as High Availability, Scalability, Elasticity, Agility, Fault Tolerance, and Disaster Recovery

High availability. The ability to keep **services up and running for long periods of time**, with very **little downtime**, depending on the service in question.

Scalability. The ability to **increase or decrease resources for any given workload**. You can add additional resources to service a workload (known as scaling out), or add additional capabilities to manage an increase in demand to the existing resource (known as scaling up). **Scalability doesn't have to be done automatically.**

Scaling out - add additional resources (scaling in - decrease resources)

scaling up - add additional capabilities (scaling down - decrease capabilities)

Elasticity. The ability to **automatically or dynamically increase or decrease resources as needed**. Elastic resources match the current needs, and resources are added or removed **automatically** to meet future needs when it's needed (and from the most advantageous geographic location). **A distinction between scalability and elasticity is that elasticity is done automatically.**

Agility. The **ability to react quickly**. Cloud services can allocate and deallocate resources quickly. They are provided on-demand via self-service, so vast amounts of computing resources can be provisioned in minutes. There is no manual intervention in provisioning or deprovisioning services.

Fault tolerance. The **ability to remain up and running** even in the event of a component (or service) no longer functioning. **Typically, redundancy is built** into cloud services architecture, so if one component fails, a backup component takes its place. This type of service is said to be tolerant of faults.

Disaster recovery. The **ability to recover from an event which has taken down a cloud service.** Cloud services disaster recovery can happen very quickly, with automation and services being readily available to use.

https://azure.microsoft.com/en-us/overview/cloud-computing-dictionary/

• Describe the principles of economies of scale

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

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

This is apparent to end users in a number of ways, one of which is the **ability to acquire hardware at a lower cost than if a single user**

or smaller business were purchasing it.

• Describe the differences between Capital Expenditure (CapEx) and Operational Expenditure (OpEx)

Capital Expenditure (CapEx): This is the up front spending of money on physical infrastructure, and then deducting that up front expense over time. The up front cost from CapEx has a value that reduces over time.

Operational Expenditure (OpEx): This is spending money on services or products now and being billed for them now. You can deduct this expense in the same year you spend it. There is no up front cost, as you pay for a service or product as you use it.

• Describe the consumption-based model

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

A consumption-based model has many benefits, including:

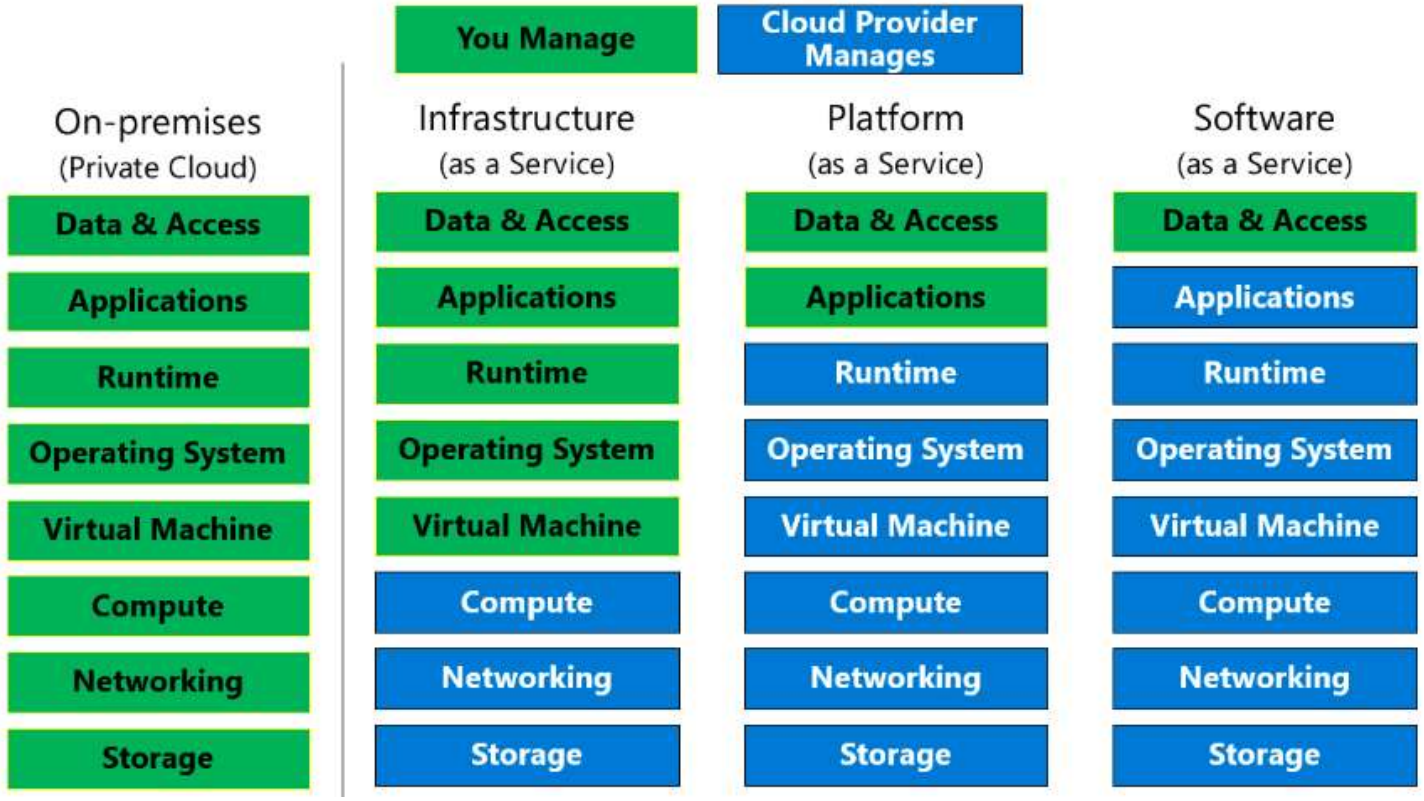
- No upfront costs.
- No need to purchase and manage costly infrastructure that they may or may not use to its fullest.
- The ability to pay for additional resources when they are needed.
- The ability to stop paying for resources that are no longer needed.

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

Describe the differences between Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS)

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

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



IaaS requires the **most user management of all the cloud services**. The **user** is responsible for managing the **operating systems, data, and applications**.

PaaS requires less user management. The **cloud provider manages the operating systems**, and the **user** is responsible for the **applications and data** they run and store.

SaaS requires the **least amount of management**. The **cloud provider is responsible for managing everything**, and the end **user** just **uses the software**.

• Describe Infrastructure-as-a-Service (IaaS),

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

IaaS characteristics:

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

Common IaaS usage scenarios:

Migrating workloads. Typically, IaaS facilities are managed in a similar way as on-premises infrastructure and provide an easy migration path for moving existing applications to the cloud.

Test and development. Teams can quickly set up and dismantle test and development environments, bringing new applications to market faster. IaaS makes scaling development testing environments up and down fast and economical.

Website hosting. Running websites using IaaS can be less expensive than traditional web hosting.

Storage, backup, and recovery. Organizations avoid the capital outlay and complexity of storage management, which typically requires a skilled staff to manage data and meet legal and compliance requirements. IaaS is useful for managing unpredictable demand and steadily growing storage needs. It can also simplify the planning and management of backup and recovery systems.

• Describe Platform-as-a-Service (PaaS)

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

PaaS characteristics:

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

Common PaaS usage scenarios:

Development framework. PaaS provides a framework that developers can build upon to develop or customize cloud-based applications. Similar to the way you create a Microsoft Excel macro, PaaS lets developers create applications using built-in software components. Cloud features such as scalability, high-availability, and multi-tenant capability are included, reducing the amount of coding that developers must do.

Analytics or business intelligence. Tools provided as a service with PaaS allow organizations to analyze and mine their data. They can find insights and patterns, and predict outcomes to improve business decisions such as forecasting, product design, and investment returns.

• Describe Software-as-a-Service (SaaS)

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

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

SaaS characteristics:

Users have **no upfront costs**; they **pay a subscription**, typically on a **monthly or annual basis**.

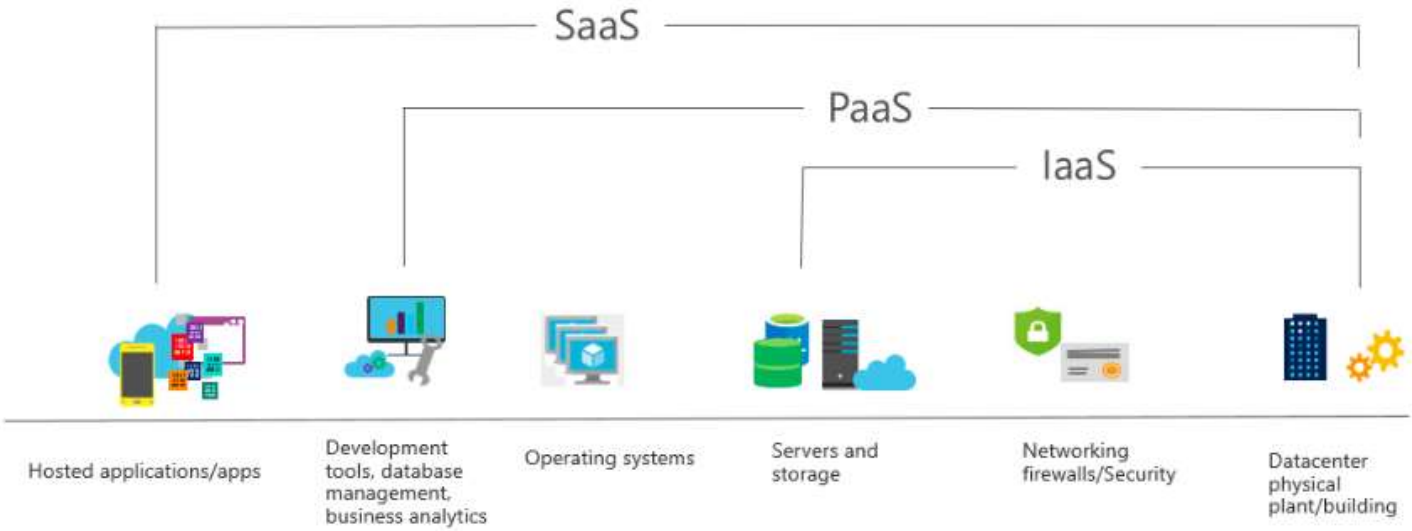
Users just **use the application software**; they are **not responsible** for any **maintenance or management** of that software.

The **cloud provider** is responsible for the **provision, management, and maintenance of the application software**.

Common SaaS usage scenarios:

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

• Compare and contrast the three different service types



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

Services	Advantage	Disadvantage
IaaS	**No CapEx** **Agile** **Consumption-based model** **No** deep technical **skills** are required Organizations can **leverage the skills and expertise of the cloud provider** IaaS is the **most flexible** cloud service	The **user manages and maintains the services** they have provisioned, and the **cloud provider manages and maintains the cloud infrastructure**.
PaaS	**No CapEx** **Agile** **Consumption-based model** **No** deep technical **skills** are required Organizations can **leverage the skills and expertise of the cloud provider** Users can **focus on application development only**, as **all platform management is handled by the cloud provider.**	There **may be some limitations to a cloud platform** that could affect how an application runs. Any **limitations should be taken into consideration** when considering which PaaS platform is best suited for a workload.
SaaS	**No CapEx** **Agile** **Pay-as-you-go pricing model**: Users pay for the software they use on a subscription model, typically monthly or yearly, regardless of how much they use the software. **Flexibility**. Users can **access the same application data from anywhere**.	**Software limitations.** There may be some limitations to a software application that might affect how users work. Since you are using as-is software you don't have direct control of features. Any business needs and software limitations should be taken into consideration when considering which SaaS platform is best suited for a workload.

Describe the differences between Public, Private and Hybrid cloud models

• Describe Public cloud

A **public cloud** is **owned by the cloud services provider** (also known as a hosting provider). It provides resources and services to multiple organizations and users, who connect to the cloud service via a secure network connection, typically over the internet.
Public cloud models have the following characteristics:
Ownership - Ownership refers to the resources that an organization or end user uses. Examples include storage and processing power. **Resources** do not belong to the organization that is utilizing them, but rather they are **owned and operated by a third party**, such as **the cloud service provider**.
Multiple end users - Public cloud modes may make their resources available to multiple organizations.
Public access - Public access allows the public to access the desired cloud services.
Availability - Public cloud is the most common cloud-type deployment model.
Connectivity - Users and organizations are typically connected to the public cloud over the internet using a web browser.
Skills - Public clouds do not require deep technical knowledge to set up and use its resources.

• Describe Private cloud

A **private cloud** is **owned and operated by the organization that uses the resources from that cloud**. They create a cloud environment in their own datacenter and provide self-service access to compute resources to users within their organization. The organization remains the owner, entirely responsible for the operation of the services they provide.
Private cloud models have the following characteristics:
Ownership - The **owner and user of the cloud services are the same**.
Hardware - The **owner** is entirely **responsible for the purchase, maintenance, and management of the cloud hardware**.
Users - A private cloud **operates only within one organization** and cloud computing **resources are used exclusively by a single business or organization**.
Connectivity - A connection to a private cloud is **typically made over a private network that is highly secure**.
Public access - Does **not provide access to the public**.
Skills - **Requires deep technical knowledge to set up, manage, and maintain**.

• Describe Hybrid cloud

A **hybrid cloud** combines **both public and private clouds**, allowing you to **run your applications in the most appropriate location**.
Hybrid cloud models have the following characteristics:
Resource location - **Specific resources run or are used in a public cloud**, and **others run or are used in a private cloud**.
Cost and efficiency - Hybrid cloud models allow an organization to **leverage some of the benefits of cost, efficiency, and scale that are available with a public cloud model.**
Control - Organizations **retain management control in private clouds.**
Skills - **Technical skills are still required to maintain the private cloud and ensure both cloud models can operate together.**

• Compare and contrast the three different cloud models

Cloud Model	Advantage	Disadvantage
Public	No CapEx Agility Consumption-based model Maintenance Skills	Security Compliance Ownership Specific scenarios
Private	Control Security Compliance Specific scenarios	Upfront CapEx Agility Maintenance Skills
Hybrid	Flexibility Costs Control Security Compliance Specific scenarios	Upfront CapEx Costs Skills Ease of management

Describe Core Azure Services (30-35%)

Describe the core Azure architectural components

• Describe Regions

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

Region Pairs

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

Things to know about regional pairs:

Physical isolation. When possible, Azure prefers **at least 300 miles of separation between datacenters in a regional pair**, although this isn't practical or possible in all geographies. Physical datacenter separation reduces the likelihood of natural disasters, civil unrest, power outages, or physical network outages affecting both regions at once.
Platform-provided replication. Some **services such as Geo-Redundant Storage** provide **automatic replication to the paired region**.
Region recovery order. In the **event of a broad outage, recovery of one region is prioritized out of every pair**. Applications that are deployed across paired regions are guaranteed to have one of the regions recovered with priority.
Sequential updates. Planned **Azure system updates are rolled out to paired regions sequentially (not at the same time) to minimize downtime**, the effect of bugs, and logical failures in the rare event of a bad update.

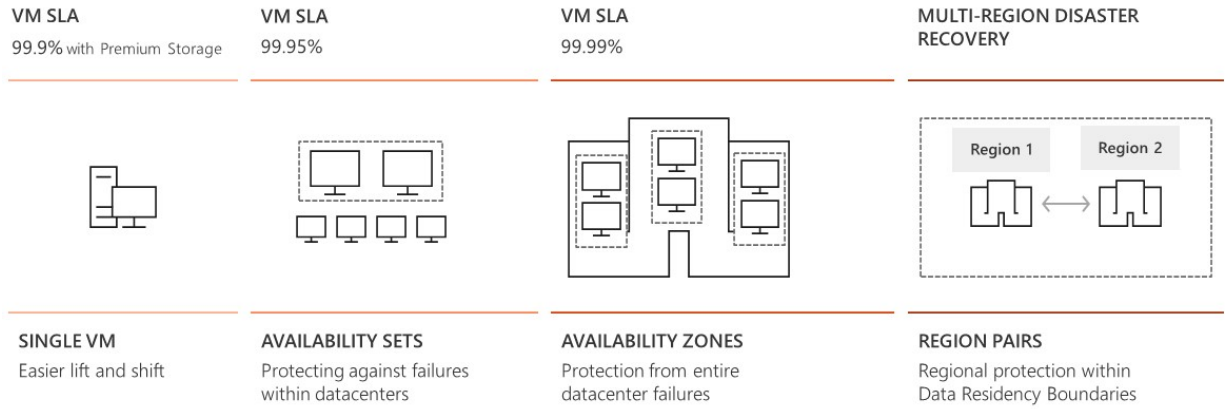
Geographies

Azure **divides the world into geographies** that are defined by **geopolitical boundaries** or **country borders**. An Azure geography is a discrete market **typically containing two or more regions** that **preserves data residency** and **compliance boundaries**.
Geographies are broken up into the following areas:
Americas

Europe
Asia Pacific
Middle East and Africa

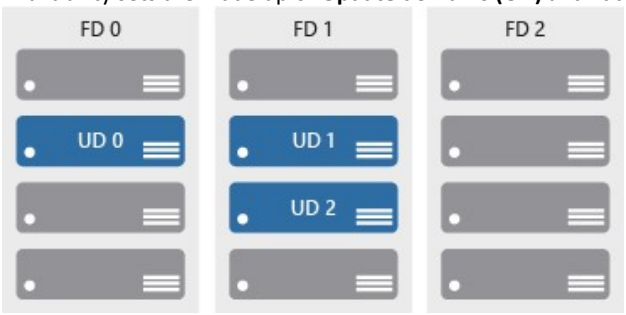
✔ **Each region belongs to a single geography** and has specific service availability, compliance, and data residency/sovereignty rules applied to it. Check the documentation for more information (a link is available in the summary unit).

• Describe Availability Zones



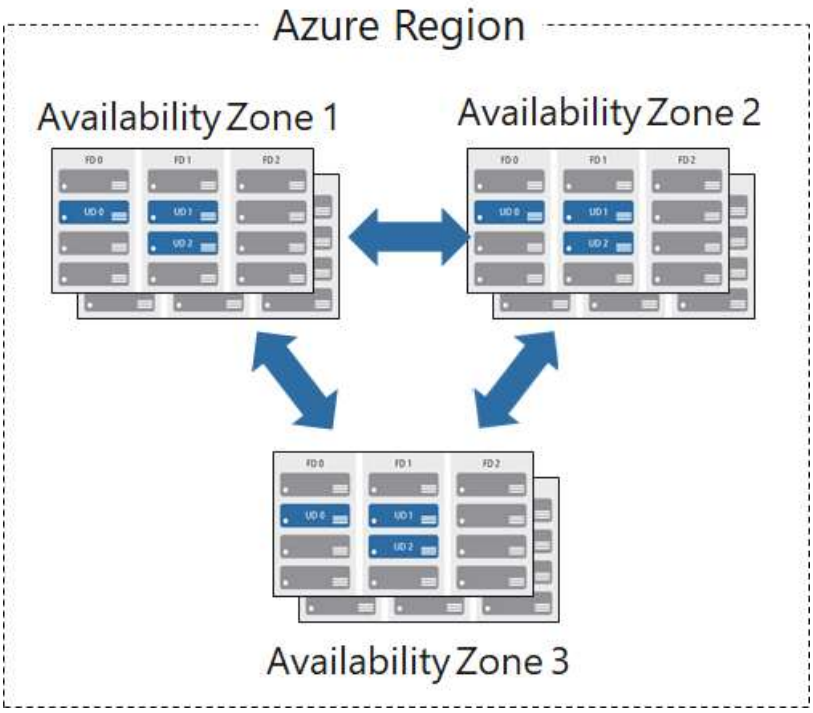
A **single virtual machine with premium storage has an SLA of 99.9%**. You can quickly migrate existing virtual machines to Azure through "lift and shift". Lift and shift is a no-code option where each application is migrated as-is, providing the benefits of the cloud without the risks or costs of making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

Availability sets are a way for you to ensure your **application remains online if a high-impact maintenance event is required**, or if a **hardware failure occurs**.
Availability sets are made up of **Update domains (UD)** and **Fault domains (FD)**.

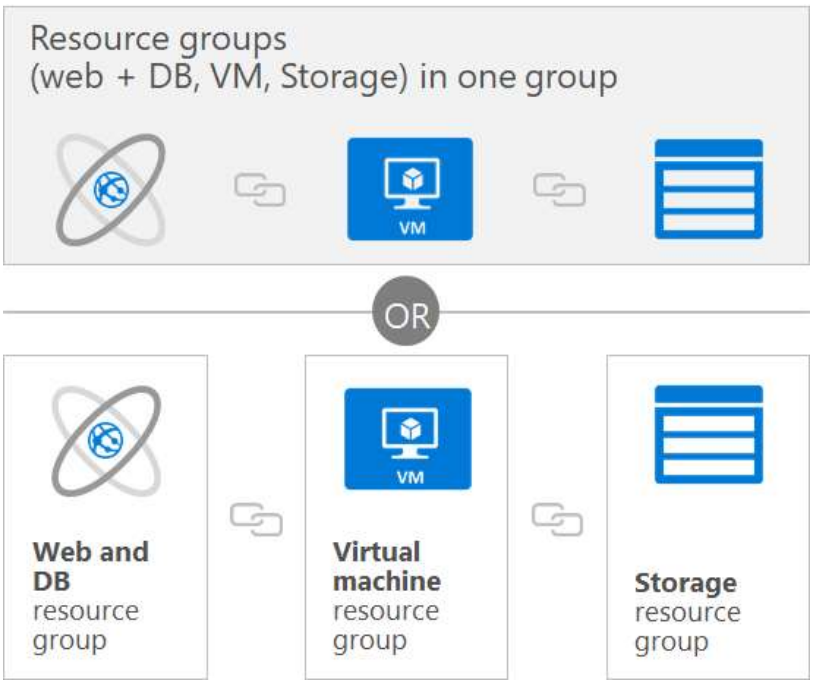


Update domains. When a **maintenance event occurs** (such as a performance update or critical security patch applied to the host), **the update is sequenced through update domains.** Sequencing updates using update domains ensures that the entire datacenter isn't unavailable during platform updates and patching. **Update domains are a logical section of the datacenter**, and they are implemented with software and logic.
Fault domains. Fault domains provide for the **physical separation of your workload across different hardware in the datacenter**. This **includes power, cooling, and network hardware that supports the physical servers located in server racks.** In the event the hardware that supports a server rack becomes unavailable, only that rack of servers would be affected by the outage.

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



Availability Zone features:
Each availability zone is an **isolation boundary containing one or more datacenters** equipped with **independent power, cooling, and networking**.
If **one availability zone goes down, the other continues working**.
The **availability zones** are typically **connected to each other through very fast, private fiber-optic networks**.
Availability zones allow customers to **run mission-critical applications** with **high availability** and **low-latency replication**.
Availability zones are offered as **a service within Azure**, and to **ensure resiliency**, there's a **minimum of three separate zones** in all enabled regions.
✔ Regions that support Availability Zones include **Central US**, **North Europe**, **SouthEast Asia**, and more.
Availability Zones are primarily for **VMs**, **managed disks**, **load balancers**, and **SQL databases**.
Azure services that support Availability Zones fall into two categories:
Zonal services – you pin the resource to a specific zone (for example, virtual machines, managed disks, IP addresses)
Zone-redundant services – platform replicates automatically across zones (for example, zone-redundant storage, SQL Database).
• Describe Resource Groups
A **resource group** is a **unit of management for your resources in Azure**. You can think of your resource group as a **container that allows you to aggregate and manage all the resources required for your application in a single manageable unit**. This allows you to manage the application collectively over its lifecycle, rather than manage components individually. Before any resource can be provisioned, you need a resource group for it to be placed in.
You can manage and apply the following resources at resource group level:
Metering and billing
Policies
Monitoring and alerts
Quotas
Access control
Remember that when you **delete a resource group** you **delete all resources contained within it**.



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

Resource Group - **Logical grouping** of resources.
Resource Group - if **deleted, all resource within it will be deleted**
Resource Group - a scope for applying **role-based access control (RBAC) permissions**.

Resource groups can be created by using the following methods:
Azure portal
Azure PowerShell
Azure CLI
Templates
Azure SDKs (like .NET, Java)
• Describe Azure Resource Manager
Azure Resource Manager is a **management layer** in which **resource groups** and **all the resources** within it are **created**, **configured**, **managed**, and **deleted**. It provides a consistent management layer which **allows you automate the deployment and configuration of resources using different automation and scripting tools**, such as **Microsoft Azure PowerShell**, Azure Command-Line Interface (**Azure CLI**), Azure **portal**, **REST API**, and **client SDKs**.

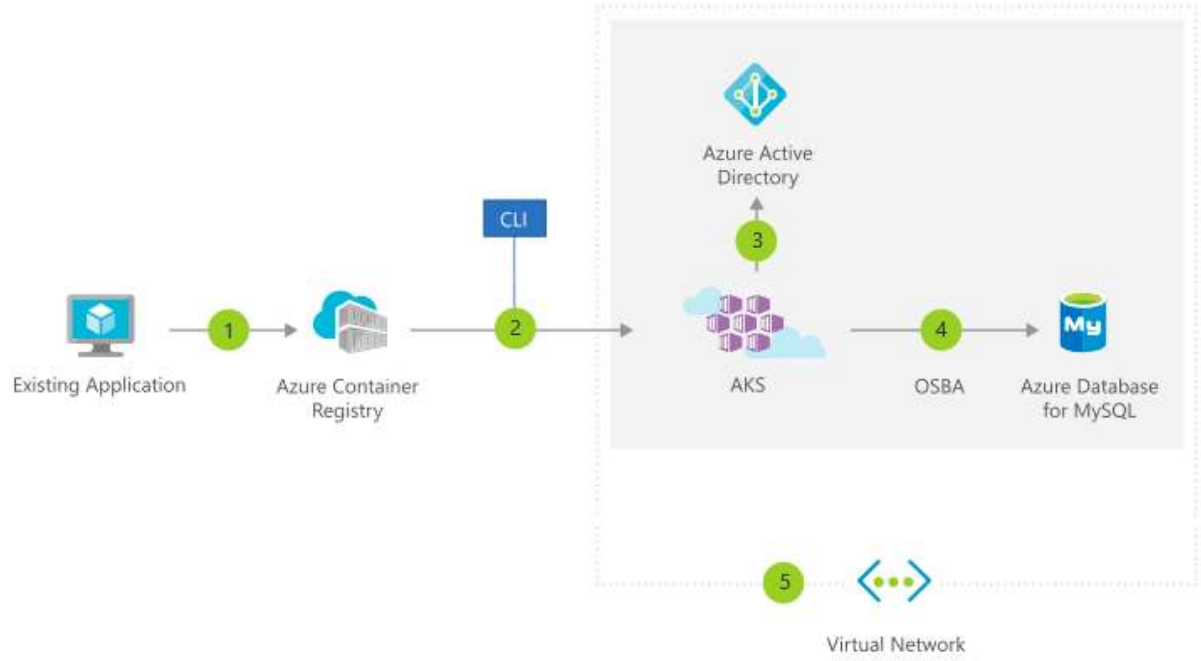
Check your knowledge

1. Azure Resource Manager templates use which format?
HTML
JSON
That's correct. Resource Manager templates are JSON files that define the resources you need to deploy for your solution. You can use template to easily re-create multiple versions of your infrastructure, such as staging and production.
XML
2. Which of the following locations ensure data-residency and compliance needs are met for customers who need to keep their data and applications close?
Geographies
That's correct. Geographies allow customers with specific data-residency and compliance needs to keep their data and applications close. Geographies ensure that data residency, sovereignty, compliance, and resiliency requirements are honored within geographical boundaries.
Regions

Zones
3. As a best practice, all resources that are part of an application and share the same lifecycle should exist in the same?
Availability set
Region
Resource group
That's correct. For ease of management, resources that are part of an application and share its lifecycle should be placed in the same resource group.
4. Microsoft Azure datacenters are organized and made available by?
Geographies
Regions
That's correct. Microsoft Azure datacenters are organized and made available by region.
Zones
5. Which of the following services are used to ensure availability during maintenance events?
Availability Set
That's correct. Availability sets provide VM redundancy and availability. This configuration within a datacenter (Availability Zone) ensures that during either a planned or unplanned maintenance event, at least one virtual machine is available and meets the 99.95% Azure SLA.
Availability Zone
Scale Set
• Describe the benefits and usage of core Azure architectural components
Describe some of the core products available in Azure
• Describe products available for Compute such as Virtual Machines, Virtual Machine Scale Sets, App Services, Azure Container Instances (ACI) and Azure Kubernetes Service (AKS)
Azure virtual machines let you **create and use virtual machines in the cloud**. It provides **IaaS** and can be used in a variety of different ways. When you n**eed total control over an operating system and environment**, Azure VMs are an ideal choice. Just like a physical computer, you're able to customize all the software running on the VM. This ability is helpful when you are **running custom software or custom hosting configurations**.
Virtual machine scale sets are an Azure compute resource that you can use to **deploy and manage a set of identical VMs**. With all VMs configured the same, virtual machine scale sets are **designed to support true autoscale**; **no pre-provisioning of VMs is required**; and as such makes it easier to build large-scale services targeting big compute, big data, and containerized workloads. So, as demand goes up **more virtual machine instances can be added**, and as demand goes down **virtual machines instances can be removed**. The process can be **manual**, **automated**, or a **combination of both**.
With ***App services*** , you can quickly **build, deploy, and scale enterprise-grade web, mobile, and API apps running on any platform**. You can meet rigorous performance, scalability, security, and compliance requirements while using a fully managed platform to perform infrastructure maintenance. App Services is a **platform as a service (PaaS)** offering.
Azure ***Functions*** are ideal when you're concerned only about the **code running your service and not the underlying platform or infrastructure.** They're commonly used when you need to **perform work in response to an event** (often via a **REST** request), **timer**, or **message from another Azure service**, and when that work can be completed quickly, within seconds or less.
Azure Container Instances offers the **fastest and simplest way to run a container in Azure** without having to manage any virtual machines or adopt any additional services. It is a **PaaS offering** that allows you to upload your containers, which it will run for you.
The task of automating, managing, and interacting with a large number of containers is known as orchestration. ***Azure Kubernetes Service (AKS)*** is a c**omplete orchestration service for containers** with distributed architectures and large volumes of containers. Orchestration is the task of automating and managing a large number of containers and how they interact.

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

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



The preceding figure depicts this process as follows:
You **convert** an existing application to **one or more containers** and then **publish one or more container images** to the **Azure Container Registry**.
By using the Azure portal or the command line, you **deploy the containers** to an **AKS cluster**.
Azure AD controls access to AKS resources.
You **access** SLA-backed Azure services, such as **Azure Database for MySQL**, via **OSBA**.
Optionally, **AKS** is deployed with a **virtual network**.

• Describe products available for Networking such as Virtual Network, Load Balancer, VPN Gateway, Application Gateway and Content Delivery Network

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

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

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

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

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

• Describe products available for Storage such as Blob Storage, Disk Storage, File Storage, and Archive Storage

Data categories in Azure:

Structured data

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

Semi-structured data

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

Unstructured data

Unstructured data has **no designated structure**.
Unstructured data **can hold any kind of data**.
Unstructured data is **becoming more prominent** as businesses try to tap into new data sources.
Examples of unstructured data include a PDF document, a JPG image, a JSON file, and video content.

Azure Storage**:**

Azure Storage is a service that you can use to **store files, messages, tables, and other types of information**. You can use Azure Storage on its own (for example as a **file share**), but developers also often use it as a **store for working data**. Such stores can be used by websites, mobile apps, desktop applications, and many other types of custom solutions. Azure Storage is also **used by IaaS virtual machines**, and **PaaS cloud services**.

Disk storage provides **disks for virtual machines, applications, and other services** to access and use as they need, similar to how they would in on-premises scenarios. Disk storage **allows data to be persistently stored** and **accessed from an attached virtual hard disk**. The disks **can be managed** or **unmanaged by Azure**, and **therefore managed and configured by the user**. Typical scenarios for using disk storage are if you want to **lift and shift applications** that **read and write data** to **persistent disks**, or if you are **storing data** that is **not required to be accessed from outside the virtual machine** to which the disk is attached.
Disks come in many different sizes and performance levels, from **solid-state drives (SSDs)** to traditional spinning **hard disk drives (HDDs)**, with varying performance abilities. Details on pricing are available on the Managed Disks pricing page.

Azure Blob storage is Microsoft's **object storage solution** for the cloud. Blob storage is **optimized for storing massive amounts of unstructured data**, such as **text** or **binary** data.
Blob storage is ideal for:
Serving **images or documents directly to a browser**.
Storing **files for distributed access**.
Streaming video and audio.
Storing **data for backup and restore, disaster recovery, and archiving**.
Storing **data for analysis by an on-premises or Azure-hosted service**.

Azure Files enables you to set up **highly available network file shares** that can be **accessed by using the standard Server Message Block (SMB) protocol**. That means that **multiple VMs can share** the same files with both read and write access. You can **also read the files using the REST interface** or the **storage client libraries**.
One thing that distinguishes Azure Files from files on a corporate file share is that you can access the files from anywhere in the world using a URL that points to the file and includes a shared access signature (SAS) token. You can generate SAS tokens; they allow specific access to a private asset for a specific amount of time.
File shares can be used for many common scenarios:
Many on-premises applications use file shares. This feature makes it **easier to migrate those applications that share data to Azure**. If you **mount the file share to the same drive letter** that the on-premises application uses, the part of your application that accesses the file share should work with minimal, if any, changes.
Configuration files can be **stored on a file share** and **accessed from multiple VMs**. **Tools and utilities** used by multiple developers in a group can be **stored on a file share**, ensuring that **everybody can find them**, and that they use the same version.
Diagnostic logs, metrics, and crash dumps are just three **examples of data** that can be **written to a file share** and processed or analyzed later.

The ***Azure Queue*** service is **used to store and retrieve messages**. Queue messages can be **up to 64 KB in size**, and a **queue can contain millions of messages**. Queues are generally used to **store lists of messages to be processed asynchronously**.
For example, say you want your customers to be able to upload pictures, and you want to create thumbnails for each picture. You could have your customer wait for you to create the thumbnails while uploading the pictures. An alternative would be to use a queue. When the **customer finishes their upload**, **write a message to the queue**. Then have an **Azure Function retrieve the message from the queue and create the thumbnails**. Each of the parts of this processing can be scaled separately, giving you more control when tuning it for your usage.

Azure Table storage **stores large amounts of structured data**. The **service is a NoSQL datastore which accepts authenticated calls from inside and outside the Azure cloud.** Azure tables are **ideal for storing structured, non-relational data**. Common uses of Table storage include:
Storing **TBs of structured data capable of serving web scale applications.**
Storing **datasets that don't require complex joins, foreign keys, or stored procedures and can be denormalized for fast access.**
Quickly **querying data using a clustered index.**
You can use Table storage to **store and query huge sets of structured, non-relational data**, and your **tables will scale** as demand increases.

• Describe products available for Databases such as Cosmos DB, Azure SQL Database, Azure Database for MySQL, Azure Database for PostgreSQL, Azure Database Migration service

Microsoft Azure Cosmos DB is a **globally distributed database service** that enables you to **elastically and independently scale throughput and storage** across any number of Azure's geographic regions. It **supports schema-less data** that lets you build highly responsive and Always On applications to support constantly changing data. You **can use Cosmos DB to store data that is updated and maintained by users around the world**. It makes it **easy to build scalable**, **highly responsive applications at global scale**.
Azure SQL Database is a **relational database as a service (DaaS)** based on the **latest stable version of Microsoft SQL Server database engine**. SQL Database is a **high-performance, reliable, fully managed and secure database** that you **can use to build data-driven applications and websites in the programming language of your choice** without needing to manage infrastructure.
The ***Azure Database Migration Service*** is a **fully managed service** designed to enable **seamless migrations** from **multiple database sources to Azure data platforms** with **minimal downtime (online migrations)**. The service uses the **Microsoft Data Migration Assistant** to **generate assessment reports that provide recommendations** to help guide you through required changes prior to performing a migration. Once you assess and perform any remediation required, you're ready to begin the migration process. The **Azure Database Migration Service performs all of the required steps**.
• Describe the Azure Marketplace and its usage scenarios
Azure Marketplace is a **service on Azure** that **helps connect end users with Microsoft partners**, **independent software vendors (ISVs)**, and **start-ups that are offering their solutions and services**, which are **optimized to run on Azure**. Azure Marketplace **allows customers**—mostly IT professionals and cloud developers—to **find, try, purchase, and provision applications and services** from **hundreds of leading service providers**, all certified to run on Azure.
Knowledge check:
1. Which Azure compute resource can be used to deploy to manage a set of identical virtual machines?
Virtual machine availability sets
Virtual machine availability zones
Virtual machine scale sets
That's correct. Virtual machine scale sets let you deploy and manage a set of identical virtual machines.
2. Which of the following should be used when the primary concern is to perform work in response to an event (often via a REST command) that needs a response in a few seconds?
Azure App Service
Azure Container Instances
Azure Functions
That's correct. Azure Functions are used when you need to perform work in response to an event (often via a REST request), timer, or message from another Azure service, and when that work can be completed quickly, within seconds or less.
3. Which of the following services is a distributed network of servers that can efficiently deliver web content to users?
Azure App Services
Azure Content Delivery Network
That's correct. A Content Delivery Network is a distributed network of servers that can efficiently deliver web content to users.
Azure Cosmos DB
4. Which of the following is optimized for storing massive amounts of unstructured data, such as videos and images?
Blobs
That's correct. Azure Blob storage is Microsoft's object storage solution for the cloud. Blob storage is optimized for storing massive amounts of unstructured data, such as text or binary data.
Files
Queues
5. Which is true about Azure Load Balancer?
Azure Load Balancer distributes traffic among similar systems, making your services more highly available.
That's correct. If one system is unavailable, Azure Load Balancer stops sending traffic to it. It then directs traffic to one of the responsive servers.
Azure Load Balancer works with internet-facing traffic only.
You must use Azure Load Balancer if you want to distribute traffic among your virtual machines running in Azure.
Describe some of the solutions available on Azure
• Describe Internet of Things (IoT) and products that are available for IoT on Azure
such as IoT Hub and IoT Central
People can access more information than ever before. It began with personal digital assistants (PDAs), then morphed into **smartphones**. Now there are **smart watches**, **smart thermostats**, even **smart refrigerators**. Personal computers used to be the norm. Now the internet allows any item that's online capable to access valuable information. The ***Internet of Things (IoT)*** is the **ability for devices to garner** and then **relay information for data analysis**.
IoT Central is a **fully managed global IoT software as a service (SaaS) solution** that makes it **easy to connect, monitor, and manage your IoT assets at scale**. No cloud expertise is required to use IoT Central. As a result, you can bring your connected products to market faster while staying focused on your customers.
Azure IoT Hub is a **managed service** hosted in the cloud that **acts as a central message hub** for **bi-directional communication between your IoT application and the devices it manages**. You can **use Azure IoT Hub to build IoT solutions** with **reliable and secure communications between millions of IoT devices** and a **cloud-hosted solution backend**. You **can connect virtually any device** to your IoT Hub.
IoT Hub **supports communications both** from the **device to the cloud** and from the **cloud to the device**. It also **supports multiple messaging patterns** such as **device-to-cloud telemetry**, **file upload from devices**, and **request-reply methods** to control your devices

from the cloud. IoT Hub monitoring helps you **maintain the health of your solution** by **tracking events** such as **device creation**, **device failures**, and **device connections**.
IoT Hub's capabilities help you **build scalable, full-featured IoT solutions** such as **managing industrial equipment** used in **manufacturing**, **tracking valuable assets** in **healthcare**, and **monitoring office building usage**.
• Describe Big Data and Analytics and products that are available for Big Data and Analytics such as Azure Synapse Analytics, HDInsight, and Azure Databricks
Big data and analytics
Data comes in all types of forms and formats. When we talk about big data, we're referring to **large volumes of data**. Data from **weather systems, communications systems, imaging platforms**, and many other scenarios generate large amounts of data. This amount of data becomes increasingly hard to make sense of and make decisions around. The **volumes are so large** that **traditional forms of processing and analysis are no longer appropriate**.
Open source cluster technologies have been developed, over time, to try to deal with these large data sets. Microsoft Azure supports a broad range of technologies and services to provide big data and analytic solutions. Some of the most common big data and analytic service types in Azure are **Azure SQL Data Warehouse**, **HDInsight**, and **Data Lake Analytics**.
Azure Synapse Analytics (formerly Azure SQL Data Warehouse) is a **limitless analytics** service that **brings together enterprise data warehousing** and **big data analytics**.
Azure HDInsight is a **fully managed, open-source analytics service for enterprises**. It is a cloud service that makes it **easier, faster,** and **more cost-effective to process massive amounts of data**. HDInsight allows you to **run popular open-source frameworks** and **create cluster types** such as **Apache Spark** ,**Apache Hadoop** ,**Apache Kafka** , **Apache HBase** ,**Apache Storm** ,**Machine Learning Services** . HDInsight also **supports a broad range of scenarios** such as **extraction**, **transformation**, and **loading** (ETL); **data warehousing**; **machine learning**; and **IoT**.
Azure Data Lake Analytics is an **on-demand analytics job service** that **simplifies big data**. Instead of deploying, configuring, and tuning hardware, you **write queries** to **transform** your **data and extract valuable insights**. The analytics service **can handle jobs of any scale** instantly by setting the dial for how much power you need. You only **pay for your job when it is running**, making it **more cost-effective**.
• Describe Artificial Intelligence (AI) and products that are available for AI such as Azure Machine Learning Service and Studio
Artificial Intelligence, in the context of cloud computing, is **based around a broad range of services**, the **core** of which is **Machine Learning**. ***Machine Learning*** is a **data science technique** that **allows computers to use existing data** to **forecast future behaviors**, **outcomes**, and **trends**. Using machine learning, **computers learn** without being explicitly programmed.

Forecasts or **predictions** from machine learning **can make apps and devices smarter**. For example, when you shop online, machine learning helps recommend other products you might like based on what you've purchased. Or when your credit card is swiped, machine learning compares the transaction to a database of transactions and helps detect fraud. And when your robot cleaner vacuums a room, machine learning helps it decide whether the job is done.
Azure Cognitive Services
Cognitive services are a **collection of domain-specific pre-trained AI models that can be customized with your data**. They are categorized broadly into **vision, speech, language, and search**. For more information about each service, see the links in the resources section.
Vision makes it possible for apps and services to **accurately identify and analyze content within images and videos**.
Speech services can **convert spoken language into text**, or **produce natural-sounding speech from text** using standard (or customizable) voice fonts.
Language services can **understand the meaning of unstructured text** or **recognize the speaker's intent**.
Knowledge services **create rich knowledge resources** that **integrate into apps and services**.
Enable apps and services to **harness the power of a web-scale, ad-free search engine**. Use ***search*** services to **find information across billions of web pages, images, videos, and news search results**.
The ***Azure Machine Learning*** service provides a cloud-based environment you can use to **develop, train, test, deploy, manage, and track machine learning models.** It **fully supports open-source technologies**, so you **can use tens of thousands of open-source Python packages** with machine learning components such as **TensorFlow** and **scikit-learn**. **Rich tools**, such as **Jupyter notebooks** or the **Visual Studio Code Tools for AI**, make it easy to interactively explore data, transform it, and then develop, and test models. Azure Machine Learning service also **includes features that automate model generation and tuning** to help you create models with ease, efficiency, and accuracy.
The Azure Machine Learning service **can auto-generate a model** and **auto-tune it for you**. It will **let you start training on your local machine, and then scale out to the cloud**. When you have the right model, you can **easily deploy it in a container such as Docker** in Azure. **Use Machine Learning service if you work in a Python environment**, you want **more control over your machine learning algorithms**, or you want to **use open-source machine learning libraries**.
• Describe Serverless computing and Azure products that are available for serverless computing such as Azure Functions, Logic Apps and Event Grid
Serverless computing is a cloud-hosted execution environment that **runs your code but abstracts the underlying hosting environment**. You create an instance of the service and you add your code. **No infrastructure configuration or maintenance is required**, or **even allowed**.
You configure your serverless apps to **respond to events**. An event could be a **REST endpoint**, a **periodic timer**, or even a **message received from another Azure service**. The serverless app **runs only when it's triggered by an event**.
Scaling and performance are handled automatically, and you are billed only for the exact resources you use. You don't even need to

reserve resources.
Some of the most common serverless service types in Azure are **Azure Functions**, **Azure Logic Apps**, and **Azure Event Grid**.
Azure Functions are ideal when you're only **concerned with the code running your service and not the underlying platform or infrastructure**. Azure Functions are commonly used when you **need to perform work in response to an event**—often via a REST request, timer, or message from another Azure service—and when that work can be completed quickly, within seconds or less.
Azure Functions **scale automatically**, and charges accrue only when a function is triggered, so they're a solid choice when demand is variable. For example, you may be receiving messages from an IoT solution that monitors a fleet of delivery vehicles. You'll likely have more data arriving during business hours. Azure Functions can scale out to accommodate these busier times.
Furthermore, Azure Functions are **stateless**; they **behave as if they're restarted every time they respond to an event**. This is ideal for **processing incoming data**. And **if state is required**, they **can be connected to an Azure storage service**.
Logic Apps is a cloud service that helps you **automate and orchestrate tasks, business processes, and workflows** when you need to **integrate apps, data, systems, and services** across enterprises or organizations. Logic Apps **simplifies how you design and build scalable solutions**—whether in the cloud, on premises, or both—for app integration, data integration, system integration, **enterprise application integration (EAI), and business-to-business (B2B) integration**.
Logic Apps are **designed in a web-based designer** and can **execute logic triggered by Azure services without writing any code**. To build enterprise integration solutions with Azure Logic Apps, you can choose from a **growing gallery of over 200 connectors**. These include services such as **Salesforce, SAP, Oracle DB, and file shares**.
Event Grid allows you to **easily build applications with event-based architectures**. It's a **fully managed, intelligent event routing service** that uses a **publish-subscribe model** for uniform event consumption. Event Grid has **built-in support for events coming from Azure services, such as storage blobs and resource groups.** You can use Event Grid to **support your own non-Azure-based events in near-real time, using custom topics**. You can use **filters to route specific events** to different endpoints, and ensure your events are reliably delivered.
• Describe DevOps solutions available on Azure such as Azure DevOps and Azure DevTest Labs
DevOps (Development and Operations) **brings together people, processes, and technology, automating software delivery to provide continuous value to your users.** Azure DevOps Services allows you to **create, build, and release pipelines that provide continuous integration, delivery, and deployment for your applications.** You can **integrate repositories** and **application tests,** perform **application monitoring**, and **work with build artifacts**. You can also **work with and backlog items for tracking**, **automate infrastructure deployment**, and **integrate a range of third-party tools** and **services** such as **Jenkins** and **Chef**. All these functions and many more are closely integrated with Azure to allow for consistent, repeatable deployments for your applications to provide streamlined build and release processes.
DevOps Services provides **development collaboration tools** including **high-performance pipelines**, free private **Git repositories**, configurable **Kanban boards**, and extensive automated and cloud-based **load testing**. DevOps Services was **formerly known as Visual Studio Team Services (VSTS)**.
Lab Services is a service that helps **developers and testers quickly create environments in Azure**, while **minimizing waste** and **controlling cost**. Users can test their latest application versions by quickly provisioning Windows and Linux environments using reusable templates and artifacts. You can easily integrate your deployment pipeline with DevTest Labs to provision on-demand environments. With DevTest Labs you can scale up your load testing by provisioning multiple test agents and create pre-provisioned environments for training and demos. Lab Services was **formerly known as DevOps Test**.
• Describe the benefits and outcomes of using Azure solutions
Describe Azure management tools
With ***Azure App Service*** you can quickly and easily build web and mobile apps for any platform or device. Azure App Service enables you to build and host web apps, mobile back ends, and RESTful APIs in the programming language of your choice without managing infrastructure. It offers auto-scaling and high availability, supports both Windows and Linux, and enables automated deployments from GitHub, Azure DevOps, or any Git repo.
Key features of Azure App Service:
Multiple languages and frameworks. App Service has first-class support for ASP.NET, ASP.NET Core, Java, Ruby, Node.js, PHP, or Python. You can also run PowerShell and other scripts or executables as background services.
DevOps optimization. Set up continuous integration and deployment with Azure DevOps, GitHub, BitBucket, Docker Hub, or Azure Container Registry. Promote updates through test and staging environments. Manage your apps in App Service by using Azure PowerShell or the cross-platform command-line interface (CLI).
Global scale with high availability. Scale up or out manually or automatically. Host your apps anywhere in Microsoft's global datacenter infrastructure, and the App Service SLA promises high availability.
Connections to SaaS platforms and on-premises data. Choose from more than 50 connectors for enterprise systems (such as SAP), SaaS services (such as Salesforce), and internet services (such as Facebook). Access on-premises data using Hybrid Connections and Azure Virtual Networks.
Security and compliance. App Service is ISO, SOC, and PCI compliant. Authenticate users with Azure Active Directory or with social login (Google, Facebook, Twitter, and Microsoft). Create IP address restrictions and manage service identities.
Application templates. Choose from an extensive list of application templates in the Azure Marketplace, such as WordPress, Joomla, and Drupal.
Visual Studio integration. Dedicated tools in Visual Studio streamline the work of creating, deploying, and debugging.
API and mobile features. App Service provides turn-key CORS support for RESTful API scenarios, and simplifies mobile app scenarios by enabling authentication, offline data sync, push notifications, and more.

Serverless code. Run a code snippet or script on-demand without having to explicitly provision or manage infrastructure, and pay only for the compute time your code actually uses.

Check your knowledge:

1. Which of the following is used when someone is only concerned about the code running the service, instead of the underlying platform or infrastructure?

Azure App Service

Azure Container Instances

Azure Functions

That's correct. Azure Functions is ideal when someone is only concerned about the code running the service, but isn't worried about the underlying platform or infrastructure.

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

HDInsight

Azure Machine Learning service

That's correct. Machine Learning service provides a cloud-based environment that can be used to develop, train, test, deploy, manage, and track machine learning models.

Azure DevTest Labs

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

Azure DevOps Services

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

Azure Event Grid

HDInsight

• Describe Azure tools such as Azure Portal, Azure PowerShell, Azure CLI and Cloud Shell

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

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

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

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

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

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

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

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

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

Check the status and important metrics of your services

Stay informed with notifications and alerts about important health issues

Quickly diagnose and fix issues anytime, anywhere

Review the latest Azure alerts

Start, stop, and restart virtual machines or web apps

Connect to your virtual machines

Manage permissions with role-based access control (RBAC)

Use the Azure Cloud Shell to run saved scripts or perform unplanned administrative tasks

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

• Describe Azure Advisor

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

With Azure Advisor, you can:

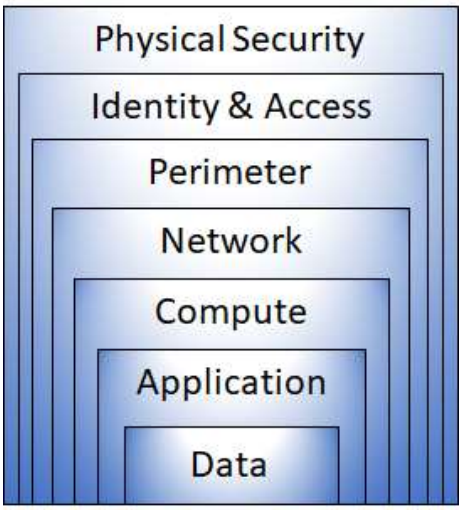
Get proactive, actionable, and personalized best practices recommendations.

Improve the performance, security, and high availability of your resources as you identify opportunities to reduce your overall Azure

costs.
Get recommendations with proposed actions inline.
Check your knowledge:
1. Which of the following terms ensure that both data-residency and compliance needs are met for customers who need to keep their data and applications close?
Geographies
That's correct. Geographies allow customers with specific data-residency and compliance needs to keep their data and applications close. Geographies ensure that data residency, sovereignty, compliance, and resiliency requirements are honored within geographical boundaries.
Regions
Zones
2. While away from the office on a business trip, there is need to restart a virtual machine and one of the Azure web apps. You only have access to your Android phone. What tool will let you connect to Azure and restart these two items?
Azure Mobile App
That's correct. While it's technically possible to open the Azure portal in your browser on your phone, it is not a better option than using the mobile app.
Azure portal
PowerShell

Describe Security, Privacy, Compliance, and Trust (25-30%)

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



Physical security is the first line of defense to protect computing hardware in the datacenter.
Identity & access controls access to infrastructure and change control.
Perimeter layer uses distributed denial-of-service (DDoS) protection to filter large-scale attacks before they can cause a denial of service for end users.
Networking layer limits communication between resources through segmentation and access controls.
Compute layer secures access to virtual machines.
Application layer ensures applications are secure and free of vulnerabilities.
Data - In almost all cases, attackers are after data:
Stored in a database
Stored on disk inside virtual machines
Stored on a SaaS application such as Microsoft 365
Stored in cloud storage
Azure helps alleviate your security concerns. But security is still a **shared responsibility**. How much of that **responsibility falls on us depends on which model we use with Azure**. We use the defense in depth rings as a guideline for considering what protections are adequate for our data and environments.
Security is a shared responsibility:

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

• Describe Network Security Groups (NSG)

Network Security Groups (NSG) allow you to **filter network traffic to and from Azure resources** in an Azure virtual network. An NSG **can contain multiple inbound and outbound security rules** that enable you to filter traffic to and from resources by **source and destination IP address, port, and protocol**.

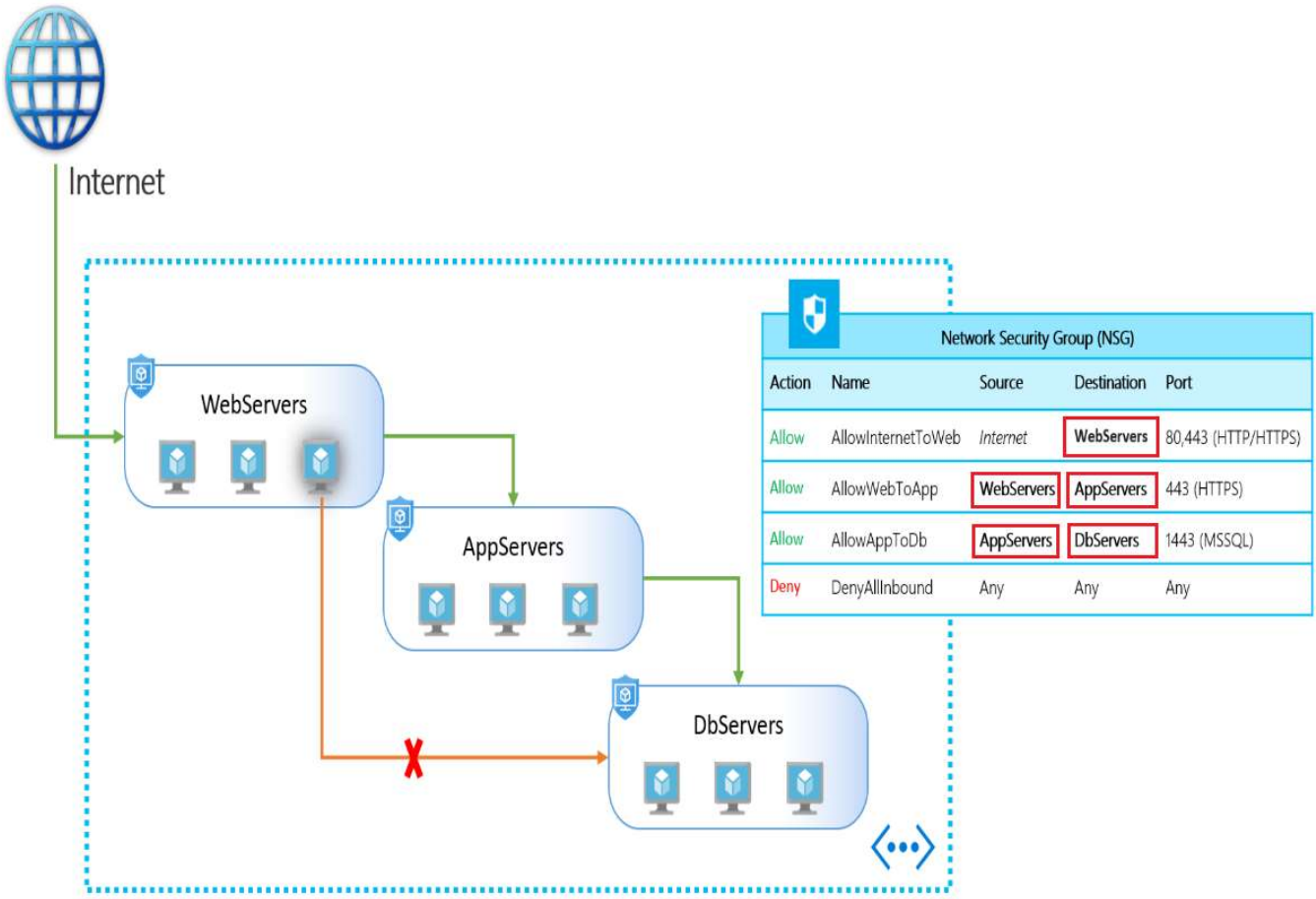
Property	Explanation
Name	Unique name of the Network Security Group (NSG)
Priority	A number between 100 and 4096. Rules are processed in priority order, with lower numbers processed before higher numbers.
Source or Destination	Individual IP address or IP address range, service tag, or application security group.
Protocol	TCP, UDP, or Any.
Direction	Whether the rule applies to inbound or outbound traffic.
Port Range	An individual port or range of ports.
Action	Allow or Deny.

When you create a network security group, **Azure creates a series of default rules to provide a baseline level of security.** You **cannot remove the default rules**, but you can **override them** by creating **new rules with higher priorities**.

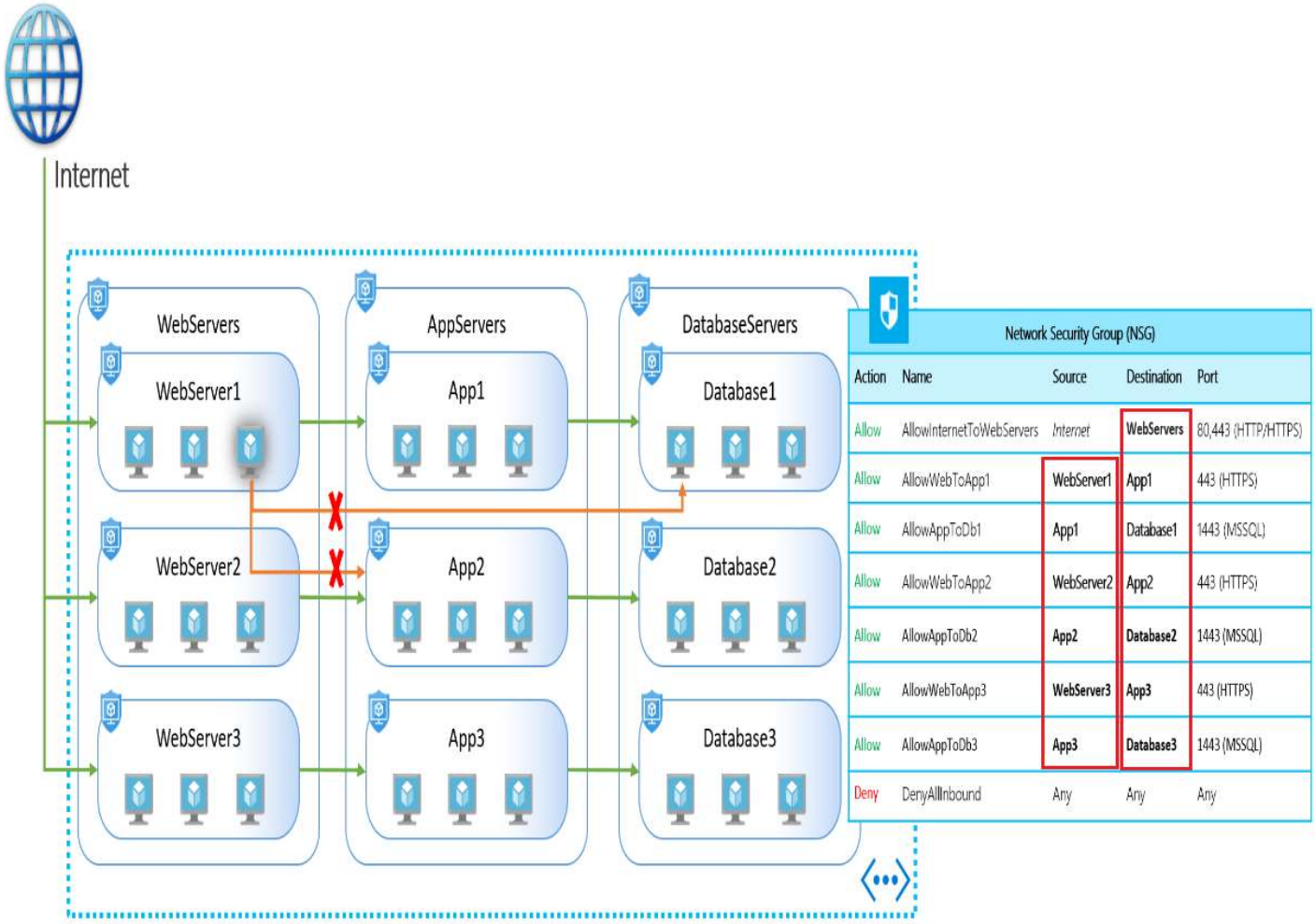
• Describe Application Security Groups (ASG)

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

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



In the below example, multiple applications are deployed into the same virtual network. Based on the security rules described, workloads are isolated from each other. If a **virtual machine from one of the applications is compromised (e.g. WebServer1)**, lateral exploration is limited, minimizing the potential impact of an attacker. In this example, let's assume one of the web server virtual machines from application1 is compromised, the **rest of the application will continue to be protected**, even **access to critical workloads like database servers will still be unreachable**. This implementation **provides multiple extra layers of security to your network**, making this intrusion less harmful and easy to react on such events.



Knowledge check:

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

Azure Active Directory

Azure Firewall

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

VPN Gateway

2. Which of the following services would filter internet traffic in an Azure virtual network?

Azure Firewall

Network Security Group

That's correct. NSGs allow you to filter network traffic to and from Azure resources in an Azure virtual network. An NSG can contain multiple inbound and outbound security rules that enable you to filter traffic to and from resources by source and destination IP address, port, and protocol.

VPN Gateway

- Describe User Defined Rules (UDR)
- Describe Azure Firewall

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

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

Azure Firewall provides many features, including:

Built-in high availability.

Unrestricted cloud scalability.

Inbound and outbound filtering rules.

Azure Monitor logging.

With Azure Firewall you can configure:

Application rules that define **fully qualified domain names (FQDNs) that can be accessed from a subnet**.

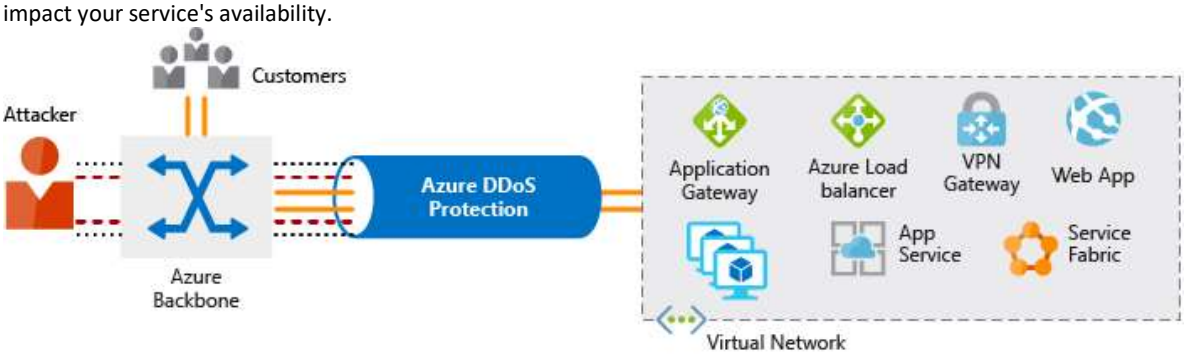
Network rules that define **source address**, **protocol**, **destination port**, and **destination address**.

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

• Describe Azure DDoS Protection

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

The Azure DDoS Protection service **protects your Azure applications by scrubbing traffic** at the Azure network edge before it can impact your service's availability.



• Choose an appropriate Azure security solution

Describe core Azure Identity services

• Describe the difference between authentication and authorization

Authentication. Authentication is the **process of establishing the identity of a person or service** looking to access a resource. It involves the act of challenging a party for legitimate credentials and provides the basis for creating a security principal for identity and access control use. It establishes if they are **who** they say they are.

Authorization. Authorization is the **process of establishing what level of access** an authenticated person or service has. It specifies **what data they're allowed to access** and **what they can do** with it.

• Describe Azure Active Directory

Azure Active Directory is a Microsoft cloud-based **identity and access management service**. Azure AD helps employees of an organization sign in and access resources:

External resources might include **Microsoft 365**, the **Azure portal**, and thousands of other **software as a service (SaaS)** applications.

Internal resources might include **apps on your corporate network** and intranet, along with any **cloud apps developed by your own organization**.

Azure AD provides services such as:

Authentication. This includes **verifying identity** to access applications and resources, and providing functionality such as self-service password reset, multi-factor authentication (MFA), a custom banned password list, and smart lockout services.

Single sign-on (SSO). Enables users to remember **only one ID** and **one password** to **access multiple applications**. A single identity is tied to a user, simplifying the security model. As users change roles or leave an organization, access modifications are tied to that identity, greatly reducing the effort needed to change or disable accounts.

Application management. You can manage your cloud and on-premises apps using Azure AD Application Proxy, single sign-on, the My apps portal (also referred to as Access panel), and SaaS apps.

Business to business (B2B) identity services. Manage your guest users and external partners while maintaining control over your own corporate data

Business-to-customer (B2C) identity services. Customize and control how users sign up, sign in, and manage their profiles when using your apps with services.

Device management. Manage how your cloud or on-premises devices access your corporate data.

Azure AD is intended for:

IT administrators. Administrators can use Azure AD to control access to apps and their resources, based on your business requirements.

App developers. Developers can use Azure AD to provide a standards-based approach for adding functionality to applications that you build, such as adding Single-Sign-On functionality to an app, or allowing an app to work with a user's pre-existing credentials and other functionality.

Microsoft 365, Microsoft Office 365, Azure, or Microsoft Dynamics CRM Online subscribers. These subscribers are already using Azure AD. Each Microsoft 365, Office 365, Azure, and Dynamics CRM Online tenant is automatically an Azure AD tenant. You can immediately start to manage access to your integrated cloud apps using Azure AD.

• Describe Azure Multi-Factor Authentication

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

Something you know could be a **password** or the **answer to a security question**.

Something you possess might be a **mobile app** that receives a notification, or a **token-generating device**.

Something you are is typically some sort of **biometric property**, such as a **fingerprint** or **face scan** used on many mobile devices.

Multi-factor authentication (MFA) comes as part of the following Azure service offerings:
Azure Active Directory premium licenses. These licenses provide full-featured use of Azure Multi-Factor Authentication Service (cloud) or Azure Multi-Factor Authentication Server (on-premises).
Multi-factor authentication for Microsoft 365. A subset of Azure Multi-Factor Authentication capabilities is available as a part of your Microsoft 365 subscription.
Azure Active Directory global administrators. Because global administrator accounts are highly sensitive, a subset of Azure Multi-Factor Authentication capabilities are available to protect these accounts.
Knowledge check:
1. Which of the following could require both a password and a phone verification for full authentication?
Azure Firewall
Application Gateway
Multi-Factor Authentication
That's correct. MFA can require two or more elements for full authentication.
2. Which of these options helps to easily disable an account when an employee leaves your company?
Enforce multi-factor authentication (MFA)
Monitor sign-on attempts
Use single sign-on (SSO)
That's correct. SSO centralizes user identity, so you can disable an inactive account in a single step.
3. Connecting to a secure resource requires both authentication and authorization. What is the purpose of authentication?
To validate that the user logging into the resource is who they say they are with a password, fingerprint, or other mechanism.
That's correct. Authentication uses things like something you know, something you are, and something you have to verify identity.
To validate the specific resources the user has access to. Then grant them a token to allow access to use the resource requested.
To allow the administrator to assign access to a secure resource, to limit the number of users who has access.
Describe security tools and features of Azure
• Describe Azure Security Center
Azure Security Center is a monitoring service that provides threat protection across all of your services both in Azure, and on-premises.
Security Center can:
Provide security recommendations based on your configurations, resources, and networks.
Monitor security settings across on-premises and cloud workloads, and **automatically apply required security** to new services as they come online.
Continuously monitor all your services and perform **automatic security assessments** to identify potential vulnerabilities before they can be exploited.
Use machine learning to **detect and block malware** from being installed on your virtual machines and services. You can also **define a list of allowed applications** to ensure that only the apps you validate can execute.
Analyze and identify potential inbound attacks and help to investigate threats and any post-breach activity that might have occurred.
Provide just-in-time access control for ports, reducing your attack surface by ensuring the network only allows traffic that you require.
• Describe Azure Security Center usage scenarios
You can use Security Center during the detect, assess, and diagnose stages. Here are examples of how Security Center can be useful during the three initial incident response stages:
Detect - Review the first indication of an event investigation. For example, use the Security Center dashboard to review the initial verification that a high-priority security alert was raised.
Assess - Perform the initial assessment to obtain more information about the suspicious activity. For example, obtain more information about the security alert.
Diagnose - Conduct a technical investigation and identify containment, mitigation, and workaround strategies. For example, follow the remediation steps described by Security Center in that particular security alert.

Security policies and recommendations
A ***security policy*** defines the **set of controls** that are **recommended for resources** within that specified subscription or resource group. In Security Center, you define policies according to your company's security requirements.
Security Center analyzes the security state of your Azure resources. When Security Center **identifies potential security vulnerabilities**, it creates ***recommendations*** based on the controls set in the security policy. The recommendations **guide you through the process of configuring the needed security controls**. For example, if you have workloads that do not require the Azure SQL Database Transparent Data Encryption (TDE) policy, turn off the policy at the subscription level and enable it only in the resources groups where SQL TDE is required.
• Describe Key Vault
Azure Key Vault is a centralized cloud service for **storing your applications' secrets**. Key Vault **helps you control your applications' secrets** by keeping them in a **single, central location** and by providing **secure access, permissions control, and access logging capabilities**.
• Describe Azure Information Protection (AIP)
Azure Information Protection is a cloud-based solution that **helps organizations classify and (optionally) protect its documents and emails by applying labels.** Labels can be **applied automatically** (by administrators who define rules and conditions), **manually** (by users), or with a **combination of both** (where users are guided by recommendations).

• Describe Azure Advanced Threat Protection (ATP)

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

Azure Advanced Threat Protection components:

Azure Advanced Threat Protection (ATP) portal. Azure ATP has its **own portal**, through which you can **monitor and respond to suspicious activity**. The Azure ATP portal allows you to create your **Azure ATP instance**, and **view the data** received from Azure ATP sensors. You can also use the portal to monitor, manage, and investigate threats in your network environment.

Azure Advanced Threat Protection (ATP) sensor. Azure ATP sensors are **installed directly on your domain controllers.** The sensor monitors domain controller traffic **without requiring a dedicated server or configuring port mirroring.**

Azure Advanced Threat Protection (ATP) cloud service. Azure ATP cloud service **runs on Azure infrastructure** and is currently **deployed in the United States, Europe, and Asia**. Azure ATP cloud service is **connected to Microsoft's intelligent security graph**.

Knowledge check:

1. Which of the following choices enables stored passwords and secrets in Azure so you can centrally manage them for your services and applications?

Azure Advanced Threat Protection

Azure Key Vault

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

Azure Security Center

2. What is Azure Information Protection (AIP)?

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

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

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

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

Describe Azure governance methodologies

• Describe policies and initiatives with Azure Policy

Azure Policy is a service in Azure that you use to **create, assign, and, manage policies**. These policies **enforce different rules and effects over your resources**, so those **resources stay compliant** with your **corporate standards** and **service-level agreements (SLAs)**. Azure Policy comes with a **number of built-in policy** and initiative definitions that you can use, under categories such as **Storage, Networking, Compute, Security Center, and Monitoring**.

A ***policy definition*** expresses **what to evaluate** and **what action to take**. For example, you could prevent VMs from being deployed if they are exposed to a public IP address. You also could prevent a hard disk from being used when deploying VMs to control costs.

Here are some example policy definitions:

Allowed storage account SKUs. This policy definition has a set of conditions/rules that **determine whether a storage account that is being deployed is within a set of SKU sizes**. Its effect is to **deny all storage accounts that do not adhere to the set of defined SKU sizes**.

Allowed resource type. This policy definition has a set of conditions/rules to specify the **resource types that your organization can deploy**. Its effect is to **deny all resources that are not part of the defined list**.

Allowed locations. This policy enables you to **restrict the locations that your organization can specify when deploying resources.** Its effect is used to **enforce your geographic compliance requirements**.

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

Assign a definition to a scope of resources

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

Review the policy evaluation results

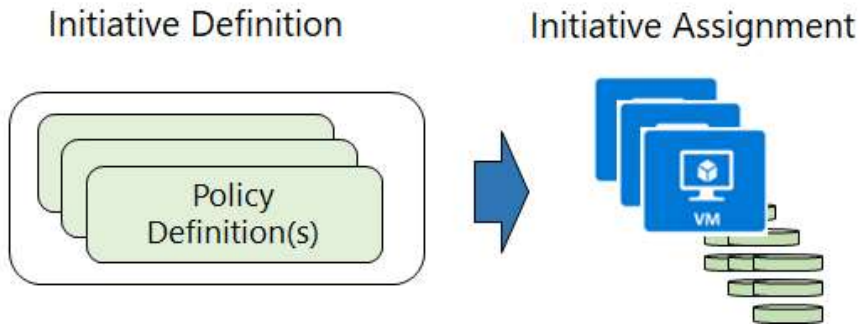
When a condition is evaluated against your existing resources it is **marked compliant or non-compliant**. You can r**eview the non-compliant policy results** and **take any action that is needed**.

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

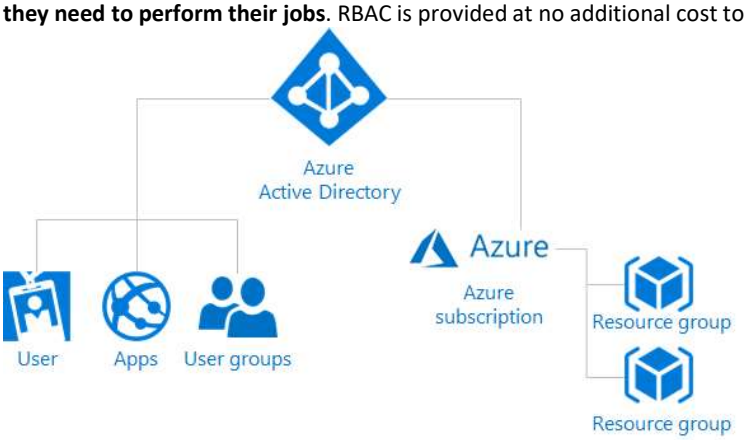
An ***initiative definition*** is a **set of policy definitions** to help track your compliance state for a larger goal. Initiative assignments reduce the need to make several initiative definitions for each scope.

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

Under this initiative, you would have the following policy definitions:
Monitor unencrypted SQL Database in Security Center – For monitoring unencrypted SQL databases and servers.
Monitor OS vulnerabilities in Security Center – For monitoring servers that do not satisfy the configured baseline.
Monitor missing Endpoint Protection in Security Center – For monitoring servers without an installed endpoint protection agent.



Like a policy assignment, an ***initiative assignment*** is an initiative definition **assigned to a specific scope**. Initiative assignments reduce the need to make several initiative definitions for each scope. This scope could also range from a management group to a resource group.
You can define initiatives using the Azure portal, or command-line tools. In the portal, you use the "Authoring" section.
• Describe Role-Based Access Control (RBAC)
Role-based access control provides **fine-grained access management for Azure resources**, enabling you to **grant users** only the **rights they need to perform their jobs**. RBAC is provided at no additional cost to all Azure subscribers.



Examples of when you might use RBAC include when you want to:
Allow one user to manage VMs in a subscription, and another user to manage virtual networks.
Allow a database administrator (DBA) group to manage SQL databases in a subscription.
Allow a user to manage all resources in a resource group, such as VMs, websites, and subnets.
Allow an application to access all resources in a resource group.
RBAC uses an allow model. This means that when you are assigned a role, RBAC allows you to perform certain actions, such as read, write, or delete. Therefore, if one role assignment grants you read permissions to a resource group, and a different role assignment grants you write permissions to the same resource group, you will have write permissions on that resource group.
• Describe Locks
resource locks help you **prevent accidental deletion** or **modification** of your Azure resources. You can manage these locks from within the Azure portal. To view, add, or delete locks, go to the SETTINGS section of any resource's settings blade.
CanNotDelete means authorized admins **can still read and modify a resource**, but they **can't delete** the resource.
ReadOnly means authorized admins **can read a resource**, but they **can't delete or update the resource.** Applying this lock is like restricting all authorized users to the permissions granted by the Reader role.
• Describe Azure Advisor security assistance
• Describe Azure Blueprints
Azure Blueprints enable cloud architects to **define a repeatable set of Azure resources** that **implement and adhere to an organization's standards, patterns, and requirements.** Azure Blueprint **enables** development teams to **rapidly build and deploy new environments with the knowledge that they're building within organizational compliance** with a set of built-in components that speed up development and delivery.
Azure Blueprint is a declarative way to orchestrate the deployment of various resource templates and other artifacts, such as:
Role assignments
Policy assignments
Azure Resource Manager templates
Resource groups
The process of implementing Azure Blueprint consists of the following high-level steps:
Create an Azure Blueprint.

Assign the blueprint.
Track the blueprint assignments.
Knowledge check:
1. Which of the following can be used to help enforce resource tagging so the billing can be managed?
Azure Policy
That's correct. Azure Policy can be used to enforce tagging values and rules on resources.
Azure Service Health
Compliance Manager
2. Which of the following can be used to define a repeatable set of Azure resources that implement organizational requirements?
Azure Blueprint
That's correct. Azure Blueprints enable cloud architects to define a repeatable set of Azure resources that implement and adhere to an organization's standards, patterns, and requirements. Azure Blueprint enables development teams to rapidly build and deploy new environments with the knowledge that they're building within organizational compliance with a set of built-in components that speed up development and delivery.
Azure Policy
Azure Resource Groups
3. Which of the following grants users only the rights they need to perform their jobs?
Azure Policy
Compliance Manager
Role-Based Access Control
That's correct. RBAC grants users the specific rights they need to perform their jobs.
4. Which of the following approaches would be the most efficient way to ensure a naming convention was followed across a subscription?
Send out an email with the details of the naming conventions and hope it is followed.
Create a policy with the naming requirements and assign it to the scope of the subscription
That's correct. Using Azure Policy ensures that not only a naming standard recommended, but it is able to be reported on its adoption.
Give all other users read-only access to the subscription. Have all requests to create resources sent back so the names can be reviewed while assigned to resources, and then create them.
5. Which of the following items would be good use of a resource lock?
An ExpressRoute circuit with connectivity back to the on-premises network
That's correct. Protecting this mission critical resource from accidental deletion is a great idea.
A non-production virtual machine used to test occasional application builds
A storage account used to temporarily store images processed in a development environment
Describe monitoring and reporting options in Azure
You apply ***tags*** to your Azure resources giving **metadata to logically organize them into a taxonomy**. Each tag consists of a **name** and a **value pair**. For example, you can apply the name Environment and the value Production to all the resources in production, or tag by company departments. For example, the name of Department with a value of IT.
Tag limitations:
Not all resource types support tags.
Each **resource or resource group** can have **a maximum of 50 tag name/value pairs.** Currently, **storage accounts** only **support 15 tags**, but that limit will be raised to 50 in a future release. If you **need to apply more tags** than the maximum allowed number, **use a JSON string for the tag value**. The JSON string can contain many values that are applied to a single tag name. A resource group can contain many resources that each have 50 tag name/value pairs.
The **tag name** is limited to **512 characters**, and the **tag value** is limited to **256 characters**. For **storage accounts, the tag name is limited to 128 characters**, and the **tag value is limited to 256 characters.**
Virtual Machines and Virtual Machine Scale Sets are limited to a **total of 2048 characters for all tag names and values.**
Tags applied to the resource group are **not inherited** by the resources in that resource group.
You **can use Azure Policy** to **enforce tagging values** and rules on resources.
• Describe Azure Monitor
Azure Monitor **maximizes the availability and performance of your applications** by delivering a comprehensive solution for collecting, analyzing, and acting on telemetry from your cloud and on-premises environments. It **helps you understand how your applications are performing** and **proactively identifies issues** affecting them and the resources they depend on.
Azure Monitor can collect data from a variety of sources. You can think of monitoring data for your applications in tiers ranging from your application, any operating system and services it relies on, down to the platform itself. Azure Monitor collects data from each of the following tiers:
Application monitoring data: Data about the **performance and functionality of the code you have written**, regardless of its platform.
Guest OS monitoring data: Data about the **operating system on which your application is running**. This could be running in Azure, another cloud, or on-premises.
Azure resource monitoring data: Data about the **operation of an Azure resource**.
Azure subscription monitoring data: Data about the **operation and management of an Azure subscription**, as well as data about the **health and operation of Azure itself**.
Azure tenant monitoring data: Data about the **operation of tenant-level Azure services**, such as **Azure Active Directory**.

Enabling diagnostics

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

Enable guest-level monitoring

Performance counters: collect performance data

Event Logs: enable various event logs

Crash Dumps: enable or disable

Sinks: send your diagnostic data to other services for more analysis

Agent: configure agent settings

• Describe Azure Service Health

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

Knowledge check:

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

Azure Monitor

Azure Security Center

Azure Service Health

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

2. Which of the following services provides up-to-date status information about the health of Azure services?

Compliance Manager

Azure Monitor

Azure Service Health

That's correct. Azure Service Health is the correct answer, because it provides you with a global view of the health of Azure services. With Azure Status, a component of Azure Service Health, you can get up-to-the-minute information on service availability.

• Describe the use cases and benefits of Azure Monitor and Azure Service Health

Describe privacy, compliance and data protection standards in Azure

• Describe industry compliance terms such as GDPR, ISO and NIST

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

Current compliance offerings: https://docs.microsoft.com/en-us/microsoft-365/compliance/offering-home?view=o365-worldwide

The ***General Data Protection Regulation (GDPR)*** introduces new rules for organizations that offer goods and services to people in the European Union (EU), or that collect and analyze data for EU residents no matter where you or your enterprise are located. This document guides you to information to help you honor rights and fulfill obligations under the GDPR when using Microsoft products and services. A Recommended action plan for GDPR and Accountability Readiness Checklists provide additional resources for assessing and implementing GDPR compliance.

International Organization of Standards/International Electrotechnical Commission (ISO/IEC) 27018. Microsoft is the first cloud provider to have adopted the ISO/IEC 27018 code of practice, covering the processing of personal information by cloud service providers.

National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF). NIST CSF is a voluntary Framework that

consists of standards, guidelines, and best practices to manage cybersecurity-related risks. Microsoft cloud services have undergone independent, third-party Federal Risk and Authorization Management Program (FedRAMP) Moderate and High Baseline audits and are certified according to the FedRAMP standards. Additionally, through a validated assessment performed by the Health Information Trust Alliance (HITRUST), a leading security and privacy standards development and accreditation organization, Microsoft 365 is certified to the objectives specified in the NIST CSF.

• Describe the Microsoft Privacy Statement

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

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

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

Your privacy is important to us.

• Describe the Trust center

The ***Trust Center*** is a **website resource** containing **information and details** about how **Microsoft implements and supports security, privacy, compliance, and transparency in all Microsoft cloud products and services.** The Trust Center is an important part of the Microsoft Trusted Cloud Initiative and **provides support and resources for the legal and compliance community**.

The Trust Center site provides:

In-depth information about security, privacy, compliance offerings, policies, features, and practices across Microsoft cloud products.

Recommended resources in the form of a curated **list of the most applicable and widely used resources** for each topic.

Information specific to **key organizational roles, including business managers, tenant admins or data security teams, risk assessment and privacy officers, and legal compliance teams**.

Cross-company document search, which is coming soon and will enable existing cloud service customers to search the Service Trust Portal.

Direct guidance and support for when you can't find what you're looking for.

• Describe the Service Trust Portal

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

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

ISO
SOC
NIST
FedRAMP

https://servicetrust.microsoft.com/

• Describe Compliance Manager

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

Compliance Manager provides the following features:

Detailed information provided by Microsoft **to auditors and regulators**, as part of various **third-party audits of Microsoft 's cloud services against various standards (for example, ISO 27001, ISO 27018, and NIST)**.

Information that Microsoft **compiles internally for its compliance with regulations (such as HIPAA)**.

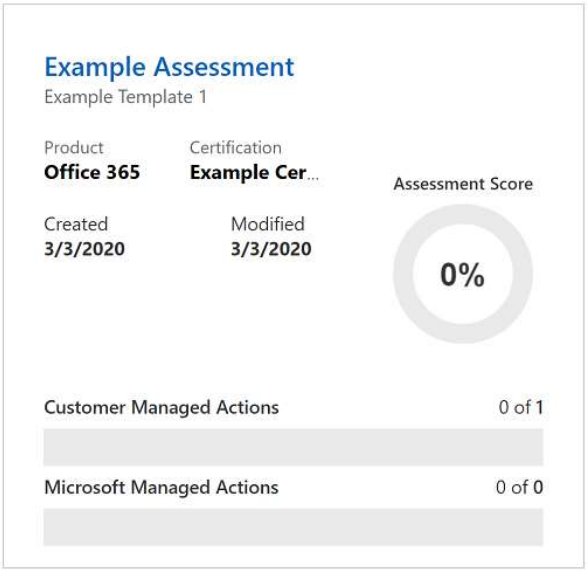
An **organization's self-assessment of their own compliance** with these standards and regulations.

Enables you to **assign, track, and record compliance and assessment-related activities**, which can help your organization cross team barriers to achieve your organization's compliance goals.

Provides a Compliance Score to help you track your progress and prioritize auditing controls that will help reduce your organization's exposure to risk.

Provides a **secure repository** in which to upload and manage **evidence and other artifacts** related to **compliance activities**.

Produces richly **detailed reports in Microsoft Excel** that document the compliance activities performed by Microsoft and your organization, which can be provided to auditors, regulators, and other compliance stakeholders.



https://servicetrust.microsoft.com/Documents/TrustDocuments

• Determine if Azure is compliant for a business need

• Describe Azure Government cloud services

Azure Government is a **separate instance of the Microsoft Azure service**. It addresses the **security and compliance needs of US federal agencies, state and local governments, and their solution providers.** Azure Government **offers physical isolation** from **non-US government deployments** and provides **screened US personnel**.

Azure Government services **handle data that is subject to certain government regulations and requirements**, such as FedRAMP, NIST 800.171 (DIB), ITAR, IRS 1075, DoD L4, and CJIS. To provide the highest level of security and compliance, Azure Government **uses physically isolated datacenters and networks (located only in the US)**. Azure Government customers (US federal, state, and local government or their partners) are subject to validation of eligibility.

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

https://docs.microsoft.com/en-us/azure/azure-government/compare-azure-government-global-azure

• Describe Azure China cloud services

Azure China 21Vianet is **operated by 21Vianet** is a **physically separated** instance of cloud services **located in China**, **independently operated and transacted by Shanghai Blue Cloud Technology Co., Ltd. ("21Vianet")**, a wholly owned subsidiary of Beijing 21Vianet Broadband Data Center Co., Ltd.

The Azure **services are based on the same Azure**, Microsoft 365, and Power BI technologies that make up the Microsoft global cloud service, with comparable service levels. Azure **agreements and contracts in China**, where applicable, are **signed between customers and 21Vianet**.

As the **first foreign public cloud service provider offered in China** in compliance with government regulations, Azure China 21Vianet provides **world-class security as discussed on the Trust Center**, as required by Chinese regulations for all systems and applications built on its architecture.

Azure includes the **core components of IaaS, PaaS, and SaaS**. These components include **network, storage, data management, identity management, and many other services**.

Azure China 21Vianet **supports most of the same services that global Azure has**, such as geosynchronous data replication and autoscaling. Even if you already use global Azure services, **to operate in China you may need to rehost or refactor some or all your applications or services**.

According to the China Telecommunication Regulation (in Chinese), **providers of cloud services (IaaS and PaaS) must have value-added telecom permits.** Only **locally registered companies** with **less than 50-percent foreign investment** qualify for these permits. To comply with this regulation, the Azure service in China is operated by 21Vianet, based on the technologies licensed from Microsoft.

Knowledge check:

1. What tool or service allows download of published audit reports and how Microsoft builds and operates its cloud services?

Azure Policy

Azure Service Health

Service Trust Portal

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

2. What site explains details about the personal data Microsoft processes, how Microsoft processes it, and for what purposes?

Microsoft Privacy Statement

That's correct. The Microsoft Privacy Statement explains what personal data Microsoft processes, how Microsoft processes it, and for what purposes.

Compliance Manager
Azure Service Health

Describe Azure Pricing, Service Level Agreements, and Lifecycles (20-25%)

Describe Azure subscriptions

• Describe an Azure Subscription

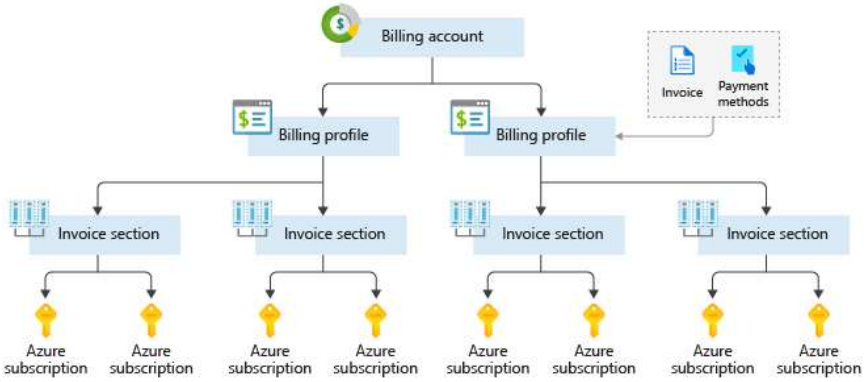
Using Azure requires an ***Azure subscription*** which provides you with **authenticated and authorized access to Azure products and services** and allows you to **provision resources**. An Azure subscription is a **logical unit of Azure services that links to an Azure account**, which is an **identity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

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

There are two types of subscription boundaries that you can use, including:

Billing boundary. This subscription type **determines how an Azure account is billed** for using Azure. You can **create multiple subscriptions** for **different types of billing requirements**, and Azure will **generate separate billing reports and invoices** for each subscription so that you can organize and manage costs.

Access control boundary. Azure will **apply access-management policies at the subscription level**, and you can **create separate subscriptions to reflect different organizational structures**. An example is that within a business, you have different departments to which you apply distinct Azure subscription policies. This allows you to manage and control access to the resources that users provision with specific subscriptions.



• Describe the uses and options with Azure subscriptions such access control and offer types

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

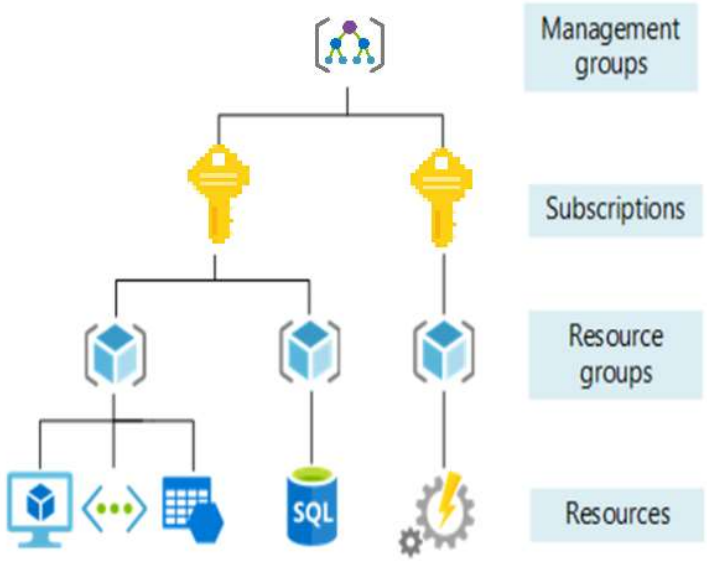
A free account. Get started with **12 months of popular free services**, a **credit** to explore any **Azure service for 30 days, and 25+ services that are always free.** Your Azure **services are disabled when the trial ends** or when your credit expires for paid products, unless you upgrade to a paid subscription.

Pay-As-You-Go. This subscription allows you to **pay for what you use by attaching a credit or debit card to your account.** Organizations can apply to Microsoft for invoicing privileges.

Member offers. Your **existing membership to certain Microsoft products and services affords you credits for your Azure account** and reduced rates on Azure services. For example, member offers are available to **Microsoft Visual Studio subscribers**, **Microsoft Partner Network members**, **Microsoft BizSpark members**, and **Microsoft Imagine members**.

• Describe subscription management using Management groups

The **organizing structure for resources** in Azure has **four levels**: **management groups, subscriptions, resource groups, and resources**. The following image shows the relationship of these levels i.e. the hierarchy of organization for the various objects



Management groups: These are **containers that help you manage access, policy, and compliance for multiple subscriptions.** All **subscriptions in a management group** automatically **inherit the conditions** applied to the management group.

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

Subscriptions: A subscription **groups together user accounts and the resources that have been created by those user accounts.** For each subscription, there are **limits or quotas on the amount of resources you can create and use.** Organizations can use subscriptions to manage costs and the resources that are created by users, teams, or projects.

Resource groups: A resource group is a **logical container** into which **Azure resources** like web apps, databases, and storage accounts are deployed and managed.

Resources: Resources are **instances of services that you create**, like virtual machines, storage, or SQL databases.

Knowledge check:

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

Azure Initiatives

Management Groups

That's correct. Management groups facilitate the hierarchical ordering of Azure resources into collections, at a level of scope above subscriptions. Distinct governance conditions can be applied to each management group, with Azure Policy and Azure RBACs, to manage Azure subscriptions effectively. The resources and subscriptions assigned to a management group automatically inherit the conditions applied to the management group.

Resource Groups

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

Azure Subscription

That's correct. Azure subscription is a logical unit of Azure services that links to an Azure account.

Management Group

Resource Group

3. Which of the following statements is a valid statement about an Azure subscription?

Using Azure does not require a subscription

An Azure subscription is a logical unit of Azure services

That's correct. A subscription is a set of Azure services bundled together for tracking and billing purposes.

You can't have more than one subscription

4. Your billing is based on your usage of Azure resources and is invoiced at what frequency?

Annually

Monthly

That's correct. You will be billed monthly.

Daily

5. When you create an Azure resource like a virtual machine, you have to select where its usage will be paid; what is this called?

Billing account

Billing profile

Azure subscription

That's correct. Exactly, you need to have a subscription to create the resource within.

6. Which Azure support plan is best for business-critical workloads?

Azure Developer

Azure Professional Direct
That's correct. The best way to ensure your solutions are running nearly all the time.
Azure Standard
Describe planning and management of costs
• Describe options for purchasing Azure products and services
There are **three main customer types** on which the available purchasing options for Azure products and services is contingent, including:
Enterprise. Enterprise customers **sign an Enterprise Agreement with Azure** that commits them to spending a negotiated amount on Azure services, which they **typically pay annually**. Enterprise customers also have **access to customized Azure pricing**.
Web direct. Web direct customers **pay public prices for Azure resources**, and their **monthly billing and payments** occur **through the Azure website**.
Cloud Solution Provider. Cloud Solution Provider (CSP) typically are **Microsoft partner companies** that a customer hires to **build solutions on top of Azure.** Payment and billing for Azure usage **occurs through the customer's CSP**.
• Describe options around Azure Free account
• Describe the factors affecting costs such as resource types, services, locations, ingress and egress traffic
When you provision an Azure resource, Azure **creates one or more meter instances for that resource.** The meters track the resources' **usage, and each meter generates a usage record** that is used to calculate your bill.
For example, a **single virtual machine** that you provision in Azure might have the following meters tracking its usage:
Compute Hours
IP Address Hours
Data Transfer In
Data Transfer Out
Standard Managed Disk
Standard Managed Disk Operations
Standard IO-Disk
Standard IO-Block Blob Read
Standard IO-Block Blob Write
Standard IO-Block Blob Delete
Costs are resource-specific, so the **usage** that a meter tracks and the number of meters associated with a resource **depend on the resource type**.
Azure usage rates and billing periods can ***differ between Enterprise, Web Direct, and Cloud Solution Provider (CSP) customers.*** Some subscription types also include usage allowances, which affect costs.
The Azure team develops and offers first-party products and services, while products and services from third-party vendors are available in the **Azure Marketplace. Different billing structures apply to each of these categories.**
The Azure infrastructure is globally distributed, and ***usage costs might vary between locations*** that offer Azure products, services, and resources.
• Describe Zones for billing purposes
Billing zones help determine the cost of services you are using.
Bandwidth refers to **data moving in and out of Azure datacenters**. Some inbound data transfers, such as **data going into Azure datacenters, are free**. For outbound data transfers, such as **data going out of Azure datacenters**, **data transfer pricing is based on *Zones*.**
A ***Zone*** is a **geographical grouping of Azure Regions for billing purposes.** the following Zones exist and include the sample regions as listed below:
Zone 1 – West US, East US, Canada West, West Europe, France Central and others
Zone 2 – Australia Central, Japan West, Central India, Korea South and others
Zone 3 - Brazil South
DE Zone 1 - Germany Central, Germany Northeast
• Describe the Pricing calculator
The ***Pricing Calculator*** is a **tool that helps you estimate the cost of Azure products.** It displays Azure products in categories, and you choose the Azure products you need and configure them according to your specific requirements. Azure then **provides a detailed estimate of the costs** associated with your selections and configurations.
Get a new estimate from the Pricing Calculator by adding, removing, or reconfiguring your selected products. You also can access pricing details, product details, and documentation for each product from the Pricing Calculator.
• Describe the Total Cost of Ownership (TCO) calculator
The ***Total Cost of Ownership Calculator*** is a tool that you **use to estimate cost savings you can realize by migrating to Azure.** To use the TCO calculator, complete the three steps that the following sections explain.

https://azure.microsoft.com/pricing/tco/calculator

• Describe best practices for minimizing Azure costs such as performing cost analysis, creating spending limits and quotas, using tags to identify cost owners, using Azure reservations and using Azure Advisor recommendations

Minimizing costs:

Perform cost analyses. **Carefully consider the products, services, and resources you need**, and read the relevant documentation to understand how each of your choices are metered and billed. Additionally, you should c**alculate your projected costs by using the Azure Pricing and Total Cost of Ownership (TCO) calculators**, only adding the products, services, and resources you need.

Monitor usage with Azure Advisor. The Azure Advisor feature **identifies unused or under-utilized resources,** and you can implement its recommendations by removing unused resources and configuring your resources to match your actual demand.

Use spending limits. Free trial customers and some credit-based Azure subscriptions can use the Spending Limits feature. Azure provides the ***Spending Limits feature to help prevent you from exhausting the credit on your account*** within each billing period. If you have a credit-based subscription and you reach your configured spending limit, Azure suspends your subscription until a new billing period begins.

The spending limit feature is not available for customers who aren't using credit-based subscriptions, such as Pay-As-You-Go subscribers.

Use Azure Reservations. Azure Reservations **offer discounted prices on certain Azure products and resources.** To get a discount, you reserve products and resources by **paying in advance.** You can pre-pay for one year or three years of use of Virtual Machines, SQL Database Compute Capacity, Azure Cosmos Database Throughput, and other Azure resources.

Azure Reservations are only available to Enterprise or CSP customers and for Pay-As-You-Go subscriptions.

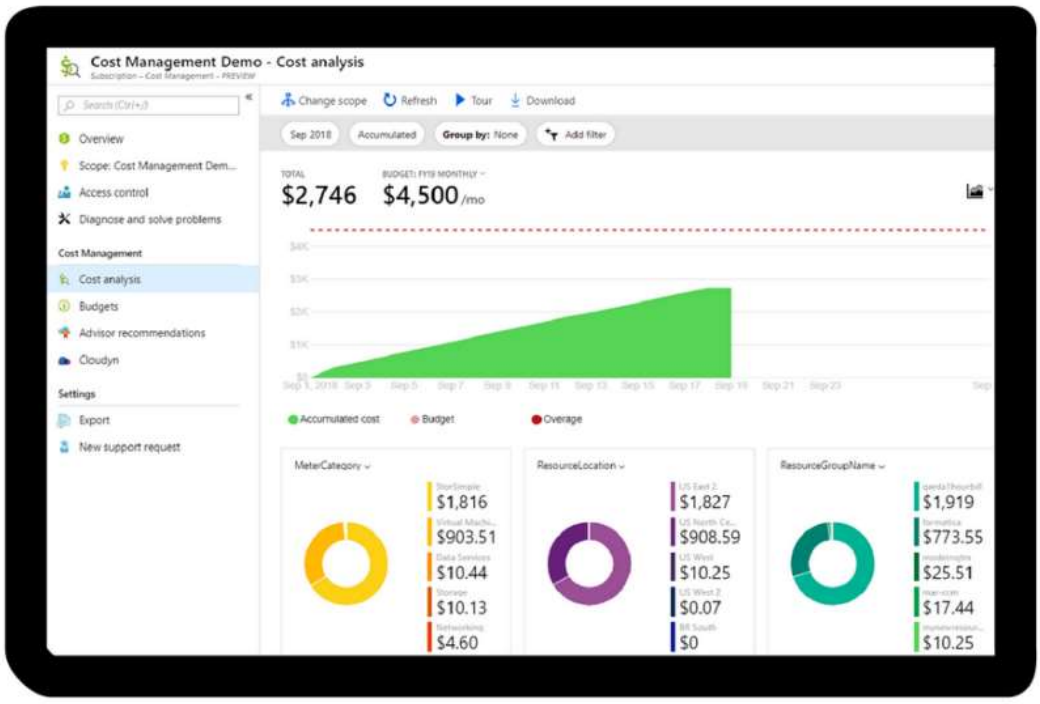
Choose low-cost locations and regions. The cost of Azure products, services, and resources can v**ary across locations and regions**, and if possible, you should u**se them in those locations and regions where they cost less**.

Research available cost-saving offers. Keep up-to-date with the latest Azure customer and subscription offers, and switch to offers that provide the greatest cost-saving benefit.

Apply tags to identify cost owners. Tags help you manage costs associated with the different groups of Azure products and resources. You can **apply tags** to groups of Azure products and resources **to organize billing data**. For example, if you run several virtual machines for different teams, you can use tags to categorize costs by department, such as Human Resources, Marketing, or Finance, or by environment, such as Production or Test. Tags make it easy to identify groups that generate the biggest Azure costs, so you can adjust your spending accordingly.

• Describe Azure Cost Management

Cost Management is an Azure product that **provides a set of tools for monitoring, allocating, and optimizing your Azure costs**.



The main features of the Azure Cost Management toolset include:

Reporting. Generate reports using historical data to forecast future usage and expenditure.

Data enrichment. Improve accountability by categorizing resources with tags that correspond to real-world business and organizational units.

Budgets. Create and manage cost and usage budgets by monitoring resource demand trends, consumption rates, and cost patterns.

Alerting. Get alerts based on your cost and usage budgets.

Recommendations. Receive recommendations to eliminate idle resources and to optimize the Azure resources you provision.
Price. Free to Azure customers.
Knowledge Check:
1. Which of the following provides a set of tools for monitoring, allocating, and optimizing your Azure costs?
Azure Cost Management
That's correct. Azure Cost Management is an Azure product that provides a set of tools for monitoring, allocating, and optimizing your Azure costs.
Azure Pricing Calculator
Total Cost of Ownership Calculator (TCO)
2. Which of the following can be used to estimate cost savings when migrating to Azure?
Pricing calculator
Total Cost of Ownership calculator
That's correct. The TCO calculator is a tool that you use to estimate cost savings you can realize by migrating to Azure.
Usage meter
3. What are the capabilities that Azure Advisor can provide recommendations for?
Costs only
High availability, security, performance, operational excellence, and cost
That's correct. Azure Advisor provides recommendations on many different capabilities for your solutions.
High availability, performance, and cost
4. What can you use Azure Cost Management for?
See historical breakdowns of what services you are spending your money on.
That's correct. You can use the historical breakdowns to change how and why you spend on Azure.
See estimates of what your services might cost if you make a change.
A tool in Azure that lets you define how much you want to spend, then cuts off services when that allocation is met.
5. Which tab of the Azure pricing calculator will you use to put together your estimate?
Estimate
Products
That's correct. The products tab lets you pick what capabilities your solutions and cloud infrastructure needs.
Features
Describe Azure Service Level Agreements (SLAs)
• Describe a Service Level Agreement (SLA)
Microsoft maintains its commitment to providing customers with high-quality products and services by adhering to comprehensive operational policies, standards, and practices. Formal documents known as ***Service-Level Agreements (SLAs)*** capture the specific terms that **define the performance standards that apply to Azure**.
SLAs describe **Microsoft's commitment to providing Azure customers with certain performance standards**.
There are SLAs for **individual Azure products and services**.
SLAs also **specify what happens if a service or product fails to perform to a governing SLA's specification**.
A SLA **defines performance targets for an Azure product or service.** The performance targets that a SLA defines are specific to each Azure product and service.
For example, performance targets for some Azure services are expressed in terms of **uptime** or **connectivity rates**.
A typical SLA specifics performance-target commitments that **range from 99.9 percent ("three nines") to 99.99 percent ("four nines"), for each corresponding Azure product or service**. These targets can apply to such performance criteria as uptime, or response times for services.
SLA downtime estimates
The following table lists the potential cumulative downtime for various SLA levels over different durations:

SLA DOWNTIME ESTIMATES:

SLA percentage	Downtime per week	Downtime per month	Downtime per year
99	1.68 hours	7.2 hours	3.65 days
99.9	10.1 minutes	43.2 minutes	8.76 hours
99.95	5 minutes	21.6 minutes	4.38 hours
99.99	1.01 minutes	4.32 minutes	52.56 minutes
99.999	6 seconds	25.9 seconds	5.26 minutes

Service Credits. SLAs also describe how Microsoft will respond if an Azure product or service fails to perform to its governing SLA's specification.
SERVICE CREDITS:

Monthly Uptime Percentage	Service Credit Percentage
< 99.9	10
< 99	25
< 95	100

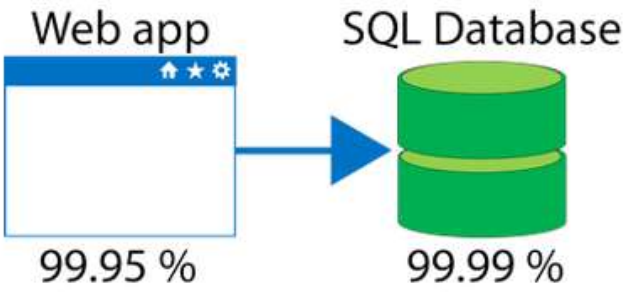
• Describe Composite SLAs

When **combining SLAs across different service offerings**, the resultant SLA is a called a ***Composite SLA***. The resulting composite SLA can provide higher or lower uptime values, depending on your application architecture.

Consider an App Service web app that writes to Azure SQL Database. At the time of this writing, these Azure services have the following SLAs:

App Service Web Apps is 99.95 percent.

SQL Database is 99.99 percent.

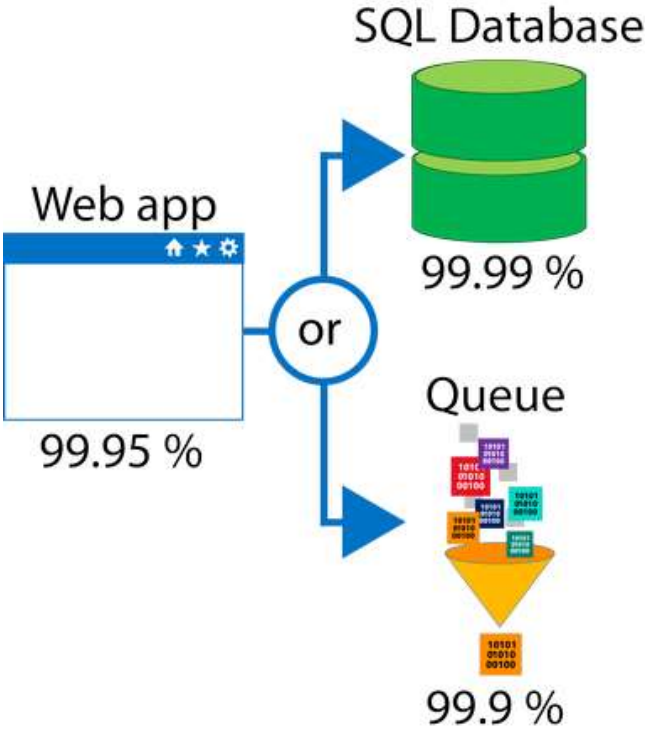


Maximum downtime you would expect for this example application

In the example above, if **either service fails the whole application will fail**. In general, the **individual probability values for each service are independent**. However, the composite SLA value for this application is:

99.95 percent × 99.99 percent = approx 99.94 percent

Conversely, you can **improve the composite SLA** by creating **independent fallback paths**. For example, if SQL Database is unavailable, you can **put transactions into a Queue for processing at a later time**.



With the design shown in the image above, the application is still available even if it can't connect to the database. However, it fails if both the SQL Database and the Queue fail simultaneously. If the expected percentage of time for a simultaneous failure is 0.0001 × 0.001, i.e. (1.0 - 0.9999) x (1.0 - 0.999), the composite SLA for this combined path would be:

Database *OR* Queue = 1.0 − (0.0001 × 0.001) = 99.99999 percent

Therefore, the total composite SLA is:

Web app *AND* (Database *OR* Queue) = 99.95 percent × 99.99999 percent = ~ 99.95 percent

• Describe how to determine an appropriate SLA for an application

Azure customers can use SLAs to evaluate how their Azure solutions meet their business requirements and the needs of their clients and users. By creating your own SLAs, you can set performance targets to suit your specific Azure application.

When creating an ***Application SLA*** consider the following:

Identify workloads. A workload is a distinct capability or task that is logically separated from other tasks, in terms of business logic and data storage requirements. Each workload has different requirements for availability, scalability, data consistency, and disaster

recovery. To ensure that application architecture meets your business requirements, define target SLAs for each workload. Account for the cost and complexity of meeting availability requirements, in addition to application dependencies.
Plan for usage patterns. Usage patterns also play a role in requirements. Identify differences in requirements during critical and non-critical periods. For example, a tax-filing application can't fail during a filing deadline. To ensure uptime, plan redundancy across several regions in case one fails. Conversely, to minimize costs during non-critical periods, you can run your application in a single region.
Establish availability metrics — mean time to recovery (MTTR) and mean time between failures (MTBF). MTTR is the average time it takes to restore a component after a failure. MTBF is how long a component can reasonably expect to last between outages. Use these measures to determine where to add redundancy and to determine service-level agreements (SLAs) for customers.
Establish recovery metrics — recovery time objective and recovery point objective (RPO). RTO is the maximum acceptable time an application can be unavailable after an incident. RPO is the maximum duration of data loss that is acceptable during a disaster. To derive these values, conduct a risk assessment and make sure you understand the cost and risk of downtime or data loss in your organization.
Implement resiliency strategies. Resiliency is the ability of a system to recover from failures and continue to function. Implement resiliency design patterns, such as isolating critical resources, using compensating transactions, and performing asynchronous operations whenever possible.
Build availability requirements into your design. Availability is the proportion of time your system is functional and working. Take steps to ensure that application availability conforms to your service-level agreement. For example, avoid single points of failure, decompose workloads by service-level objective, and throttle high-volume users.

Resiliency is the **ability of a system to recover from failures and continue to function.** It's **not about avoiding failures**, but **responding to failures in a way that avoids downtime or data loss.** The goal of resiliency is to r**eturn the application to a fully functioning state following a failure.** High availability and disaster recovery are two crucial components of resiliency.
When designing your architecture you need to design for resiliency, and you should **perform a Failure Mode Analysis (FMA).** The goal of an ***FMA*** is to **identify possible points of failure** and to **define how the application will respond to those failures.**
Knowledge check:
1. Which of the following answers define performance targets, like uptime, for an Azure product or service?
Service-Level Agreements
That's correct. The SLA defines performance targets for an Azure product or service.
Support Plans
Usage Meters
2. You have two services with different SLAs. The composite SLA is determined by?
Adding the SLAs percentages together
Multiplying the SLAs percentages together
That's correct. To determine a composite SLA, you multiply the individual SLAs together.
Taking the lowest SLA percentage
3. Deploying an app can be done directly to what level of physical granularity?
Region
That's Correct. Azure organizes infrastructure around regions, which include multiple datacenters. You can pick the region you want resources deployed into. You can't select a specific datacenter or location within a datacenter.
Datacenter
Server rack
4. To use Azure datacenters that are made available with power, cooling, and networking capabilities independent from other datacenters in a region, choose a region that supports _____?
Geography distribution
Service-Level Agreements (SLAs)
Availability Zones
That's Correct. Availability Zones are datacenters set up to be an isolation boundary from others in the region, with their own power, cooling, and networking. If one zone in a region goes down, other Availability Zones in the region continue to work.
5. Application availability refers to what?
The Service-Level Agreement of the associated resource.
Application support for an availability zone.
The overall time that a system is functional and working.
That's Correct. The time that a system is working is referred to as the application availability.
Describe service lifecycle in Azure
• Describe Public and Private Preview features
Microsoft offers previews of Azure services, features, and functionality for evaluation purposes. With ***Azure Previews***, you can **test pre-release features, products, services, software, and even regions.** Previews allow users **early access to functionality**. Additionally, users providing feedback on the preview features helps Microsoft improve the Azure service.
There are two categories of preview that are available:
Private preview - An Azure feature is **available to certain Azure customers** for evaluation purposes.
Public preview - An Azure feature is **available to all Azure customers** for evaluation purposes.
Azure portal Preview
You can access preview features that are specific to the Azure portal from the https://preview.portal.azure.com page. Typical portal

preview features provide performance, navigation, and accessibility improvements to the Azure portal interface.

• Describe the term General Availability (GA)

Once a **feature is evaluated and tested successfully**, it may release to customers as part of Azure.

In other words, the feature may be made available for all Azure customers. A feature released to all Azure customers typically goes to ***General Availability or GA***.

• Describe how to monitor feature updates and product changes

Knowledge Check:

1. Which of the following give all Azure customers a chance to test beta and other pre-release features?

General Availability

General Preview

Public Preview

That's correct. Public Preview means that an Azure feature is available to all Azure customers for evaluation purposes.

2. Releasing a feature to all Azure customers is called?

General Availability (GA)

That's correct. GA is when a feature released to all Azure customers.

General Preview

Public Preview