



AZ-900

Estera Kot

kote@ee.pw.edu.pl

Skills measured

Understand Cloud Concepts (15-20%)

Understand Core Azure Services (30-35%)

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

Understand Azure Pricing and Support (25-30%)



Describe the benefits and considerations of using cloud services

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

understand the principles of economies of scale

understand the differences between Capital Expenditure (CapEx) and Operational Expenditure (OpEx)

understand the consumption-based model

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

describe Infrastructure-as-a-Service (IaaS)

describe Platform-as-a-Service (PaaS)

describe Software-as-a-Service (SaaS)

compare and contrast the three different service types

Describe the differences between Public, Private and Hybrid cloud models

describe Public cloud

describe Private cloud

describe Hybrid cloud

compare and contrast the three different cloud models

Skills measured

Understand Cloud Concepts (15-20%)

Understand Core Azure Services (30-35%)

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

Understand Azure Pricing and Support (25-30%)



Understand the core Azure architectural components

describe Regions

describe Availability Zones

describe Resource Groups

describe Azure Resource manager

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 Service and Functions

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

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

describe products available for Databases such as CosmosDB, Azure SQL Database, Azure Database Migration service, and Azure SQL Data Warehouse

describe the Azure Marketplace and its usage scenarios

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 Fundamentals, IoT Hub and IoT Central

describe Big Data and Analytics and products that are available for Big Data and Analytics such as SQL Data Warehouse, HDInsight and Data Lake Analytics

describe Artificial Intelligence (AI) and products that are available for AI such as Azure Machine Learning Service and Studio

describe Serverless computing and Azure products that are available for serverless computing such as Azure Functions, Logic Apps and App grid

describe the benefits and outcomes of using Azure solutions

Understand Azure management tools

understand Azure tools such as Azure CLI, PowerShell, and the Azure Portal

understand Azure Advisor

Skills measured

Understand Cloud Concepts (15-20%)

Understand Core Azure Services (30-35%)

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

Understand Azure Pricing and Support (25-30%)



Understand securing network connectivity in Azure

describe Azure Firewall
describe Azure DDoS Protection
describe Network Security Group (NSG)
choose an appropriate Azure security solution

Describe core Azure Identity services

understand the difference between authentication and authorization
describe Azure Active Directory
describe Azure Multi-Factor Authentication

Describe security tools and features of Azure

describe Azure Security
understand Azure Security center usage scenarios
describe Key Vault
describe Azure Information Protection (AIP)
describe Azure Advanced Threat Protection (ATP)

Describe Azure governance methodologies

describe Azure Policies
describe Initiatives
describe Role-Based Access Control (RBAC)
describe Locks
describe Azure Advisor security assistance

Understand monitoring and reporting options in Azure

describe Azure Monitor
describe Azure Service Health
understand the use cases and benefits of Azure Monitor and Azure Service Health

Understand privacy, compliance and data protection standards in Azure

understand industry compliance terms such as GDPR, ISO and NIST
understand the Microsoft Privacy Statement
describe the Trust center
describe the Service Trust Portal
describe Compliance Manager
determine if Azure is compliant for a business need
understand Azure Government services
understand Azure Germany services

Skills measured

Understand Cloud Concepts (15-20%)

Understand Core Azure Services (30-35%)

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

Understand Azure Pricing and Support (25-30%)



Understand Azure subscriptions

describe an Azure subscription

understand the uses and options with Azure subscriptions

Understand planning and management of costs

understand options for purchasing Azure products and services

understand options around Azure Free account

understand the factors affecting costs such as resource types, services, locations, ingress and egress traffic

understand Zones for billing purposes

understand the Pricing calculator

understand the Total Cost of Ownership (TCO) calculator

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

describe Azure Cost Management

Understand the support options available with Azure

understand support plans that are available such as Dev, Standard, Professional Direct and Premier

understand how to open a support ticket

understand available support channels outside of support plan channels

describe the Knowledge Center

Describe Azure Service Level Agreements (SLAs)

describe a Service Level Agreement (SLA)

determine SLA for a particular Azure product or service

Understand service lifecycle in Azure

understand Public and Private Preview features

understand how to access Preview features

understand the term General Availability (GA)

monitor feature updates

Understand Cloud Concepts

It's cost-effective

It's scalable

It's elastic

It's current

It's global

It's secure

Today, the cloud can be used to get up and running quickly. You can start providing services to customers without significant upfront costs or equipment setup time.

These two approaches to investment are referred to as:

Capital Expenditure (CapEx): CapEx is the spending of money on physical infrastructure up front, and then deducting that expense from your tax bill over time. **CapEx is an upfront cost**, which has a value that reduces over time.

Operational Expenditure (OpEx): **OpEx is spending money on services or products now and being billed for them now**. You can deduct this expense from your tax bill in the same year. There's no upfront cost. You pay for a service or product as you use it.

What is cloud computing?

Cloud computing is the delivery of computing services over the Internet using a pay-as-you-go pricing mode

Benefits of using cloud services

- Elasticity
- Agility
- Economics of scale

Public cloud

This is the most common deployment model. In this case, you have no local hardware to manage or keep up-to-date – everything runs on your cloud provider’s hardware. In some cases, you can save additional costs by sharing computing resources with other cloud users. Businesses can use multiple public cloud providers of varying scale. Microsoft Azure is an example of a public cloud provider.

Advantages

- High scalability/agility – you don’t have to buy a new server in order to scale
- Pay-as-you-go pricing – you pay only for what you use, no CapEx costs
- You’re not responsible for maintenance or updates of the hardware
- Minimal technical knowledge to set up and use - you can leverage the skills and expertise of the cloud provider to ensure workloads are secure, safe, and highly available
- A common use case scenario is deploying a web application or a blog site on hardware and resources that are owned by a cloud provider. Using a public cloud in this scenario allows cloud users to get their website or blog up quickly, and then focus on maintaining the site without having to worry about purchasing, managing or maintaining the hardware on which it runs.

Disadvantages

Not all scenarios fit the public cloud. Here are some disadvantages to think about:

- There may be specific security requirements that cannot be met by using public cloud
- There may be government policies, industry standards, or legal requirements which public clouds cannot meet
- You don't own the hardware or services and cannot manage them as you may want to
- Unique business requirements, such as having to maintain a legacy application might be hard to meet

Advantages:

No CapEx. You don’t have to buy a new server in order to scale.

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

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

Maintenance. Organizations have no responsibility for hardware maintenance or updates.

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

Disadvantages:

Security. There may be specific security requirements that cannot be met by using public cloud.

Compliance. There may be government policies, industry standards, or legal requirements which public clouds cannot meet.

Ownership. Organizations don't own the hardware or services and cannot manage them as they may wish.

Specific scenarios. If organizations have a unique business requirement, such as having to maintain a legacy application, it may be hard to meet that requirement with public cloud services.

Private cloud

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

Advantages

This approach has several advantages:

- You have complete control over the resources and can ensure the configuration can support any scenario or legacy application
- You have complete control (and responsibility) over security
- Private clouds can meet strict security, compliance, or legal requirements in ways a public cloud might not be able to

Disadvantages

- Some reasons teams move away from the private cloud are:
- You have upfront CapEx costs and must purchase the hardware for startup and maintenance
- Owning the equipment limits the agility - to scale you must buy, install, and setup new hardware
- Private clouds require IT skills and expertise that's hard to come by
- A use case scenario for a private cloud would be when an organization has data that cannot be put in the public cloud, perhaps for legal reasons. For example, they may have medical data that cannot be exposed publicly. Another scenario may be where government policy requires specific data to be kept in-country or privately.
- A private cloud can provide cloud functionality to external customers as well, or to specific internal departments such as Accounting or Human Resources.

Advantages:

Control. Organizations have complete control over the resources.

Security. Organizations have complete control over security.

Compliance. If organizations have very strict security, compliance, or legal requirements, a private cloud may be the only viable option.

Specific scenarios. If an organization has a specific scenario not easily supported by a public cloud provider (such as having to maintain a legacy application), it may be preferable to run the application locally.

Disadvantages:

Upfront CapEx. Hardware must be purchased for start-up and maintenance.

Agility. Private clouds are not as agile as public clouds, because you need to purchase and set up all the underlying infrastructure before they can be leveraged.

Maintenance. Organizations have the responsibility for hardware maintenance and updates.

Skills. Private clouds requires in-house IT skills and expertise that may be hard to get or be costly.

Hybrid cloud

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

This is helpful when you have some things that cannot be put in the cloud, maybe for legal reasons. For example, you may have some specific pieces of data that cannot be exposed publicly (such as medical data) which needs to be held in your private datacenter. Another example is one or more applications that run on old hardware that can't be updated. In this case, you can keep the old system running locally, and connect it to the public cloud for authorization or storage.

Advantages

Some advantages of a hybrid cloud are:

- You can keep any systems running and accessible that use out-of-date hardware or an out-of-date operating system
- You have flexibility with what you run locally versus in the cloud
- You can take advantage of economies of scale from public cloud providers for services and resources where it's cheaper, and then supplement with your own equipment when it's not
- You can use your own equipment to meet security, compliance, or legacy scenarios where you need to completely control the environment

Disadvantages

- Some concerns you'll need to watch out for are:
- It can be more expensive than selecting one deployment model since it involves some CapEx cost up front
- It can be more complicated to set up and manage

Advantages:

Flexibility. The most flexible scenario; with a hybrid cloud setup, an organization can decide to run their applications either in a private cloud or in a public cloud.

Costs. Organizations can take advantage of economies of scale from public cloud providers for services and resources as they wish. This allows them to access cheaper storage than they can provide themselves.

Control. Organizations can still access resources over which they have total control.

Security. Organizations can still access resources for which they are responsible for security.

Compliance. Organizations maintain the ability to comply with strict security, compliance, or legal requirements as needed.

Specific scenarios. Organizations maintain the ability to support specific scenarios not easily supported by a public cloud provider, such as running legacy applications. In this case, they can keep the old system running locally, and connect it to the public cloud for authorization or storage. Additionally, they could host a website in the public cloud, and link it to a highly secure database hosted in their private cloud.

Disadvantages:

Upfront CapEx. Upfront CapEx is still required before organizations can leverage a private cloud.

Costs. Purchasing and maintaining a private cloud to use alongside the public cloud can be more expensive than selecting a single deployment model.

Skills. Deep technical skills are still required to be able to set up a private cloud.

Ease of management. Organizations need to ensure there are clear guidelines to avoid confusion, complications or misuse.

Infrastructure as a service (IaaS)

Infrastructure as a Service is the most flexible category of cloud services. It aims to give you complete control over the hardware that runs your application (IT infrastructure servers and virtual machines (VMs), storage, networks, and operating systems). Instead of buying hardware, with IaaS, you rent it. It's an instant computing infrastructure, provisioned and managed over the internet.

Note

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

IaaS is commonly used in the following 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 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.

IaaS has the following characteristics:

Upfront costs. IaaS has no upfront costs. Users pay only for what they consume.

User ownership. The user is responsible for the purchase, installation, configuration, and management of their own software operating systems, middleware, and applications.

Cloud provider ownership. The cloud provider is responsible for ensuring that the underlying cloud infrastructure (such as virtual machines, storage and networking) is available for the user.

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

Common usage scenarios:

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

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

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

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

Platform as a service (PaaS)

PaaS provides an environment for building, testing, and deploying software applications. The goal of PaaS is to help you create an application quickly without managing the underlying infrastructure. For example, when deploying a web application using PaaS, you don't have to install an operating system, web server, or even system updates.

PaaS is a complete development and deployment environment in the cloud, with resources that enable organizations to deliver everything from simple cloud-based apps to sophisticated cloud-enabled enterprise applications. Resources are purchased from a cloud service provider on a pay-as-you-go basis and accessed over a secure Internet connection.

PaaS is commonly used in the following scenarios:

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

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

Software as a service (SaaS)

SaaS is software that is centrally hosted and managed for the end customer. It is usually based on an architecture where one version of the application is used for all customers, and licensed through a monthly or annual subscription. Office 365, Skype, and Dynamics CRM Online are perfect examples of SaaS software.

PaaS has the following characteristics:

Upfront costs. There are no upfront costs, and users pay only for what they consume.

User ownership. The user is responsible for the development of their own applications. However, they are not responsible for managing the server or infrastructure. This allows the user to focus on the application or workload they want to run.

Cloud provider ownership. The cloud provider is responsible for operating system management, and network and service configuration. Cloud providers are typically responsible for everything apart from the application that a user wants to run. They provide a complete managed platform on which to run an application.

Common usage scenarios:

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

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

SaaS has the following characteristics:

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

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

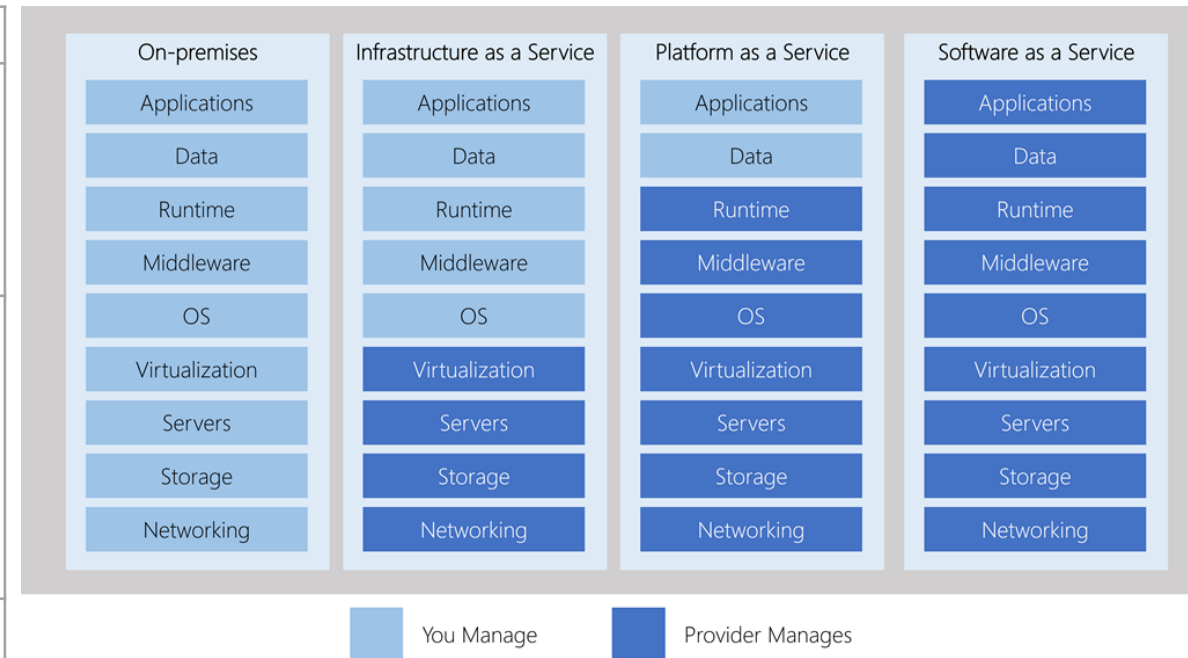
Cloud provider ownership. The cloud provider is responsible for the provision, management, and maintenance of the application software.

Common usage scenarios:

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

Cost and Ownership

	IaaS	PaaS	SaaS
Upfront costs	There are no upfront costs. Users pay only for what they consume.	There are no upfront costs. Users pay only for what they consume.	Users have no upfront costs; they pay a subscription, typically on a monthly or annual basis.
User ownership	The user is responsible for the purchase, installation, configuration, and management of their own software operating systems, middleware, and applications.	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.	Users just use the application software; they are not responsible for any maintenance or management of that software.
Cloud provider ownership	The cloud provider is responsible for ensuring that the underlying cloud infrastructure (such as virtual machines, storage, and networking) is available for the user.	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.	The cloud provider is responsible for the provision, management, and maintenance of the application software.



- 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.

IAAS

Advantages:

No CapEx. Users have no upfront costs.

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

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

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

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

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

Disadvantages:

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

PAAS

Advantages:

No CapEx. Users have no upfront costs.

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

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

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

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

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

Disadvantages:

Platform limitations. There may be some limitations to a particular 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 particular workload.

SaaS

SAAS

Advantages:

No CapEx. Users don't have any upfront costs.

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

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

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

Disadvantages

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

Architectural components of Azure

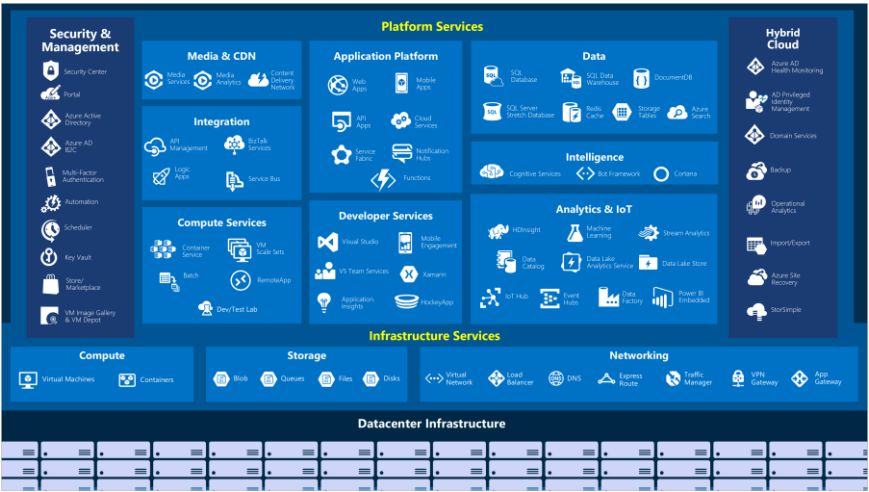
- Region
- Availability zone
- Resource group
- Availability set

Azure services

Compute

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

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



Deploying containers;

- Azure Kubernetes services
- Azure container instances
- Azure app services
- Azure service fabric

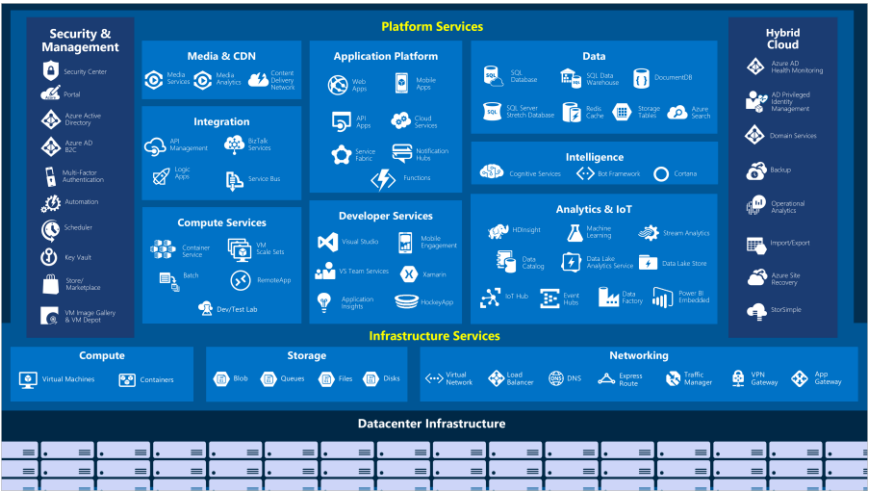
Azure services

Networking

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

Azure networking facilities have the following features:

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



Azure services

Storage

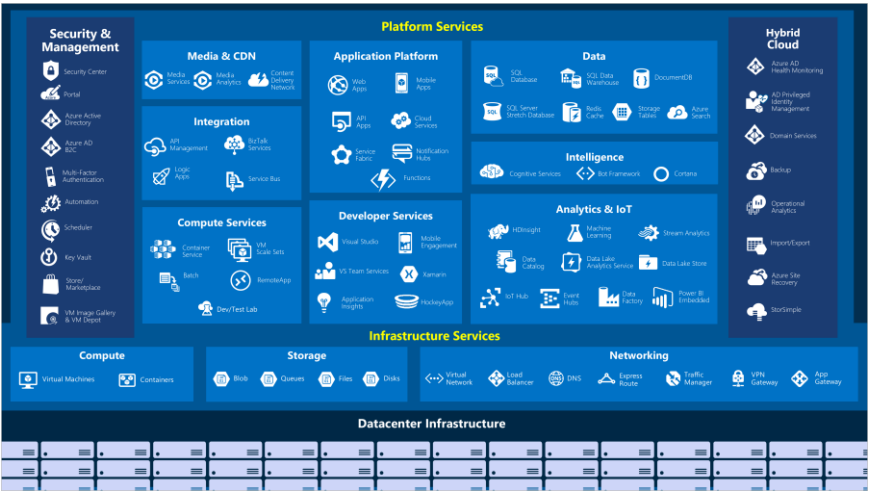
Azure provides four main types of storage services. These services are:

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

Blob storage has no restrictions on the data types it can hold, is highly scalable and can support simultaneous uploads

These services all share several common characteristics:

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



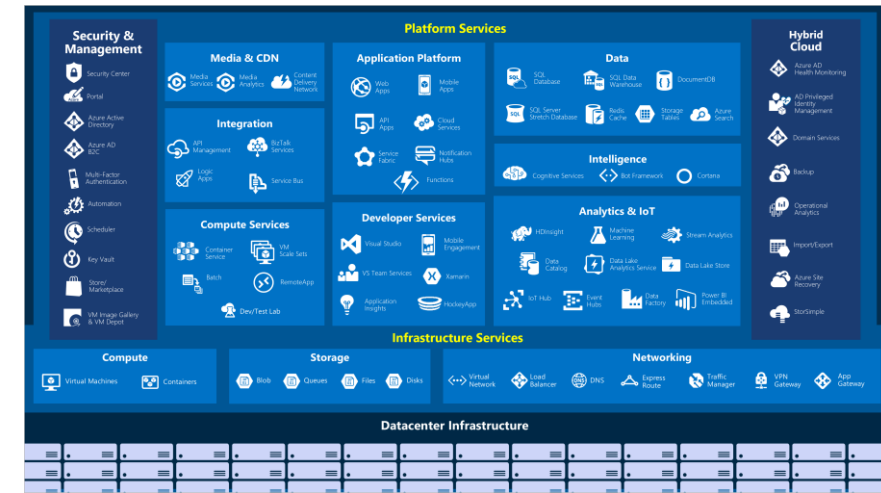
Azure services

Mobile

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

Other features of this service include:

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

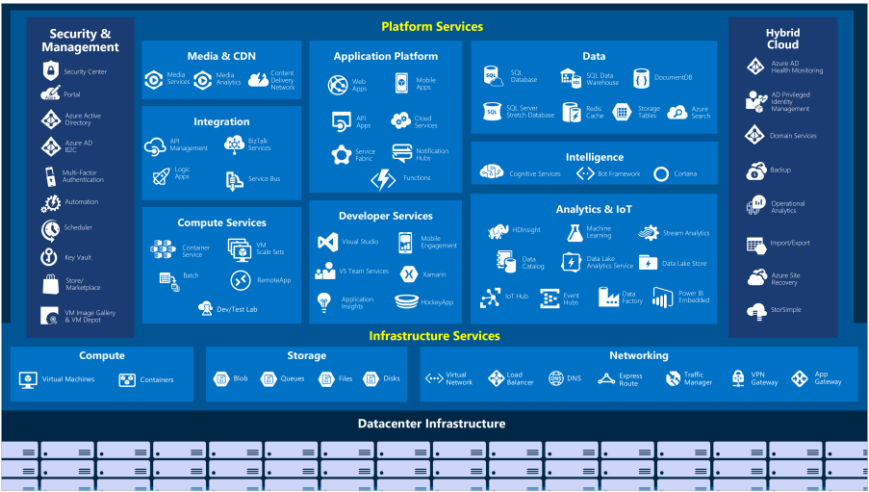


Azure services

Databases

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

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



Azure services

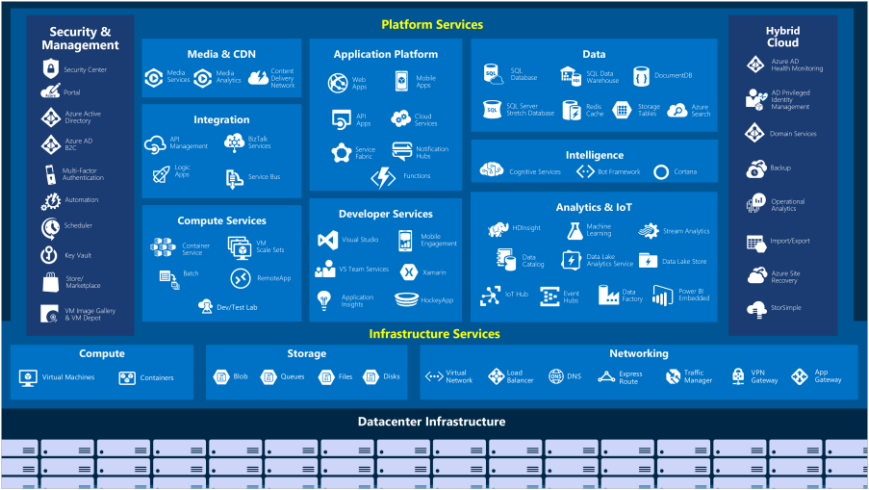
Web

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

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

Internet of Things

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



Service Name	Description
IoT Central	Fully-managed global IoT software as a service (SaaS) solution that makes it easy to connect, monitor, and manage your IoT assets at scale
Azure IoT Hub	Messaging hub that provides secure communications and monitoring between millions of IoT devices
IoT Edge	Push your data analysis onto your IoT devices instead of in the cloud allowing them to react more quickly to state changes.

Azure services

Big Data

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

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

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

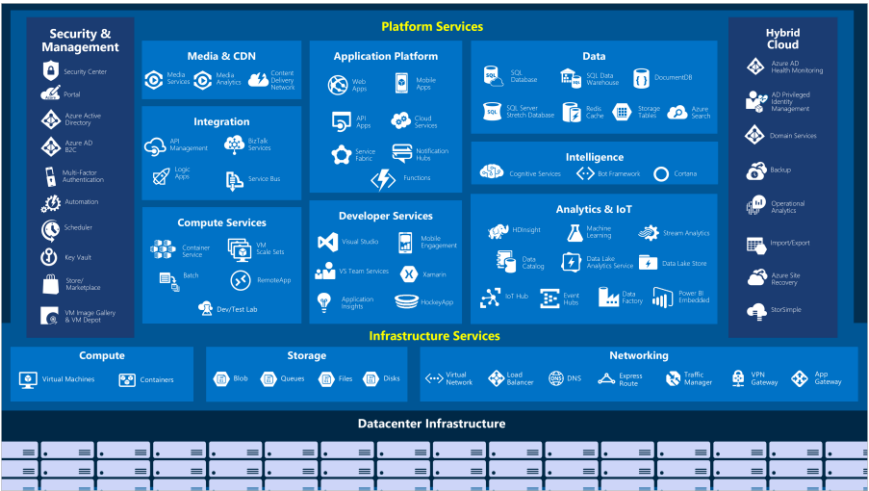
Artificial Intelligence

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

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

Some of the most common Artificial Intelligence and Machine Learning service types in Azure are:

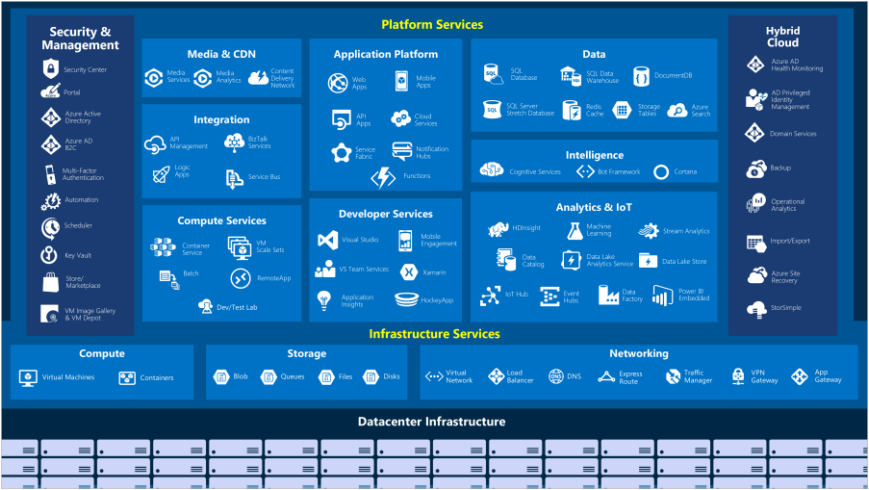
Service Name	Description
Azure Machine Learning Service	Cloud-based environment you can use to develop, train, test, deploy, manage, and track machine learning models. It can auto-generate a model and auto-tune it for you. It will let you start training on your local machine, and then scale out to the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



Azure services

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

Service Name	Description
Vision	Image-processing algorithms to smartly identify, caption, index, and moderate your pictures and videos.
Speech	Convert spoken audio into text, use voice for verification, or add speaker recognition to your app.
Knowledge mapping	Map complex information and data in order to solve tasks such as intelligent recommendations and semantic search.
Bing Search	Add Bing Search APIs to your apps and harness the ability to comb billions of webpages, images, videos, and news with a single API call.
Natural Language processing	Allow your apps to process natural language with pre-built scripts, evaluate sentiment and learn how to recognize what users want.



DevOps

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

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

VM

What is a virtual machine?

A virtual machine, or VM, is a software emulation of a physical computer

What defines a virtual machine on Azure?

A virtual machine is defined by a number of factors, including its size and location. Before you bring up your VM, let's briefly cover what's involved.

Size

A VM's *size* defines its processor speed, amount of memory, initial amount of storage, and expected network bandwidth. Some sizes even include specialized hardware such as GPUs for heavy graphics rendering and video editing.

Region

Azure is made up of data centers distributed throughout the world. A *region* is a set of Azure data centers in a named geographic location. Every Azure resource, including virtual machines, is assigned a region. East US and North Europe are examples of regions.

Network

A *virtual network* is a logically isolated network on Azure. Each virtual machine on Azure is associated with a virtual network. Azure provides cloud-level firewalls for your virtual networks called *network security groups*.

Resource groups

Virtual machines and other cloud resources are grouped into logical containers called *resource groups*. Groups are typically used to organize sets of resources that are deployed together as part of an application or service. You refer to a resource group by its name.

What is scale?

Scale refers to adding network bandwidth, memory, storage, or compute power to achieve better performance.

You may have heard the terms *scaling up* and *scaling out*.

Scaling up, or vertical scaling, means to increase the memory, storage, or compute power on an existing virtual machine. For example, you can add additional memory to a web or database server to make it run faster.

Scaling out, or horizontal scaling, means to add extra virtual machines to power your application. For example, you might create many virtual machines configured in exactly the same way and use a load balancer to distribute work across them.

What is a region?

A region is a geographical area on the planet containing at least one, but potentially multiple datacenters that are nearby and networked together with a low-latency network.

Special Azure regions

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

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

Regions are what you use to identify the location for your resources



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 preserve data residency and compliance boundaries. This division has several benefits.

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

What is an Availability Zone?

Availability Zones are physically separate datacenters within an Azure region.

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

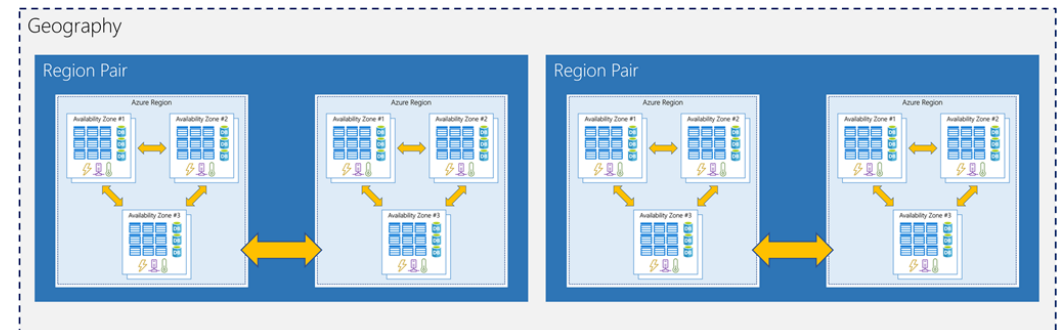
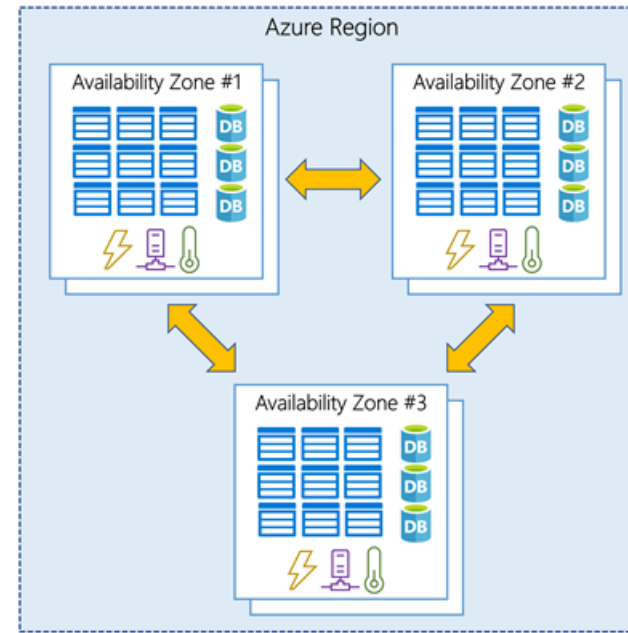
Supported regions

Not every region has support for Availability Zones. The following regions have a minimum of three separate zones to ensure resiliency.

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

What is a region pair?

Each Azure region is always paired with another region within the same geography (such as US, Europe, or Asia) at least 300 miles away. This approach allows for the replication of resources (such as virtual machine storage) across a geography that helps reduce the likelihood of interruptions due to events such as natural disasters, civil unrest, power outages, or physical network outages affecting both regions at once. Examples of region pairs in Azure are West US paired with East US, and SouthEast Asia paired with East Asia.

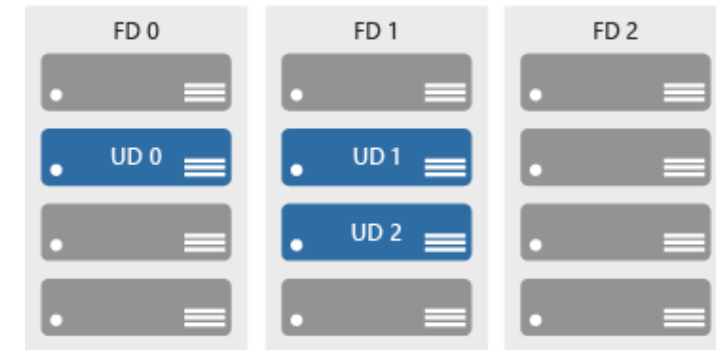


Availability sets

Availability sets are a way for you to ensure your application remains online if a high-impact maintenance event is required, or a hardware failure occurs. Availability sets are made up of update domains and fault domains.

Update domains (UD). 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 (FD). 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.



To guaranteed availability of 99.99% the minimum number of virtual machines and minimum number of availability zones you should recommend for the deployment

Minimum number of virtual machines: 2

Minimum number of availability zones: 2

Service Level Agreements for Azure

Microsoft maintains its commitment to providing customers with high-quality products and services by adhering to comprehensive operational policies, standards, and practices. Formal documents called *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 specific 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.

Important

Azure does not provide SLAs for most services under the *Free* or *Shared* tiers. Also, free products such as Azure Advisor do not typically have an SLA.

SLAs for Azure products and services

There are three key characteristics of SLAs for Azure products and services:

- 1.Performance Targets
- 2.Uptime and Connectivity Guarantees
- 3.Service credits

Resiliency

Resiliency is the ability of a system to recover from failures and continue to function. It's not about avoiding failures, but responding to failures in a way that avoids downtime or data loss.

Availability refers to the time that a system is functional and working. Maximizing availability requires implementing measures to prevent possible service failures. However, devising preventative measures can be difficult and expensive, and often results in complex solutions.

As your solution grows in complexity, you will have more services depending on each other. Therefore, you might overlook possible failure points in your solution if you have several interdependent services.

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 life cycle, rather than manage components individually.

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

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

When creating and placing resources within resource groups there are a few considerations to take into account:

- 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.

What is an Azure account?

An *Azure account* is tied to a specific identity and holds information like:

- Name, email, and contact preferences
- Billing information such as a credit card

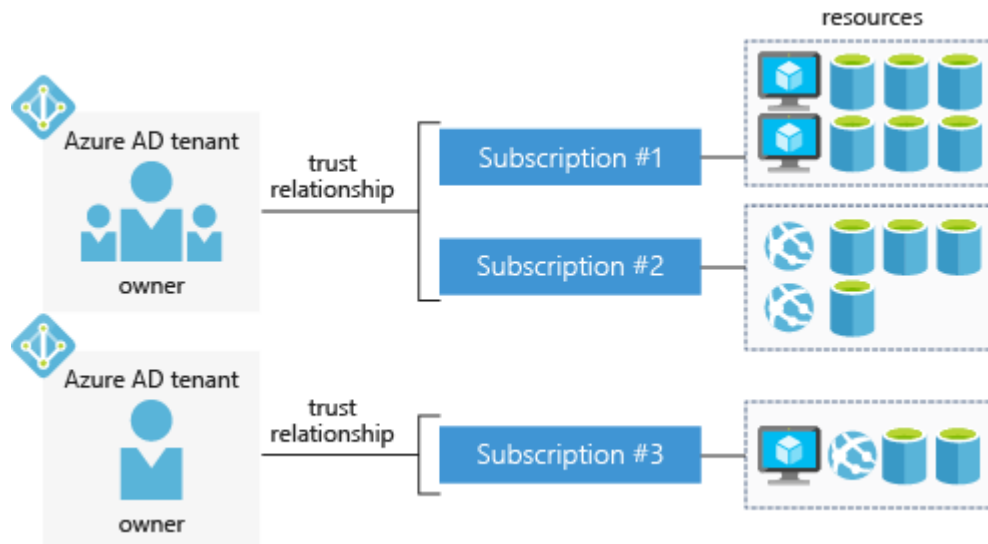
An Azure account is what you use to sign in to the Azure website and administer or deploy services. Every Azure account is associated with one or more *subscriptions*.

What is an Azure subscription?

An *Azure subscription* is a logical container used to provision resources in Microsoft Azure. It holds the details of all your resources like virtual machines, databases, etc. or

An Azure subscription is a logical unit of Azure that is linked to an Azure account

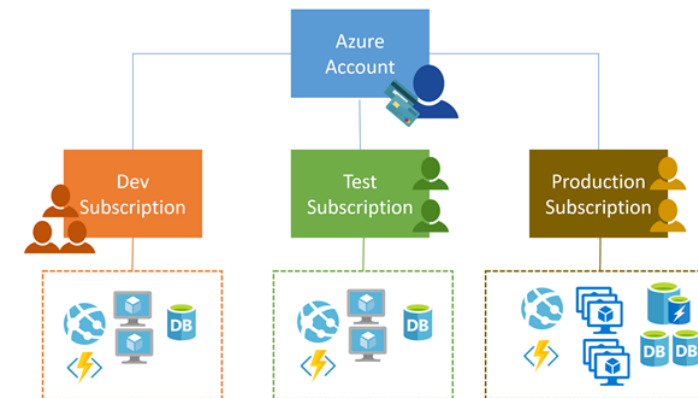
An Azure subscription provides authentication and authorized access to Azure products and services



Subscription types

Azure offers free and paid subscription options to suit different needs and requirements. The most commonly used subscriptions are:

- Free
- Pay-As-You-Go
- Enterprise Agreement
- CSP
- Student



Billing

One bill is generated for every Azure subscription on a monthly basis. The payment is charged automatically to the associated account credit or debit card within 10 days after the billing period ends. On your credit card statement, the line item would say MSFT Azure.

Azure support options

Every Azure subscription includes free access to the following essential support services:

- Billing and subscription support
- Azure products and services documentation
- Online self-help documentation
- Whitepapers
- Community support forums

Azure support plans

Microsoft offers four paid Azure support plans for customers who require technical and operational support: **Developer, Standard, Professional Direct, and Premier**.

	Basic	Developer	Standard	Professional Direct	Premier
Scope	Available to all Microsoft Azure accounts	Trial and non-production environments	Production workload environments	Business-critical dependence	Substantial dependence across multiple products
Technical Support		Business hours access to Support Engineers via email	24x7 access to Support Engineers via email and phone	24x7 access to Support Engineers via email and phone	24x7 access to Support Engineers via email and phone
Case Severity/Response Times		Minimal business impact (Sev C): <8 business hours	Critical business impact (Sev A): <1 hour	Critical business impact (Sev A): <1 hour	Critical business impact (Sev A): <1 hour <15 minutes (with Azure Rapid Response or Azure Event Management)
Architecture Support		General guidance	General guidance	Architectural guidance based on best practice delivered by ProDirect Delivery Manager	Customer-specific architectural support such as design reviews, performance tuning, configuration, and more
Operations Support				Onboarding services, service reviews, Azure Advisor consultations	Technical account manager-led service reviews and reporting
Training				Azure Engineering-led web seminars	Azure Engineering-led web seminars, on-demand training
Proactive Guidance				ProDirect Delivery Manager	Designated Technical Account Manager
Launch Support					Azure Event Management (available for additional fee)

Know the support plans!

Other support options

Several additional support channels are available outside Azure's official support plans.

Channel	Description
Azure Knowledge Center	The Azure Knowledge Center is a searchable database that contains answers to common support questions, from a community of Azure experts, developers, customers, and users. You can browse through all responses within the Azure Knowledge Center. Find specific solutions by entering keyword search terms into the text-entry field and further refine your search results by selecting products or tags from the lists provided by two dropdown lists.
Microsoft Developer Network (MSDN) Forums	Get support by reading responses to Azure technical questions from Microsoft's developers and testers on the MSDN Azure discussion forums .
Stack Overflow	You can review answers to questions from the development community on StackOverflow .
Server Fault	Review community responses to questions about System and Network Administration in Azure on ServerFault .
Azure Feedback Forums	Read ideas and suggestions for improving Azure made by Azure users and customers on the Azure feedback forums .
Twitter	Tweet @AzureSupport to get answers and support from the official Microsoft Azure Twitter channel .

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.

With Azure Resource Manager, you can:

- Deploy Application resources. Update, manage, and delete all the resources for your solution in a single, coordinated operation.
- Organize resources. Manage your infrastructure through declarative templates rather than scripts. You can see which resources are linked by a dependency, and you can apply tags to resources to categorize them for management tasks, such as billing.
- Control access and resources. You can control who in your organization can perform actions on the resources. You manage permissions by defining roles, adding users or groups to the roles, and applying policies at resource group level. Examples of elements you may wish to control are: enforcing naming convention on resources, limiting which types and instances of resources can be deployed, or limiting which regions can host a type of resource.

ARM templates are JSON files

Azure management options

Tools that are commonly used for day-to-day management and interaction include:

- Azure portal for interacting with Azure via a Graphical User Interface (GUI)
- Azure PowerShell and Azure Command-Line Interface (CLI) for command line and automation-based interactions with Azure
- Azure Cloud Shell for a web-based command-line interface
- Azure mobile app for monitoring and managing your resources from your mobile device

[Azure Cloud Shell](#) is a browser-based scripting environment for command-line administration of Azure resources. It provides support for two shell environments. Linux users can opt for a Bash experience, while Windows users can use PowerShell.

Both environments support the Azure CLI and Azure PowerShell CLIs. Linux defaults to the Azure CLI (with the az command pre-installed), but you can switch to PowerShell for Linux by typing pwsh. The Windows-based environment has both CLI tools pre-installed. In addition to these administrative tools, the Cloud Shell has a suite of developer tools, text editors, and other tools available including:

Developer Tools

.NET Core

Python

Java

Node.js

Go

Editors

code (Cloud Shell Editor)

vim

nano

emacs

Other tools

git

maven

make

npm

[and more...](#)

Powershell

```
New-AzureRmVm `
  -ResourceGroupName
"MyResourceGroup" `
  -Name "TestVm" `
  -Image "UbuntuLTS"
...
```

Azure CLI

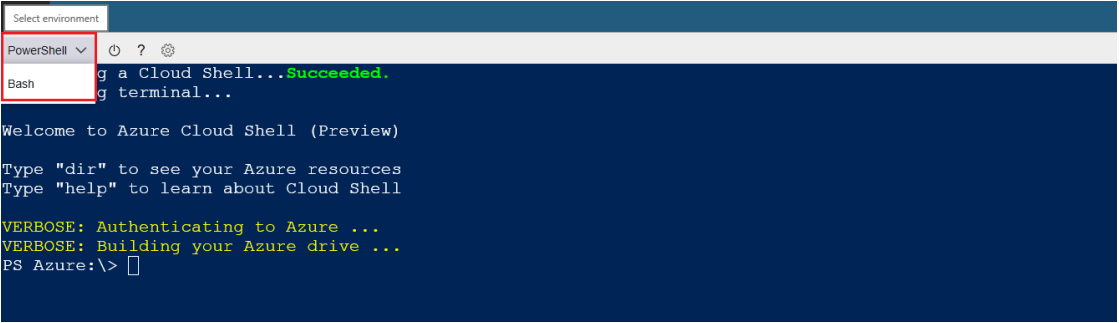
```
az vm create \
  --resource-group MyResourceGroup \
  --name TestVm \
  --image UbuntuLTS
--generate-ssh-keys
...
```

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 current 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 ad hoc administrative tasks
- and more...

Azure management option	windows	linux	Mac OS
Azure portal (web based)	x	x	x
Azure Powershell on windows powershell	x		
Azure Cli	x	x	x
Azure powershell on Powershell core	x	x	x
Azure cloudshell (web based)	x	x	x
Azure mobile APP			

cloudshell



What is Azure compute?

Azure compute is an on-demand computing service for running cloud-based applications. It provides computing resources like multi-core processors and supercomputers via virtual machines and containers. It also provides serverless computing to run apps without requiring infrastructure setup or configuration. The resources are available on-demand and can typically be created in minutes or even seconds. You pay only for the resources you use and only for as long as you're using them.

There are four common techniques for performing compute in Azure:

- Virtual machines
- Containers
- Azure App Service
- Serverless computing

Virtual machines, or VMs, are software emulations of physical computers. They include a virtual processor, memory, storage, and networking resources

Containers are a virtualization environment for running applications. Just like virtual machines, containers are run on top of a host operating system but unlike VMs, they don't include an operating system for the apps running *inside* the container.

Azure App Service is a platform-as-a-service (PaaS) offering in Azure that is designed to host enterprise-grade web-oriented applications

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

Scaling VMs in Azure

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

- Availability sets
- Virtual Machine Scale Sets
- Azure Batch

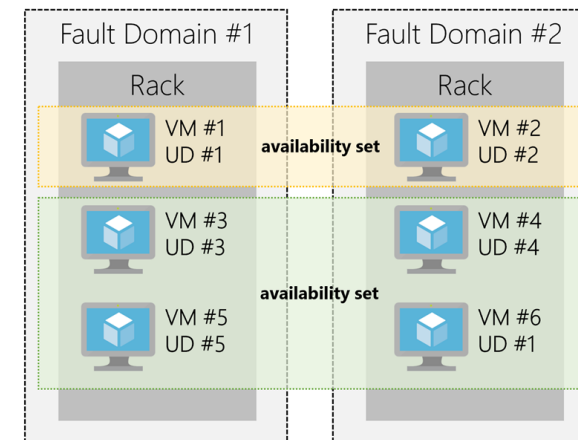
An **availability set** is a logical grouping of two or more VMs that help keep your application available during planned or unplanned maintenance.

A **planned maintenance event** is when the underlying Azure fabric that hosts VMs is updated by Microsoft. **Unplanned maintenance events** involve a hardware failure in the data center, such as a power outage or disk failure.

With an availability set, you get:

Up to three fault domains that each have a server rack with dedicated power and network resources

Five logical update domains



What are virtual machine scale sets?

Azure Virtual Machine Scale Sets let you create and manage a group of identical, load balanced VMs

What is Azure Batch?

Azure Batch enables large-scale job scheduling and compute management with the ability to scale to tens, hundreds, or thousands of VMs.

Containers in Azure

Azure supports Docker containers, and there are several ways to manage containers in Azure.

- Azure Container Instances (ACI)
- Azure Kubernetes Service (AKS)

Types of web apps

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

- Web Apps
- API Apps
- WebJobs
- Mobile Apps

Serverless computing in Azure

Azure has two implementations of serverless compute:

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

Functions vs. Logic Apps

Functions and Logic Apps can both create complex orchestrations. An orchestration is a collection of functions or steps, that are executed to accomplish a complex task. With Azure **Functions, you write code to complete each step, with Logic Apps, you use a GUI to define** the actions and how they relate to one another.

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

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

Benefits of using Azure to store data

Here are some of the important benefits of Azure data storage:

- Automated backup and recovery: mitigates the risk of losing your data if there is any unforeseen failure or interruption.
- Replication across the globe: copies your data to protect it against any planned or unplanned events, such as scheduled maintenance or hardware failures. You can choose to replicate your data at multiple locations across the globe.
- Support for data analytics: supports performing analytics on your data consumption.
- Encryption capabilities: data is encrypted to make it highly secure; you also have tight control over who can access the data.
- Multiple data types: Azure can store almost any type of data you need. It can handle video files, text files, and even large binary files like virtual hard disks. It also has many options for your relational and NoSQL data.
- Data storage in virtual disks: Azure also has the capability of storing up to 8 TB of data in its virtual disks. This is a significant capability when you're storing heavy data such as videos and simulations.
- Storage tiers: storage tiers to prioritize access to data based on frequently used versus rarely used information.

Types of data

There are three primary types of data that Azure Storage is designed to hold.

1.Structured data. Structured data is data that adheres to a schema, so all of 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 referred to as *relational data*, as the data's schema defines the table of data, the fields in the table, and the clear relationship between the two.

Structured data is straightforward in that it's easy to enter, query, and analyze. All of the data follows the same format. Examples of structured data include sensor data or financial data.

2.Semi-structured data. Semi-structured data doesn't fit neatly into tables, rows, and columns. Instead, semi-structured data **uses tags or keys** that organize and provide a hierarchy for the data. Semi-structured data is also referred to as *non-relational* or *NoSQL* data.

3.Unstructured data. Unstructured data encompasses data that has **no designated structure** to it. This also means that there are no restrictions on the kinds of data it can hold. For example, a blob can hold a PDF document, a JPG image, a JSON file, video content, etc. As such, unstructured data is becoming more prominent as businesses try to tap into new data sources.

- Azure SQL Database
- Azure Cosmos DB
- Azure Blob storage
- Azure Data Lake Storage Gen2
- Azure Files
- Azure Queue
- Disk Storage

Storage tiers

Azure offers three storage tiers for blob object storage:

- Hot storage tier: optimized for storing data that is accessed frequently.
- Cool storage tier: optimized for data that is infrequently accessed and stored for at least 30 days.
- Archive storage tier: for data that is rarely accessed and stored for at least 180 days with flexible latency requirements.

Encryption for storage services

The following encryption types are available for your resources:

1. **Azure Storage Service Encryption (SSE) for data at rest** helps you secure your data to meet the organization's security and regulatory compliance. It encrypts the data before storing it and decrypts the data before retrieving it. The encryption and decryption are transparent to the user.
2. **Client-side encryption is where the data is already encrypted** by the client libraries. Azure stores the data in the encrypted state at rest, which is then decrypted during retrieval.

Azure Cosmos DB is a globally distributed database service. It supports schema-less data that lets you build highly responsive and Always On applications to support constantly changing data

Azure Blob Storage is *unstructured*, meaning that there are no restrictions on the kinds of data it can hold

The Data Lake feature allows you to perform analytics on your data usage and prepare reports. Data Lake is a large repository that stores both structured and unstructured data

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

Azure Queue storage is a service for storing large numbers of messages that can be accessed from anywhere in the world.

You can use queue storage to:

- Create a backlog of work and to pass messages between different Azure web servers.
- Distribute load among different web servers/infrastructure and to manage bursts of traffic.
- Build resilience against component failure when multiple users access your data at the same time.

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. 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.

Comparison between Azure data storage and on-premises storage

Cost effectiveness

An on-premises storage solution requires dedicated hardware that needs to be purchased, installed, configured, and maintained. This can be a significant up-front expense (or capital cost)

Azure data storage provides a pay-as-you-go pricing model which is often appealing to businesses as an operating expense instead of an upfront capital cost. It's also scalable, allowing you to scale up or scale out as demand dictates and scale back when demand is low. You are charged for data services only as you need them.

Reliability

On-premises storage requires data backup, load balancing, and disaster recovery strategies. These can be challenging and expensive as they often each need dedicated servers requiring a significant investment in both hardware and IT resources.

Azure data storage provides data backup, load balancing, disaster recovery, and data replication as services to ensure data safety and high availability.

Storage types

Sometimes multiple different storage types are required for a solution, such as file and database storage. An on-premises approach often requires numerous servers and administrative tools for each storage type.









Azure data storage provides a variety of different storage options including distributed access and tiered storage. This makes it possible to integrate a combination of storage technologies providing the best storage choice for each part of your solution.

Agility

Requirements and technologies change. For an on-premises deployment this may mean provisioning and deploying new servers and infrastructure pieces, which is a time consuming and expensive activity.

Azure data storage gives you the flexibility to create new services in minutes. This flexibility allows you to change storage back-ends quickly without needing a significant hardware investment.

The following illustration shows differences between on-premises storage and Azure data storage.

Needs	On-premise	Azure Data Storage
 Compliance and Security	1 Dedicated servers required for privacy and security	Client side encryption and encryption at rest
 Store structured and unstructured data	2 Additional IT resources with dedicated servers required	Azure Data Lake and portal analyzes and manages all types of data
 Replication and High Availability	3 More resources, licensing, and servers required	Built-in replication and redundancy features available
 Application sharing and access to shared resources	4 File sharing requires additional administration resources	File sharing options available without additional license
 Relational Data storage	5 Needs a database server with database admin role	Offers Database-as-a-Service option
 Distributed storage and data access	6 Expensive storage, networking, and compute resources needed	Azure Cosmos DB provides price-winning distributed access
 Messaging and load balancing	7 Hardware redundancy impacts budget and resources	Azure Queue provides effective load balancing
 Tiered storage	8 Management of tiered storage needs technology and labor skillset	Azure offers automated tiered storage of data

An architectural pattern that can be used to build loosely coupled systems is *N-tier*. An **N-tier architecture** divides an application into two or more logical tiers. Architecturally, a higher tier can access services from a lower tier, but a lower tier should never access a higher tier. Tiers help separate concerns and are ideally designed to be reusable. Using a tiered architecture also simplifies maintenance. Tiers can be updated or replaced independently, and new tiers can be inserted if needed.

What's an Azure region?

A *region* is one or more Azure data centers within a specific geographic location. East US, West US, and North Europe are examples of regions

A **virtual network** is a logically isolated network on Azure. Azure virtual networks will be familiar to you if you've set up networks on Hyper-V, VMware, or even on other public clouds. A virtual network allows Azure resources 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 together using **virtual network peering**.

Virtual networks can be segmented into one or more **subnets**. Subnets help you organize and secure your resources in discrete sections. VM has a public IP address along with a private IP address.

A **VPN gateway** (or virtual network gateway). It can provide a secure connection between an Azure Virtual Network and an on-premises location over the internet.

Azure manages the physical hardware for you. You configure virtual networks and gateways through software, which enables you to treat a virtual network just like your own network.

You choose which networks your virtual network can reach, whether that's the public internet or other networks in the private IP address space.

A **network security group**, or NSG, allows or denies inbound network traffic to your Azure resources. Think of a network security group as a cloud-level firewall for your network.

Availability refers to how long your service is up and running without interruption. **High availability, or highly available, refers to a service that's up and running for a long period of time.**

Resiliency refers to a system's ability to stay operational during abnormal conditions.

These conditions include:

- Natural disasters
- System maintenance, both planned and unplanned, including software updates and security patches.
- Spikes in traffic to your site
- Threats made by malicious parties, such as distributed denial of service, or DDoS, attacks

A **load balancer** distributes traffic evenly among each system in a pool. A load balancer can help you achieve both high availability and resiliency.

Azure Load Balancer is a load balancer service that Microsoft provides. 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.

Application Gateway is a load balancer designed for web applications. It uses Azure Load Balancer at the transport level (TCP) and applies sophisticated URL-based routing rules to support several advanced scenarios. This type of routing is known as application layer (OSI layer 7) load balancing since it understands the structure of the HTTP message.

Benefits; cookie affinity, SSL termination, web application firewall (WAF), URL-based routes, rewrites HTTP headers

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.

DNS, or Domain Name System, is a way to map user-friendly names to their IP addresses. You can think of DNS as the phonebook of the internet.

Latency refers to the time it takes for data to travel over the network. Latency is typically measured in milliseconds.

Compare latency to bandwidth. **Bandwidth** refers to the amount of data that can fit on the connection. Latency refers to the time it takes for that data to reach its destination.

Azure Traffic Manager. Traffic Manager uses the DNS server that's closest to the user to direct user traffic to a globally distributed endpoint.

Traffic Manager doesn't see the traffic that's passed between the client and server. Rather, it directs the client web browser to a preferred endpoint. Traffic Manager can route traffic in a few different ways, such as to the endpoint with the lowest latency.

Azure Load Balancer distributes traffic within the same region to make your services more highly available and resilient. Traffic Manager works at the DNS level, and directs the client to a preferred endpoint. This endpoint can be to the region that's closest to your user.

(performance, round robin, failover)

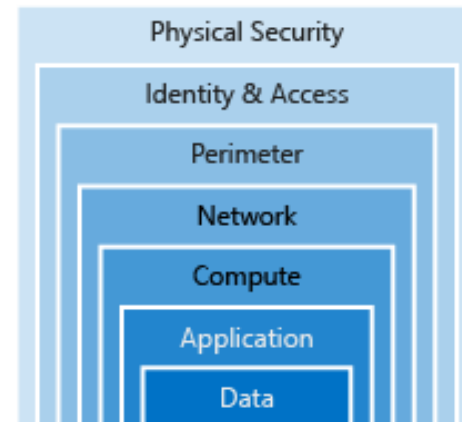
Load Balancer and Traffic Manager both help make your services more resilient, but in slightly different ways. When Load Balancer detects an unresponsive VM, it directs traffic to other VMs in the pool. Traffic Manager monitors the health of your endpoints. In contrast, when Traffic Manager finds an unresponsive endpoint, it directs traffic to the next closest endpoint that is responsive.

Responsibility	On-prem	IaaS	PaaS	SaaS
Data governance & rights management	Customer	Customer	Customer	Customer
Client endpoints	Customer	Customer	Customer	Customer
Account & access management	Customer	Customer	Customer	Customer
Identity & directory infrastructure	Customer	Customer	Microsoft	Microsoft
Application	Customer	Customer	Microsoft	Microsoft
Network controls	Customer	Customer	Microsoft	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

Microsoft
Customer

Defense in depth is a strategy that employs a series of mechanisms to slow the advance of an attack aimed at acquiring unauthorized access to information. Each **layer** provides protection so that if one layer is breached, a subsequent layer is already in place to prevent further exposure. Microsoft applies a layered approach to security, both in physical data centers and across Azure services. The objective of defense in depth is to protect and prevent information from being stolen by individuals who are not authorized to access it.

Defense in depth can be visualized as a set of concentric rings, with the data to be secured at the center. Each ring adds an additional layer of security around the data. This approach removes reliance on any single layer of protection and acts to slow down an attack and provide alert telemetry that can be acted upon, either automatically or manually.



Data

In almost all cases, attackers are after data:

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

It's the responsibility of those storing and controlling access to data to ensure that it's properly secured.

Application

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

Integrating security into the application development life cycle will help reduce the number of vulnerabilities introduced in code

Compute

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

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

Networking

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

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

Perimeter

Use distributed denial of service (DDoS) protection to filter large-scale attacks before they can cause a denial of service for end users.

Use perimeter firewalls to identify and alert on malicious attacks against your network.

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

Identity and access

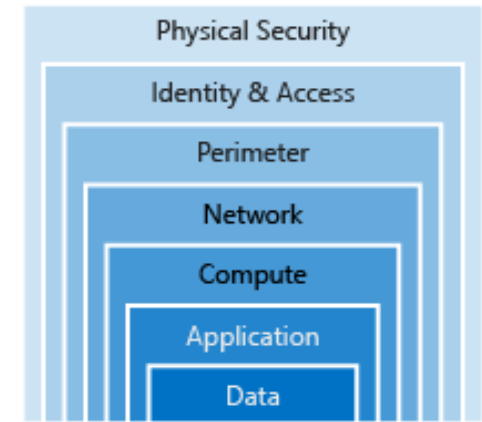
- Control access to infrastructure and change control.
- Use single sign-on and multi-factor authentication.
- Audit events and changes.

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

Physical security

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

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



Azure Security Center. 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 are allowed to execute.
- Analyze and identify potential inbound attacks, and help to investigate threats and any post-breach activity that might have occurred.
- Provide just-in-time access control for ports, reducing your attack surface by ensuring the network only allows traffic that you require.

Azure Security Center is part of the [Center for Internet Security \(CIS\) recommendations](#).

Azure Security Center is available in two tiers:

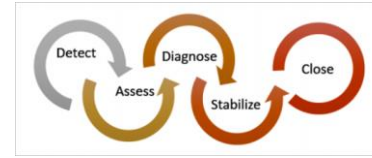
Free. Available as part of your Azure subscription, this tier is limited to assessments and recommendations of Azure resources only.

Standard. This tier provides a full suite of security-related services including continuous monitoring, threat detection, just-in-time access control for ports, and more.

- 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 are allowed to 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.

Use Security Center for incident response.

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



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

Detect. Review the first indication of an event investigation. For example, you can 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.

Use Security Center recommendations to enhance security.

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

Authentication and authorization

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

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 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.

Azure AD is a cloud-based identity service. It has built in support for synchronizing with your existing on-premises Active Directory or can be used stand-alone. This means that all your applications, whether on-premises, in the cloud (including Office 365), or even mobile can share the same credentials. Administrators and developers can control access to internal and external data and applications using centralized rules and policies configured in Azure AD.

Azure AD provides services such as:

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

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.

Azure AD functions

Category	description
Application management	Manage your cloud and on-premises apps using Application Proxy, single sign-on, the My Apps portal (also known as the Access panel), and Software as a Service (SaaS) apps.
Authentication	Manage Azure Active Directory self-service password reset, Multi-Factor Authentication, custom banned password list, and smart lockout, SSO.
Business-to-Business (B2B)	Manage your guest users and external partners, while maintaining control over your own corporate data, identity services
Business-to-Customer (B2C)	Customize and control how users sign up, sign in, and manage their profiles when using your apps, identity services
Conditional access	Manage access to your cloud apps.
Azure Active Directory for developers	Build apps that sign in all Microsoft identities, get tokens to call Microsoft Graph, other Microsoft APIs, or custom APIs.
Device Management	Manage how your cloud or on-premises devices access your corporate data
Domain services	Join Azure virtual machines to a domain without using domain controllers
Enterprise users	Manage license assignment, access to apps, and set up delegates using groups and administrator roles.
Hybrid identity	Use Azure Active Directory Connect and Connect Health to provide a single user identity for authentication and authorization to all resources, regardless of location (cloud or on-premises).
Identity governance	Manage your organization's identity through employee, business partner, vendor, service, and app access controls. You can also perform access reviews
Identity protection	Detect potential vulnerabilities affecting your organization's identities, configure policies to respond to suspicious actions, and then take appropriate action to resolve them
Managed identities for Azure resources	Provides your Azure services with an automatically managed identity in Azure AD that can authenticate any Azure AD-supported authentication service, including Key Vault
Privileged identity management (PIM)	Manage, control, and monitor access within your organization. This feature includes access to resources in Azure AD and Azure, and other Microsoft Online Services, like Office 365 or Intune.
Reports and monitoring	Gain insights into the security and usage patterns in your environment.

Multi-factor authentication (MFA) provides additional security for your identities by requiring two or more elements for full authentication. These elements fall into three categories:

- Something you know
- Something you possess
- Something you are

MFA comes as part of the following Azure service offerings:

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

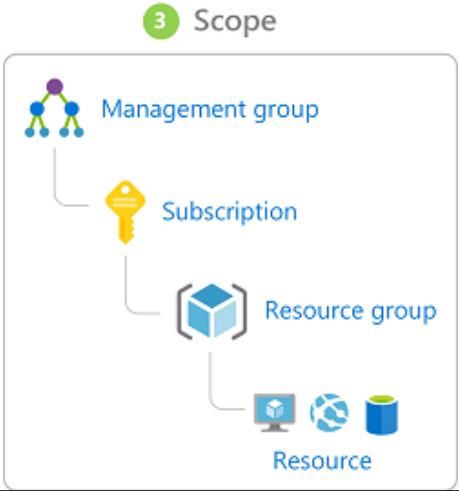
An **identity** is just a thing that can be authenticated. Obviously, this includes users with a user name and password, but it can also include applications or other servers, which might authenticate with secret keys or certificates. As a bonus definition, an account is data associated with an identity.

A **principal** is an identity acting with certain roles or claims. Usually, it is not useful to consider identity and principal separately, but think of using sudo on a Bash prompt in Linux or on Windows using "run as Administrator." In both those cases, you are still logged in as the same identity as before, but you've changed the role under which you are executing. Groups are often also considered principals because they can have rights assigned.




A service principal is an identity that is used by a service or application. And like other identities, it can be assigned roles.

Managed identities for Azure services

The creation of service principals can be a tedious process, and there are a lot of touch points that can make maintaining them difficult. Managed identities for Azure services are much easier and will do most of the work for you.



Roles are sets of permissions, like "Reader", "Owner" or "Contributor", that users can be granted to access an Azure service instance. Identities are mapped to roles directly or through group membership. Separating security principals, access permissions, and resources provides simple access management and fine-grained control. Administrators are able to ensure the minimum necessary permissions are granted. Roles can be granted at the individual service instance level, but they also flow down the Azure Resource Manager hierarchy. Here's a diagram that shows this relationship. Roles assigned at a higher scope, like an entire subscription, are inherited by child scopes, like service instances.

	Role			
	Reader	Resource-specific or custom role	Contributor	Owner
Scope	 Subscription	Observers		Admins
	 Resource group	Users managing resources		
	 Resource	Automated processes		

In addition to managing Azure resource access with role-based access control (RBAC), a comprehensive approach to infrastructure protection should consider including the ongoing auditing of role members as their organization changes and evolves. **Azure AD Privileged Identity Management (PIM)** is an additional, paid-for offering that provides oversight of role assignments, self-service, and just-in-time role activation and Azure AD and Azure resource access reviews.

Overview

Quick start

TASKS

My roles

My requests

Approve requests

Review access

MANAGE

Roles

Members

Alerts

Access reviews

Wizard

Settings

ACTIVITY

Directory roles audit history

My audit history

TROUBLESHOOTING + SUPPORT

Troubleshoot

New support request

Refresh

Admin viewMy view

Directory activation history for the past 7 days

SECURITY AD...

PRIVILEGED ...

GLOBAL AD...

4

3

2

1

0

2 PM

DIRECTORY ACTIVATIONS...

6

Notifications

There are too many global administrators

Alerts

Request on: Security Administrator , Action: Activate, Time: 8/21/2018, 2:00:00 PM

Audits

Directory users distribution

6Users

ELIGIBLE

PERMANENT

ACTIVE

Directory roles distribution

6Users

SECURITY ADMI...

GLOBAL ADMINI...

PRIVILEGED ROL...

Directory roles

ROLE NAME	MFA ENABLED	MEMBERS	ACTIVE	ELIGIBLE
Global Administrator	Yes	4	4 (100%)	0 (0%)
Privileged Role Administrator	Yes	1	1 (100%)	0 (0%)
Security Administrator	Yes	1	1 (100%)	0 (0%)

What is encryption?

Encryption is the process of making data unreadable and unusable to unauthorized viewers. To use or read the encrypted data, it must be *decrypted*, which requires the use of a secret key. There are two top-level types of encryption: symmetric and asymmetric.

Symmetric encryption uses the same key to encrypt and decrypt the data. Consider a desktop password manager application. You enter your passwords and they are encrypted with your own personal key (your key is often derived from your master password). When the data needs to be retrieved, the same key is used, and the data is decrypted.

Asymmetric encryption uses a public key and private key pair. Either key can encrypt but a single key can't decrypt its own encrypted data. To decrypt, you need the paired key. Asymmetric encryption is used for things like Transport Layer Security (TLS) (used in HTTPS) and data signing.

Both symmetric and asymmetric encryption play a role in properly securing your data. Encryption is typically approached in two ways:

Encryption at rest

Encryption in transit

Encrypt raw storage

Azure Storage Service Encryption for data at rest helps you protect your data to meet your organizational security and compliance commitments. With this feature, the Azure storage platform automatically encrypts your data before persisting it to Azure Managed Disks, Azure Blob storage, Azure Files, or Azure Queue storage, and decrypts the data before retrieval. The handling of encryption, encryption at rest, decryption, and key management in Storage Service Encryption is transparent to applications using the services.

Encrypt virtual machine disks

Storage Service Encryption provides low-level encryption protection for data written to physical disk, but how do you protect the virtual hard disks (VHDs) of virtual machines? If malicious attackers gained access to your Azure subscription and got the VHDs of your virtual machines, how would you ensure they would be unable to access the stored data?

Encrypt databases

Transparent data encryption (TDE) helps protect Azure SQL Database and Azure Data Warehouse against the threat of malicious activity. It performs real-time encryption and decryption of the database, associated backups, and transaction log files at rest without requiring changes to the application. By default, TDE is enabled for all newly deployed Azure SQL Database instances.

Encrypt secrets

We've seen that the encryption services all use keys to encrypt and decrypt data, so how do we ensure that the keys themselves are secure? Corporations may also have passwords, connection strings, or other sensitive pieces of information that they need to securely store. In Azure, we can use **Azure Key Vault** to protect our secrets.

Azure Key Vault is a centralized cloud service for storing your application 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. It is useful for a variety of scenarios:

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

The benefits of using Key Vault include:

- *Centralized application secrets.* Centralizing storage for application secrets allows you to control their distribution, and reduces the chances that secrets may be accidentally leaked.
- *Securely stored secrets and keys.* Azure uses industry-standard algorithms, key lengths, and HSMs, and access requires proper authentication and authorization.
- *Monitor access and use.* Using Key Vault, you can monitor and control access to company secrets.
- *Simplified administration of application secrets.* Key Vault makes it easier to enroll and renew certificates from public Certificate Authorities (CAs). You can also scale up and replicate content within regions, and use standard certificate management tools.
- *Integrate with other Azure services.* You can integrate Key Vault with storage accounts, container registries, event hubs and many more Azure services.

Because Azure AD identities can be granted access to use Azure Key Vault secrets, applications with managed service identities enabled can automatically and seamlessly acquire the secrets they need.

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

To provide inbound protection at the perimeter, you have several choices.

- 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. Azure Firewall provides inbound protection for non-HTTP/S protocols. Examples of non-HTTP/S protocols include: Remote Desktop Protocol (RDP), Secure Shell (SSH), and File Transfer Protocol (FTP). It also provides outbound, network-level protection for all ports and protocols, and application-level protection for outbound HTTP/S.
- Azure Application Gateway is a load balancer that includes a Web Application Firewall (WAF) that provides protection from common, known vulnerabilities in websites. It is specifically **designed to protect HTTP traffic**.
- Network virtual appliances (NVAs) are ideal options for **non-HTTP services or advanced configurations**, and are similar to hardware firewall appliances.

Azure Firewall provides many features, including:

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

Centrally create, enforce and log applications and network connectivity policies across subscriptions and virtual networks

Ddos

Any resource exposed on the internet is at risk of being attacked by a denial of service attack. These types of attacks attempt to overwhelm a network resource by sending so many requests that the resource becomes slow or unresponsive.

When you combine Azure DDoS Protection with application design best practices, you help provide defense against DDoS attacks. DDoS Protection leverages the scale and elasticity of Microsoft's global network to bring DDoS mitigation capacity to every Azure region

Azure DDoS Protection provides the following service tiers:

- Basic. The Basic service tier is automatically enabled as part of the Azure platform. Always-on traffic monitoring and real-time mitigation of common network-level attacks provide the same defenses that Microsoft's online services use. Azure's global network is used to distribute and mitigate attack traffic across regions.
- Standard. The Standard service tier provides additional mitigation capabilities that are tuned specifically to Microsoft Azure Virtual Network resources. DDoS Protection Standard is simple to enable and requires no application changes. Protection policies are tuned through dedicated traffic monitoring and machine learning algorithms. Policies are applied to public IP addresses which are associated with resources deployed in virtual networks, such as Azure Load Balancer and Application Gateway. DDoS standard protection can mitigate the following types of attacks:
 - Volumetric attacks. The attackers goal is to flood the network layer with a substantial amount of seemingly legitimate traffic.
 - Protocol attacks. These attacks render a target inaccessible, by exploiting a weakness in the layer 3 and layer 4 protocol stack.
 - Resource (application) layer attacks. These attacks target web application packets to disrupt the transmission of data between hosts.

Virtual network security

Once inside a virtual network (VNet), it's crucial that you limit communication between resources to only what is required.

For communication between virtual machines, **Network Security Groups (NSGs)** are a critical piece to restrict unnecessary communication.

Network Security Groups 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. They provide a list of allowed and denied communication to and from network interfaces and subnets, and are fully customizable.

You can completely remove public internet access to your services by restricting access to service endpoints. With service endpoints, Azure service access can be limited to your virtual network.

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

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

Virtual private network (VPN) connections are a common way of establishing secure communication channels between networks. Connection between Azure Virtual Network and an on-premises VPN device is a great way to provide secure communication between your network and your VNet on Azure.

Microsoft **Azure Information Protection (MSIP or sometimes referred to as AIP)** is a cloud-based solution that helps organizations classify and optionally protect documents and emails by applying labels.

Labels can be applied automatically based on rules and conditions, manually, or a combination of both where users are guided by recommendations.

What is the difference between Network Security Groups (NSGs) and Azure Firewall?

The **Azure Firewall** service complements network security group functionality. Together, they provide better "defense-in-depth" network security. **Network security groups provide distributed network layer traffic filtering to limit traffic to resources within virtual networks in each subscription. Azure Firewall is a fully stateful, centralized network firewall as-a-service, which provides network- and application-level protection across different subscriptions and virtual networks.**

If you need basic network level access control (based on IP address and the TCP or UDP protocols), you can use **Network Security Groups (NSGs)**. An **NSG is a basic, stateful, packet filtering firewall, and it enables you to control access based on a 5-tuple. NSGs include functionality to simplify management and reduce the chances of configuration mistakes:**

Augmented security rules simplify NSG rule definition and allow you to create complex rules rather than having to create multiple simple rules to achieve the same result.

Service tags are Microsoft created labels that represent a group of IP addresses. They update dynamically to include IP ranges that meet the conditions that define inclusion in the label. For example, if you want to create a rule that applies to all Azure storage on the east region you can use Storage.EastUS

Application security groups allow you to deploy resources to application groups and control the access to those resources by creating rules that use those application groups. For example, if you have web servers deployed to the 'Web servers' application group you can create a rule that applies a NSG allowing 443 traffic from the Internet to all systems in the 'Web servers' application group.

NSGs do not provide application layer inspection or authenticated access controls.

5-tuple

- Source IP address
- Source IP port number
- Destination IP address
- Destination Address port
 - protocol

ATP

Azure Advanced Threat Protection (Azure ATP) is a cloud-based security solution that identifies, detects, and helps you investigate advanced threats, compromised identities, and malicious insider actions directed at your organization.

Azure ATP is capable of detecting known malicious attacks and techniques, security issues, and risks against your network.

Azure ATP consists of several components.

- Azure ATP portal
- Azure ATP has its own portal, through which you can monitor and respond to suspicious activity. The Azure ATP portal allows you to create your Azure ATP instance, and view the data received from Azure ATP sensors. You can also use the portal to monitor, manage, and investigate threats in your network environment. You can sign in to the Azure ATP portal at <https://portal.atp.azure.com>. You must sign in with a user account that is assigned to an Azure AD security group that has access to the Azure ATP portal.
- Azure ATP sensor
- Azure ATP sensors are installed directly on your domain controllers. The sensor monitors domain controller traffic without requiring a dedicated server or configuring port mirroring.
- Azure ATP cloud service
- Azure ATP cloud service runs on Azure infrastructure and is currently deployed in the United States, Europe, and Asia. Azure ATP cloud service is connected to Microsoft's intelligent security graph.

Azure Policy is a service in Azure that you use to define, assign, and, manage standards for resources in your environment. It can prevent the creation of disallowed resources, ensure new resources have specific settings applied, and run evaluations of your existing resources to scan for non-compliance.

Azure Policy comes with many built-in policy and initiative definitions that you can use, under categories such as Storage, Networking, Compute, Security Center, and Monitoring

The process of creating and implementing an Azure Policy begins with creating a *policy definition*. Every policy definition has conditions under which it is enforced. And, it has an accompanying effect that takes place if the conditions are met. To apply a policy, you will:

1. **Create a policy definition**
2. **Assign a definition to a scope of resources**
3. **View policy evaluation results**

A *policy definition* expresses what to evaluate and what action to take.

The policy definition itself is represented as a JSON file - you can use one of the pre-defined definitions in the portal or create your own

Once you've defined one or more policy definitions, you'll need to assign them. A *policy assignment* is a policy definition that has been assigned to take place within a specific scope.

Policy definition	Description
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 this 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.
Not allowed resource types	Prevents a list of resource types from being deployed.

Policy Effect	What happens?
Deny	The resource creation/update fails due to policy.
Disabled	The policy rule is ignored (disabled). Often used for testing.
Append	Adds additional parameters/fields to the requested resource during creation or update. A common example is adding tags on resources such as Cost Center or specifying allowed IPs for a storage resource.
Audit, AuditIfNotExists	Creates a warning event in the activity log when evaluating a non-compliant resource, but it doesn't stop the request.
DeployIfNotExists	Executes a template deployment when a specific condition is met. For example, if SQL encryption is enabled on a database, then it can run a template after the DB is created to set it up a specific way.

Managing a few policy definitions is easy, but once you have more than a few, you will want to organize them. That's where *initiatives* come in.

Initiatives work alongside policies in Azure Policy. An ***initiative definition*** is a set or group of policy definitions to help track your compliance state for a larger goal. Even if you have a single policy, we recommend using initiatives if you anticipate increasing the number of policies over time.

Initiative definitions simplify the process of managing and assigning policy definitions by grouping a set of policies into a single item. 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:

Policy definition	Purpose
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

Azure Management Groups are containers for managing access, policies, and compliance across multiple Azure subscriptions. Management groups allow you to order your Azure resources hierarchically into collections, which provide a further level of classification that is above the level of subscriptions. All subscriptions within a management group automatically inherit the conditions applied to the management group. Management groups give you enterprise-grade management at a large scale no matter what type of subscriptions you might have.

Azure management group operate at the level of scope that is above subscription

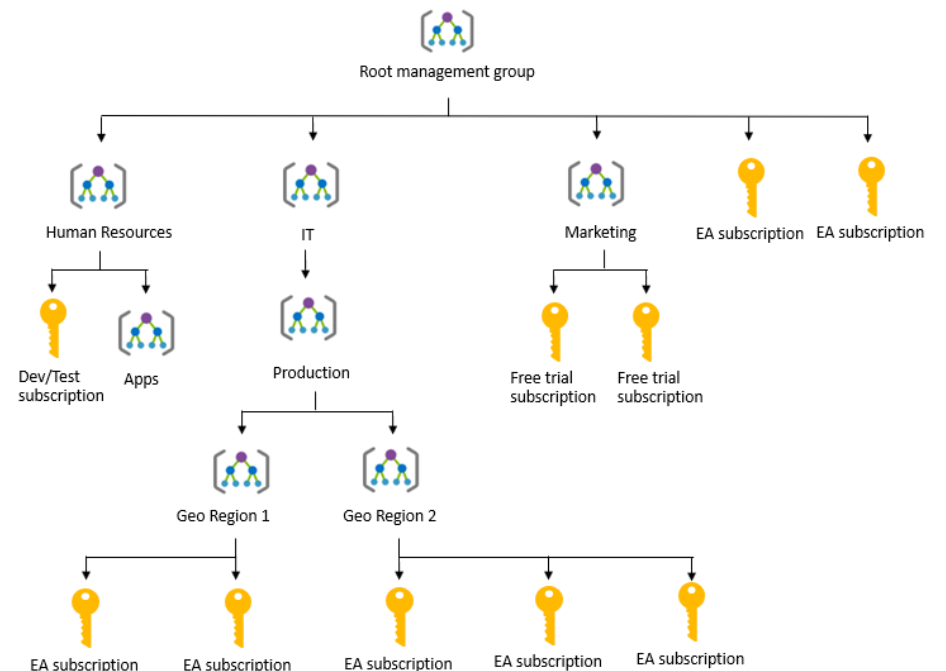
Azure Blueprint allows you to define a repeatable set of Azure resources that implement and adhere to your organization's standards, patterns, and requirements. Blueprint enables development teams to rapidly build and deploy new environments with the knowledge that they're building within organizational 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:

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

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



Governing your own resources and how they are used is only part of the solution when using a cloud provider. You also have to understand how the *provider* manages the underlying resources you are building on.

Microsoft takes this management very seriously and provides full transparency with four sources:

1. Microsoft Privacy Statement
2. Microsoft Trust Center
3. Service Trust Portal
4. Compliance Manager

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

The statement applies to the interactions Microsoft has with you and Microsoft products such as Microsoft services, websites, apps, software, servers, and devices. It is intended to provide openness and honesty about how Microsoft deals with personal data in its products and services.

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 including:

- 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.

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

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

- ISO
- SOC
- NIST
- FedRAMP
- GDPR

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

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

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 Office 365, Dynamics 365, and Azure.

Compliance Manager provides the following features:

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

Compliance Manager provides ongoing risk assessments with a risk-based scores reference displayed in a dashboard view for regulations and standards.

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

Important

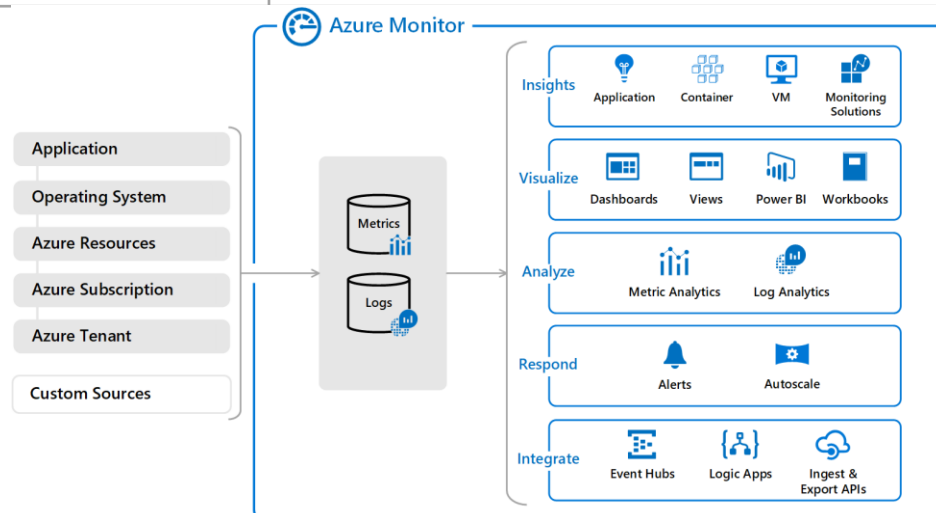
Compliance Manager is a dashboard that provides a summary of your data protection and compliance stature and recommendations for improvement. The Customer Actions provided in Compliance Manager are recommendations only

Defining policy and access provides fine-grained control over resources in your cloud IT infrastructure. Once those resources are deployed, you will want to know about any issues or performance problems they might encounter. Azure provides two primary services to monitor the health of your apps and resources.

- Azure Monitor
- Azure Service Health

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.

Data tier	Description
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.



As soon as you create an Azure subscription and start adding resources such as virtual machines and web apps, Azure Monitor starts collecting data. *Activity Logs* record when resources are created or modified and *Metrics* tell you how the resource is performing and the resources that it's consuming.

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

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

- Dashboards
- Views
- Power B

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.

Azure Service Health is composed of the following views.

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

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

Providing up to date status information about the health of azure services is done via Azure service Health

Resource groups are a fundamental element of the Azure platform. **A resource group is a logical container for resources deployed on Azure.** These resources are anything you create in an Azure subscription like virtual machines, Application Gateways, and CosmosDB instances. All resources must be in a resource group and a resource can only be a member of a single resource group. Resources can be moved between resource groups at any time. Resource groups can't be nested. Before any resource can be provisioned, you need a resource group for it to be placed in. If you delete a resource group, all resources contained within are also deleted. Resource groups are also a scope for applying role-based access control (RBAC) permissions. By applying RBAC permissions to a resource group, you can ease administration and limit access to allow only what is needed.

Resource groups can be created by using the following methods:

Azure portal

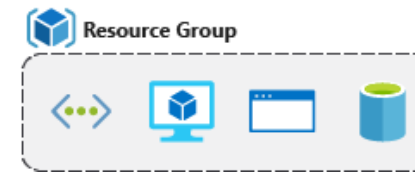
Azure PowerShell

Azure CLI

Templates

Azure SDKs (like .NET, Java)

Resource groups can be organized in a number of ways. There are a few factors that can play into the strategy you use to organize resources: **authorization, resource life cycle, and billing.**



Tags are **name/value pairs of text data that you can apply to resources and resource groups.** Tags allow you to associate custom details about your resource, in addition to the standard Azure properties a resource has:

- department (like finance, marketing, and more)
- environment (prod, test, dev),
- cost center
- life cycle and automation (like shutdown and startup of virtual machines).

A resource can have **up to 15 tags**. The **name** is **limited to 512 characters for all types of resources except storage accounts, which have a limit of 128 characters.** The tag **value is limited to 256 characters** for all types of resources. **Tags aren't inherited from parent resources.** Not all resource types support tags, and tags can't be applied to classic resources. **Not all resource types support tag.** Tags can be added and manipulated through the **Azure portal, Azure CLI, Azure PowerShell, Resource Manager templates, and through the REST API.**

RBAC uses an allow model for access. When you are assigned to a role, RBAC *allows* you to perform specific 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.

Here are some best practices you should use when setting up resources.

- Segregate duties within your team and grant only the amount of access to users that they need to perform their jobs. Instead of giving everybody unrestricted permissions in your Azure subscription or resources, allow only specific actions at a particular scope.
- When planning your access control strategy, grant users the lowest privilege level that they need to do their work.
- Use Resource Locks to ensure critical resources aren't modified or deleted (more on that next!)

Resource locks are a setting that can **be applied to any resource to block modification or deletion**. Resource locks can set to either **CanNotDelete or Read-only**. Delete will allow all operations against the resource but block the ability to delete it. Read-only will only allow read activities to be performed against it, blocking any modification or deletion of the resource. Resource locks can **be applied to subscriptions, resource groups, and to individual resources, and are inherited when applied at higher levels**.

There are three main customer types on which the available purchasing options for Azure products and services are contingent, including:

- Enterprise - Enterprise customers sign an Enterprise Agreement with Azure that commits them to spend a negotiated amount on Azure services, which they typically pay annually. Enterprise customers also have access to customized Azure pricing.
- Web direct - Direct Web customers pay general 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 occur through the customer's CSP.

When you provision an Azure resource, Azure creates **one or more meter instances for that resource**. The meters **track the resources' usage, and generate a usage record that is used to calculate your bill**.

For example, a single virtual machine that you provision in Azure might have the following meters tracking its usage:

- Compute Hours
- IP Address Hours
- Data Transfer In
- Data Transfer Out
- Standard Managed Disk
- Standard Managed Disk Operations
- Standard IO-Disk
- Standard IO-Block Blob Read
- Standard IO-Block Blob Write
- Standard IO-Block Blob Delete

The meters and pricing vary per product and often have different pricing tiers based on the **size or capacity of the resource**. **At** the end of each monthly billing cycle, the usage values will be charged to your payment method and the meters are reset.

Azure customer type determine the azure products and services that are available to you for purchasing

Factors affecting cost

Just like your on-premises equipment costs, there are several elements that will affect your monthly costs when using Azure services. A few of the primary factors including **resource type, services, the user's location, and the billing zone**.

Resource type

Costs are resource-specific, so the usage that a meter tracks and the number of meters associated with a resource depend on the resource type.

services

Azure usage rates and billing periods can differ between Enterprise, Web Direct, and Cloud Solution Provider (CSP) customers. Some subscription types also include usage allowances, which affect costs.

location

Azure has datacenters all over the world. Usage costs vary between locations that offer particular Azure products, services, and resources based on popularity, demand, and local infrastructure costs.

Billing zone

Bandwidth refers to data moving in and out of Azure datacenters. Most of the time inbound data transfers (data going *into* Azure datacenters) are free. For outbound data transfers (data going *out* of Azure datacenters), the data transfer pricing is based on Billing Zones.

A Zone is a geographical grouping of Azure Regions for billing purposes. The following zones exist and include the listed countries (regions) listed.

The charge per billable unit depend on;

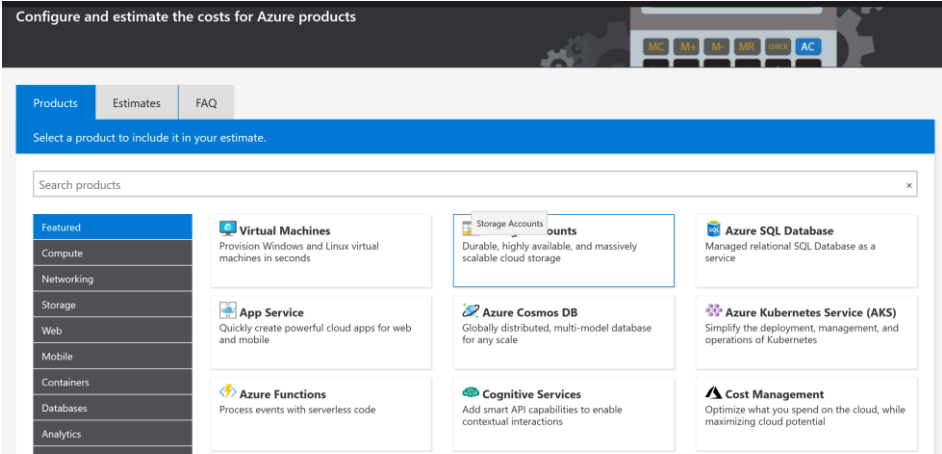
- Resource type
- location

Zone	Areas
Zone 1	United States, Europe, Canada, UK, France
Zone 2	Asia Pacific, Japan, Australia, India, Korea
Zone 3	Brazil
DE Zone 1	Germany

To make estimates easy for customers to create, Microsoft developed the **Azure pricing calculator**. The Azure pricing calculator is a free web-based tool that allows you to input Azure services and modify properties and options of the services. It outputs the costs per service and total cost for the full estimate.

The options that you can configure in the pricing calculator vary between products, but basic configuration options include:

Option	Description
Region	Lists the regions from which you can provision a product. Southeast Asia, central Canada, the western United States, and Northern Europe are among the possible regions available for some resources.
Tier	Sets the type of tier you wish to allocate to a selected resource, such as Free Tier, Basic Tier, etc.
Billing Options	Highlights the billing options available to different types of customer and subscriptions for a chosen product.
Support Options	Allows you to pick from included or paid support pricing options for a selected product.
Programs and Offers	Allows you to choose from available price offerings according to your customer or subscription type.
Azure Dev/Test Pricing	Lists the available development and test prices for a product. Dev/Test pricing applies only when you run resources within an Azure subscription that is based on a Dev/Test offer.



We can **save** the estimate, so we can come back to it later and adjust it if necessary. We can **also export it to Excel** for further analysis or **share the estimate via a URL**.

To export the estimate, click Export at the bottom of the estimate. This will download your estimate in Excel (.xlsx) format and will include all the services you added to your estimate.

We can either share the Excel spreadsheet, or we can click on the Share button in the calculator. This gives you a URL that you can use to share this estimate. Anyone with this link will be able to access it, making it easy to share with your team.

If you are logged in with your Azure account, you can save the estimate, so you can come back to it later.

Azure Advisor is a **free service built into Azure** that **provides recommendations on high availability, security, performance, and cost**. Advisor analyzes your deployed services and looks for ways to improve your environment across those four areas. We'll focus on the cost recommendations, but you'll want to take some time to review the other recommendations as well. Advisor makes cost recommendations in the following areas:

1. Reduce costs by eliminating unprovisioned Azure ExpressRoute circuits. This identifies ExpressRoute circuits that have been in the provider status of *Not Provisioned* for more than one month and recommends deleting the circuit if you aren't planning to provision the circuit with your connectivity provider.
2. Buy reserved instances to save money over pay-as-you-go. This will review your virtual machine usage over the last 30 days and determine if you could save money in the future by purchasing reserved instances. Advisor will show you the regions and sizes where you potentially have the most savings and will show you the estimated savings you might achieve from purchasing reserved instances.
3. Right-size or shutdown underutilized virtual machines. This monitors your virtual machine usage for 14 days and then identifies underutilized virtual machines. Virtual machines whose average CPU utilization is 5 percent or less and network usage is 7 MB or less for four or more days are considered underutilized virtual machines. The average CPU utilization threshold is adjustable up to 20 percent. By identifying these virtual machines, you can decide to resize them to a smaller instance type, reducing your costs.

Microsoft Azure

Search resources, services, and docs

Home > Advisor recommendations

Advisor recommendations

Download as CSV Download as PDF Configure

Subscriptions: Production_subscription1

All types Active No grouping

Overview High Availability (4) Security (9) Performance (1) Cost (2) All (16)

High Availability

4 Recommendations

0 High impact 3 Medium impact 1 Low impact

11 Impacted resources

Security

9 Recommendations

9 High impact 0 Medium impact 0 Low impact

13 Impacted resources

Performance

1 Recommendation

0 High impact 0 Medium impact 1 Low impact

1 Impacted resource

Cost

1,087 USD savings/mo *

2 Recommendations

2 High impact 0 Medium impact 0 Low impact

15 Impacted resources

Tips & tricks

- You can customize Advisor to process recommendations for resources that matter to you the most.
- You can buy virtual machine reserved instances to save money over pay-as-you-go costs.
- You can enable virtual machine backup to protect your data from corruption or accidental deletion.

Download recommendations as PDF Download recommendations as CSV

Microsoft Azure

Search resources, services, and docs

Home > Advisor recommendations

Advisor recommendations

Download as CSV Download as PDF Configure

Subscriptions: Production_subscription1

All types Active No grouping

Overview High Availability (4) Security (9) Performance (1) Cost (2) All (16)

For more cost management and optimization capabilities, try Azure Cost Management →

Total recommendations
2

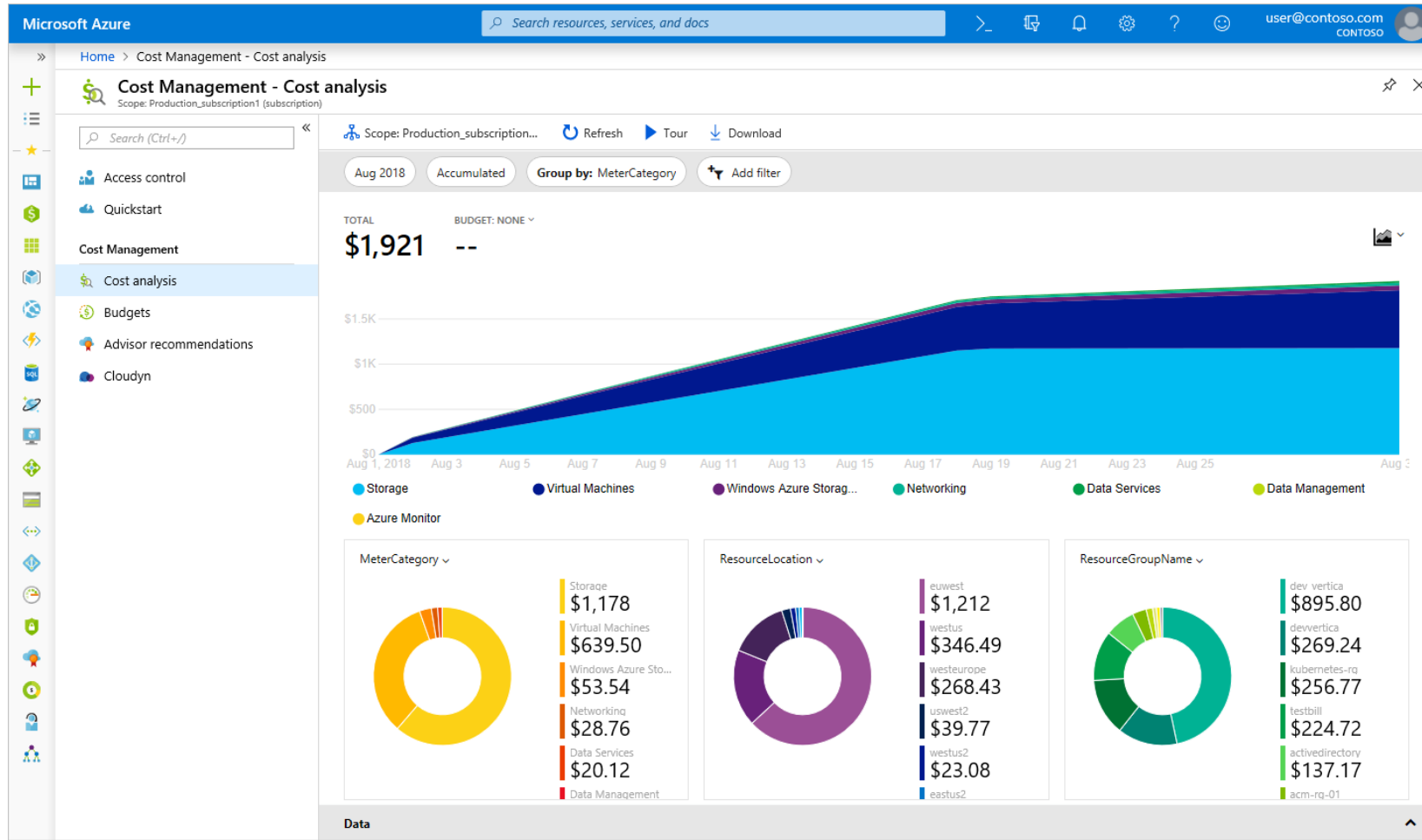
Recommendations by impact
High 2
Medium 0
Low 0

Impacted resources
15

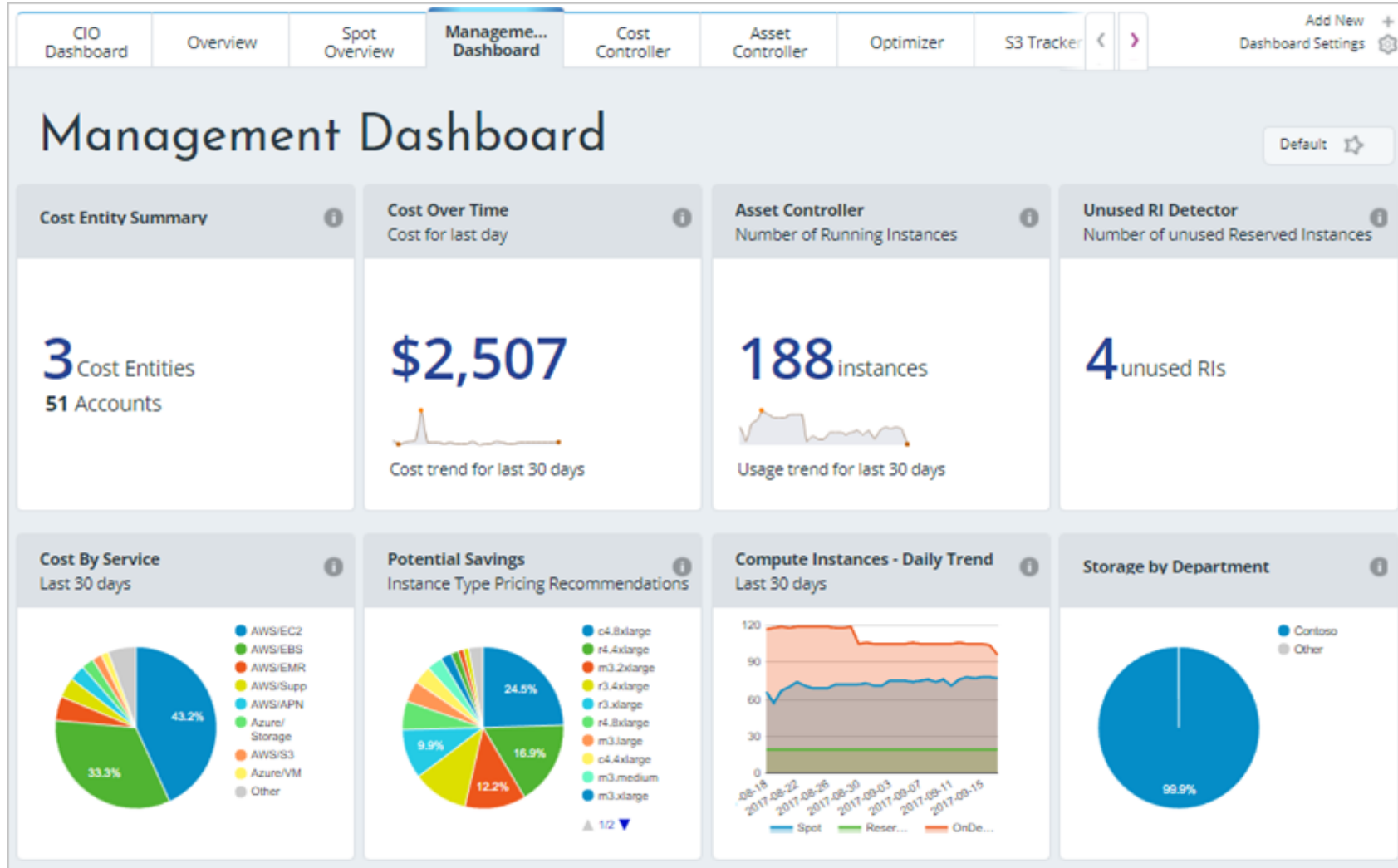
Potential monthly savings
1,087 USD

IMPACT	DESCRIPTION	POTENTIAL MONTHLY SAVINGS*	IMPACTED RESOURCES	UPDATED AT
High	Buy virtual machine reserved instances to save money over pay-as-you-go costs	384.94 USD	7 Virtual machines	9/5/2018 1:04:02 PM
High	Right-size or shutdown underutilized virtual machines	701.59 USD	8 Virtual machines	9/5/2018 1:01:58 PM

Azure Cost Management is another **free**, built-in Azure tool that can be used to gain greater insights into where your cloud money is going. You can see **historical breakdowns** of what services you are spending your money on and how it is tracking against budgets that you have set. You can **set budgets, schedule reports, and analyze your cost areas**



Cloudyn, a Microsoft subsidiary, **allows you to track cloud usage and expenditures for your Azure resources and other cloud providers including Amazon Web Services and Google.** Easy-to-understand dashboard reports help with **cost allocation and chargebacks.** Cost Management helps optimize your cloud spending by identifying underutilized resources that you can then manage and adjust. **Usage for Azure is free, and there are paid options for premium support and to view data from other clouds**



The pricing calculator and cost management advisor can help you predict and analyze your spend for new or existing services. If you are starting to migrate to the cloud, a useful tool you can use to predict your cost savings is the Total Cost of Ownership (TCO) calculator

Start by entering details about your on-premises infrastructure into the TCO calculator according to four groups:

Group	Description
Servers	Enter details of your current on-premises server infrastructure.
Databases	Enter details of your on-premises database infrastructure in the <i>Source</i> section. In the <i>Destination</i> section, select the corresponding Azure service you would like to use.
Storage	Enter the details of your on-premises storage infrastructure.
Networking	Enter the amount of network bandwidth you currently consume in your on-premises environment.

- 1 open TCO calculator

2 define workload

3 adjust assumptions

4 view report

Adjust the values of assumptions that the TCO calculator makes, which might vary between customers. To improve the accuracy of the TCO calculator, you should adjust the values, so they match the costs of your current on-premises infrastructure

Azure credits

Visual Studio subscribers can activate a monthly credit benefit which allows you to experiment with, develop, and test new solutions on Azure. Use Azure credits to try out new services such as App Service, Windows 10 VMs, Azure SQL Server databases, Containers, Cognitive Services, Functions, Data Lake, and more without incurring any monetary costs.

When you activate this benefit, you will own a separate Azure subscription under your account with a monthly credit balance that renews each month while you remain an active Visual Studio subscriber.

The credit amount varies based on the program level - \$50/month for VS Professional and \$150/month for Enterprise.

By default, Azure subscriptions which have associated monthly credits (which includes trial accounts) have a **spending limit** to ensure you aren't charged once you have used up your credits. This feature is useful for development teams exploring new solution architectures as it ensures you won't have an unexpectedly large bill at the end of the month.

If you have VM workloads that are static and predictable, particularly ones that run 24x7x365, using **reserved instances** is a fantastic way to potentially save up to 70-80%, depending on the VM size.

The cost of Azure products, services, and resources can vary across locations and regions, and if possible, you should use them in those locations and regions where they cost less.

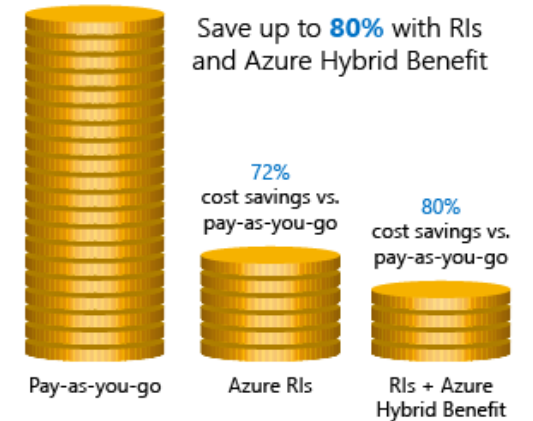
Recall from our previous discussion that Azure Cost Management and Azure Advisor might recommend **right-sizing or shutting down** VMs. Right-sizing a virtual machine is the process of resizing it to a proper size.

Resizing a VM requires it to be stopped, resized, and then restarted. This may take a few minutes depending on how significant the size change is. Plan for an outage, or shift your traffic to another instance while you perform this task.

If you have virtual machine workloads that are only used during certain periods, but you're running them every hour of every day, you're wasting money. These VMs are great candidates to shut down when not in use and start back up on a schedule, saving you compute costs while the VM is **deallocated**.

but if you aren't using a service, you should shut it down. It's not uncommon to find non-production or proof-of-concept systems left around following a project that is no longer needed.

PaaS services typically provide substantial savings in both resource and operational costs. The challenge is that depending on the type of service, varying levels of effort will be required to move to these services from both a time and resource perspective



Saving on infrastructure cost;

- Use azure credits
- Use spending limits
- Use reserved instanced
- Choose low cost location and region
- Research available cost-saving offers
- Right-size underutilized vm's
- Deallocate vm's in off hours
- Delete unused vm's
- Migrate to paas or saas services

Saving on licensing costs

Licensing is another area that can dramatically impact your cloud spending.

Linux vs. Windows

Azure Hybrid benefit for windows server

The [Enterprise Dev/Test](#) and [Pay-As-You-Go Dev/Test](#) offers are a benefit you can take advantage of to save costs on your non-production environments. This benefit gives you several discounts, most notably for Windows workloads, eliminating license charges and only billing you at the Linux rate for virtual machines. This also applies to SQL Server and any other Microsoft software that is covered under a Visual Studio subscription (formerly known as MSDN).

AHUB

To be eligible for this benefit, your Windows licenses must be covered by Software Assurance. The following guidelines will also apply:

- Each two-processor license or each set of 16-core licenses is entitled to two instances of up to 8 cores or one instance of up to 16 cores.
- Standard Edition licenses can only be used once either on-premises or in Azure. That means you can't use the same license for an Azure VM and a local computer.
- Datacenter Edition benefits allow for simultaneous usage both on-premises and in Azure so that the license will cover two running Windows machines.

For Azure SQL Database, the Azure Hybrid Benefit works as follows:

If you have Standard Edition per core licenses with active Software Assurance, you can get one vCore in the General Purpose service tier for every one license core you own on-premises.

- If you have Enterprise Edition per core licenses with active Software Assurance, you can get one vCore in the Business Critical service tier for every one license core you own on-premises. Note that the Azure Hybrid Benefit for SQL Server for the Business Critical service tier is available only to customers who have Enterprise Edition licenses.
- If you have highly virtualized Enterprise Edition per core licenses with active Software Assurance, you can get four vCores in the General Purpose service tier for every one license core you own on-premises. This is a unique virtualization benefit available only on Azure SQL Database.

For SQL Server in Azure Virtual Machines, the Azure Hybrid Benefit works as follows:

If you have Enterprise Edition per core licenses with active Software Assurance, you can get one core of SQL Server Enterprise Edition in Azure Virtual Machines for every one license core you own on-premises.

If you have Standard Edition per core licenses with active Software Assurance, you can get one core of SQL Server Standard Edition in Azure Virtual Machines for every one license core you own on-premises.

This can make a dramatic impact on your Azure spending with SQL Server workloads.

