Azure Fundamentals (AZ-900)

Lecture Slides

Good luck on your exam!

What is Cloud Computing?

cloud com·put·ing

noun

the practice of using a network of remote servers hosted on the Internet to store, manage, and process data, rather than a local server or a personal computer.

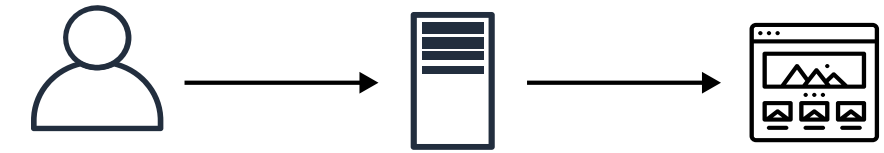
On-Premise

- You own the servers
- You hire the IT people
- You pay or rent the real-estate
- You take all the risk

Cloud Providers

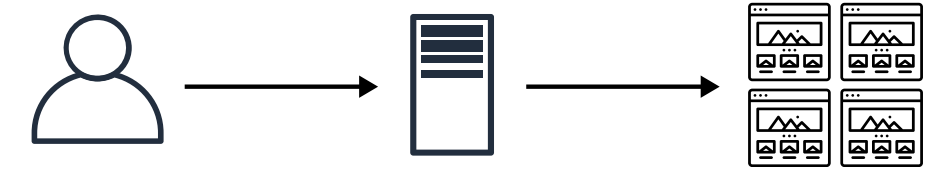
- Someone else owns the servers
- Someone else hires the IT people
- Someone else pays or rents the real-estate
- You are responsible for your configuring cloud services and code, someone else takes care of the rest.

What is Cloud Computing?



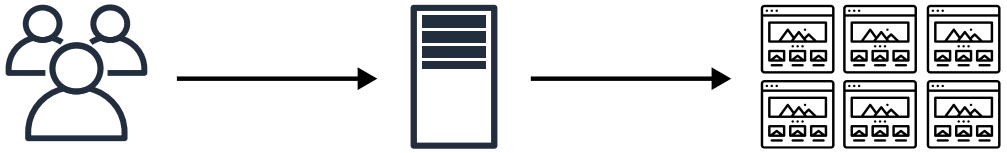
Dedicated Server

One physical machine dedicated **to single a business**.
Runs a single web-app/site.
Very Expensive, High Maintenance, High Security*



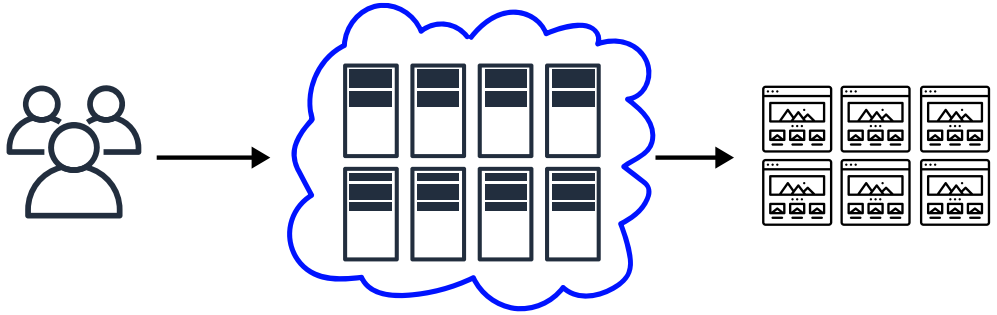
Virtual Private Server

One physical machine dedicated **to a single business**.
The physical machine is virtualized **into sub-machines**
Runs multiple web-apps/sites



Shared Hosting

One physical machine, shared by **hundred of businesses**
Relies on most tenants under-utilizing their resources.
Very Cheap, Very Limited.



Cloud Hosting

Multiple physical machines that act as one system.
The system is abstracted into multiple **cloud services**
Flexible, Scalable, Secure, Cost-Effective, High Configurability

Common Cloud Services

A cloud provider **can have hundreds of cloud services** that are grouped various types of services. The four most common types of cloud services for Infrastructure as a Service (IaaS) would be:

Compute
Imagine having a virtual computer that can run application, programs and code.

Networking
Image having the a virtual network being able to define internet connections or network isolations

Storage
Imagine having a virtual hard-drive that can store files

Databases
Imagine a virtual database for storing reporting data or a database for general purpose web-application

The term “Cloud Computing” can be used to refer to all categories, even though it has “compute” in the name.

What is Microsoft?

Microsoft

An American multinational computer technology corporation headquartered **in Redmond, Washington**

Microsoft makes software, phones, tablets, game consoles, cloud services, a search engine and more!

Microsoft has been around since the late 1970s and is well known for their **Operation System**.

What is Azure?

Microsoft calls their cloud provider service

Microsoft Azure

Commonly referred to just **Azure**

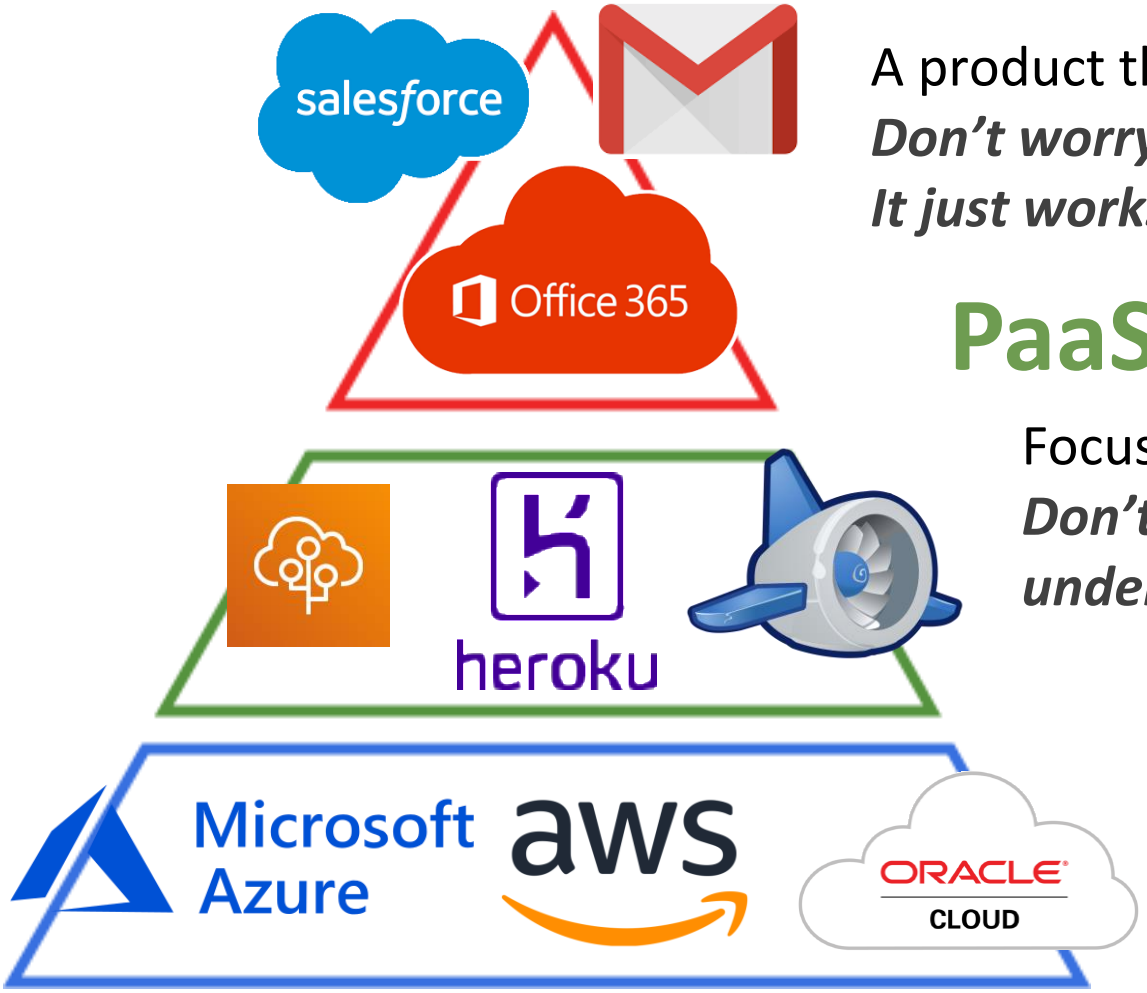
Azure literally means **“bright blue color of the cloudless sky”**

Cloud Service Providers can be initialized as **CSPs**

Benefits of Cloud Computing

Cost-effective	You **pay for what you consume**, **no up-front cost**. Pay-as-you-go (PAYG) thousands of customers sharing the cost of the resources
Global	Launch workloads **anywhere in the world**, Just choose a region
Secure	Cloud provider takes care of physical security. **Cloud services can by secure by default** or you have the ability to configure access down to granular level.
Reliable	data backup, disaster recovery, and data replication, and fault tolerance
Scalable	Increase or decrease resources and services based on demand
Elastic	**Automate** scaling during spikes and drop in demand
Current	The underlying hardware and managed software is patched, upgraded and replaced by the cloud provider without interruption to you.

Types of Cloud Computing



SaaS Software as a Service **For Customers**

A product that is run and managed by the service provider
Don't worry about how the service is maintained.
It just works and remains available.

PaaS Platform as a Service **For Developers**

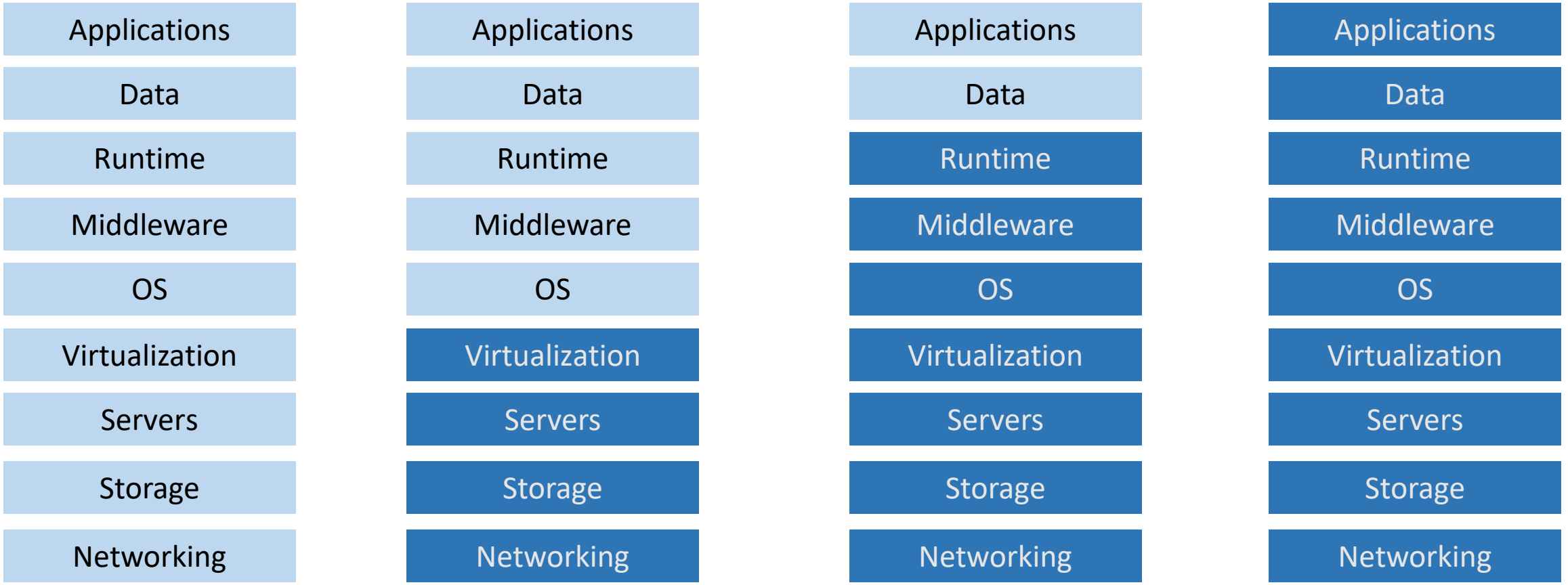
Focus on the deployment and management of your apps.
Don't worry about, provisioning, configuring or understanding the hardware or OS.

IaaS Infrastructure as a Service **For Admins**

The basic building blocks for cloud IT. Provides access to networking features, computers and data storage space.
Don't worry about IT staff, data centers and hardware.

Types of Cloud Computing Responsibilities

Cheat sheets, Practice Exams and Flash cards 👉 www.exampro.co/az-900

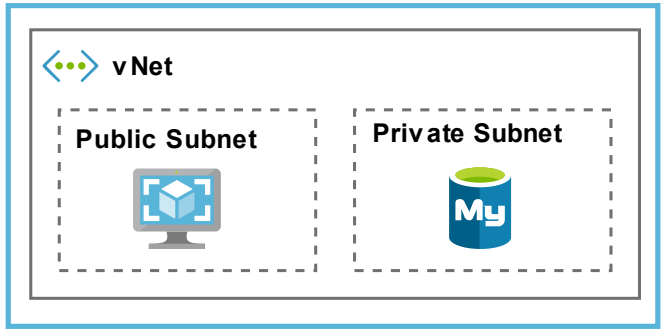


Legend: Customer is Responsible | CSP is Responsible

Azure's Deployment Models

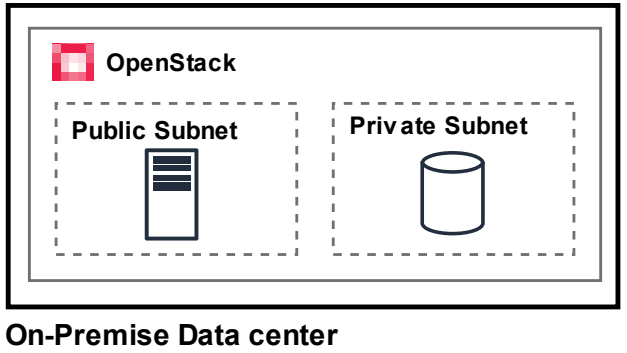
Public Cloud

Everything built on the Cloud Provider
Also known as: Cloud-Native



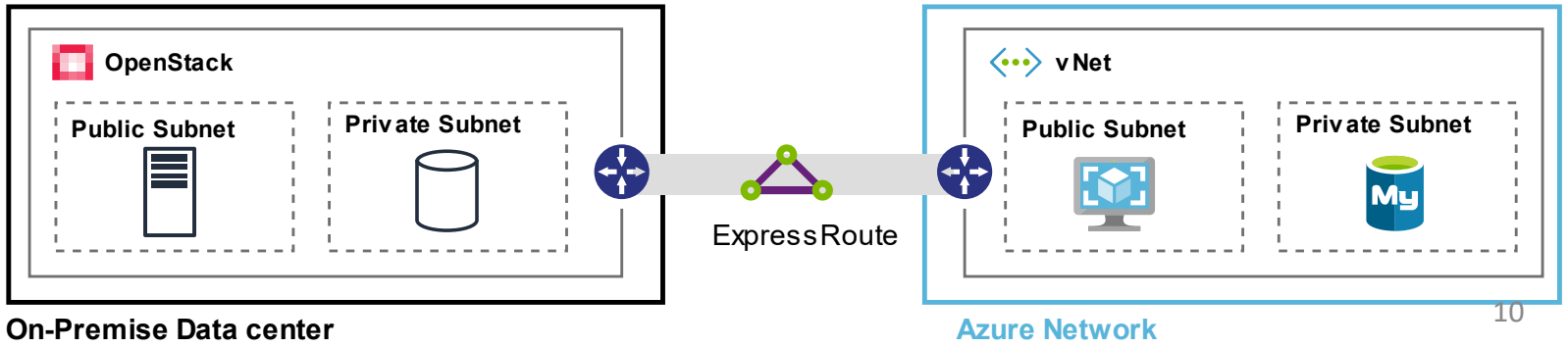
Private Cloud

Everything built on company's datacenters
Also known as **On-Premise**
The cloud could be **OpenStack**



Hybrid

Using both **On-Premise** and
A **Cloud Service Provider**



Azure's Deployment Models

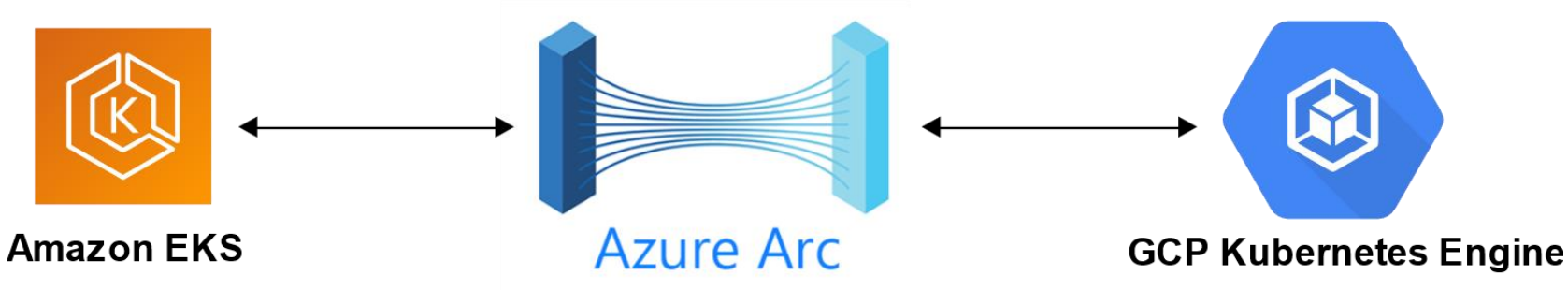
	Cost	Security	Level of Configuration	Technical Knowledge
Public Cloud	👍 Most cost-effective	👍 Security Controls by Default 👎 Might not meet security requirements	👎 Limited based on what the Cloud Service Provider exposes to you.	👍 You don't need in-depth knowledge of underlying infrastructure
Private Cloud	👎 Most expensive	👎 no guarantee its secure 👍 can meet any security compliance requirement if you put in the work.	👍 You can configure the infrastructure however you like.	👎 You need to know in-depth how to configure all levels of your infrastructure
Hybrid	👍 👎 Could be more cost-effective based on what you offload to the cloud.	👎 you now have to secure your connection to the cloud 👍 can meet all security requirements	👍 You get the best of both worlds.	👎 You need to know in-depth how to configure all levels of your infrastructure and know the CSPs services.

Deployment Models

Cross-Cloud

Using **Multiple Cloud Providers**

Aka multi-cloud, hybrid-cloud

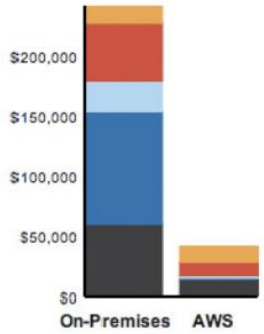


Total Cost of Ownership (TCO)

CAPEX

On-Premise

Software license Fees



OPEX

Azure

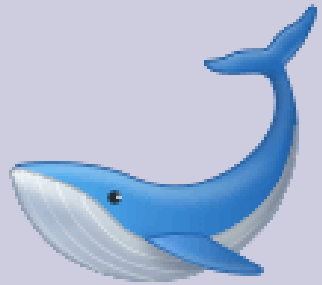
Subscription Fees

- Implementation
- Configuration
- Training
- Physical Security
- Hardware
- IT Personal
- Maintenance

Azure's Responsibility

75% Savings

- Implementation
- Configuration
- Training



Capital vs Operational Expenditure

Capital Expenditure (CAPEX)

Spending money upfront on **physical infrastructure**
Deducting that expense from your tax bill over time.

- Server Costs (computers)
- Storage Costs (hard drives)
- Network Costs (Routers, Cables, Switches)
- Backup and Archive Costs
- Disaster Recovery Costs
- Datacenter Costs (Rent, Cooling, Physical Security)
- Technical Personal

With Capital Expenses **you have to guess upfront** what you plan to spend

Operational Expenditure (OPEX)

The costs associated with an on-premises datacenter that has shifted the cost to the service provider. The customer only has to be concerned with non-physical costs.

- Leasing Software and Customizing features
- Training Employees in Cloud Services
- Paying for Cloud Support
- Billing based on cloud metrics eg.
  - compute usage
  - storage usage

With Operation Expenses you can try a product or service **without investing in equipment**

Cloud Architecture Terminologies

Availability - Your ability to maintain service accessibility, often measured by uptime. **Highly Available (HA)** ensures continuous service.

Scalability – Your ability to adjust resources to handle changing workloads. It supports rapid growth without performance issues.

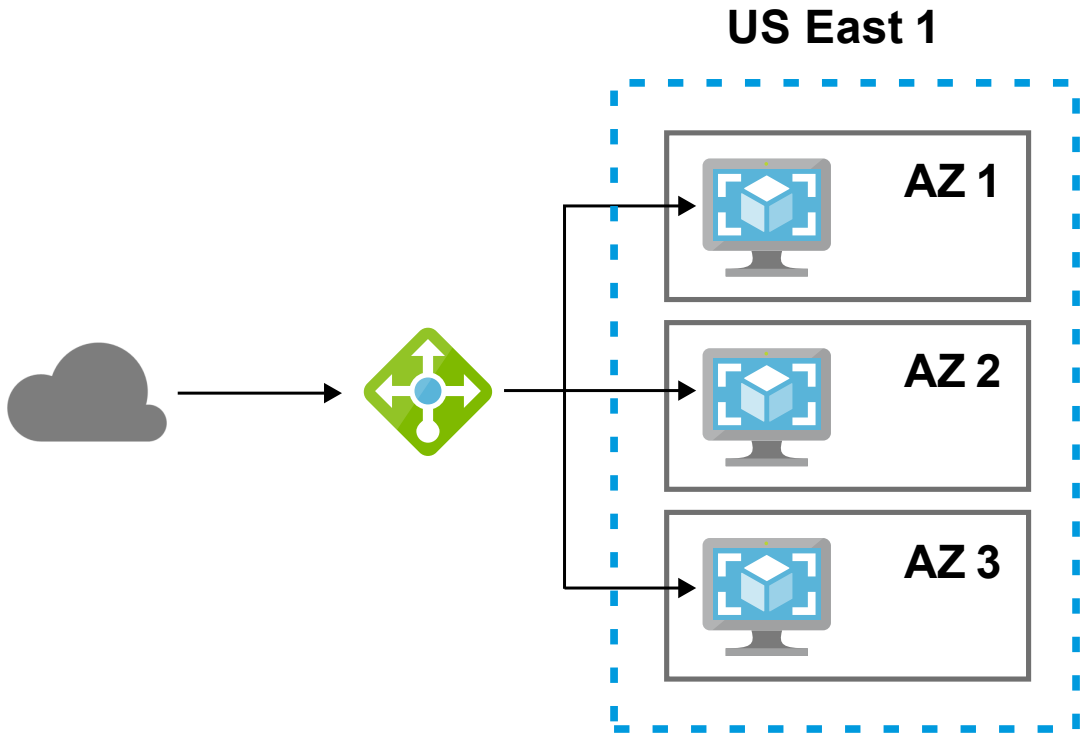
Elasticity – Your ability to dynamically allocate or de-allocate resources based on demand, optimizing cost-efficiency.

Fault Tolerance – Your ability to sustain functionality despite failures in hardware or software.

Disaster Recovery (DR) - Your ability to recover from major outages, ensuring data integrity and availability even in catastrophic events.

High Availability

Your ability for your service to **remain available** by ensuring there is ***no single point of failure** and/or ensure a certain level of performance



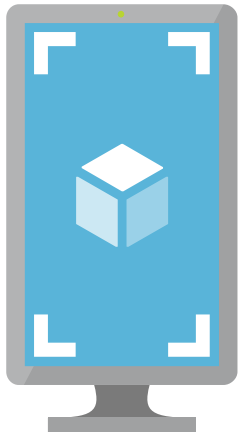
Azure Load Balancer

A load balancer allows you to evenly distribute traffic to multiple servers in one or more datacenter. If a datacenter or server becomes unavailable (unhealthy) the load balancer will route the traffic to only available datacenters with servers.

Running your workload across multiple **Availability Zones** ensures that if 1 or 2 **AZs** become unavailable your service / applications remains available.

High Scalability

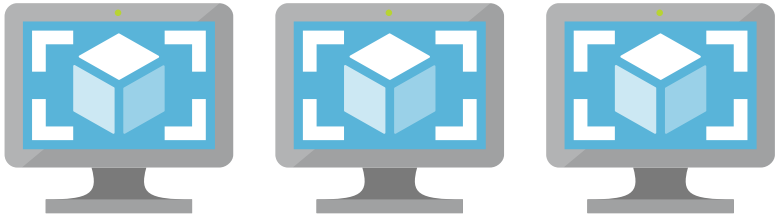
Your ability to **increase your capacity** based on the increasing demand of traffic, memory and computing power



Vertical Scaling

Scaling **Up**

Upgrade to a bigger server



Horizonal Scaling

Scaling **Out**

Add more servers of the same size

High Elasticity

Your ability to **automatically** increase or decrease your capacity based on the current demand of traffic, memory and computing power

Azure VM Scale Sets
Automatically increase or decrease in response to demand or a defined schedule.

SQL Server Stretch Database
Dynamically stretch warm and cold transactional data from Microsoft SQL Server 2016 to Microsoft Azure

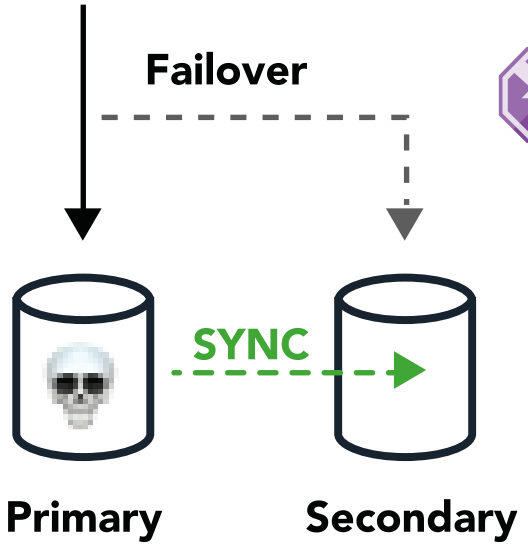
Horizonal Scaling
Scaling **Out** — Add more servers of the same size
Scaling **In** — Removing more servers of the same size

Vertical Scaling is generally hard for traditional architecture so you'll usually only see horizontal scaling described with Elasticity.

Highly Fault Tolerant

The ability to **withstand and recover** from **unexpected failures**, errors, or disruptions in a system or application, ensuring uninterrupted operation and minimal downtime

Failover involves shifting traffic from a primary system to a redundant system when issues occur



Azure Traffic Manager is a DNS-based traffic load balancer. It does not directly initiate failovers. It's primarily used for load distribution and routing traffic to healthy endpoints

A common use case is secondary replicas taking over in the event of a primary system failure. This process is typically managed through database-specific failover mechanisms.

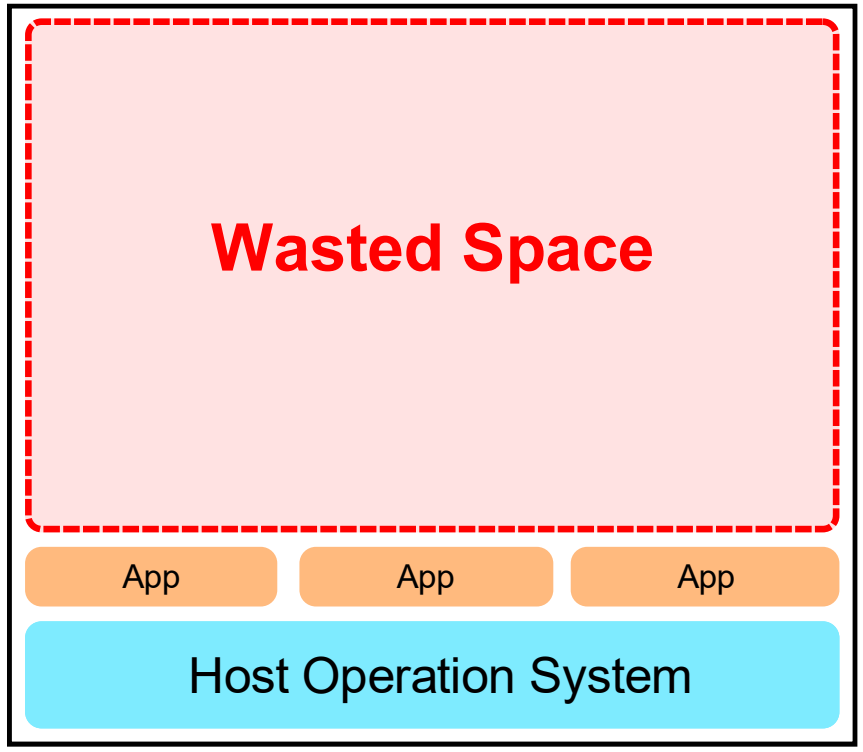
High Durability

Your ability to **recover** from a disaster and to prevent **the loss** of data
Solutions that recover from a disaster is known as **Disaster Recovery (DR)**

- Do you have a backup?
- How fast can you restore that backup?
- Does your backup still work?
- How do you ensure current live data is not corrupt?

The Evolution of Computing

***Dedicated** 👉 VMs 👉 Containers 👉 Functions

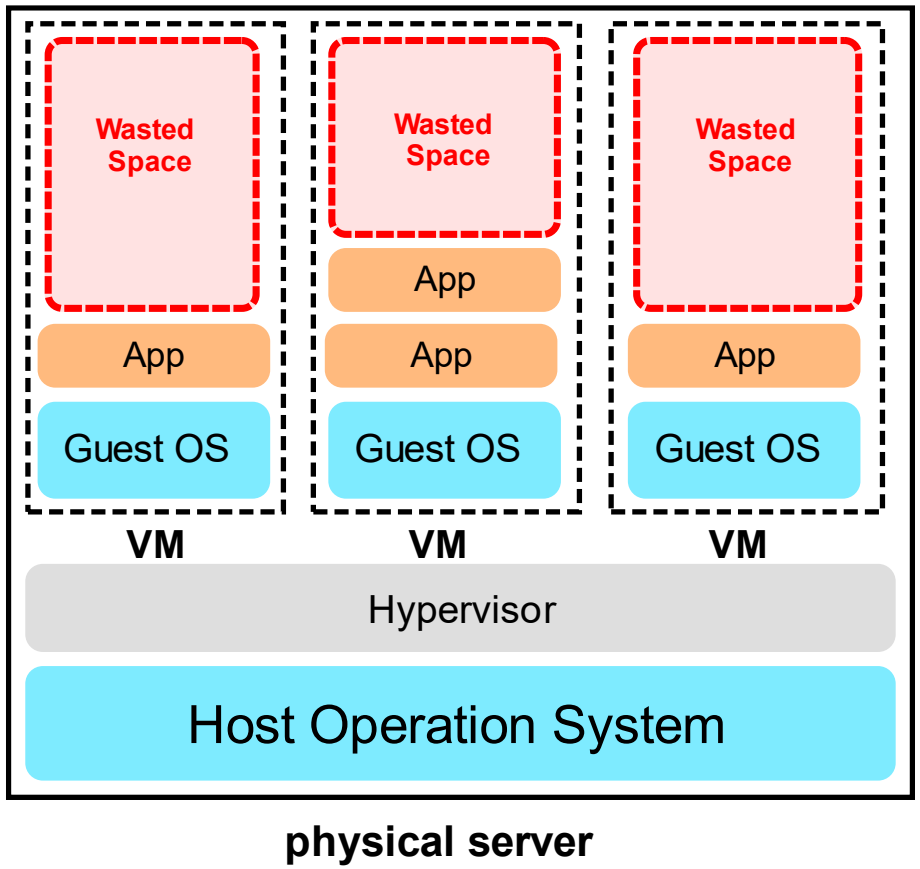


physical server

- A physical server **wholly utilized by a single customer**.
- You have to guess your capacity, you'll overpay for an underutilized server
- Upgrading beyond your capacity will be slow and expensive
- You are limited by your Operating System
- Multiple apps can result in conflicts in resource sharing
- You have a ***guarantee of security, privacy and full utility of underlying resources**

The Evolution of Computing

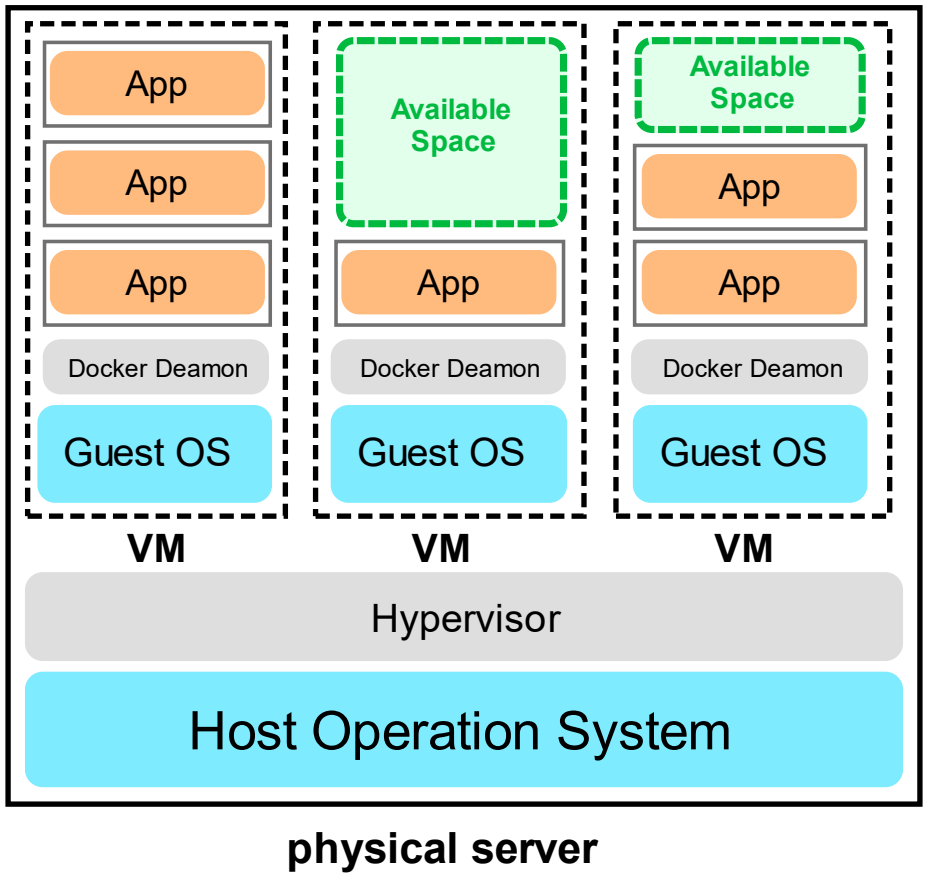
*Dedicated 👉 **VMs** 👉 Containers 👉 Functions



- You can run **multiple Virtual Machines on one machine**.
- **Hypervisor** is the software layer that lets you the VMs
- A physical server shared by multiple customers
- You are pay for a fraction of the server
- You'll overpay for an underutilized Virtual Machine
- You are limited by your Guest Operating System
- Multiple apps on a single Virtual Machine can result in conflicts in resource sharing

The Evolution of Computing

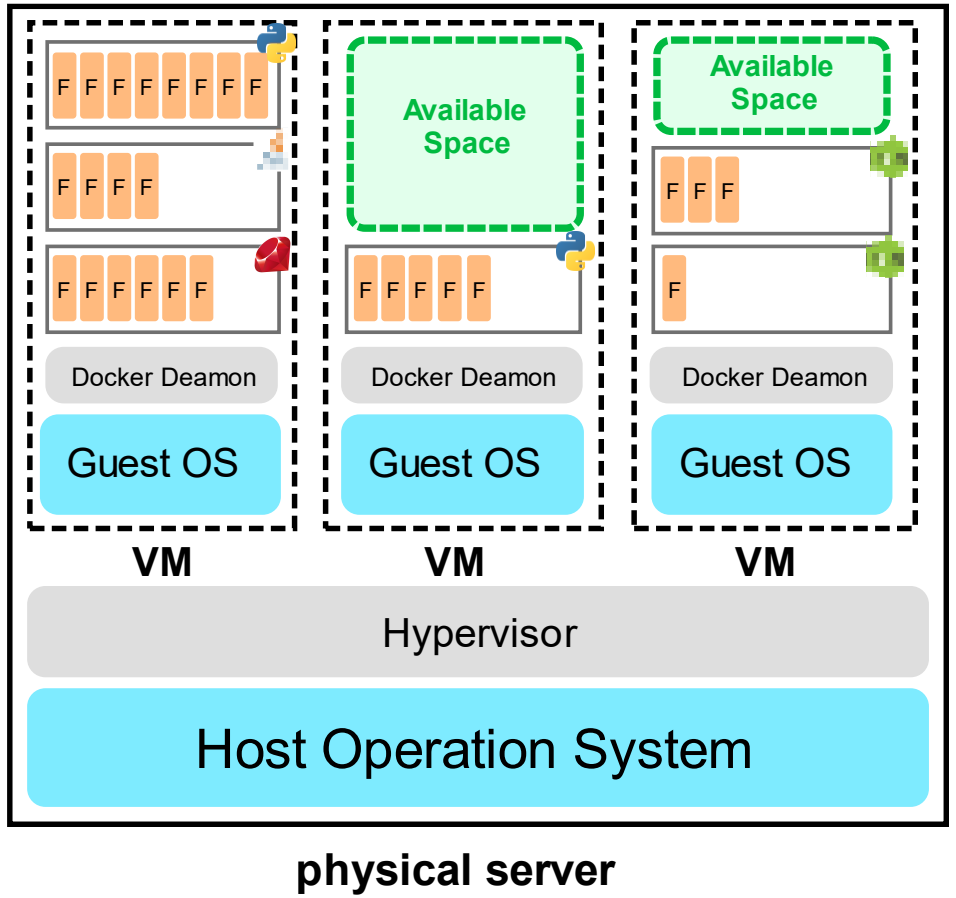
*Dedicated 👉 VMs 👉 **Containers** 👉 Functions



- Virtual Machine running multiple containers
- **Docker Deamon** is the name of the software layer that lets you run multiple containers.
- You can maximum the utilize the available capacity which is more cost-effective
- Your containers share the same underlying OS so containers are more efficient than multiple VMs
- Multiple apps can run side by side without being limited to the same OS requirements and will not cause conflicts during resource sharing

The Evolution of Computing

*Dedicated 👉 VMs 👉 Containers 👉 **Functions**



- A managed VMs running managed containers.
- Known as **Serverless Compute**
- You upload a piece of code choose the amount of memory and duration.
- Only responsible for code and data, nothing else
- Very cost-effective, only pay for the time code is running, VMs only run when there is code to be executed
- Cold Starts is a side-effect of this setup

Global Infrastructure – Regions and Geographies

A **region** is a grouping of multiple datacenters (Availability Zones)

Azure has **58 Regions** available across **140 Countries**

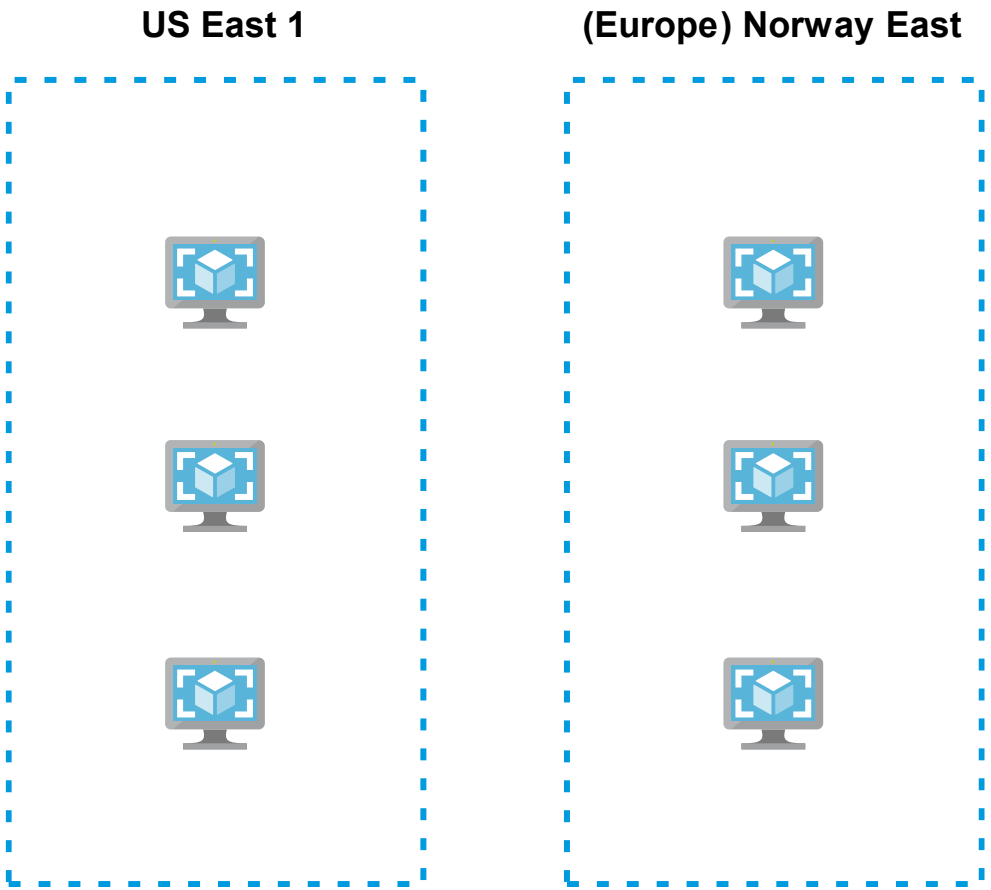
A **Geography** is discreet market of two or more regions that preserves **data residency** and **compliance boundaries**.

Azure Geographies

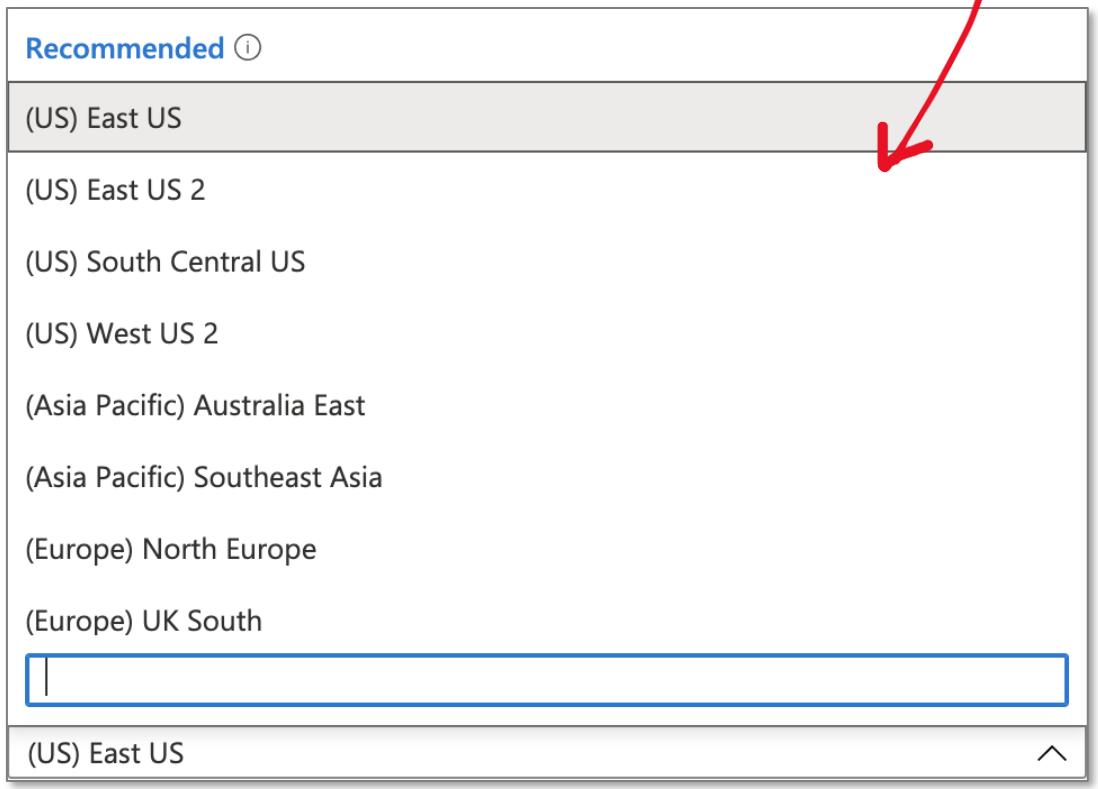
- United States
- Azure Government (US)
- Canada
- Brazil
- Mexico

Imagine you are in Canada and **you want a guarantee that data will remain within Canada**.
You would want to use Canada Azure Geographies

Global Infrastructure – Regions and Geographies



You choose the region when you launch a new cloud resource



Global Infrastructure – Paired Regions

Each region is paired with another region **300 miles** away.

Only one region is updated at a time to ensure no outages

Some Azure Services rely on Paired Regions for **Disaster Recovery**

Eg. **Azure Geo-redundant Storage (GRS)** replicates data to a secondary region automatically, ensuring that data is durable even in the event that the primary region isn't recoverable.

Canada	Canada Central	Canada East
North America	East US	West US
Germany	Germany Central	Germany Northeast

Global Infrastructure – Region Types and Service Availability

Not all Azure cloud services are available in every Region.

Recommended region

A region that provides the broadest range of service capabilities and is **designed to support Availability Zones** now, or in the future.

Alternate (other) region

A region that extends Azure's footprint within a data residency boundary where a recommended region also exists. **Not designed to support AZs.**
These Regions are label as **Other** in the Azure Portal

General availability (GA) is when a service is considered ready to be used publicly by everyone.

Azure Cloud services are grouped into **three** categories.
Their category determines when cloud services become available:

1. **Foundational.** When GA, immediately or in 12 months in Recommended and Alternate Regions
2. **Mainstream** When GA immediately or in 12 months in Recommended Regions
   May become available in Alternate Regions based on customer demand
3. **Specialized.** Available in Recommended or Alternate Region based on customer demand

Global Infrastructure – Special Regions

Azure has specialized regions to meet **compliance or legal reasons**

- US DoD Central
- US Gov Virginia
- US Gov Iowa

***Three Azure Government secret locations undisclosed**

- China East
- China North

*** Available through a unique partnership between Microsoft and 21Vianet. Microsoft does not directly maintain the datacenters.**

世纪互联®
www.21vianet.com

Global Infrastructure – AZs

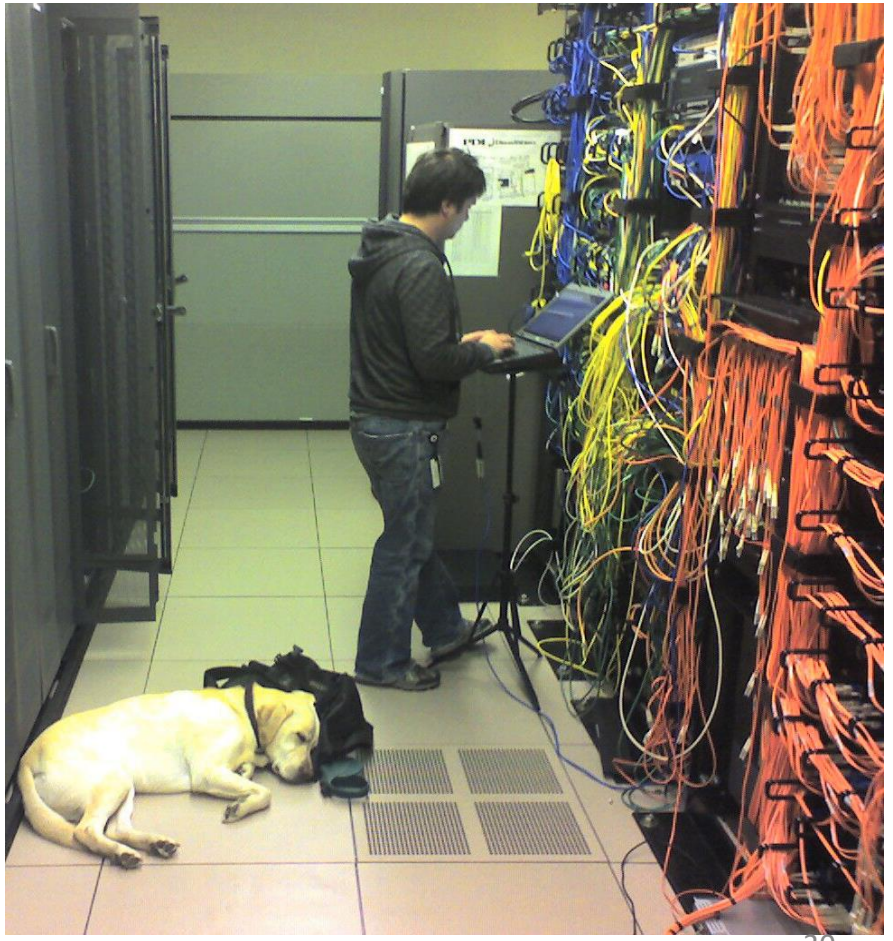
An **Availability Zone** (AZ) is physical location made up of one or more datacenter.

A datacenter is a secured building that contains hundreds of thousands of computers.

A region will ***generally** contain **3 Availability Zones**

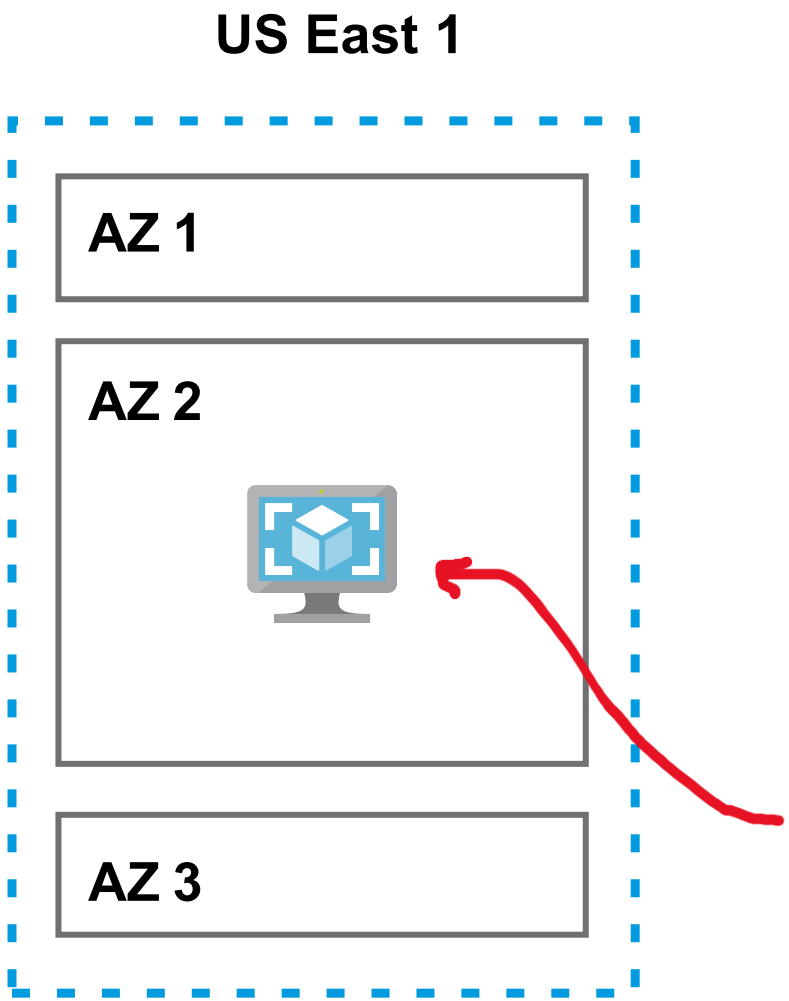
Datacenters within a region will be isolate from each other (so different buildings). But they will be close enough to provide low-latency.

Its common practice to run workloads in at least 3 AZs to ensure services remain available in case one or two datacenters fail. (High Availability)



Global Infrastructure – AZs

Cheat sheets, Practice Exams and Flash cards 👉 www.exampro.co/az-900



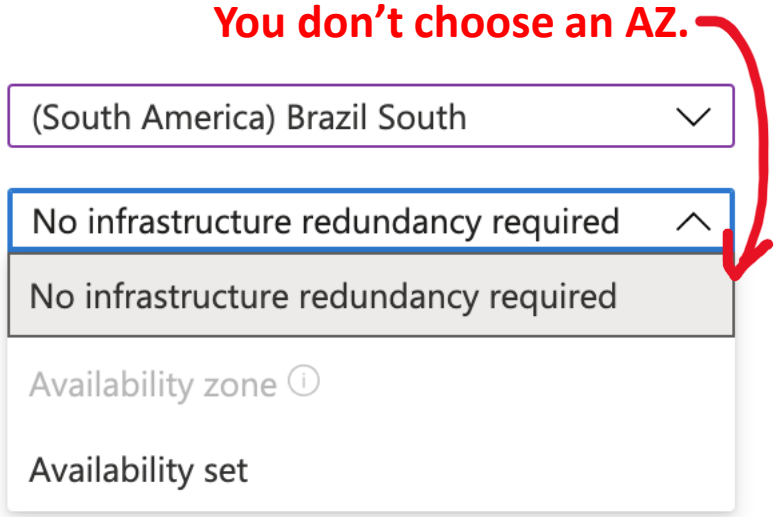
If you region has multiple AZs you choose a number. Choosing 2 means AZ-2 not that you have chosen a quantity Of 2 AZs.

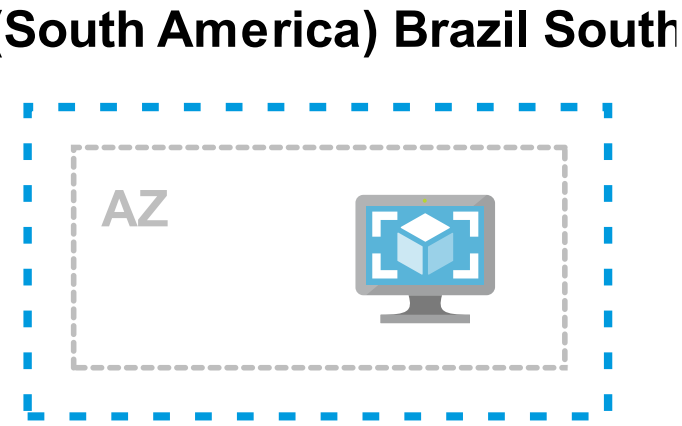
Global Infrastructure – AZ Supported Regions

Not Every Region has support for Availability Zones
These regions are known as **Alternate** or **Other**
Recommended Regions are suppose to have at least 3 AZs.

The following Regions
have a minimum of 3 AZs

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





Global Infrastructure – Fault and Update Domains

An Availability Zone (AZ) in an Azure region is
a combination of a **fault domain** and an **update domain**.

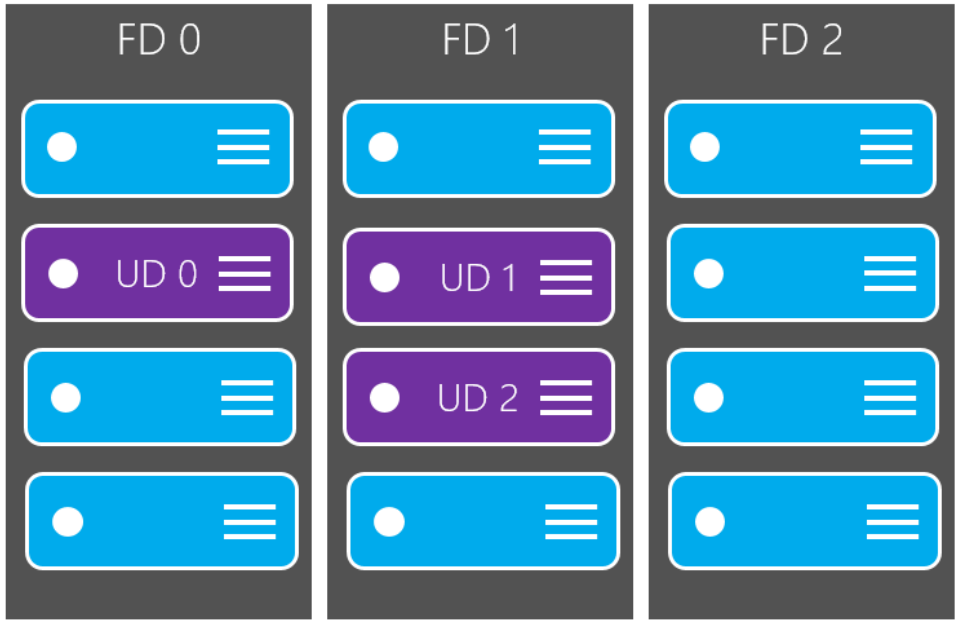
Fault Domain
A logical grouping of hardware to avoid a single point of failure within an AZ.
group of virtual machines that share a common power source and network switch.

Update Domain
Azure may need to apply updates to the underlying hardware and software.
Update domains ensure your resources do not go offline.

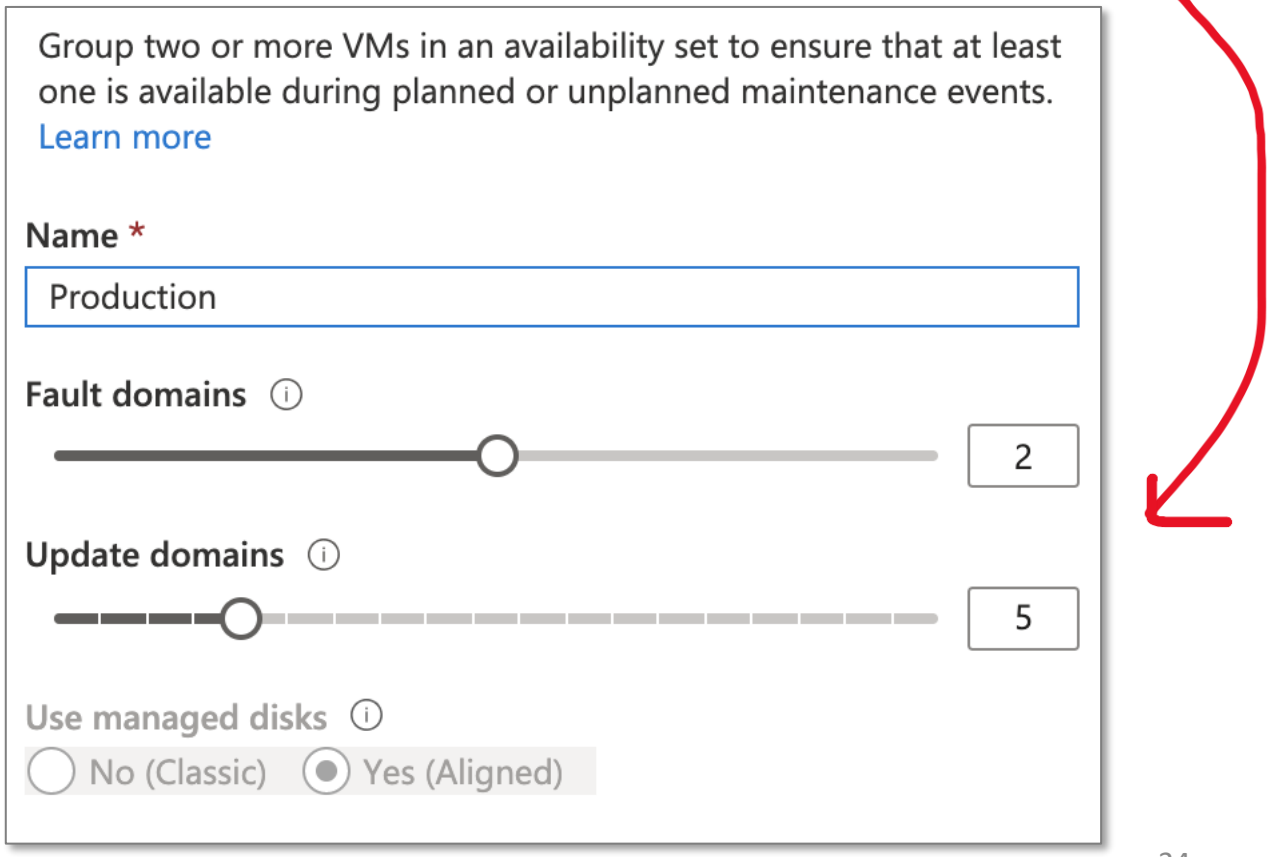
Availability Set
A logical grouping that you can use in Azure to ensure that the VMs you place in the Availability Set are different fault/update domains to avoid downtime.

Global Infrastructure – Fault and Update Domains

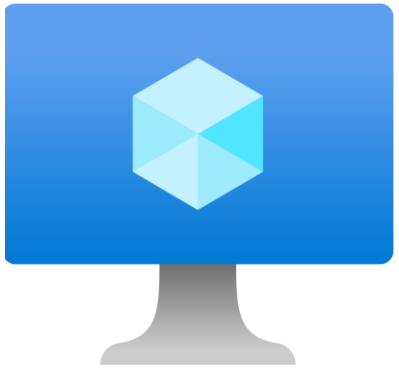
Each Virtual Machine in an Availability Set is assigned a Fault Domain and Update Domain.



Creating a Availability Set.
Choosing the amount of domains



Azure Virtual Machines



Choose an OS, Compute, Memory and Storage
and launch a **server** in minutes

Introduction to Azure VMs

Azure Virtual Machines (VMs) is a highly configurable server.
Virtualization let you run a server ***without*** **having to buy and maintain the physical hardware** that runs it

Virtual Machines still require maintenance such as:

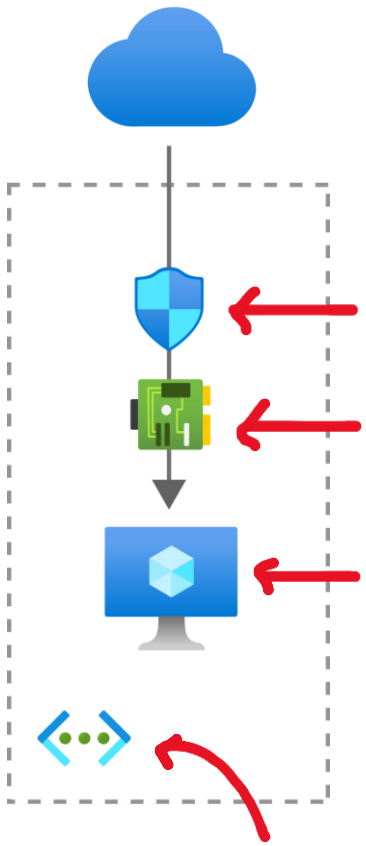
- applying OS system patches
- Installing and configuring packages

Some things you should know:

- The **size** of the virtual machine is determined by the Image
  - The image defines the combination of vCPUs, Memory and Storage Capacity
- The current limit on a per subscription basis is **25000 VMs per region**.
- Azure VMs are billed at an **hourly rate**
- A single instance VMs has an availability of 99.9% (when all storage disks are premium)
- Two instances deployed in Availability Set will give you 99.95% availability
- You can attach multiple Managed Disk to your Azure VMs

Introduction to Azure VMs

When you ***launch*** an Azure Virtual Machine other networking components will be either created or associated to your Virtual Machine.



Network Security Group (NSG) — attached to the NIC, virtual firewall with rules around ports and protocols

Network Interface (NIC) — a device that handle ip protocols and network communication

Virtual Machine instance — The actual running server

Public IP Address — The address that you will use publicly access your VM

Virtual Network (VNet) — The network where your VM will reside

Resource	Type	Status	Operation details
MyNewVirtualMachine	Microsoft.Compute/virtualMachines	OK	Operation details
mynewvirtualmachine839	Microsoft.Network/networkInterfaces	Created	Operation details
MyNewVirtualMachine_group-vnet	Microsoft.Network/virtualNetworks	OK	Operation details
MyNewVirtualMachine-nsg	Microsoft.Network/networkSecurityGroups	OK	Operation details
MyNewVirtualMachine-ip	Microsoft.Network/publicIpAddresses	OK	Operation details

Azure VMs – Operation Systems

What is an Operation System (OS)?
The OS is the program that manages all other programs in a computer.
The most commonly known operations systems are Windows ,macOS, and Linux



When you launch a Virtual Machine you need to choose an Image which has a specific Operation System.

Microsoft works closely with partners to ensure the images available are updated and optimized for an Azure runtime. Most of these images can be found in the **Azure Marketplace**

- SUSE Linux Enterprise Server
- Red Hat Enterprise Linux
- Ubuntu Server
- Debian
- FreeBSD
- Azure Marketplace - Flatcar Container Linux
- RancherOS
- Bitnami Library for Azure
- Mesosphere DC/OS on Azure
- Docker images
- CloudBees Jenkins Platform

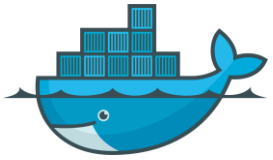
You can **Bring Your Own Linux** by creating a Linux Virtual Hard Disk (VHD)

(Hyper-V virtual hard disk (VHDX) format isn't supported in Azure, only fixed VHD)





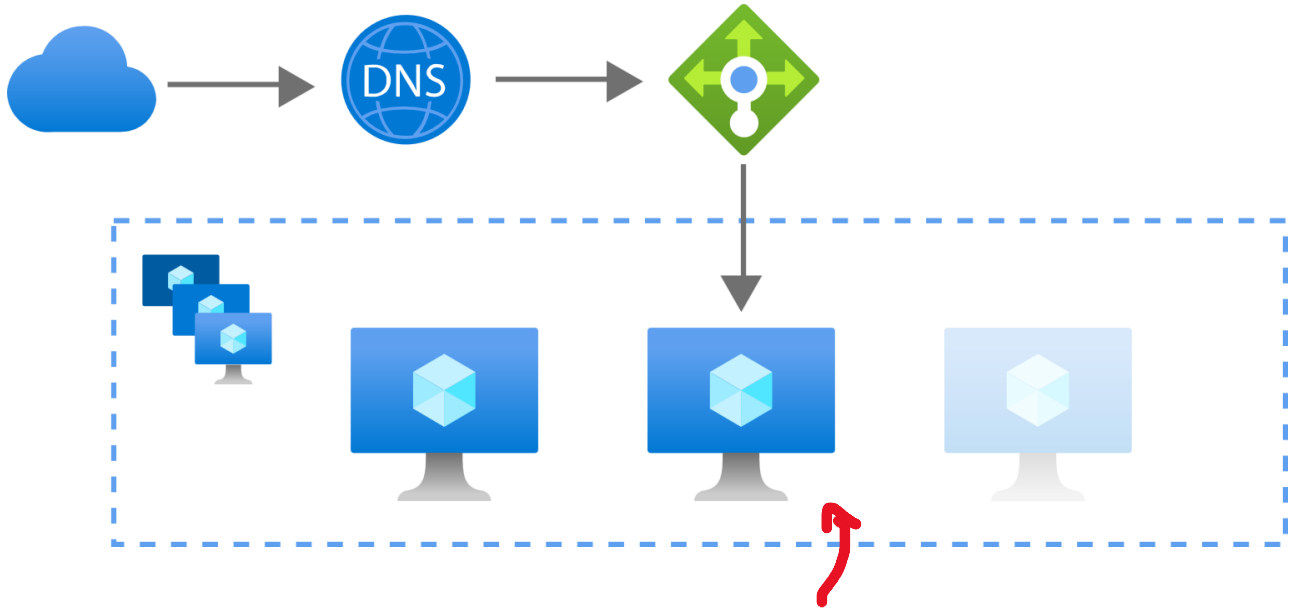




Azure Scale Sets

Azure Scale Sets allows you to **automatically** **increase** or **decrease** your VM capacity.

- Create Scaling Policies to automatically add or remove based on Host Metrics
- Create Health checks and set a Repair Policy to replace unhealthy instances
- Associate A Load Balancer to distribute VMs across AZs
- You can scale to 100s or even 1000s of VMs using scale sets

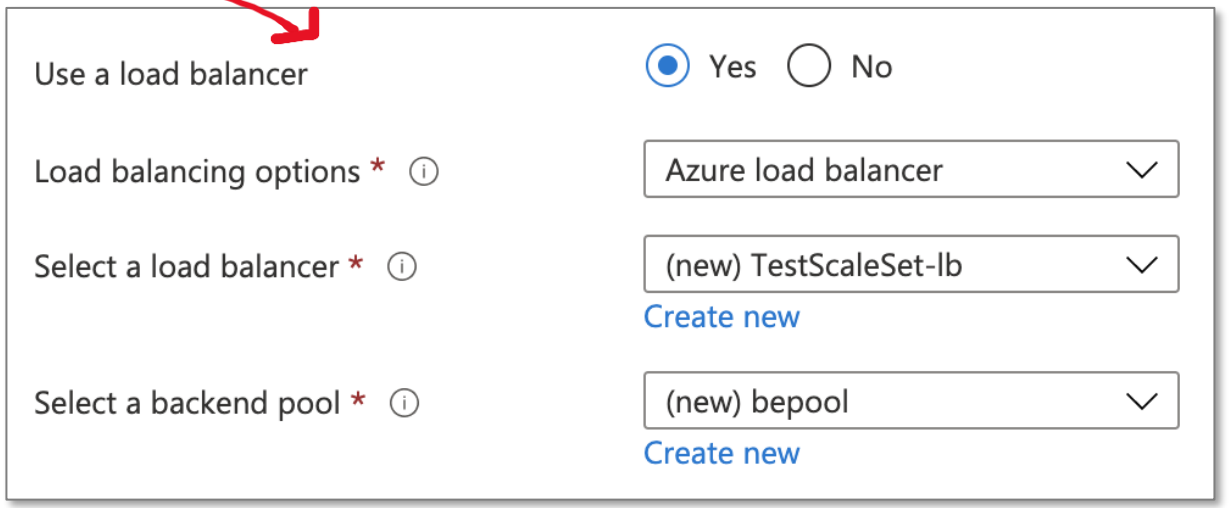


A Scale Set is a group **of** **identical VMs** (same Image and size)

Azure Scale Sets – Load Balancer

A Load Balancer can be **associated** with a Scale Set.
This will allow you to:

- evenly distribute your VMs across multiple Availability Zones to make your application Highly Available.
- Use Load Balancer probe checks for more robust Health checks

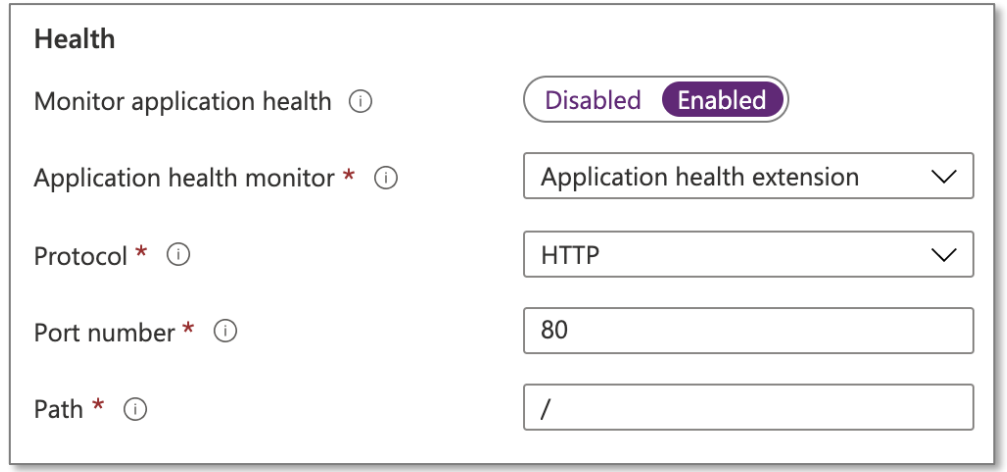


You have the choice between 2 different load balancers:

1. **Application Gateway** is an **HTTP/HTTPS** web traffic load balancer with URL-based routing, SSL termination, session persistence, and web application firewall.
2. **Azure Load Balancer** supports all **TCP/UDP** network traffic, port-forwarding, and outbound flows.

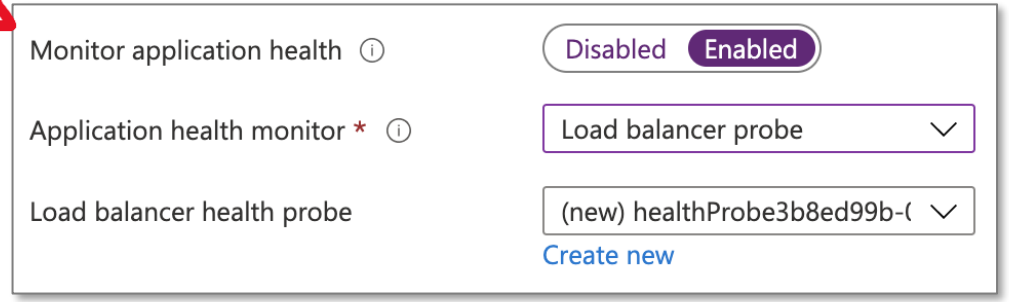
Azure Scale Sets - Health Monitoring

Health monitoring can be enabled to determine if you server is **healthy** or **unhealthy**.



There are 2 modes of health monitoring:

1. Application health extension
   - Ping an HTTP request to a specific path and except a status 200
2. Load Balancer Probe
   - Allow you to check based on TCP, UDP or HTTP requests.



Automatic repair policy

If an instance is found to be unhealthy the delete it and launch a new instance

Azure App Service

Quickly **deploy and manage Web apps** on Azure
without worrying about the underlying infrastructure

Platform as a Service

Introduction to Azure App Service

Azure App Service is an **HTTP-based service** for hosting web applications, REST APIs, and mobile back ends.

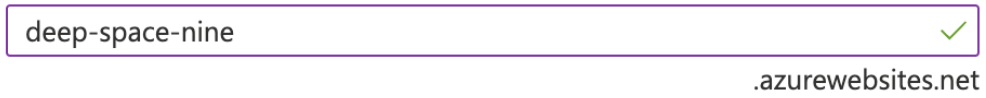
You can choose your **programming language** and either a **Windows** and **Linux** environment

It is a Platform as Service, so it's the **Heroku equivalent for Azure**.

Azure App Service takes care of the following underlying infrastructure

- Security patches for OS and languages
- Load balancing
- Autoscaling
- Automated manager

When you create your app you have to choose a unique name since it becomes a fully qualified domain



Azure App Service makes it easy to implement common Integrations and features such as:

- Azure DevOps (For deployments)
- Github Integration
- Docker Hub Integration
- Package Management
- Easy to setup staging environments
- Custom Domains
- Attaching TLS/SSL Certificates

You pay based on an Azure App Service Plan:
Shared Tier — Free, Shared (Linux not supported)
Dedicated Tier — Basic, Standard, Premium, PremiumV2, PremiumV3
Isolated Tier

Azure App Services can also run docker single or multi-containers

Azure App Service – Runtimes

What is a Runtime Environment?
A runtime software/instructions that are executed *while* your program is running.
A runtime generally means what **programming language** and **libraries** and **framework** you are using.

A runtime for Azure App Services will be a pre-defined **container** that has your programming language and commonly used library for that language installed.

With Azure App Services you choose a runtime.

- .NET
- .NET Core
- Java
- Ruby
- Node.js
- PHP
- Python

Azure App Services will have generally multiple latest versions of of a programming language eg. Ruby 2.6, 2.7

Its common to for a cloud provider to stop supporting older versions so you keep current and forces customer to keep good security practices by having latest patches



Azure App Service – Custom Container

Azure App Service allows you defined **custom containers** for **Windows or Linux**
You might want to create your own custom container to use a different runtime or bundle in a packages or software

Create your own **Docker** Container on your local environment

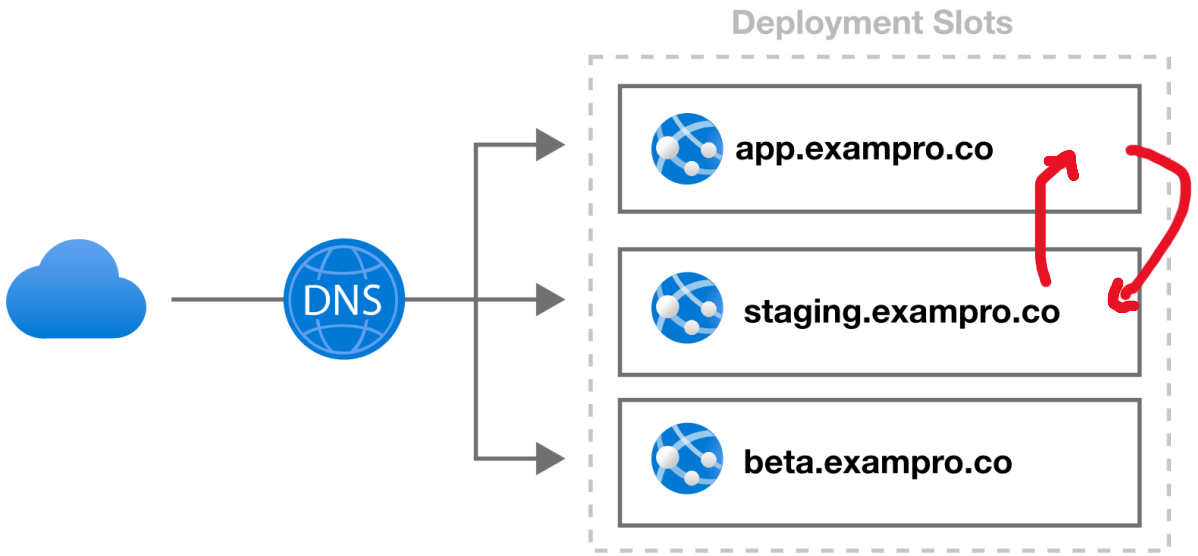
Push the Docker container to **Azure Container Registry**

Deploy your Container Image to **App Service**

Azure App Service – Deployment Slots

Deployments Slots allow you to create **different environments** of your web-application associated to a different hostname. This is useful when need a staging, or QA environment.

Think of it as a way to quickly clone your production environment for other uses.



You can also **Swap environments** This could be how you perform a Blue/Green deploy.

You can promote our staging to production by swapping, if something goes wrong you could swap them back.

Azure App Service – App Service Environment

App Service Environment (ASE) is an Azure App Service feature that provides a **fully isolated and dedicated environment** for securely running App Service apps at high scale

This allow you to host:

- Windows web apps
- Linux web apps
- Docker containers
- Mobile apps
- Functions

App Service environments (ASEs) are appropriate for application workloads that require:

- Very high scale
- Isolation and secure network access.
- High memory utilization

Customers can create multiple ASEs within a single Azure region or across multiple Azure regions making ASEs ideal for **horizontally scaling stateless application tiers** in support of **high requests per second (RPS) workloads**.

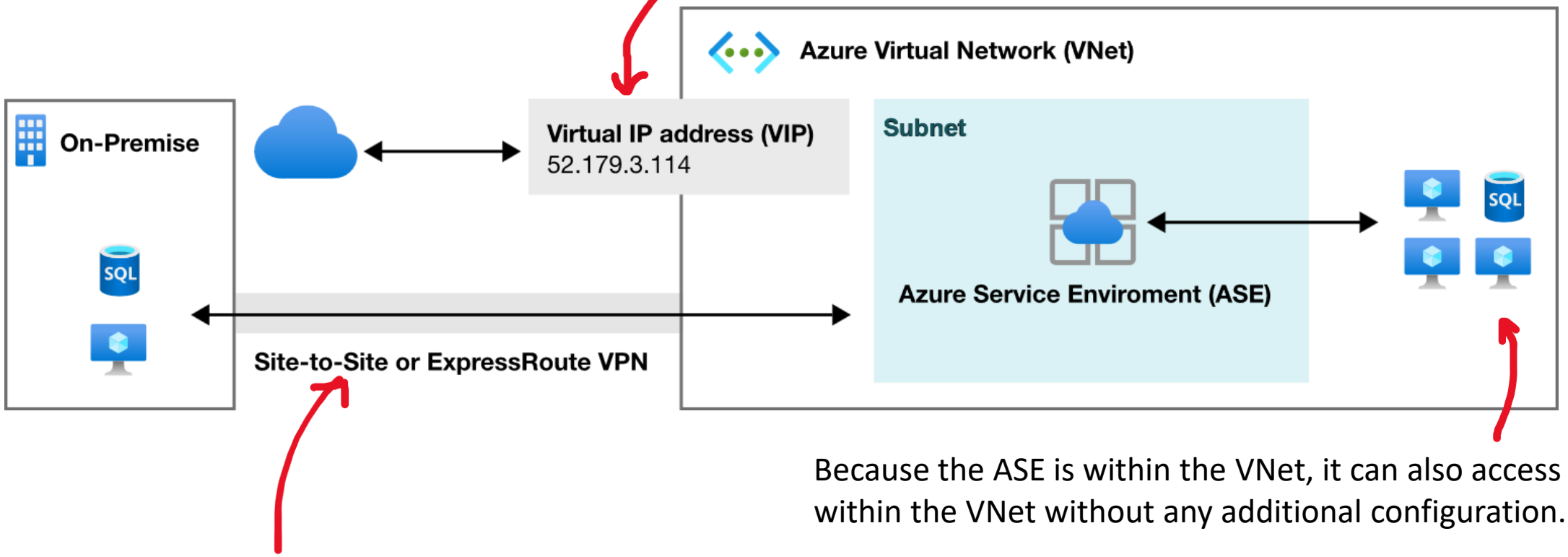
- ASE comes with its own pricing tier (Isolated Tier)
- ASEs can be used to configure security architecture
- Apps running on ASEs can have their access gated by upstream devices, such as web application firewalls (WAFs)
- App Service Environments can be deployed into Availability Zones (AZ) using zone pinning.

There are **2 deployment types** for an App Service environment (ASE):

1. External ASE
2. ILB ASE

Azure App Service – App Service Environment

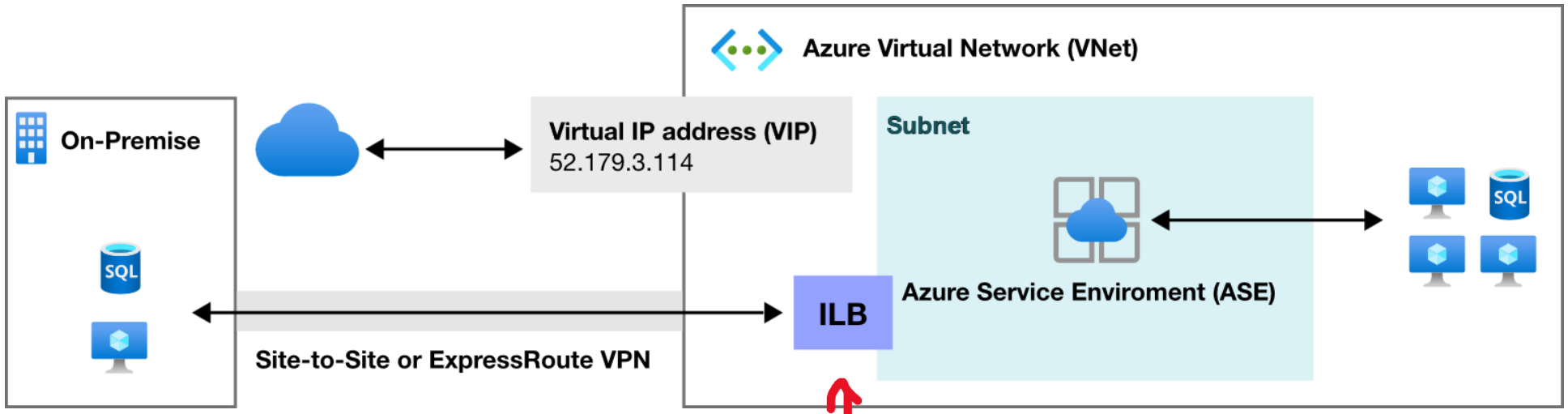
External ASE exposes the ASE-hosted apps on an **internet-accessible IP address**.



Because the ASE is within the VNet, it can also access resources within the VNet without any additional configuration.

If the VNet is connected to your on-premises network, apps in your ASE also have access to resources there without additional configuration.

Azure App Service – App Service Environment



ILB ASE exposes the ASE-hosted apps on an IP address inside your VNet.
The internal endpoint is an **internal load balancer (ILB)**

Azure App Service Plan

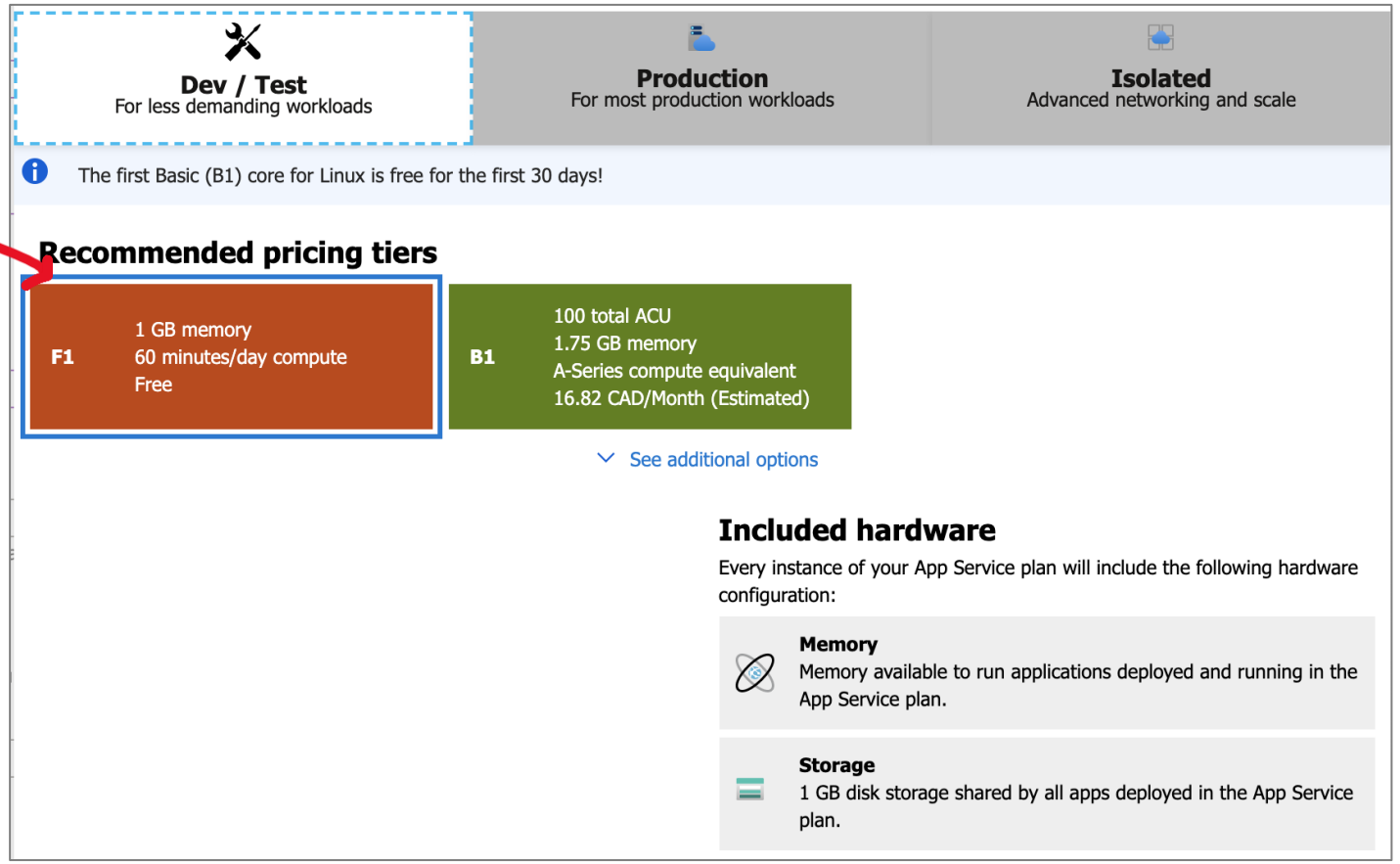
Azure App Service Plan defines **how you pay and what resources are available** to you.
There are **3 pricing tiers** for App Service Plan:

Shared Tiers
There are **2 shared:** Free, Shared

Free Tier provides:
- 1 GB of disk space
- up to 10 apps on a single shared instance
- No SLA for availability
- Each app has a compute quota of 60 minutes per day

Shared Tier provides
- up to 100 apps on a single shared instance
- No SLA for availability
- Each app has a compute quota of 240 minutes per day

Shared Tiers does not support Linux-based instances

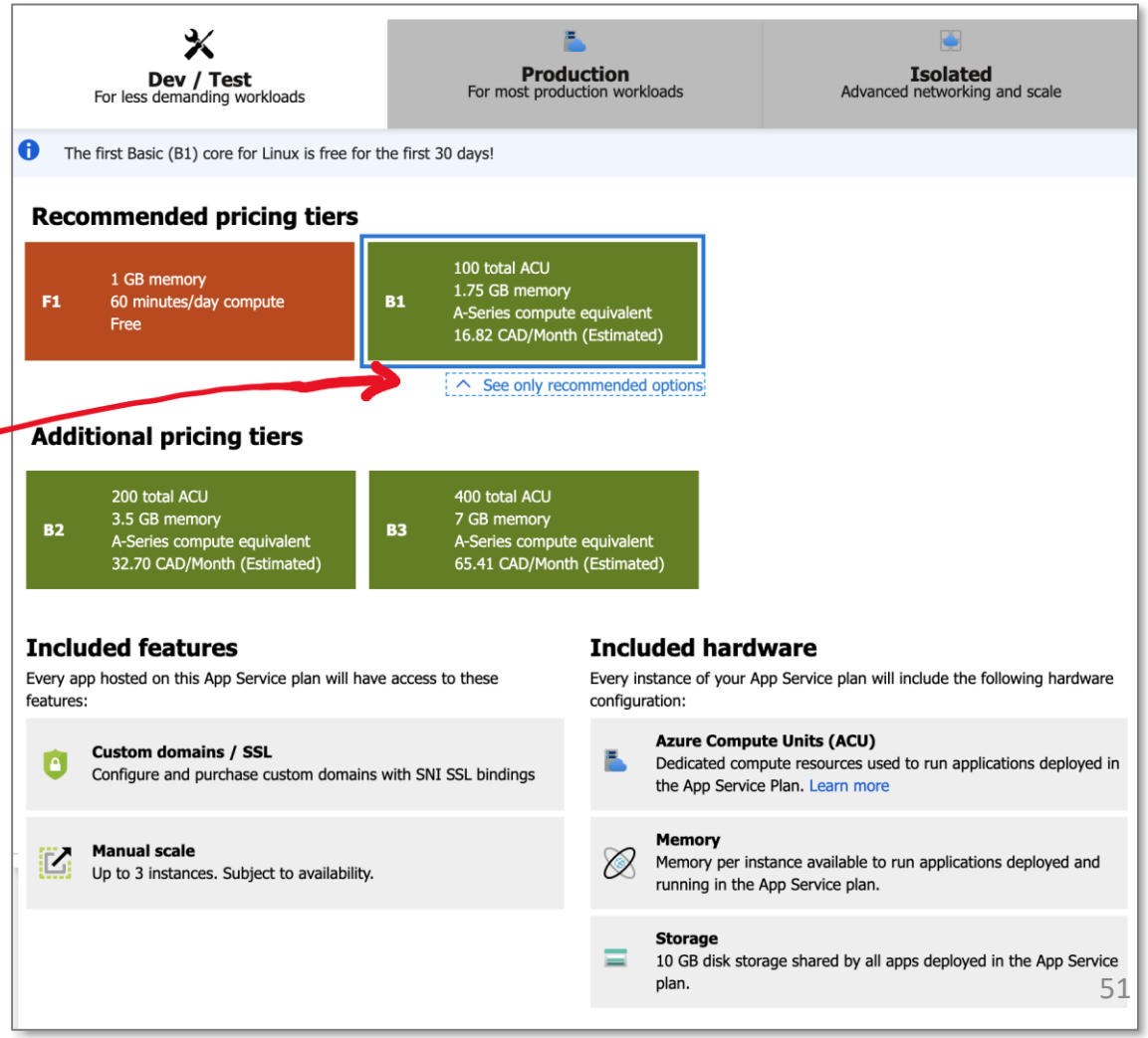


Azure App Service Plan

Azure App Service Plan defines **how you pay and what resources are available** to you.
There are **3 pricing tiers** for App Service Plan:

Dedicated Tiers
Basic, Standard, Premium, PremiumV2, PremiumV3

Basic
- More disk space
- Unlimited apps
- 3 levels in this tier that offer varying amounts of compute power, memory, and disk storage



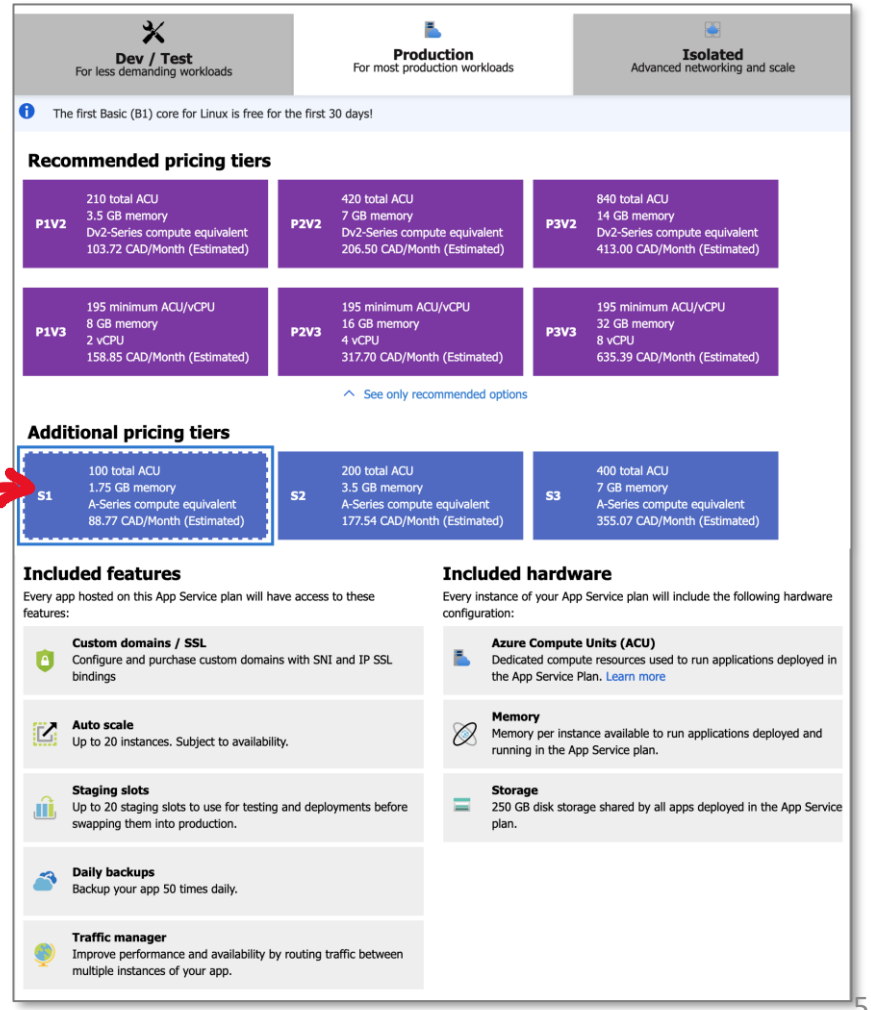
Azure App Service Plan

Azure App Service Plan defines **how you pay and what resources are available** to you.
There are **3 pricing tiers** for App Service Plan:

Dedicated Tiers
Basic, Standard, Premium, PremiumV2, PremiumV3

Basic
- More disk space
- Unlimited apps
- 3 levels in this tier that offer varying amounts of compute power, memory, and disk storage

Standard
- scale out to three dedicated instances
- SLA of 99.95% availability
- 3 levels in this tier that offer varying amounts of compute power, memory, and disk storage



Azure App Service Plan

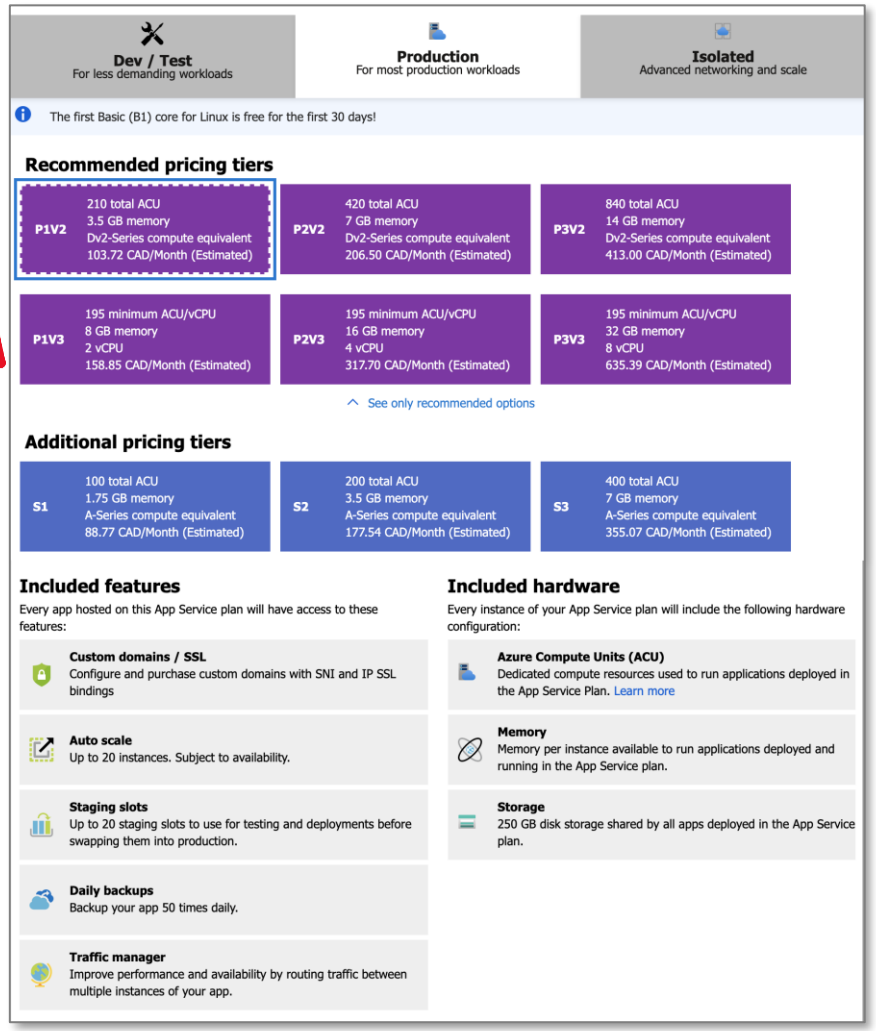
Azure App Service Plan defines **how you pay and what resources are available** to you.
There are **3 pricing tiers** for App Service Plan:

Dedicated Tiers
Basic, Standard, Premium, PremiumV2, PremiumV3

Basic
- More disk space
- Unlimited apps
- 3 levels in this tier that offer varying amounts of compute power, memory, and disk storage

Standard
- scale out to three dedicated instances
- SLA of 99.95% availability
- 3 levels in this tier that offer varying amounts of compute power, memory, and disk storage

Premium
- scale to 10 dedicated instances
- availability SLA of 99.95%
- multiple levels of hardware

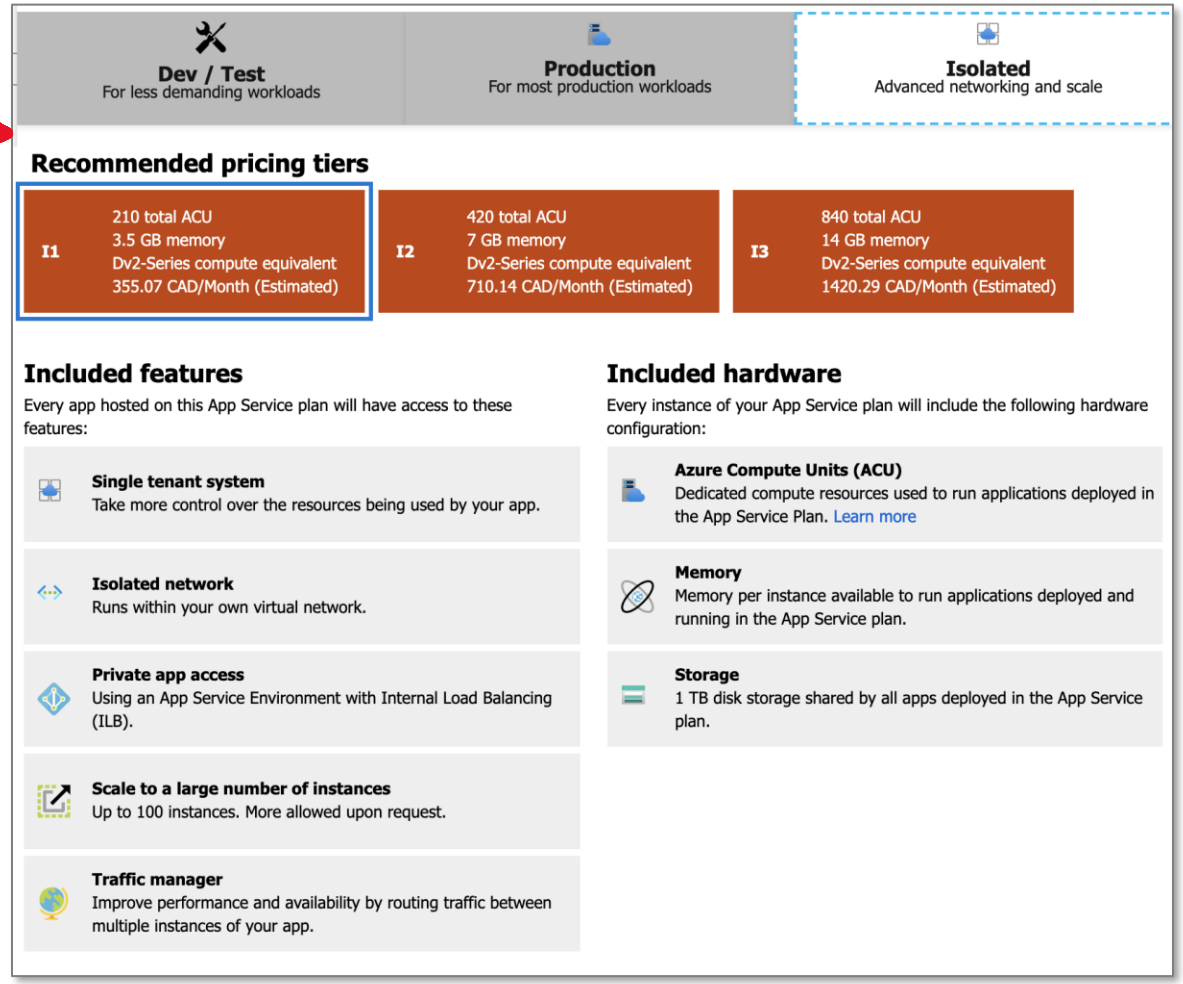


Azure App Service Plan

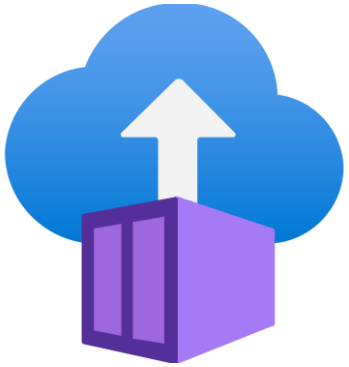
Azure App Service Plan defines **how you pay and what resources are available** to you.
There are **3 pricing tiers** for App Service Plan:

Isolated Tier

- dedicated Azure virtual network
- Full network and compute isolation
- scale out to 100 instances
- availability SLA of 99.95%



Azure Container Instances (ACI)



package, **deploy**, and **manage** cloud applications using **containers**

Fully Managed Docker as a Service

Introduction to ACI

Azure Container Instances (ACIs) allow you to **launch containers** without the need to worry about configuring or managing the underlying virtual machine

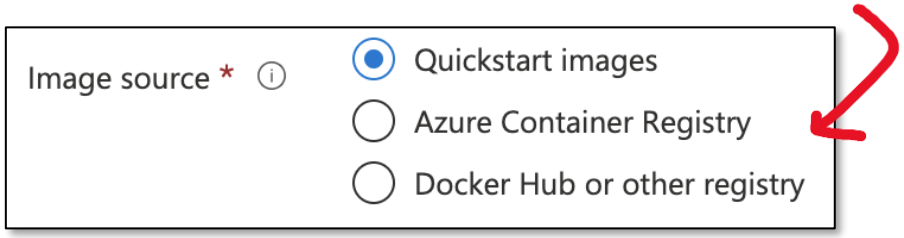
Azure Container Instances is designed for isolate containers:

- simple applications
- task automation
- build jobs

- Containers can be provisioned **within seconds** where VMs can take several minutes
- Containers are **billed per second** where VMs are billed per hour (greater savings)
- Containers have **granular and custom sizing of vCPUs, Memory and GPUs** where VMs sizes are predetermined
- ACI can deploy both **Windows** and **Linux** containers
- You can **persist storage with Azure Files** for your ACI containers
- ACIs are accessed via a fully qualified domain name (FQDN) eg *customlabel.azureregion*.azurecontainer.io.

Azure provides Quickstart images to start launching example applications but you can also **source** containers from:

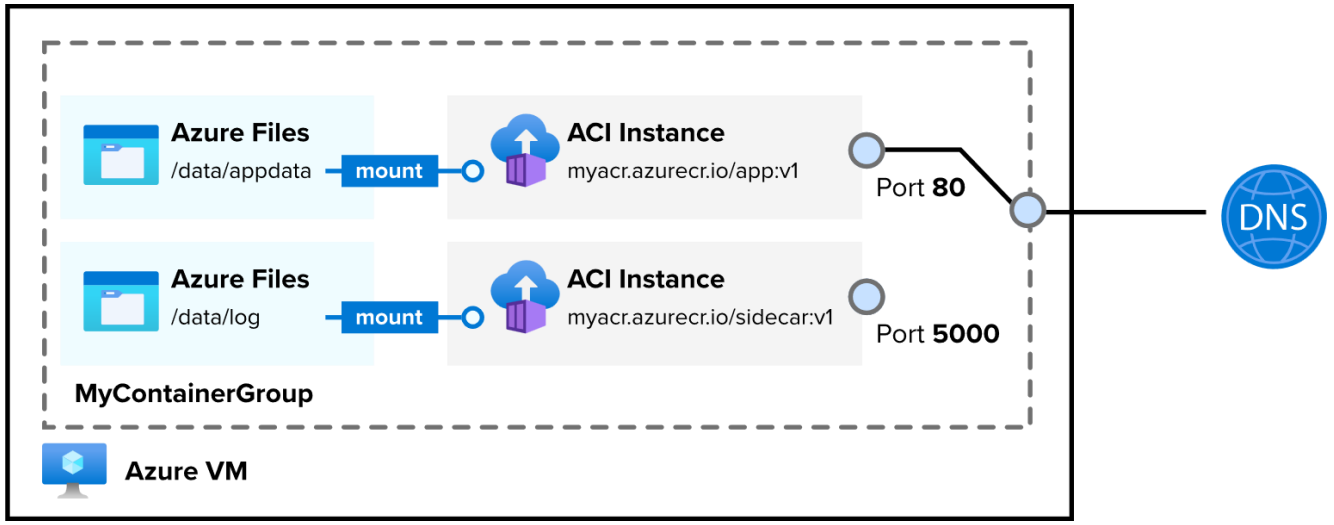
- Azure Container Registry
- Docker Hub
- Privately Hosted Container Registry



Introduction to ACI

Container Groups are collection of containers that get scheduled on the same host machine.
The containers in a container group share:

- lifecycle
- Resources
- local network
- storage volumes



*Container Groups are similar to a **Kubernetes pod***

Multi-container groups **currently support only** **Linux** containers.

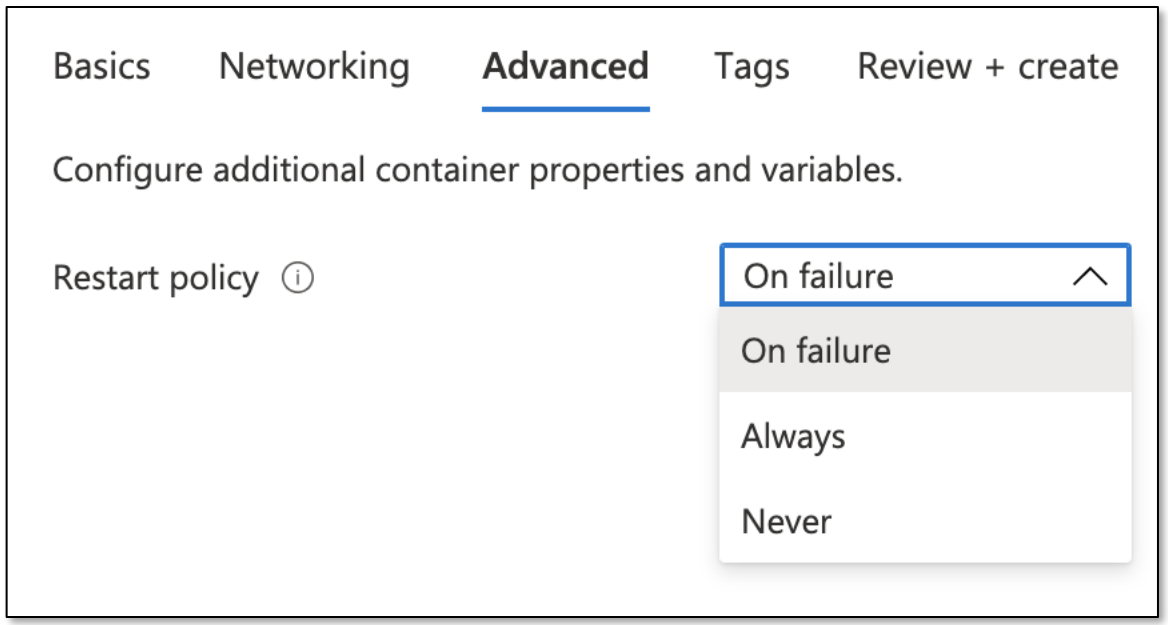
There are two ways to deploy a multi-container group:

- **Resource Manager Template (ARM template)** — when you need to deploy additional Azure service resources
- **YAML File** — when your deployment includes only container instances.

Container Restart Policies

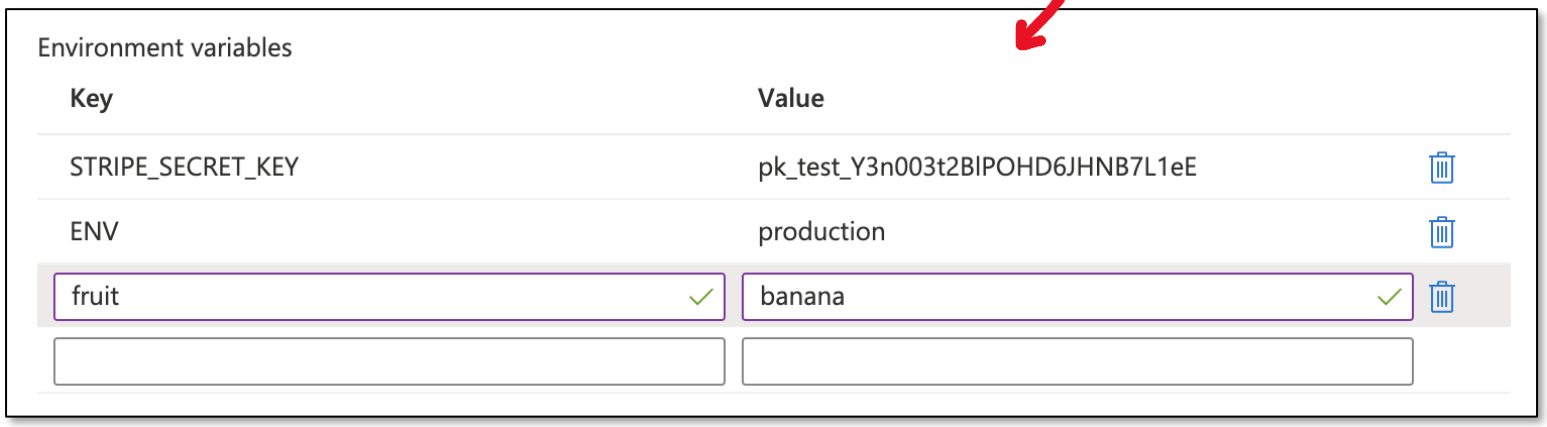
A container restart policy specifies what a container should do when their process has completed. Azure Container Instances has 3 restart-policy options:

- **Always** (default) Containers are **always restarted**. Suited for long running tasks eg. **web-servers**
- **Never** Containers **run one time only**. Suited for one off tasks. eg. **background jobs**
- **OnFailure** Containers that encounter an error



Container Environment Variables

Environment variables (Env Vars) allow you to pass configuration details to your containers.
Environment variables can be set via the **Azure Portal**, CLI or PowerShell



Secured Environment Variables
By default Environment Variables are store in plaintext.
If you need to secure your environment variables you can use the **--secure-environment-variables** flag

```
az container create \
  --resource-group aci-resource-group \
  --name aci-demo-secure \
  --image exampro/rails:backend \
  --ip-address Public \
  --location eastus \
  --secure-environment-variables \
    STRIPE_SECRET_KEY=$STRIPE_SECRET_KEY
```

Container Persistent Storage

Azure Containers are **stateless** by default.
When a container crashes or stops all state is loss.
To persist state you need to **mount** an external volume

You can mount **the following external volumes**:

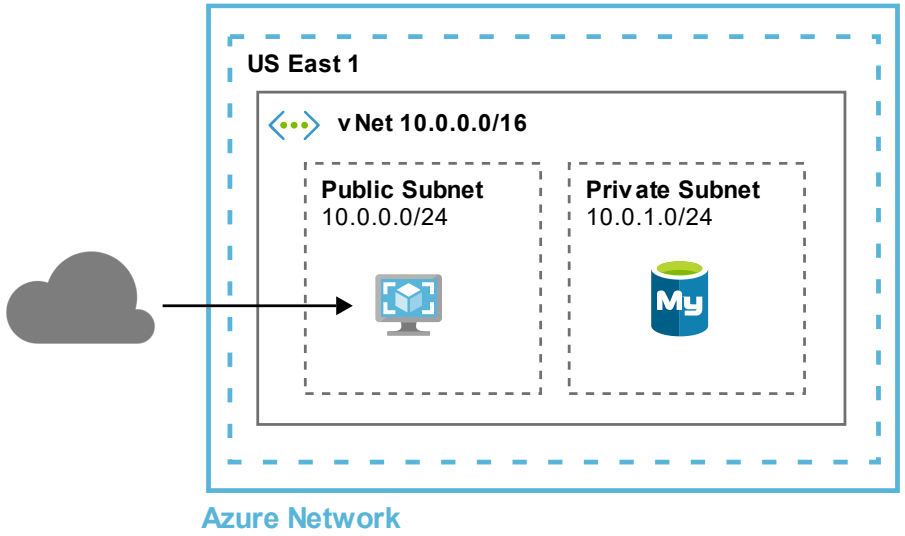
- Azure Files (file share)
- Secret volume
- Empty Directory
- Cloud git repo

To mount a file volume you need do this via PowerShell or CLI and specify the **details** to mount the drive

```
az container create \
  --resource-group exampro-resource-group \
  --name my-app \
  --image exampro/web-app \
  --location eastus \
  --ports 80 \
  --ip-address Public \
  --azure-file-volume-account-name $STORAGE_ACCOUNT_NAME \
  --azure-file-volume-account-key $STORAGE_KEY \
  --azure-file-volume-share-name my-fileshare \
  --azure-file-volume-mount-path /aci/logs/
```

Azure Virtual Network (VNet)

Virtual Network (vNet) is a logically isolated section of the Azure Network where you launch your Azure resources.



Azure DNS — manage your own DNS domain

Virtual Network (vNET) — logically isolated section of Azure network

- Address spaces
- Route Tables
- Subnets

Network Security Groups A virtual firewall at the subnet or NIC level

ExpressRoute A 50 Mbps-10 Gbps connection between on-premise to VNET

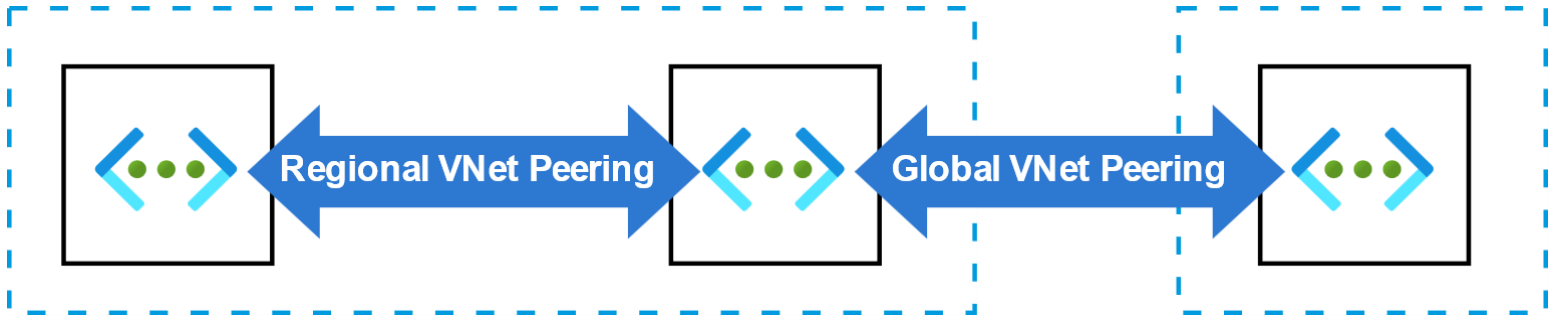
Virtual WAN a centralized network to route different network connections

Virtual Network Gateway - A site-to-site VPN connection between an VNet and local networks

Network Interfaces virtual network device to allow your VMs to communicate using IP protocols

VNeT Peering

VNET peering is when you connect multiple VNet so they act as one network.



There are 2 types of VNet Peering:

1. **Regional VNet Peering** When you peer two VNets from the same region
2. **Global VNet peering** When you peer two VNets from two different regions

Network Interfaces

What is a Network Interface?

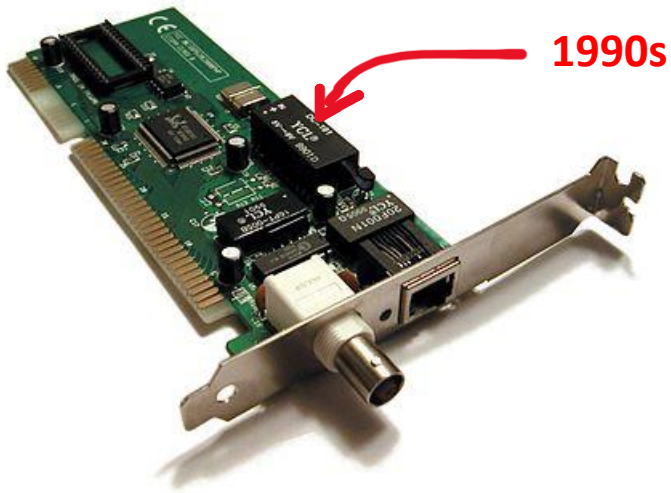
Software or hardware interface between two pieces of equipment or protocol layers in a computer network.

A Network Interface Controller (NIC)

A **computer hardware component** that connects a computer to a computer network.

Also known as:

- network interface card
- network adapter
- LAN adapter
- physical network interface

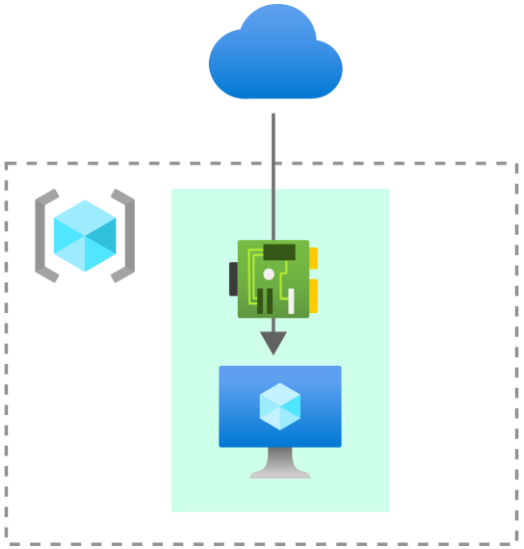


1990s Ethernet Interface Controller card

NICs are devices for both the:

- Data Link Layer (Layer 2)
- Physical Layer (Layer 1)

NICs communicate using **Internet Protocol (IP)**



Azure Network Interfaces (NICs)

Azure Network Interfaces are attached to Azure VM instance.

Without an NIC, An Azure VM instance would have no way to communicate.

An Azure VM instance has to have an NIC and can have multiple NICs.

VNeT – Subnets

What is a Subnet?
A subnet is **a logical division of an address space**. Subnets help you **define different kinds of workloads** and allows you to apply virtual isolation within your network. When you launch an Azure resource you choose the subnet you want to launch within and an IP from that subnet is assigned to your resource

Associating a Route Table
A subnet needs a Route Table so it can access

Public vs Private Subnet
Public and Private subnet describes whether a subnet is reachable from the internet or not.
Azure **has no concept of private and public subnets** and its up to you to configure our subnets to have ensure they do no reach the internet by ensuring they have no route via the their route table to the Internet Gateway

Associating Network Security Gateways (NSG)
You can associate an NSG to protect traffic entering and leaving your subnet by applying security rules that can Allow or deny access based on IP address, port and protocol.

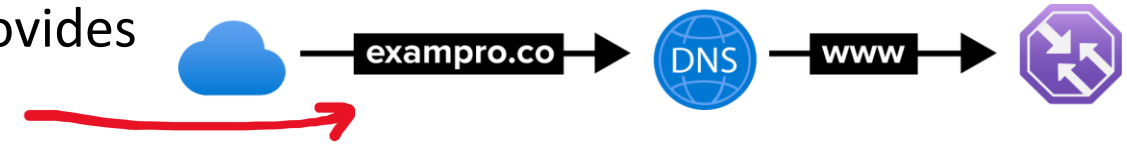
Gateway Subnet
Azure has a special type of Gateway Subnet that is used by **Azure Virtual Network Gateway** and that service Launches specialized VMs into that subnet.

Azure DNS

What is a Domain Name System (DNS)?

It is a service that is responsible for **translating (or resolving) a service name** to its IP address.

Azure DNS is a **hosting service** for **DNS domains** that provides name resolution by using Microsoft Azure infrastructure



Public DNS Internet-facing

- Allows you to manage domains for internet accessible domains
  - Pointing your domain to your website
  - Setting records to prove you own the domain
  - Records to connect you domain to your email server

Private DNS Internal-facing

- Allow you to use your own custom domains instead of the Azure provided domains
  - Many Azure Services use fully qualified domain name (FQDN) to identify services on the network.
    - eg. Azure Storage Accounts FQDN: **http://storageaccount.file.core.windows.net/**

You **can't use** Azure DNS **to buy a domain** name.

You can purchase a domain in App Services or a third-party provider and have Azure DNS manage

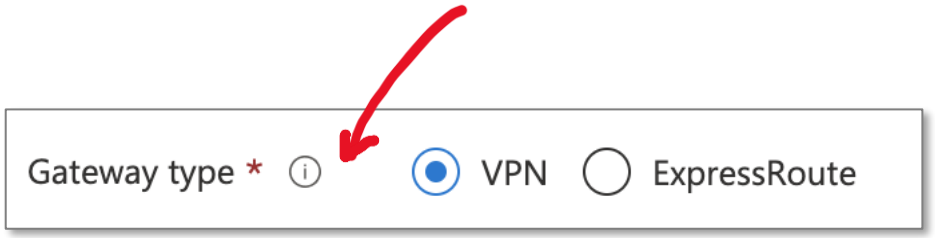
Virtual Network Gateways

What is a (Virtual Private Network) VPN?

A VPN **extends a private network across a public network** and enables users **to send and receive data across shared or public networks** as if their computing devices were directly connected to the private network.

What is a Virtual Network Gateway?

- A **virtual network gateway** is the software **VPN** device for your Azure virtual network.
- When you deploy a virtual network gateway it will deploy two or specialized VMs in specific subnet you need to create called a "gateway subnet"
- These deployed VMs contain routing tables and run specific gateway services.
- You will choose a **Gateway Type** and that will determine if it's a VPN Gateway or an ExpressRoute Gateway



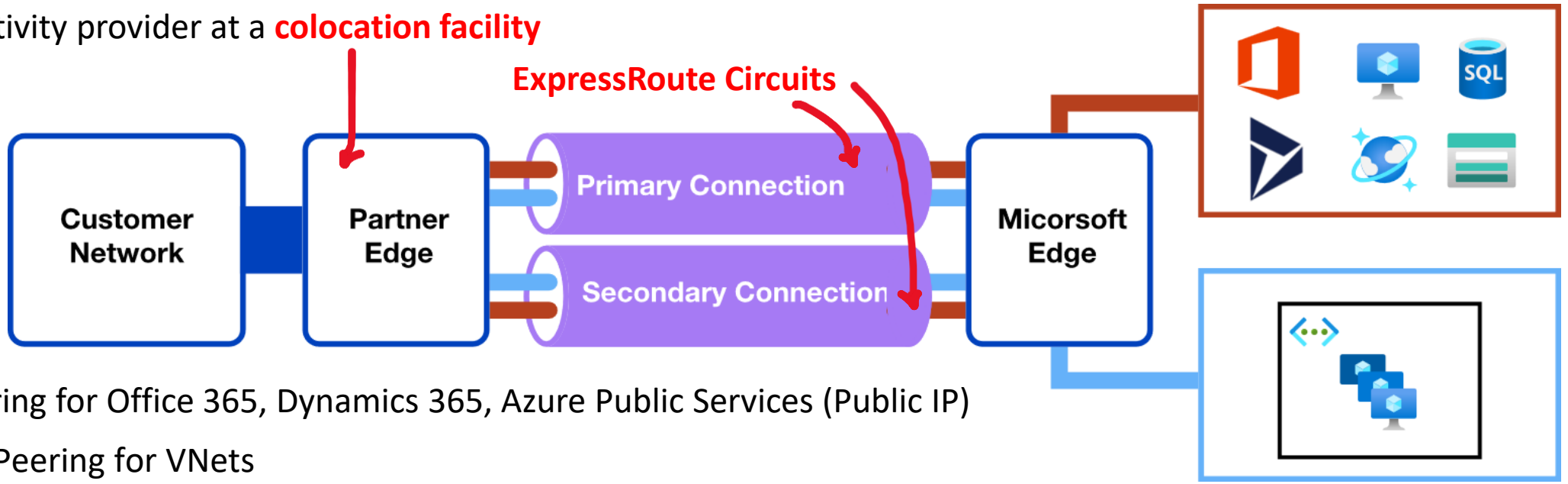
Azure ExpressRoute

Azure ExpressRoutes creates **private connections** between Azure datacenters and infrastructure on your premises or in a colocation environment

Connectivity options include:
- any-to-any (IP VPN) networks
- point-to-point Ethernet networks
- virtual cross-connection

through a connectivity provider at a **colocation facility**

ExpressRoute connections don't traverse the public Internet, ensuring **enhanced reliability**, **faster speeds**, **consistent latencies**, and **heightened security** compared to traditional internet connections.



Microsoft Peering for Office 365, Dynamics 365, Azure Public Services (Public IP)

Azure Private Peering for VNets

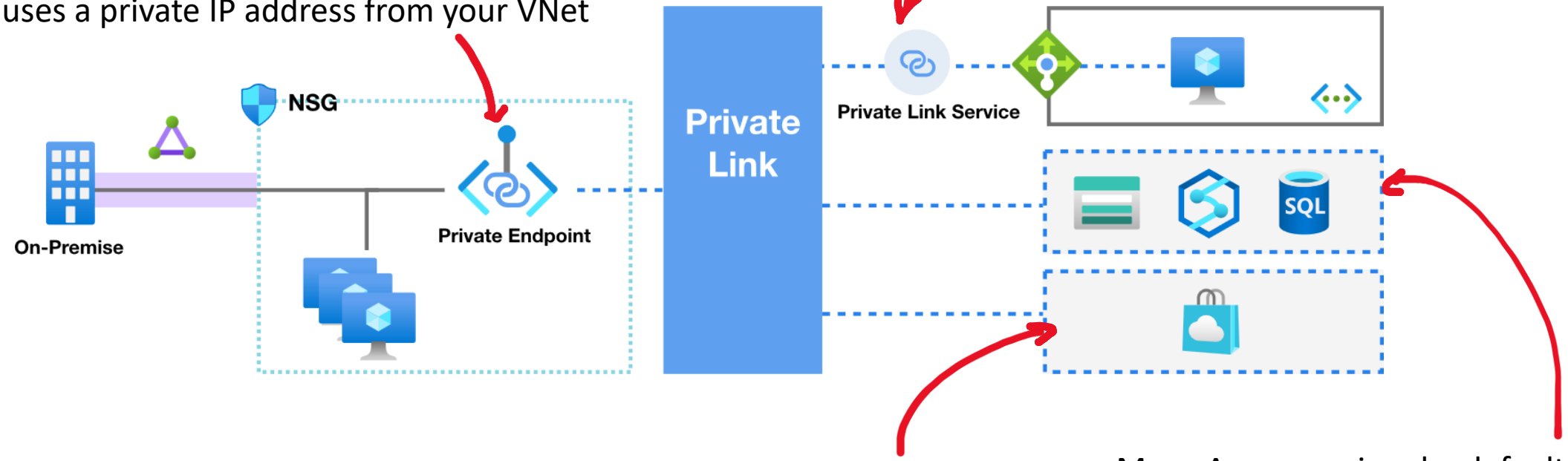
ExpressRoute Direct allows for **greater bandwidth connections** from 50 Mbps to 10 Gbps. Ideal where for hybrid solutions with massive amounts of data or where latency matters.

Private Links

Azure Private Links allows you to **establish secure connections** between Azure resources so traffic **remains within the Azure Network**

Private Link Endpoint is an **Network Interface** that connects you privately and securely to a service powered by Azure Private Link. Private Endpoint uses a private IP address from your VNet

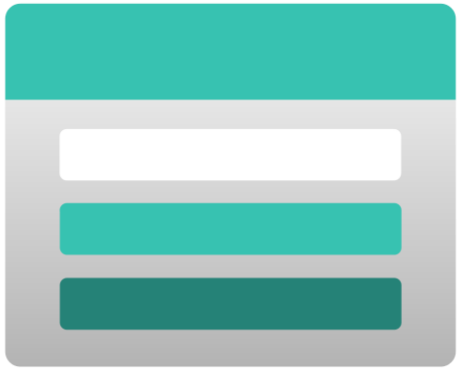
Private Link Service allows you to connect your own workload to Private Link**.** You need an **Azure Standard Internal Load Balancer** and associate it with the Link Service



Third-Party provides can be powered by Private Link

Many Azure services by default work with Private Link eg. Azure Storage, CosmoDB, SQL

Azure Storage Accounts



Contains all of your Azure Storage data objects:
blobs, **files**, **queues**, **tables**, and **disks**

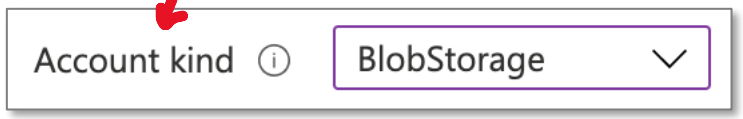
Introduction to Storage Accounts

Azure Storage offers **several types of storage** accounts.

Each with **different features** and **their own pricing models**

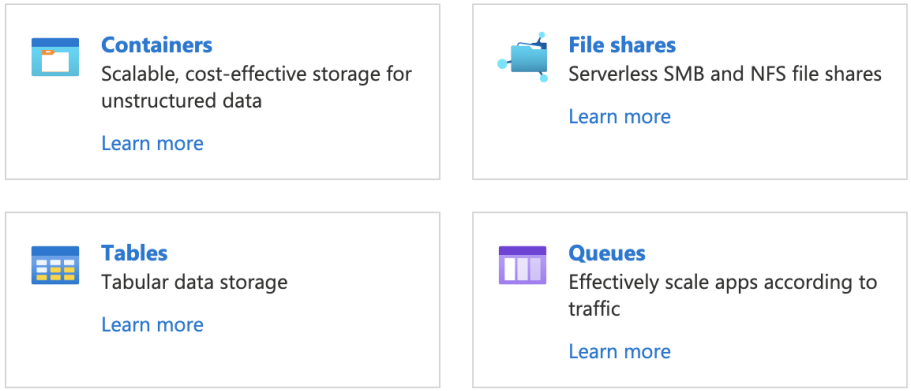
- General-purpose v1 (legacy)
- General-purpose v2
- BlobStorage (legacy)
- BlockBlobStorage
- FileStorage

Storage type and **Account Kind** means the same thing



Storage accounts vary with the following features:

Supported Services (What can I put in this storage account?)
Blob, File, Queue, Table, **Disk**, and Data Lake Gen2



Performance Tiers (how fast will my read and writes be?)
Standard and Premium

Access Tiers (how often do I need quick access to files?)
Hot, Cool, Archive

Replication (How many redundant copies should be made and where?)
LRS, GRS, RA-GRS, ZRS, GZRS, RA-GZRS

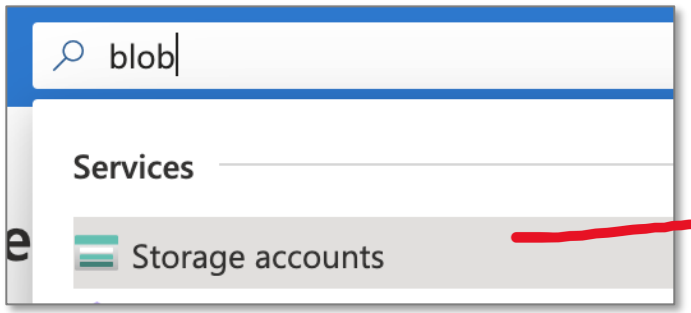
Deployment model (Who should deploy the supported services?)
Resource Manager, Classic

Introduction to Storage Accounts

Type	Service	Performance Tiers	Access Tiers	Replication	Deployment Models
General-purpose V2	Blob, File, Queue, Table, Disk, Data Lake Gen 2	Standard, Premium	Hot, Cool, Archive	LRS, GRS, RA-GRS, ZRS, GZRS, RA-GZRS	Resource Manager
General-purpose V1	Blob, File, Queue, Table, Disk	Standard, Premium	N/A	LRS, GRS, RA-GRS	Resource Manager **Classic**
BlockBlobStorage	Blob (block, append)	Premium	N/A	LRS, ZRS	Resource Manager
FileStorage	File	Premium	N/A	LRS, ZRS	Resource Manager
BlobStorage	Blob (Block, append)	Standard	Hot, Cool, Archive	LRS, GRS, RA-GRS	Resource Manager

Core Storage Services

Azure has **5 core storage** services

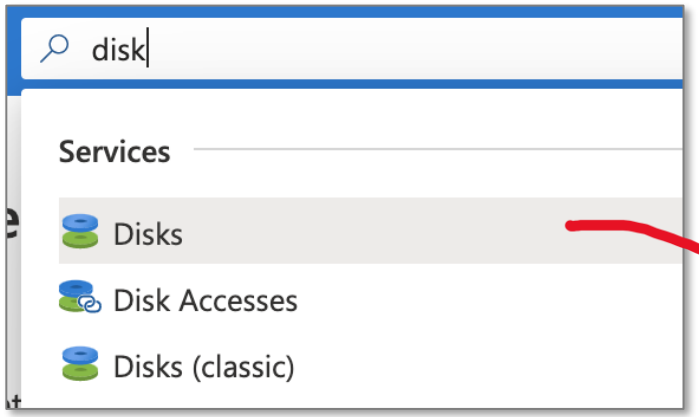


Azure Blob
A massively scalable **object store** for text and binary data.
Also includes support for big data analytics through Data Lake Storage Gen2

Azure Files
Managed **file shares** for cloud or on-premises deployments

Azure Queues
A **messaging store** for reliable messaging between application components

Azure Tables
A **NoSQL store** for schemaless storage of structured data.



Azure Disks
Block-level storage volumes for Azure VMs

Performance Tiers (Blob Storage)

There are **2 types** of performance tiers for storage accounts: Standard and Premium

IOPS stands for Input/Output Operations Per Second
The higher the IOPS the faster a drive can read and write

Premium Performance

- Stored on Solid State Drives **(SSDs)**
- Optimize for low-latency
- Higher throughput
- Use cases:
  - Interactive workloads
  - Analytics
  - AI or ML
  - Data transformation

An SSD **has no moving parts** and data is distributed randomly. This is why it can read and write so fast.

Standard Performance

- Stored on Hard Disk Drives **(HDDs)**
- Varied performance based on access tier (Hot, Cool, Archive)

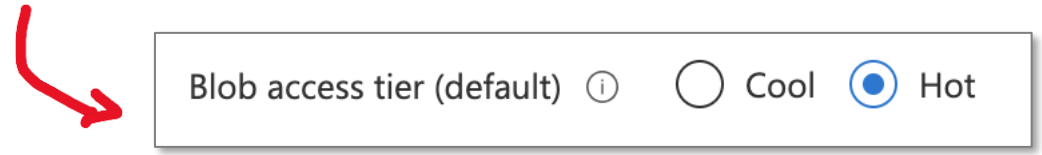
Use cases:

- Backup and disaster recovery
- Media content
- Bulk data processing

An HDD **has moving parts**, an arm that needs to read and write data sequential to a disk. It is very good a writing or reading large amounts of data that is close together

Access Tiers (Blob Storage)

There are **3 types** of access tiers for **Standard storage**: Cool, Hot and Archive



Hot
- Data that's accessed frequently.
- Highest storage cost, lowest access cost

Use Case
- Data that's in active use or expected to be accessed frequently.
- Data that's staged for processing and eventual migration to the cool access tier

Cool
- Data that's infrequently accessed and stored for at least 30 days.
- Lower storage cost, higher access cost

Use Case
- Short-term backup and disaster recovery datasets
- Older media content not viewed frequently anymore but is expected to be available immediately when accessed
- Large data sets that need to be stored cost effectively while more data is being gathered for future processing.

Archive
- Data that's rarely accessed and stored for at least 180 days
- Lowest storage cost, highest access cost

Use Case
- Long-term backup, secondary backup, and archival datasets
- Original (raw) data that must be preserved, even after it has been processed into final usable form.
- Compliance and archival data that needs to be stored for a long time and is hardly ever accessed.

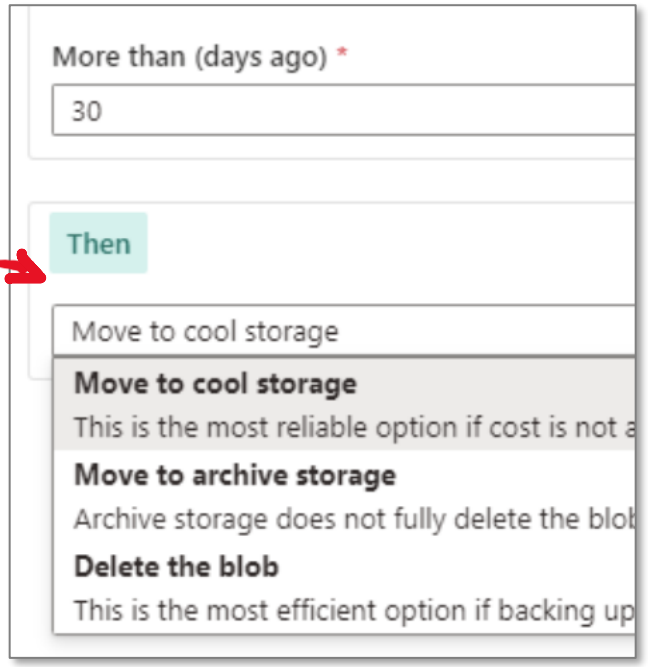
Access Tiers (Blob Storage)

Account Level Tiering
Any blob that doesn't have an explicitly assigned tier infers the tier from the Storage Account access tier setting.

Blob-Level Tiering
You can upload a blob to the tier of your choice.
Changing tiers happens instantly with the exception from moving out of archive

Rehydrating a Blob
When moving a blob out of archive into another tier it can take several hours. This is known as **"rehydrating"**

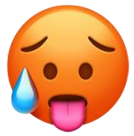
Blob Lifecycle Management
You can create role-based policies to transition data to different tiers
Eg. After 30 days move to cool storage



Access Tiers (Blob Storage)

When a blob is uploaded or moved to another tier
It's charged at the new tier's rate **immediately** upon tier change.

When moving from a **cooler tier:**
The operation is billed as a **write operation** to the destination tier.
Where the write operation (per 10,000) and data write (per GB) charges of the destination tier apply.

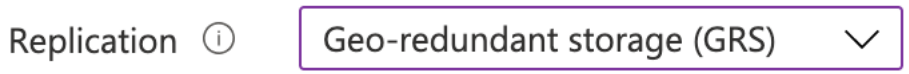


When moving from a **hotter tier**
The operation is billed as a read from the source tier
Where the **read operation** (per 10,000) and data retrieval (per GB) charges of the source tier apply
Early deletion charges for any blob moved out of the cool or archive tier may apply as well

Cool and archive early deletion
Any blob that is moved into the cool tier (GPv2 accounts only) is subject to a cool early deletion period of 30 days.
Any blob that is moved into the archive tier is subject to an archive early deletion period of 180 days. This charge is prorated.

Replication and Data Redundancy

When you create a Storage Account you need to choose a **Replication Type**



Replication stores multiple copies of your data so that it is **protected from**:

- planned events
- transient hardware failures
- network or power outages
- massive natural disasters

The greater level of redundancy the more expensive the cost of replication

$

$$

$$$

Primary Region Redundancy

- Locally Redundant Storage (LRS)
- Zone-redundant storage (ZRS)

Disaster Recovery and Failovers

Secondary Region Redundancy

- Geo redundant storage (GRS)
- Geo-zone-redundant storage (GZRS)

Disaster Recovery and Failovers

Secondary Region **Redundancy with Read Access**

- Read-access geo-redundant storage (RA- GRS)
- Read-access geo-redundant storage (RA-GZRS)

Read Replicas

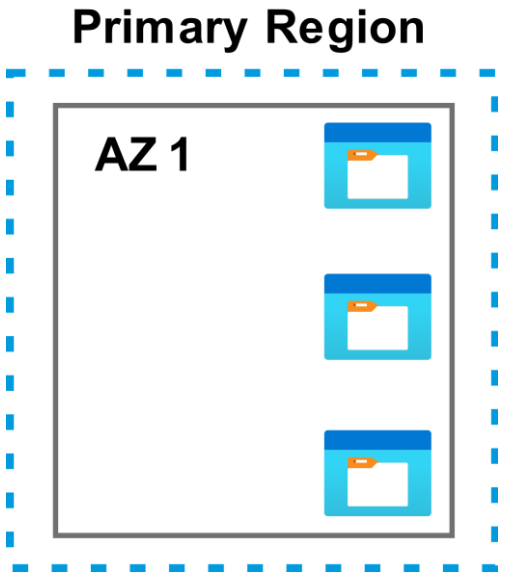
Replication and Data Redundancy

Redundancy in the Primary Region

- Data is replicated **3 times** in the primary region
- There are **two options** for storing in the primary region

Locally Redundant Storage **(LRS)**

- Copies data **synchronously** in primary region
- 99.999999999% (11 nines) durability
- **Cheapest option**



Zone-redundant storage **(ZRS)**

- Copies data **synchronously** **across 3 AZs** in primary region
- 99.9999999999% (12 9's) durability

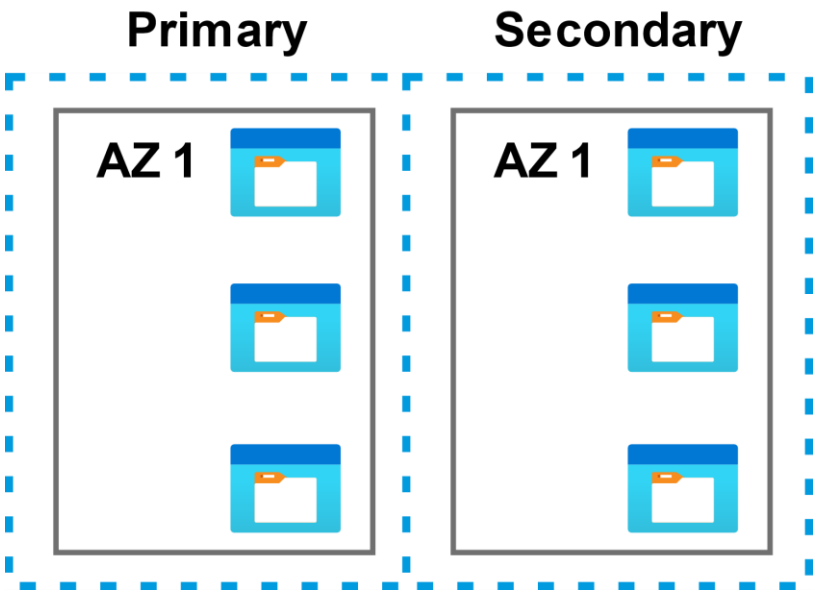
Replication and Data Redundancy

Redundancy in the Secondary Region

- Replicate to a secondary region in case of primary regional disaster
- The secondary region is determined based on your primary's pair region
- Secondary region isn't available for read or write access (except in event of failover)

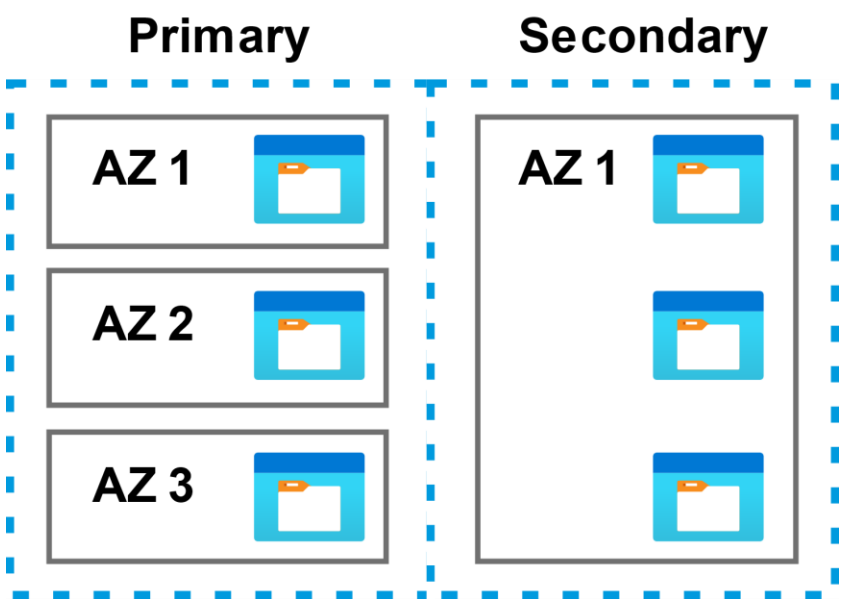
Geo Redundant Storage **(GRS)**

- Copies data **synchronously** in primary region
- Copies data **asynchronously** to another region
- 99.99999999999999% (16 9's) of durability



Geo-Zone-redundant storage **(GZRS)**

- Copies data **synchronously across 3 AZs** in a physical region
- Copies data **asynchronously** to another region
- 99.99999999999999% (16 9's) of durability



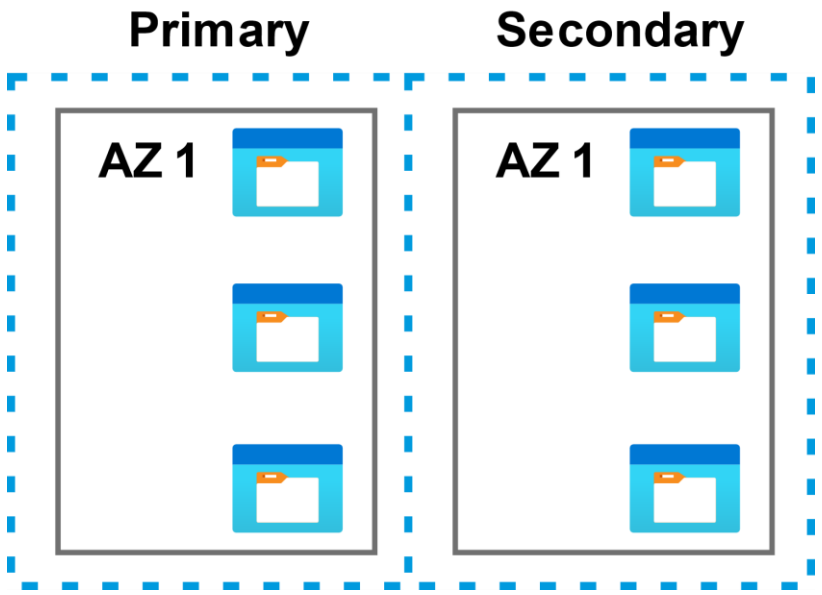
Replication and Data Redundancy

Redundancy in the Secondary Region with Read Access

- Data is replicated **synchronously** to primary region
- Your data will be "in-sync" with your primary and you'll have **read access**.

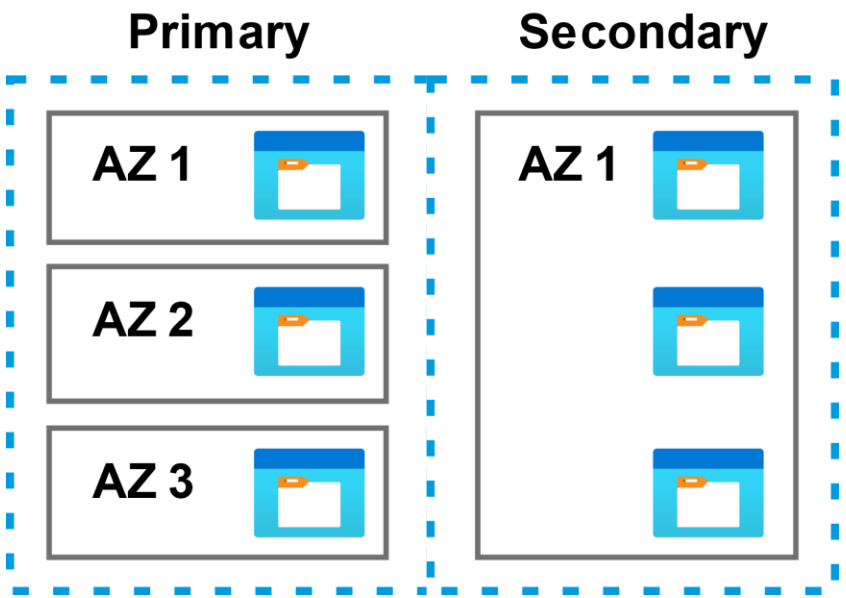
Read-Access Geo Redundant Storage **(RA-GRS)**

- Copies data **synchronously** in primary region
- Copies data **synchronously** to another region
- 99.99999999999999% (16 9's) of durability



Read-Access Geo-Zone-redundant storage **(RA-GZRS)**

- Copies data **synchronously** **across 3 AZs** in a physical region
- Copies data **synchronously** to another region
- 99.99999999999999% (16 9's) of durability



AZCopy

AZCopy is a **command-line utility** that you can use to copy blobs or files to or from a storage account.

1. Its an executable file you download

Download AzCopy

First, download the AzCopy V10 executable executable file, so there's nothing to install.

- Windows 64-bit (zip)
- Windows 32-bit (zip)
- Linux x86-64 (tar)
- macOS (zip)

2. You will need to have the level of authorization via attached roles:

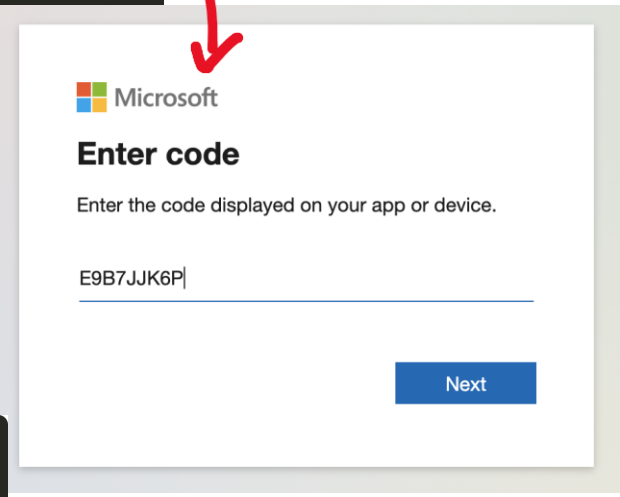
To download
- Storage Blob Data Reader

To upload:
- Storage Blob Data Contributor
- Storage Blob Data Owner

3. You gain access either via:

1. Azure Active Directory (AD)
2. Shared Access Signature (SAS)

```
~: azcopy login
To sign in, use a web browser to open the
page https://microsoft.com/devicelogin and
enter the code E9B7JJK6P to authentic
```



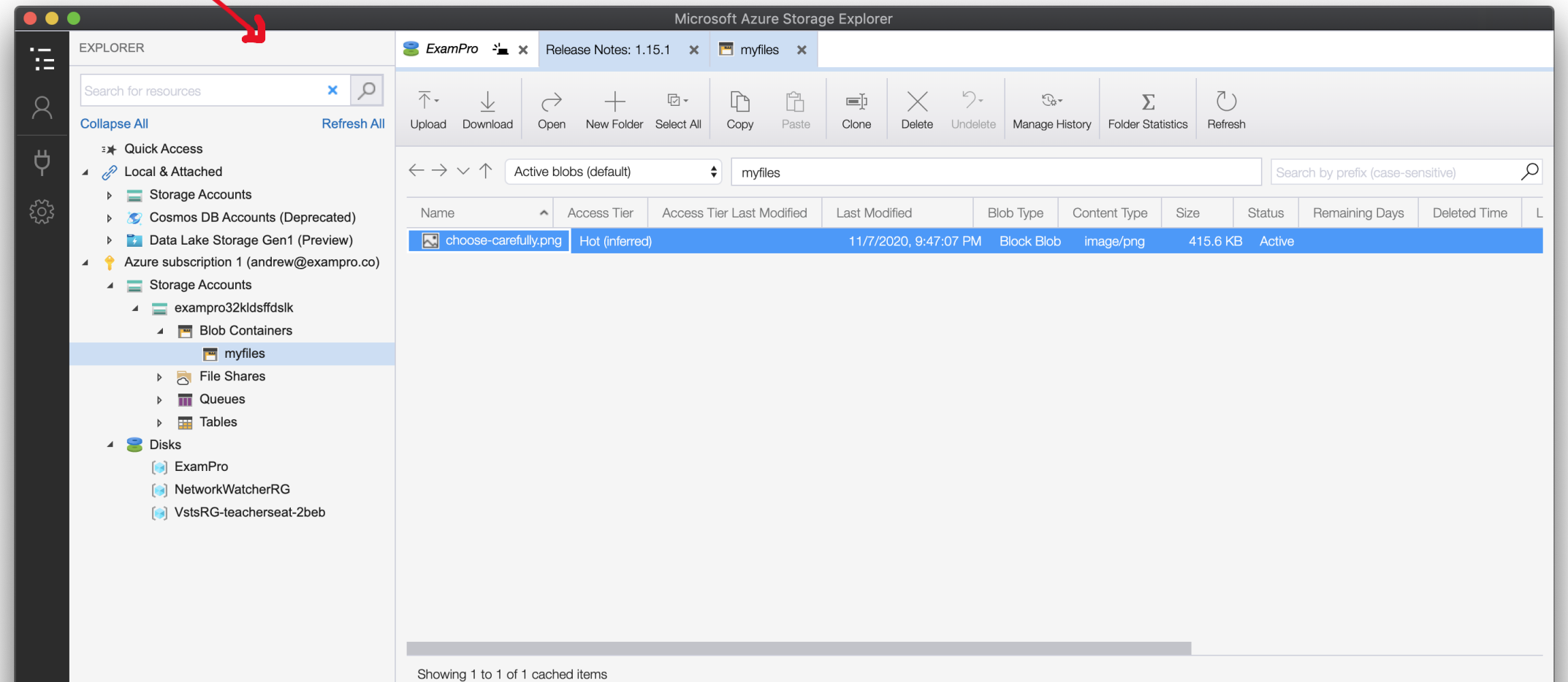
4. Use the Copy command to upload and download

```
azcopy copy \
'C:\StarTrek\jodri.txt' \
'https://enterprise.blob.core.windows.net/mycontainer/jodri.txt'
```

```
azcopy copy \
'https://enterprise.blob.core.windows.net/mycontainer/jodri.txt' \
'C:\StarTrek\jodri.txt'
```

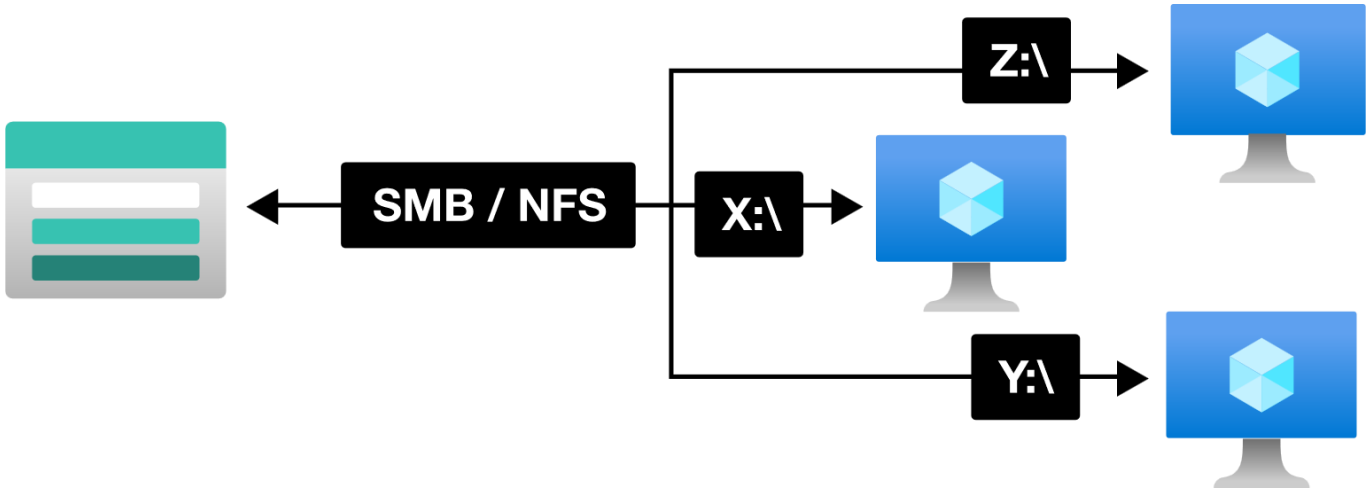
Azure Storage Explorer

A **standalone app** that makes it easy to work with Azure Storage data on Windows, macOS, and Linux.
You can create Blob containers, upload files, create snapshots of Disk, and more!



Azure Files

Azure Files is a fully managed **file share** in the cloud.
A file share is a **centralized server for storage** that allows **multiple connections**.
It like having one big shared drive that everyone (Virtual Machines) can work on at the same time.



To connect to the file share a **network protocol** is used:

- Server Message Block (SMB)
- Network File System (NFS)

When a connection is established the file share's filesystem will be accessible in the specific directory within your own directory tree. This is knowing as **mounting**

Azure Files – Use Cases

Use Cases

- Completely **replace or supplement** on-premises file servers Network Attach Storage (NAS) devices
- **Lift-and-Shift** your on-premise storage to the cloud via Classic Lift or Hybrid Lift
  - "Lift-and-Shift" means when you move workloads without rearchitecting, eg. importing local VMs to the cloud
  - Classic Lift — where both the application and its data are moved to Azure
  - Hybrid Lift — where the application data is moved to Azure Files, and the application continues to run on-premises
- **Simplify cloud development**
  - Shared application settings — Multiple VMs and developer workstations need to access the same config files.
  - Diagnostic share — All VMs log to the file share, developers can mount and debug all logs in a centralized place
  - Dev/Test/Debug — Quickly share tools for developer needed for local environments
- **Containerization**
  - You can use Azure Files to persist volumes for stateful containers

Why use Azure files instead of setting up your own File Share server?

- **Shared Access** — Already setup to work with standard networking protocols SMB and NFS
- **Fully managed** — Its kept up to date with security patches, designed to scale
- **Scripting and Tooling** — You can automate the management and creation of file shared with Azure API and PowerShell
- **Resiliency** — Build to be durable and always working

Azure Files

Backups

You can backup your file share with **shared snapshots**

- The are read-only
- Incremental (they only contain as much data as has changed since the previous snapshot)
- You can have up to **200 snapshots** per file share
- You can retain backups for **up to 10 years**
- Backups are stored within your file share (if you delete your file share you will delete your backups)

Soft Delete

You can prevent accidental deletion by turning on Soft Delete (Storage will be marked for deletion and retained for a period of time before final delete occurs

Advanced Threat Protection (ATP)

An additional layer of security intelligence that provides alerts when it detects anomalous activity on your storage account

Store Tiers:

- **Premium —** Store on to SSD with single-digit milliseconds for most IO operation
- **Transaction optimized** — Store on HDD with transaction heavy workloads that don't need the latency offered by premium file shares (historically this tier has been called **standard**)
- **Hot —** optimized for general purpose file sharing scenarios such as **team shares** and **Azure File Sync**.
- **Cool** — Stored on HDD for cost-efficient storage optimized for online archive storage scenario

Azure Files

Types of Storage

- **General purpose version 2 (GPv2)** — deployed on to HDD
- **FileStorage** — deployed onto SSD

Identity

- **On-Premise: —**Azure Storage can be joined to an on-premise Active Directory Domain Service
- **Managed —** Azure Storage can be joined to Microsoft managed Active Directory Domain Service
- **Store Account Key** — A username (storage account name) and password (account key) can be used to mount

Networking

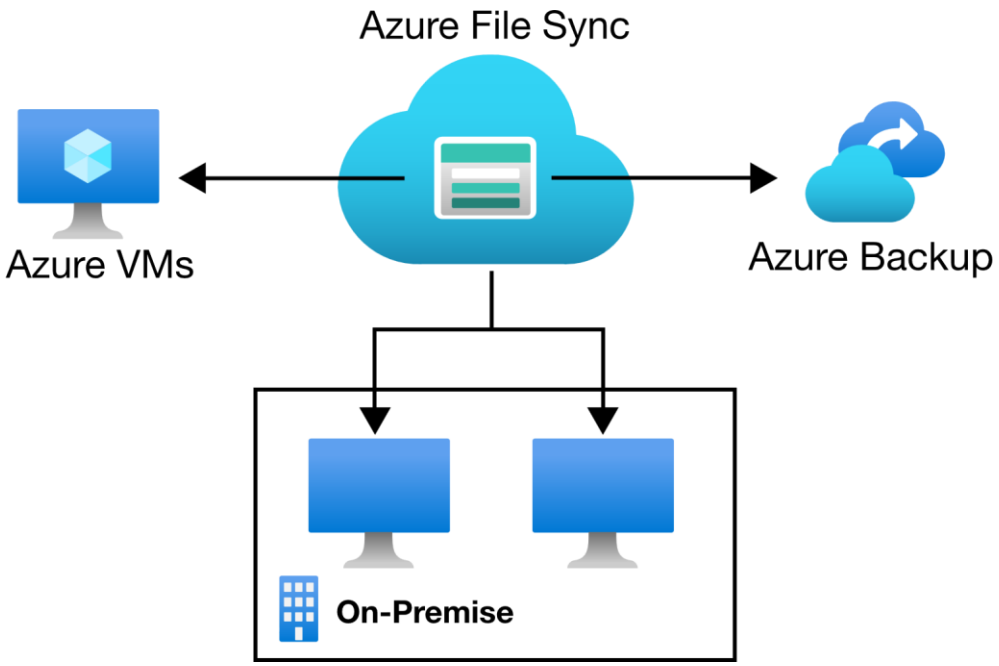
- Azure Files are accessible inside or outside your AWS Account from anywhere via storage account **public endpoint**.
- SMB connects to **port 445**, your organization may need to unblock this port so you can mount your file share

Encryption

- Azure Files is **encrypted-at-rest** using Azure Storage Service Encryption (SSE)
- Azure Files is **encrypted-in-transit** with SMB 3.0+ with encryption or HTTPS

Azure File Sync

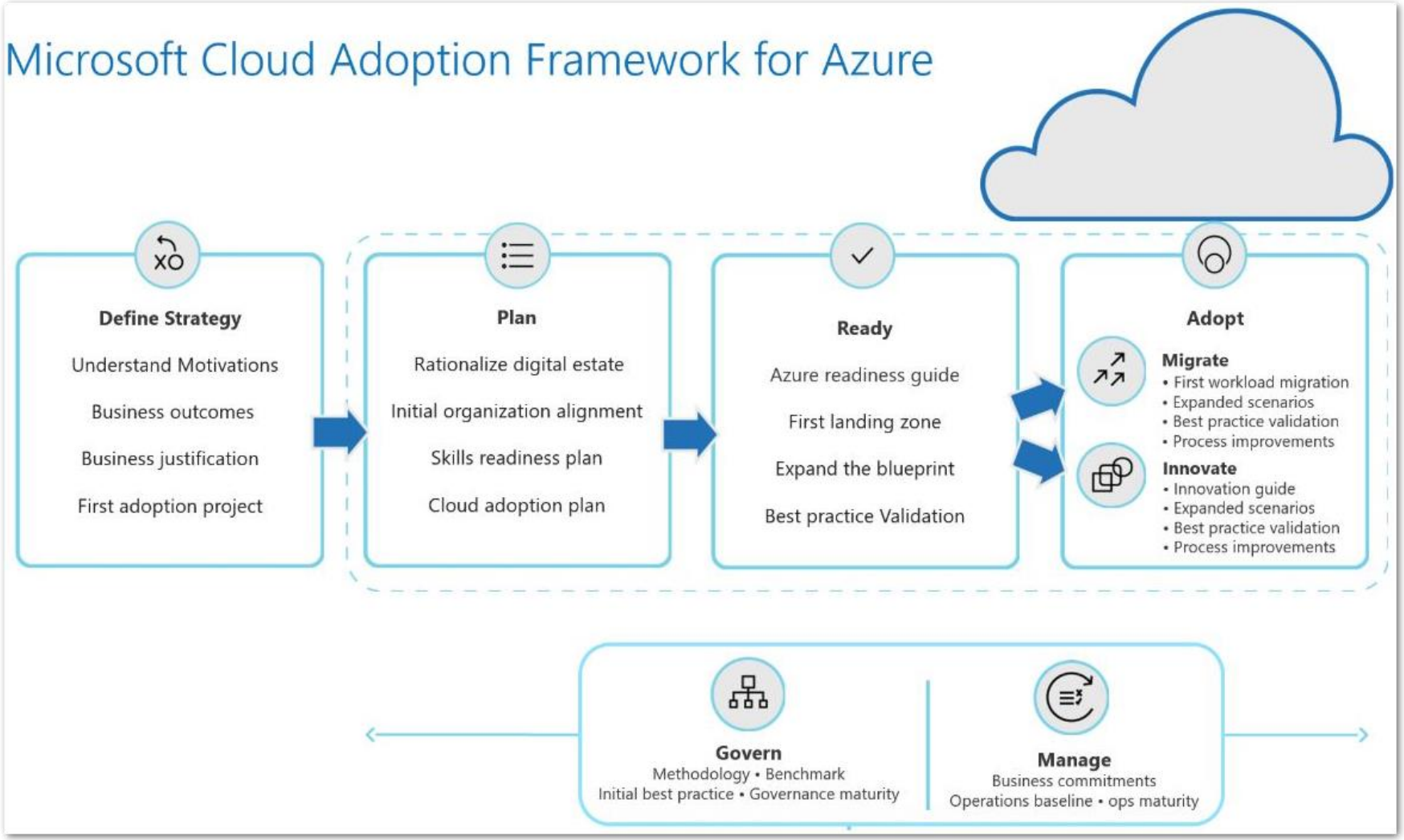
Azure File Sync is a service that allows you to **cache** Azure file shares on an **on-premises Windows Server** or **cloud VM**.



- You can use any protocol that's available on Windows Server to access your data locally, including SMB, NFS, and FTPS
- You can have as many caches as you need across the world.

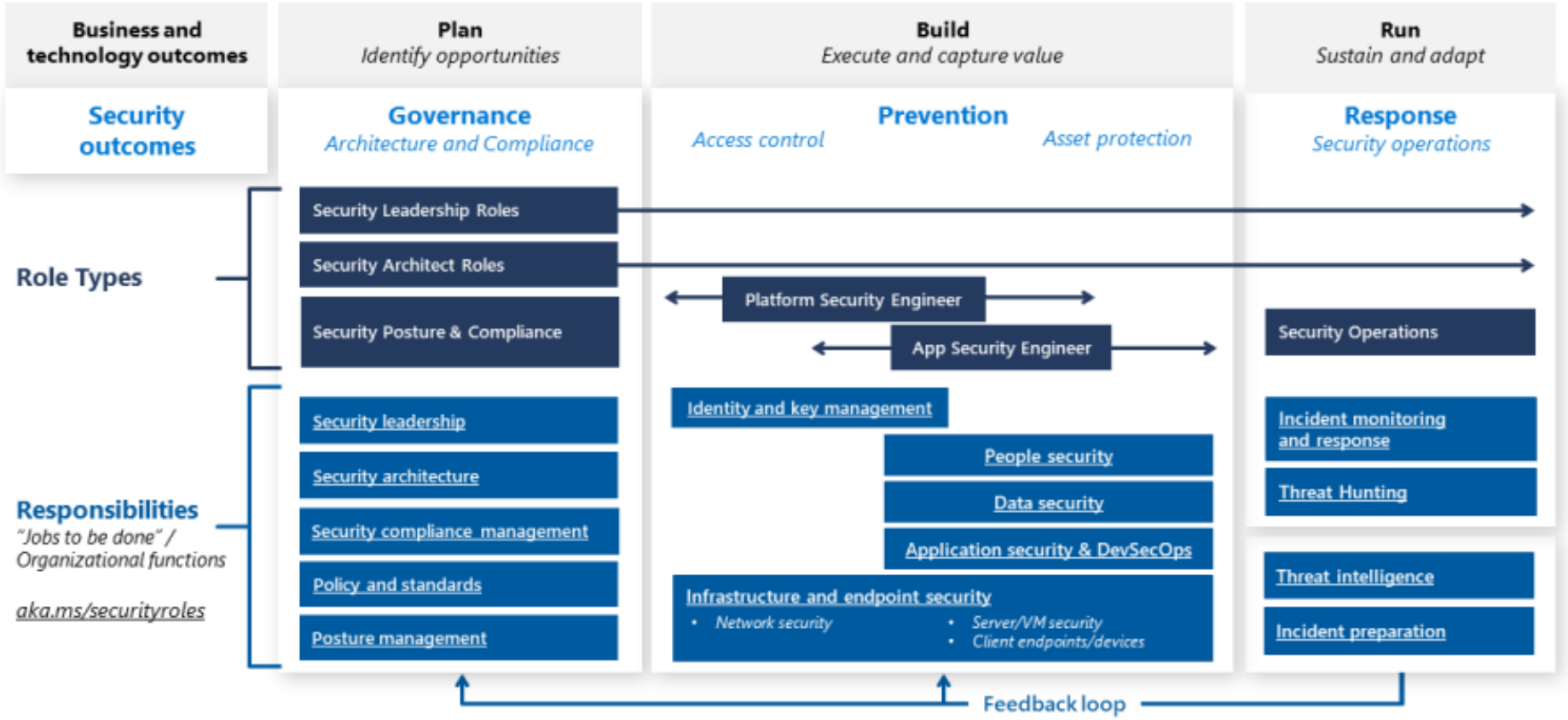
Azure Cloud Adoption Framework

Cloud Adoption Framework is a whitepaper that is a **step-by-step process** to help organizations plan and migrate their workloads to Azure



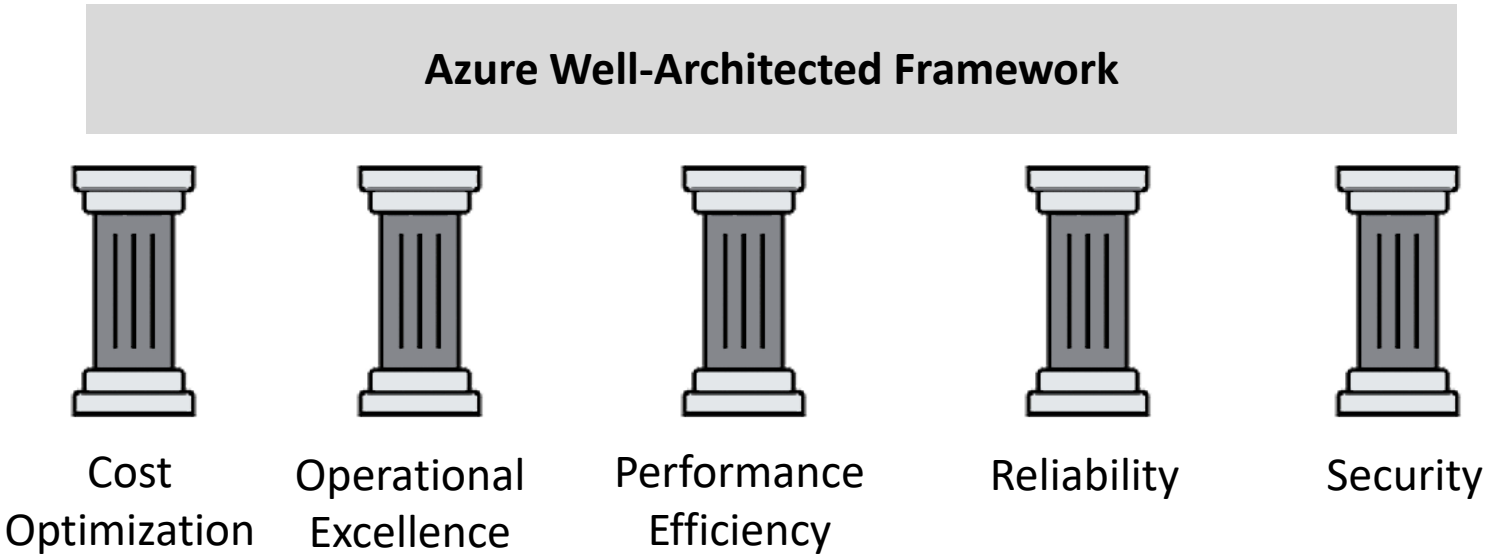
Azure Cloud Adoption Framework

Security Roles and Responsiblities



Azure Well-Architected Framework

Azure Well-Architected Framework describe **best practices for building workloads** on Azure **categorized into 5 pillars**



Cost Optimization — Managing costs to maximize the value delivered.
Operational Excellence — Operations processes that keep a system running in production.
Performance Efficiency — The ability of a system to adapt to changes in load.
Reliability — The ability of a system to recover from failures and continue to function.
Security — Protecting applications and data from threats.

Azure Migrate

Azure Migrate offers a streamlined service for **migration, modernization, and optimization on Azure**. It simplifies the pre-migration processes like discovering, assessing, and appropriately sizing on-premises resources for infrastructure, data, and applications.

With an extensible framework, Azure Migrate easily integrates with **third-party tools,** broadening its range of supported scenarios. Here's what it offers:

- **Unified Migration Platform**: A centralized portal to initiate, execute, and monitor your Azure migration journey.
- **Diverse Toolset**: Azure Migrate provides a suite of tools for both assessment and migration. It features tools such as **"Azure Migrate: Discovery and Assessment"** and **"Migration and Modernization."** It seamlessly integrates with other Azure services, tools, and third-party offerings from **independent software vendors (ISVs).**

Azure Migrate

Comprehensive Migration and Modernization Capabilities: In the Azure Migrate hub, you can **assess, migrate, and modernize**:

Servers, Databases, and Web Apps: Assess and migrate on-premises servers, web apps, and SQL Server instances to Azure.

- **Databases**: Analyze on-premises SQL Server instances and databases, and migrate them to **Azure SQL** on a VM, **Azure SQL Managed Instance**, or **Azure SQL Database**.
- **Web Applications**: Evaluate on-premises web applications and transition them to the Azure App Service or Azure Kubernetes Service.
- **Virtual Desktops**: Review your on-site **virtual desktop infrastructure (VDI)** and move it to Azure Virtual Desktop.
- **Data Transfer**: Efficiently and affordably transfer vast data volumes to Azure using **Azure Data Box** products.

Azure Migrate – Integrated tools

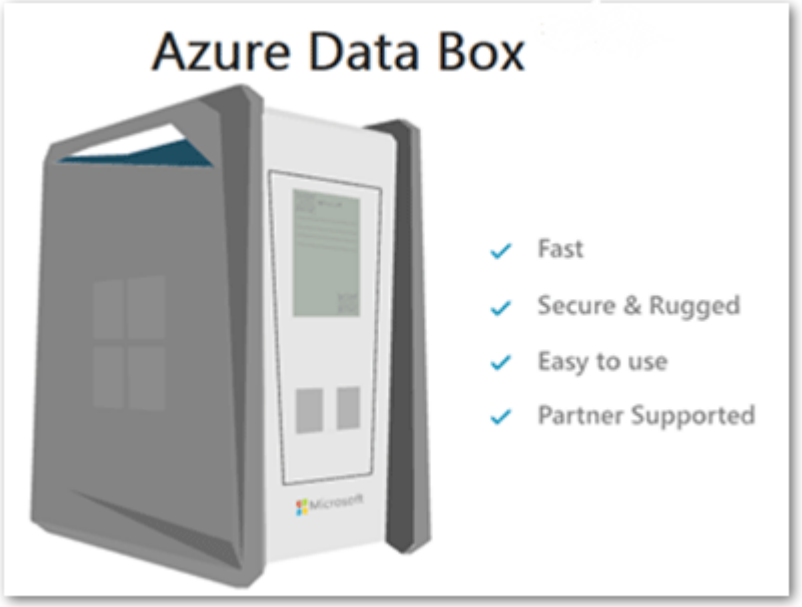
Tool	Assess and migrate	Details
Azure Migrate: Discovery and assessment	Discover and assess servers including **SQL and web apps**	Discover and assess on-premises servers running on **VMware, Hyper-V, and physical servers** in preparation for migration to Azure.
Migration and modernization	Migrate servers	Migrate VMware VMs, Hyper-V VMs, physical servers, other virtualized servers, and public cloud VMs to Azure.
Data Migration Assistant	Assess SQL Server databases for migration to Azure SQL Database, Azure SQL Managed Instance, or Azure VMs running SQL Server.	Data Migration Assistant assesses **SQL Servers**, **identifies potential migration problems**, **unsupported features**, and suggests the best path for database migration.
Azure Database Migration Service	Migrate on-premises databases to Azure VMs running SQL Server, Azure SQL Database, or SQL Managed Instances	Azure Database Migration Service is a managed service for **seamless migrations to Azure data platforms** with minimal downtime.
Movere	Assess servers	Movere is a **SaaS platform** that enhances **business intelligence** by accurately depicting IT environments within a day.
Web app migration assistant	Assess on-premises web apps and migrate them to Azure.	Azure App Service Migration Assistant is a standalone tool to **assess on-premises websites for migration to Azure App Service**.
Azure Data Box	Migrate offline data	Use Azure Data Box products to move **large amounts of offline data to Azure**.

Azure Databox

The Microsoft Azure Data Box cloud solution lets you send **terabytes of data into and out of Azure** in a quick, inexpensive, and reliable way.

Each storage device has a maximum usable storage capacity of **100 TB** and is transported to your datacenter through a regional carrier.

It is designed to help customers with slow or limited internet connectivity to move large volumes of data to the cloud.



Azure Databox

Use cases

Data Box is used to **import** data to Azure for:

- **One-time migrations**: Moving large on-premises data, transitioning offline tapes, relocating VMs, SQL servers, applications, and transferring historical data for Azure-based analysis.
- **Initial bulk transfers**: Large-scale transfers using Data Box, followed by incremental network transfers. For example, moving vast backups with partners like **Commvault**.
- **Periodic uploads**: Transferring large volumes of data generated periodically, like video content from oil rigs or windmill farms.

For **exporting** from Azure, Data Box is used for:

- **Disaster recovery**: Restoring Azure data on-premises quickly.
- **Security requirements**: Meeting mandates that require data extraction from Azure storage tiers like US Secret.
- **Migration**: Moving data back to on-premises or to a different cloud provider.

Azure Databox

Here's how Azure Data Box works:

1. Customers order a **Data Box** from the **Azure portal**.
2. When the Data Box arrives, customers connect it to their network and configure it using the Azure portal.
3. Customers copy data to the Data Box using standard file transfer protocols, such as **SMB** or **NFS**.
4. Once the data transfer is complete, customers ship **the Data Box back to Azure**.
5. Azure copies the data from the **Data Box** to the customer's **Azure storage account**.

Microsoft Entra

Previously Azure Active Directory (AD)

Cloud-based **identity and access management** service.
Manage users, identities, sign-ins and access to resources connected to Microsoft's identity services

Introduction to Entra ID (Azure AD)

Entra ID(Azure AD) is Microsoft's cloud-based **identity and access management service**, which helps manage users, sign-ins, and access to Active directory-related resources.

External Resources

- Microsoft Office 365
- Azure Portal
- SaaS applications

Internal Resources

- Applications within your internal networking
- Access to workstations on-premises

Use Entra ID to implement **Single-Sign On (SSO)**

Identity Governance: Gives you the ability to enforce rules for the automatic removal of user access based on changes in job function or employment status.

Access Management: Allows you to manage access to your apps, group memberships, and role assignments through approval workflows and dynamic policies.

Introduction to Entra ID (Azure AD)

Microsoft Entra ID comes in **four** editions

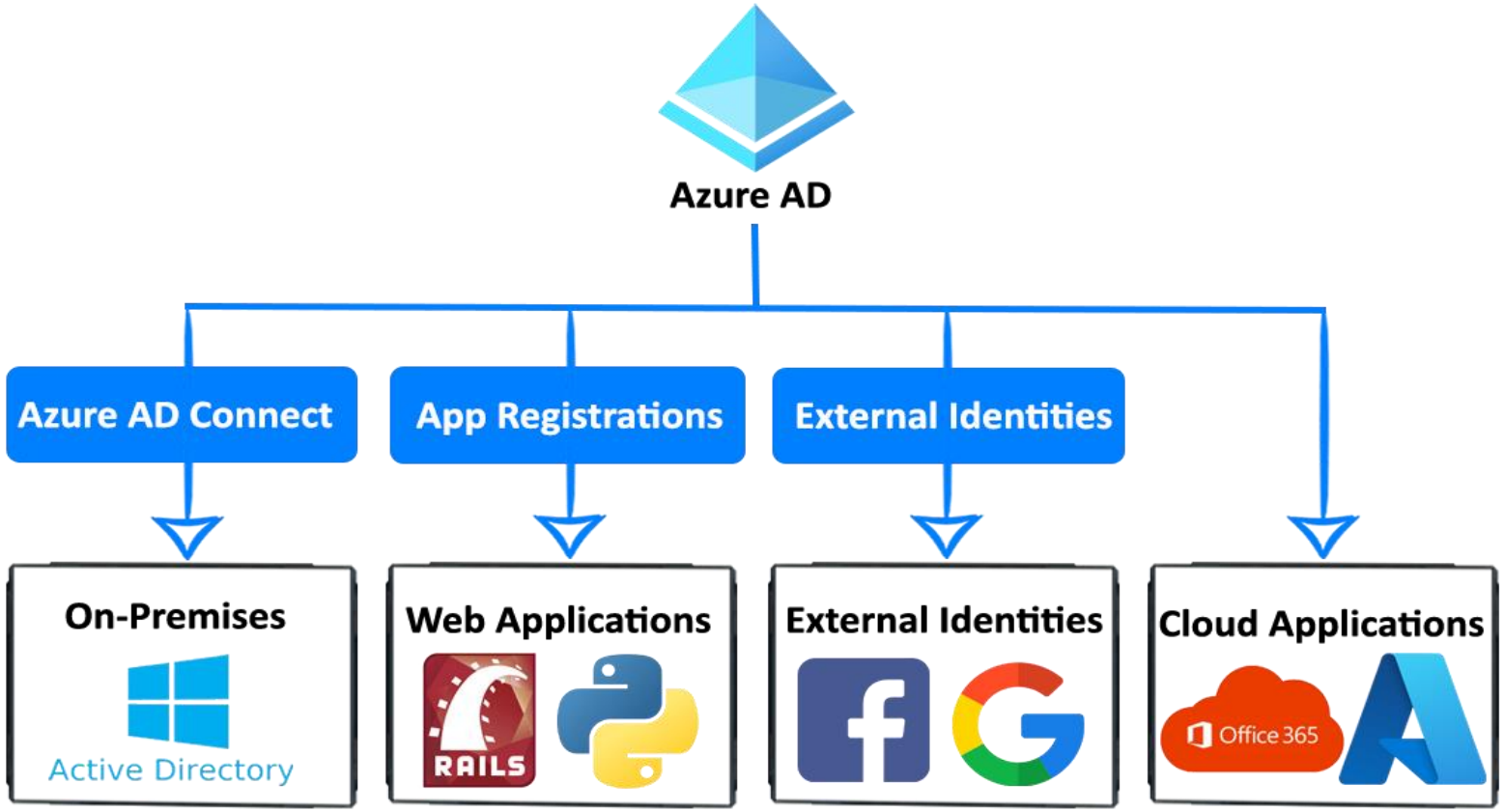
1. **Free** Multi Factor Authentication (MFA), Single Sign On (SSO), Basic Security and Usage Reports, User Management
2. **Office 365 Apps** Company Branding, Service Level Agreement (SLA), Two-Sync between On-Premises and Cloud
3. **Premium 1** Hybrid Architecture, Advanced Group Access, Conditional Access
4. **Premium 2** Identity Protection, Identity Governance

All features of the previous edition are included

Entra ID – Use Case

Entra ID can **authorize** and **authenticate** to multiple sources.

- To your on-premises AD (Active Directory)
- To your web-applications
- Allow users to login with their IdP (Identity Provider) e.g., Facebook or Google
- To Office 365 or **Microsoft Azure**



Active Directory vs Entra ID

Microsoft introduced **Active Directory** Domain Services in **Windows 2000** to give organizations the ability to manage multiple on-premises infrastructure components and systems using a single identity per user.

Entra ID takes this approach to the next level by providing organizations with an **Identity as a Service (IDaaS)** solution for all their apps **across cloud and on-premises**.

Both versions are still used today

Active Directory
The **on-premises** version

Entra ID
The **cloud** version

Active Directory Terminology

Domain
A domain is an area of a network organized by a single authentication database.
An Active Directory domain is a **logical grouping** of AD objects on a network.

Domain Controller (DC)
A domain controller is a server that **authenticates** user identities and **authorizes** their access to resources.

Domain Computer
A computer that is registered with a central authentication database. A domain computer would be an AD Object.

AD Object
An AD Object is the basic element of Active Directory such as: **Users, Groups, Printers, Computers, Shared folders**

Group Policy Object (GPO)
A virtual collection of policy settings. It controls what AD Objects have access to.

Organization Units (OU)
A subdivision within an Active Directory into which you can place users, groups, computers, and other organizational units.

Directory Service
A directory service, such as **AD DS,** provides the methods for storing directory data and making this data available to network users and administrators. A Directory service runs on a Domain Controller.

Microsoft Entra Domain Services

Also known as Azure Active Directory Domain Services (AD DS)

In some cases, you'll need to setup your own domain controller(s).

When doing a ***lift-and-shift from on-premises*** to Microsoft Azure and migrating Active Directory, Entra ID does not support some **domain services**.

Microsoft Entra Domain Services provides **managed domain service** such as:

- Domain joins
- Group policies
- Lightweight directory access protocol (LDAP)
- and Kerberos / NTLM authentication.

You can use these domain services without the need to:
deploy, **manage**, and **patch** **domain controllers (DCs)** in the cloud

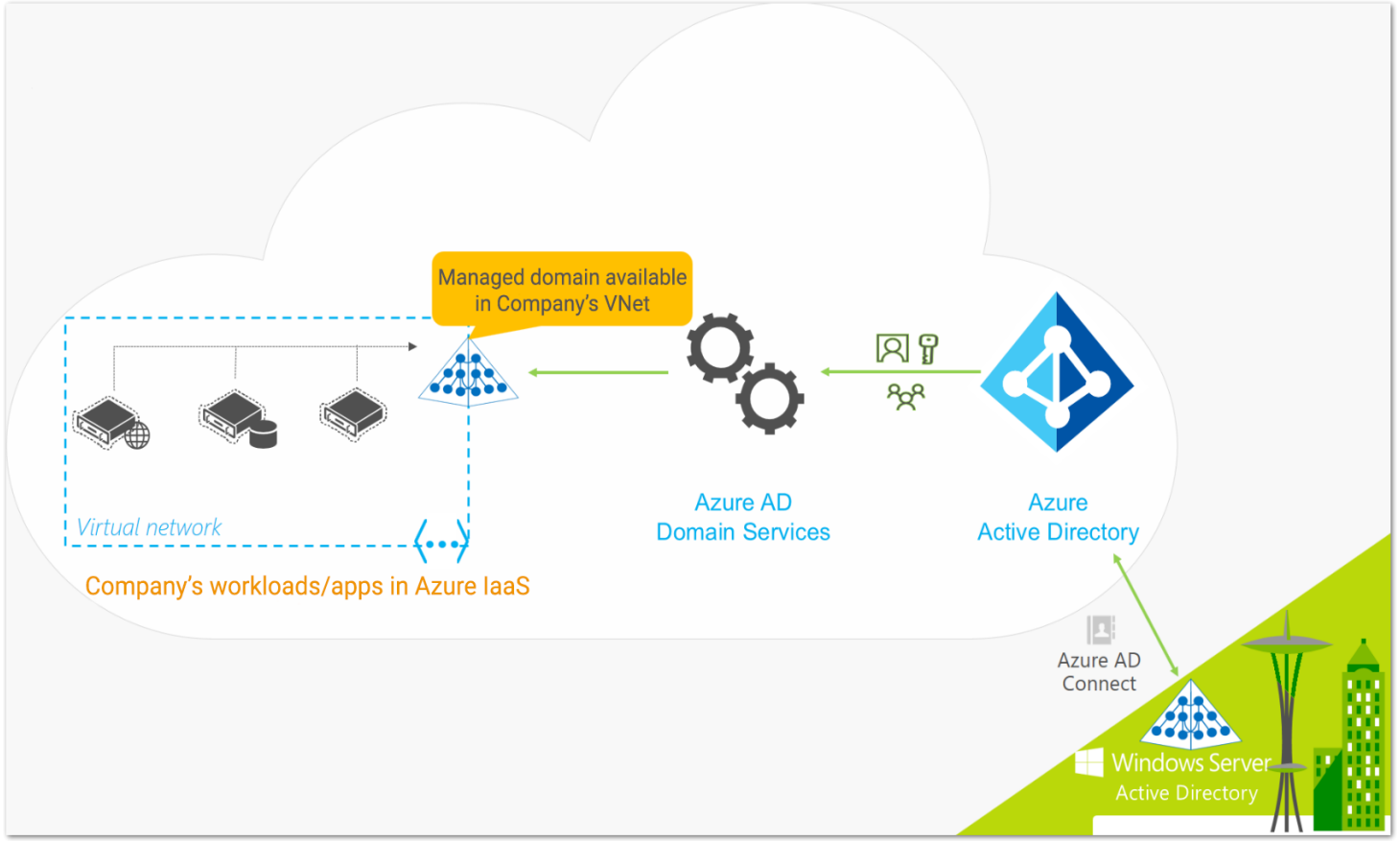
Microsoft Entra Domain Services

1. The company deploys applications, including legacy ones, and server workloads in an Azure virtual network as part of a lift-and-shift strategy.

2. They use **Entra ID Connect (Azure AD)** to sync identity information, including user accounts and group memberships, from their on-premises directory to Azure AD.

3. The IT team enables **Entra Domain Services** for their Azure AD tenant in this or a connected virtual network.

4. Applications and VMs in the Azure network can then utilize **Entra Domain Services** features like **domain join, LDAP read/bind, NTLM/Kerberos authentication,** and **Group Policy**.



Managed Identities

Managed Identities is a concept in **Microsoft Entra ID (Azure AD)** that associates **identities** with **internal resources**, where these identities have their own **roles** and **tokens**.

Managed Identities increases security by allowing you to **link** directly resources to other resources **without** having to share any **security information** over the network.
Those resources will be **authenticated** against **Entra ID (Azure AD)** to see if they have the necessary **permissions** to manipulate other resources.

For example, we can allow our applications to access **Azure Key Vault** in order to retrieve a **secret** without **exposing** any passwords.

Entra ID (Azure AD) – External Identities

External Identities in Entra ID, allow people outside your organization to access your apps and resources, while letting them sign in using whatever identity they prefer.

Your partners, distributors, suppliers, vendors, and other guest users can **"bring their own identities"**.

Supports Logins from **Google** and **Facebook**

- **Share apps with external users (B2B collaboration).**
- **Develop apps intended for other Entra ID tenants (single-tenant or multi-tenant)**
- **Develop white-labeled apps for consumers and customers (Entra ID B2C)**

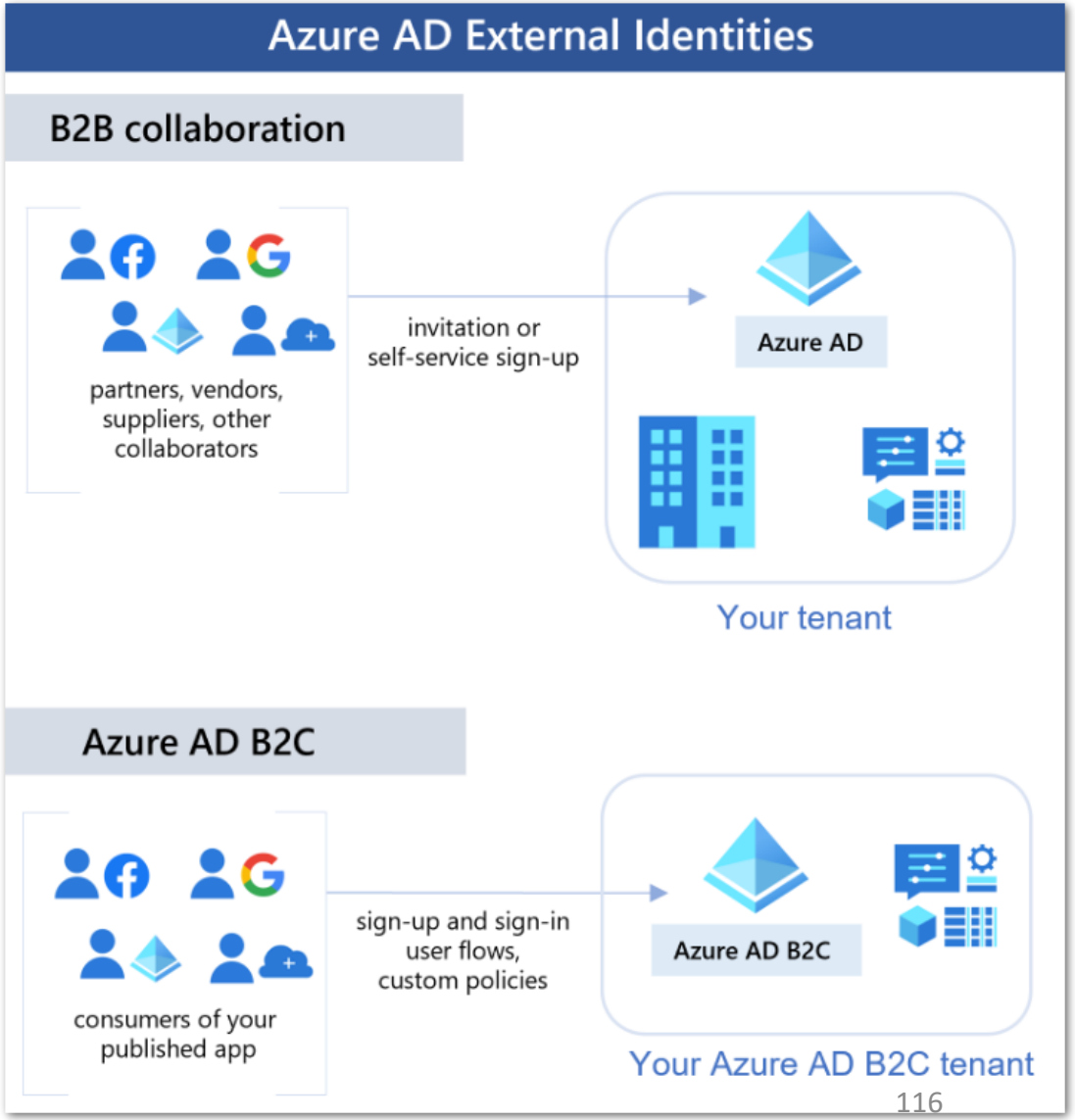
Entra ID (Azure AD) – External Identities

B2B Collaboration: Allows external users to use their **preferred identity** to access your Microsoft and enterprise applications, with users typically represented as guest users in your directory.

B2B Direct Connect: Enables a **two-way trust** with another Entra ID organization for seamless collaboration, particularly through **Teams** shared channels. Users aren't in your directory but are visible within Teams.

Entra ID B2C: Facilitates publishing **SaaS or custom apps** to consumers, utilizing Entra ID B2C for identity and access management.

Entra ID Multi-Tenant Organization: Provides **cross-tenant synchronization** for collaboration within a single Entra ID organization.



Microsoft Entra ID – Access reviews

Access reviews in **Microsoft Entra ID (Azure AD)** allow you to regularly **review** and **manage access** to resources in your organization.

- With access reviews, you can review who has access to resources and determine whether their access is still necessary.
- Access reviews are useful in maintaining security and compliance by ensuring that only **authorized individuals have access to sensitive resources**.

- Access reviews can be conducted for various types of resources, such as **applications, groups, and SharePoint Online sites**.
- You can configure access reviews to occur on a regular schedule and select reviewers to conduct the reviews.
- Reviewers can be **internal** or **external** to your organization.

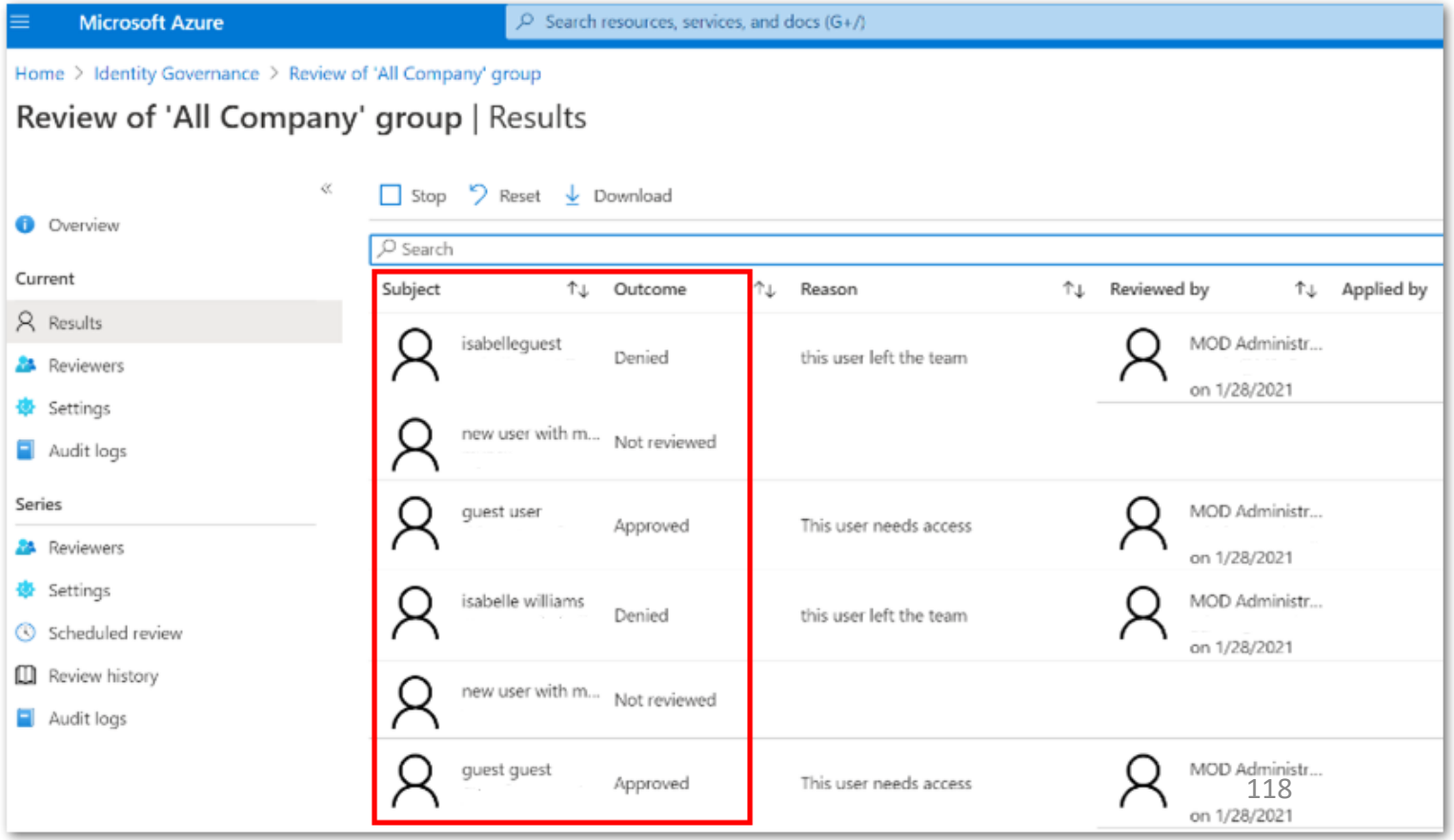
Microsoft Entra ID – Access reviews

During an access review, the reviewer will be presented with a list of people who have access to the resource being reviewed. They can choose to **approve** or **revoke access** for each individual.

- Access can be **revoked immediately** or **scheduled** for a later date.
- Reviewers can also provide a **reason** for their decision, which can be useful for auditing purposes

Access reviews are crucial in large organizations to regularly identify and resolve access issues.

They ensure resources are accessed only by necessary users and that access is revoked when no longer needed.

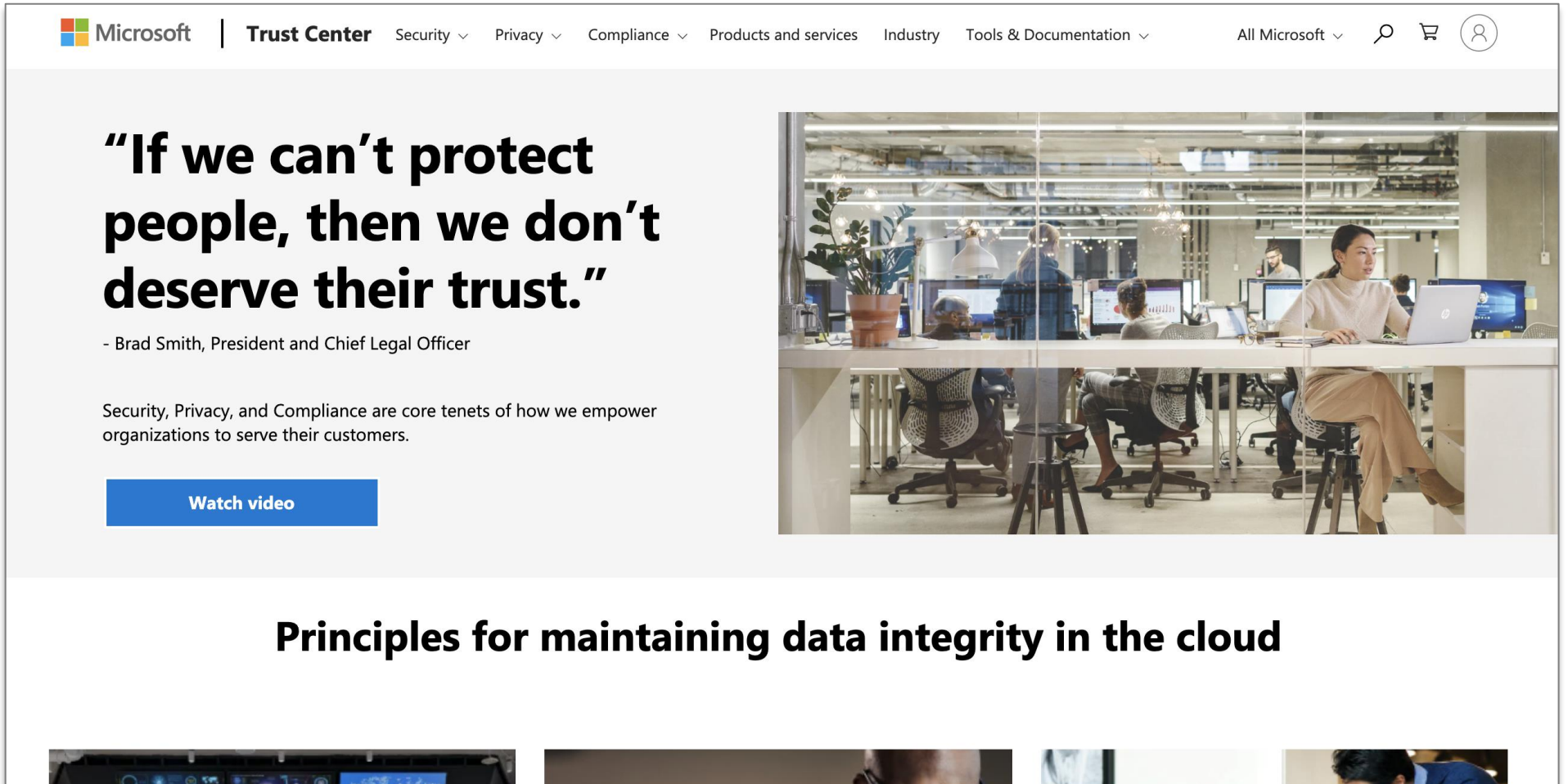


Access reviews use cases

1. **Privileged Roles**: Use access reviews to manage users with administrative access, including Global Administrators and invited guests or partners.
2. **Automation**: Conduct reviews for groups lacking automated access management to ensure necessary access continuity.
3. **Group Purpose Changes**: Request membership reviews by group owners before syncing a group to Entra ID (Azure AD)or enabling an application.
4. **Business-Critical Data Access**: Regularly reaffirm users' need for access to sensitive data to maintain security and compliance.
5. **Policy Exception Management**: Oversee exceptions to access policies to ensure compliance and provide audit evidence.
6. **Guest Access**: Validate the ongoing need for guest access, especially for sensitive content, as automated access might not cover guests.
7. **Recurring Reviews**: Set up periodic access reviews (weekly, monthly, quarterly, annually) to continuously manage user access with an intuitive interface offering smart recommendations.

Azure Trust Center

A public-facing website portal providing easy access to **privacy** and **security** and **regulatory compliance** information.



Azure Security – Compliance Programs

Enterprise Companies WILL NOT BUY your software solutions unless its 🔒 **secure**.

How are you going **to meet their security compliance requirements**?

We'll only do business with you if you are...

- **NIST 800-53**
- **PIPEDA** Compliant
- **HIPPA** Compliant
- **FIPS-140-2** Compliant

Azure Security – Compliance Programs

Cheat sheets, Practice Exams and Flash cards 👉 www.exampro.co/az-900

Criminal Justice Information Services (CJIS)
Any US state or local agency that wants to access the FBI's CJIS database is required to adhere to the CJIS Security Policy.

Cloud Security Alliance (CSA) STAR Certification
Independent third-party assessment of a cloud provider's security posture

General Data Protection Regulation (GDPR)
A European privacy law. Imposes new rules on companies, government agencies, non-profits, and other organizations that offer goods and services to people in the European Union (EU), or that collect and analyze data tied to EU residents.

EU Model Clauses
Contractual guarantees around transfers of personal data outside of the EU

Azure Security – Compliance Programs

Cheat sheets, Practice Exams and Flash cards 👉 www.exampro.co/az-900

Health Insurance Portability and Accountability Act (HIPAA).
US federal law that regulates patient Protected Health Information

International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) 27018.
Code of practice, covering the processing of personal information by cloud service providers.

Multi-Tier Cloud Security (MTCS) Singapore.
Operational Singapore security management Standard. A common standard that cloud service providers (CSPs) can apply to address customer concerns about the security and confidentiality of data in the cloud, and the impact on businesses of using cloud services.

Service Organization Controls (SOC) 1, 2, and 3.
independent third-party examination reports that demonstrate how the company achieves key compliance controls and objectives

Azure Security – Compliance Programs

Cheat sheets, Practice Exams and Flash cards 👉 www.exampro.co/az-900

National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF)
Voluntary Framework that consists of standards, guidelines, and best practices to manage cybersecurity-related risks.

UK Government G-Cloud.
Cloud computing certification for services used by government entities in the United Kingdom

Federal Information Processing Standard (FIPS) 140-2
US and Canadian government standard that specifies the security requirements for cryptographic modules that protect sensitive information.

Azure Active Directory

Azure Active Directory (Azure AD) is Microsoft's cloud-based **identity and access management service**, which helps your employees sign in and access resources

External Resources

- Microsoft Office 365
- Azure Portal
- SaaS applications

Internal Resources

Applications within your internal networking
Access to workstations on-premise

Use Azure AD to implement **Single-Sign On (SSO)**

Azure Active Directory comes in four editions

1. **Free** MFA, SSO, Basic Security and Usage Reports, User Management
2. **Office 365 Apps** Company Branding, SLA, Two-Sync between On-Premise and Cloud
3. **Premium 1** Hybrid Architecture, Advanced Group Access, Conditional Access
4. **Premium 2** Identity Protection, Identity Governance

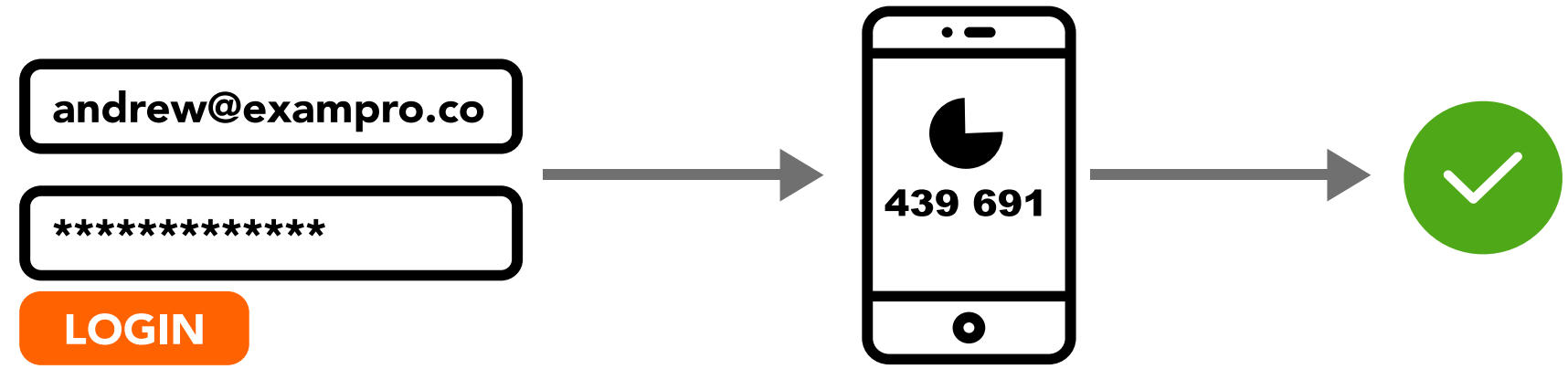
Multi-Factor Authentication

What is Multi-Factor Authentication (MFA)?

A security control where after you fill in your username/email and password **you have to use a second device** such as a phone to confirm that its you logging in.

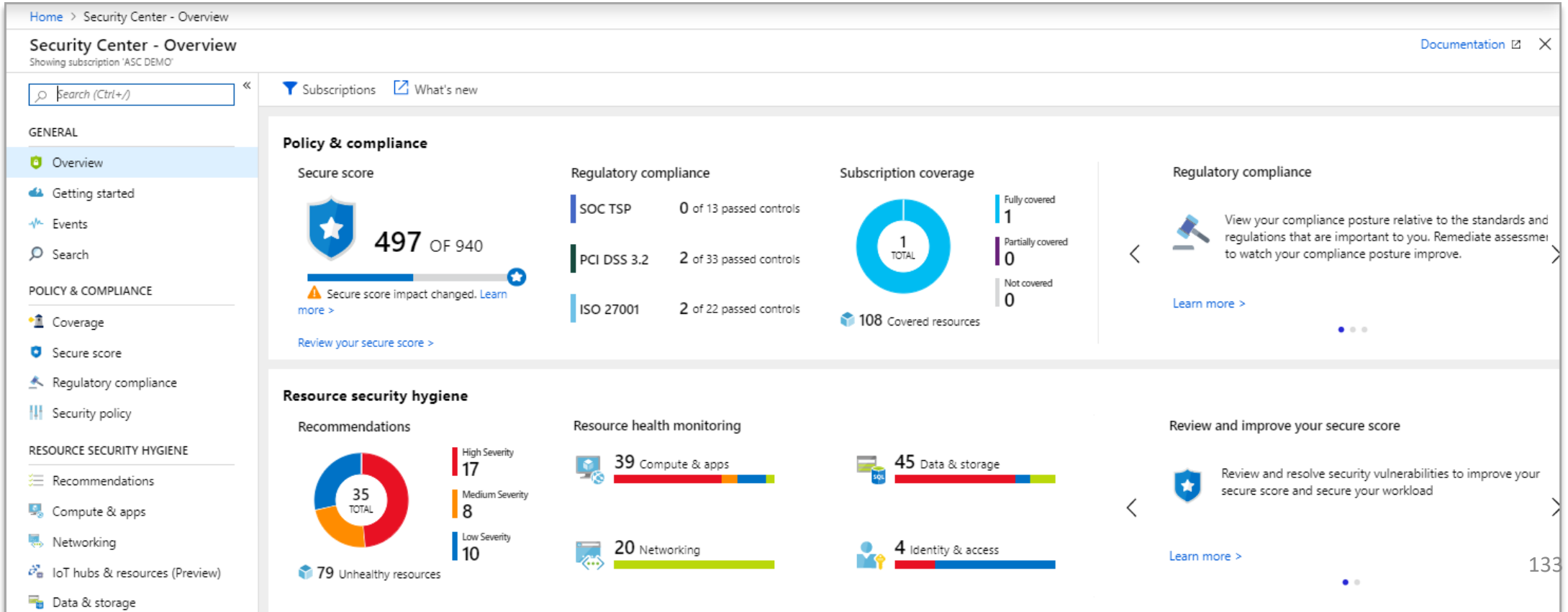
MFA **protects** against people who have stolen your password.

MFA is an option in most cloud providers and even social media websites such as Facebook.



Azure Security Center

Azure Security Center is a **unified infrastructure security management system**
It strengthens the security posture of your data centers, and provides advanced threat protection across your hybrid workloads in the cloud.



Key Vault

Azure Key Vault helps you **safeguard** **cryptographic keys and other secrets** used by cloud apps and services.

Secrets Management
store and tightly control access to **tokens, passwords, certificates, API keys, and other secrets**

Key Management
create and control the **encryption keys** used to encrypt your data

Certificate Management
easily provision, manage, and deploy public and private **SSL certificates** for use with Azure and internal connected resources.

Hardware Security Module
secrets and keys can be protected either by software or **FIPS 140-2 Level 2** validated HSMs

Key Vault

An HSM is a **Hardware Security Module**.
Its a piece of hardware designed to store encryption keys.

Federal Information Processing Standard (FIPS) 140-2
US and Canadian government standard that specifies the security requirements for cryptographic modules that protect sensitive information.

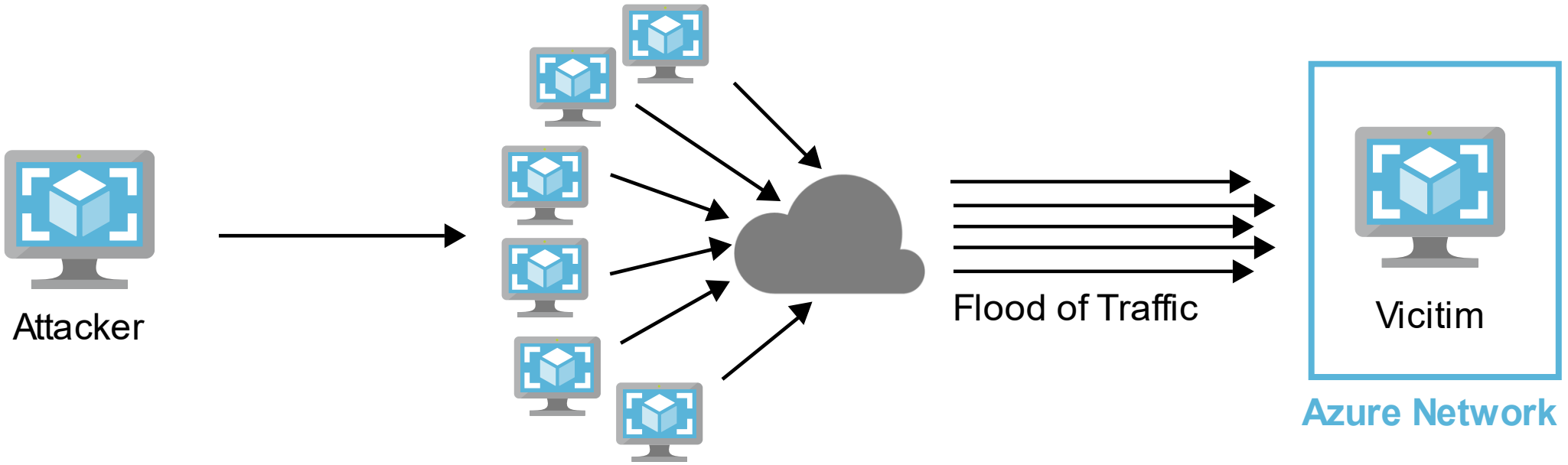
HSM's that are **multi-tenant** are **FIPS 140-2 Compliant**
(multiple customers virtually isolated on an HSM)

HSM's that are **single-tenant** are **FIPS 140-3 Compliant**
(single customer on a dedicated HSM)

Azure DDoS Protection

What is a DDoS (Distributed Denial of Service) Attack?

A malicious attempt to disrupt normal traffic by flooding a website with large amounts of fake traffic.



Azure DDoS Protection

Azure offers **two tiers** of DDoS Protection

DDoS IP Protection

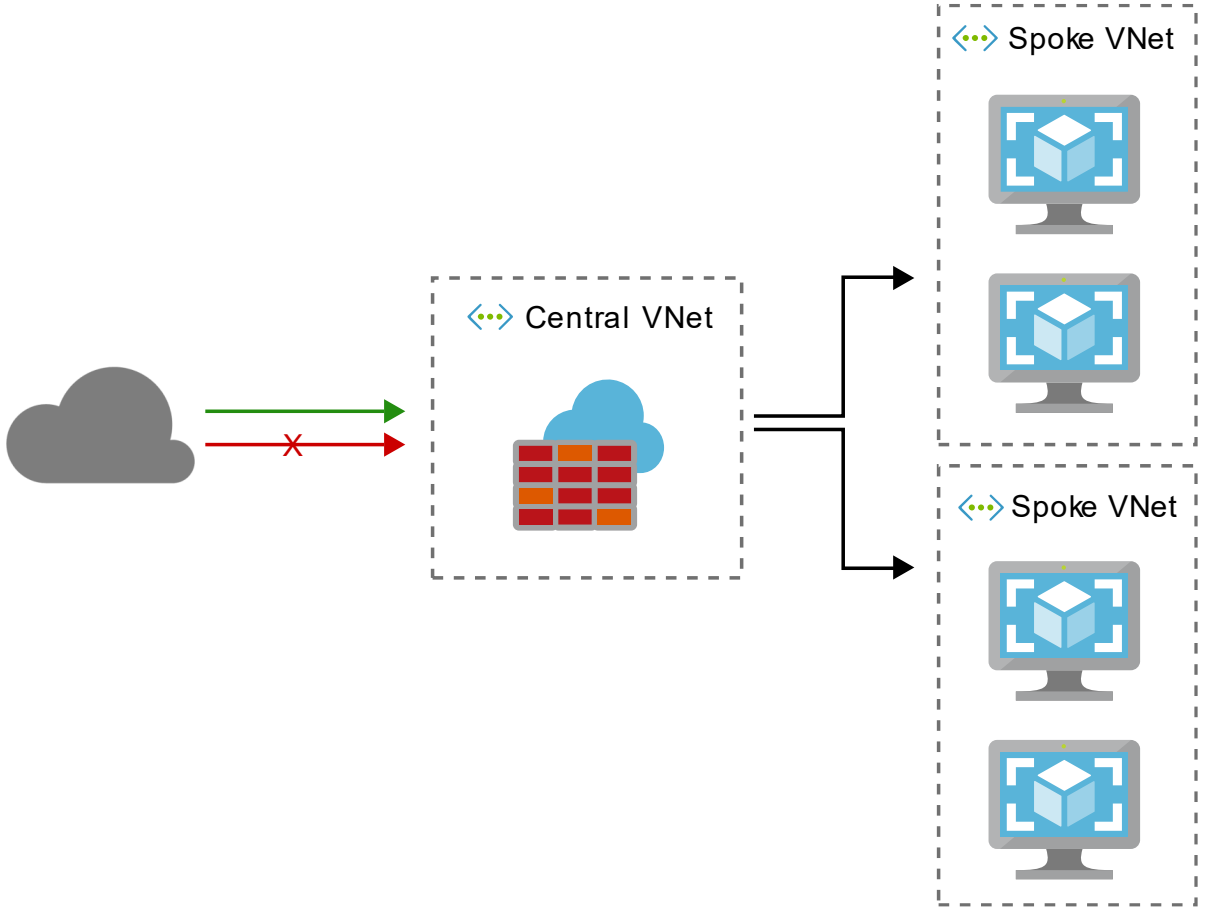
- **Pricing Model**: Charged per protected IP
- **Key Features:**
  - Active Traffic Monitoring and Detection
  - Application-based Mitigation Policies
  - Metric, Alerts, and Mitigation Reports
  - Integration with Azure Services
  - Public IP Standard Tier Protection

DDoS Network Protection

- **Pricing Model**: Charged per 100 protected IP addresses
- **Key Features**:
  - All Features of IP Protection
  - DDoS Rapid Response Support
  - Cost Protection
  - WAF Discount
  - Protection Across Subscriptions

Azure Firewall

Azure Firewall is a managed, **cloud-based network security service** that protects your Azure Virtual Network resources.



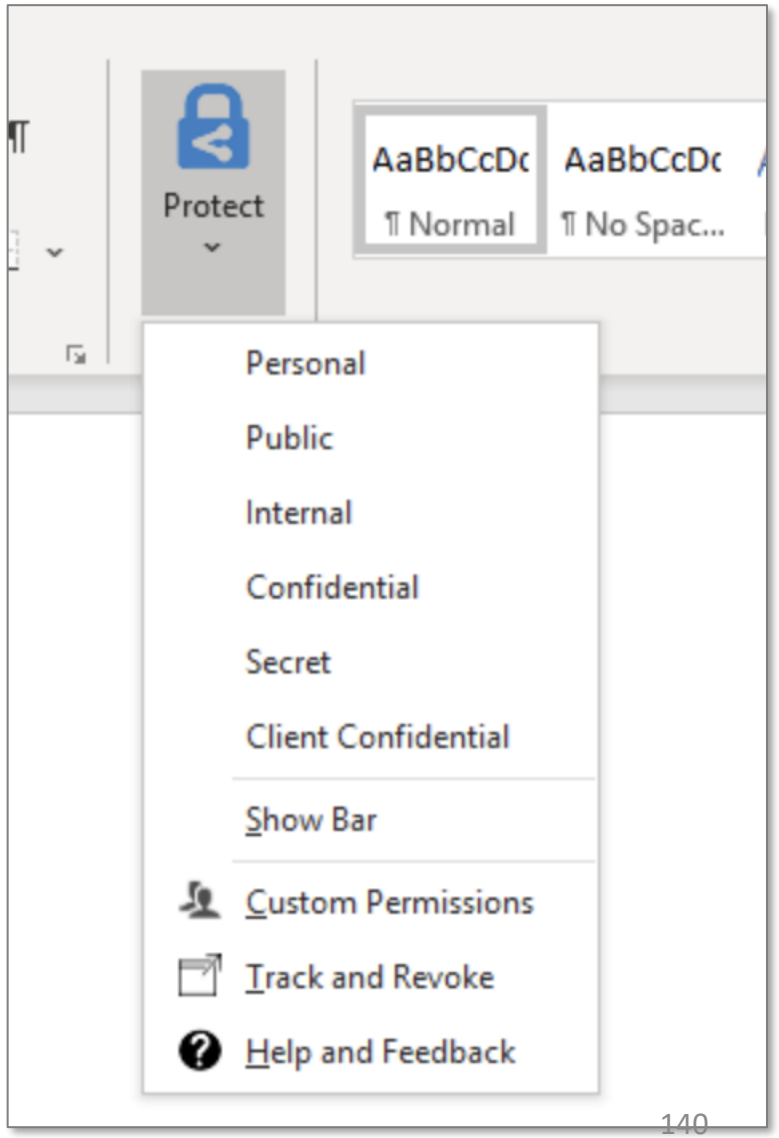
Azure Firewall

Azure Firewall Features

- Centrally create, enforce, and log application and network connectivity policies **across subscriptions** and virtual networks.
- Uses a **static public IP address** for your virtual network resources allowing outside firewalls to identify traffic originating from your virtual network
- High availability is built in**, no additional load balancers are required**
- Can configure during deployment to **span multiple AZs for increased availability**.
- There's **no additional cost** for a firewall deployed in an Availability Zone (AZ)
- There are **additional costs for inbound and outbound data transfers** associated with AZs

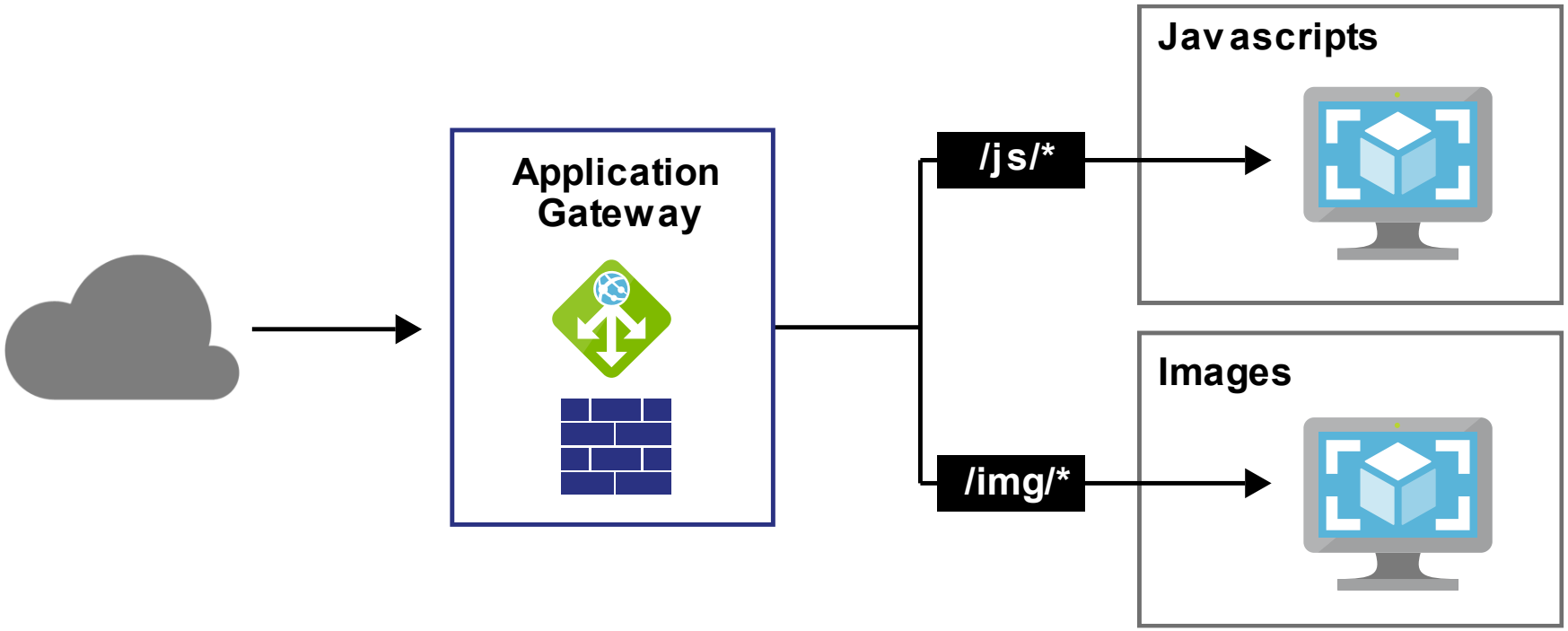
Azure Information Protection (AIP)

Protects sensitive information such as emails and documents with encryption, restricted access and rights, and integrated security in Office apps



Azure Application Gateway

Application Gateway is a **web-traffic load balancer** (Layer 7 HTTP) that re-route traffic based on a set of rules. A Web Application Firewall (WAF) can be attached for additional protection on OSI Layer 7.



Azure Advanced Threat Protection (ATP)

What is IDS/IPS?

Intrusion Detection System and Intrusion Protection System

A device or software application that monitors a network or systems for malicious activity or policy violations.

Azure Advanced Threat Protection (ATP) is a cloud-based security solution that **leverages your on-premises Active Directory** signals **to identify, detect, and investigate advanced threats, compromised identities, and malicious** insider actions directed at your organization.

Microsoft Security Development Lifecycle (SDL)

Microsoft Security Development Lifecycle (SDL) is an **industry-leading software security assurance process**.

A Microsoft-wide initiative and a mandatory policy since 2004, the SDL has played a critical role in embedding security and privacy in Microsoft software and culture.

Building security into each **SDL phase** of the development lifecycle helps you catch issues early, and it helps you reduce your development costs.

SDL Phases

Azure Security – Policies

Azure Policy is a service you can use to create, assign, and manage policies. A policy allows you to enforce or control the properties of a resource

Azure Policy evaluates resources in Azure by comparing the properties of those resources to business rules. These business rules, described in **JSON** format, are known as **Policy Definitions**.

Azure Role-Based Access Control (RBAC)

Azure role-based access control (Azure RBAC) helps you manage **who has access to Azure resources**, what they can do with those resources, and what areas they have access to.

Role Assignments the way you control access to resources

A Role Assignment is consist of these three elements

1. security principal
2. role definition
3. scope

Azure Role-Based Access Control (RBAC)

A Security Principal represents the identities requesting access to an Azure resource such as:

User An individual who has a profile in Azure Active Directory

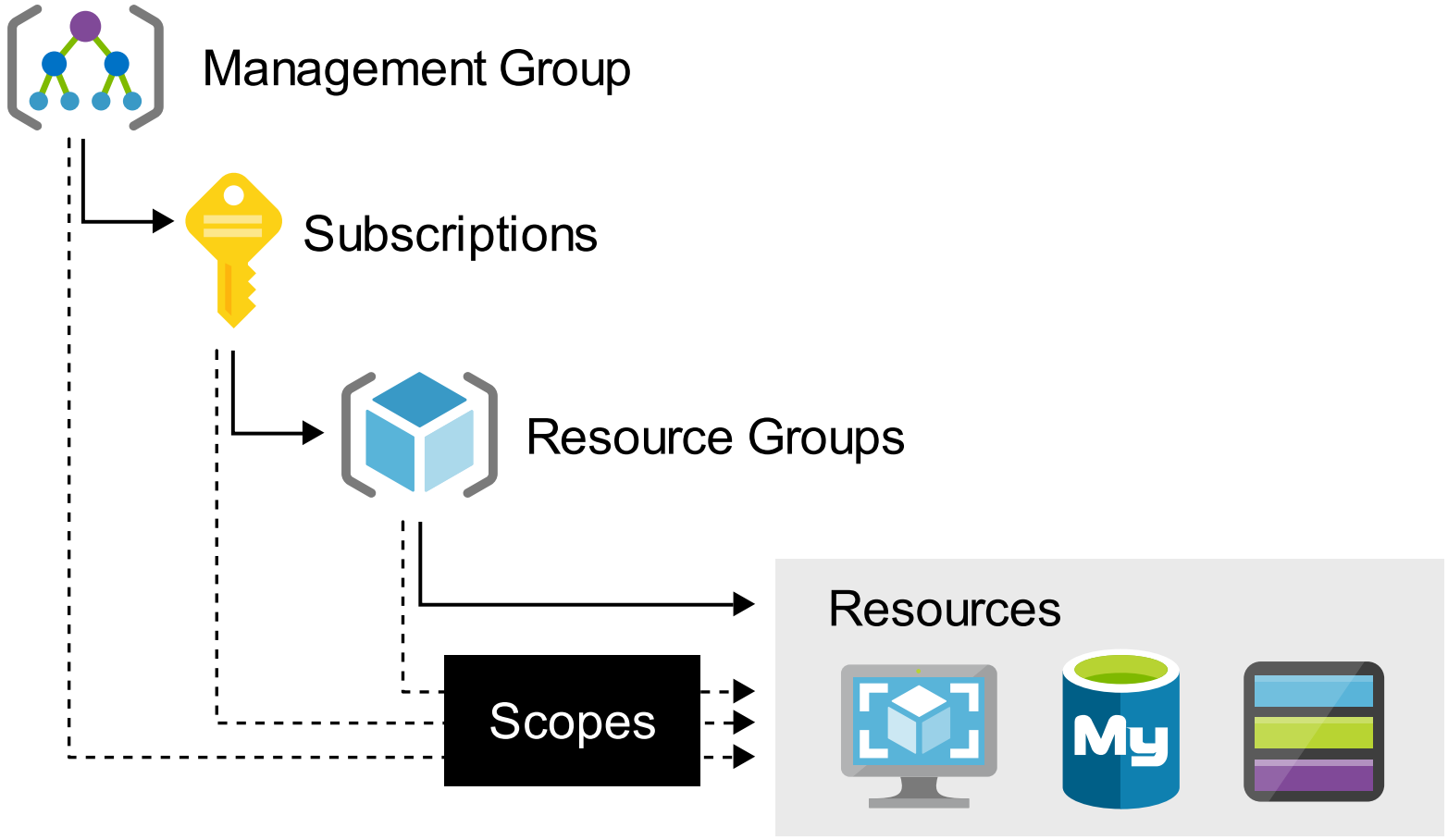
Group A set of users created in Azure Active Directory.

Service Principal A security identity used by applications or services to access specific Azure resources.

Managed identity An identity in Azure Active Directory that is automatically managed by Azure.

Azure Role-Based Access Control (RBAC)

Scope is the **set of resources** that access for the Role Assignment applies to.
Scope Access Controls at the Management, Subscription or Resource Group level.



Azure Role-Based Access Control (RBAC)

A Role Definition is a collection of permissions.
A role definition lists the operations that can be performed, such as **read, write, and delete**.
Roles can be high-level, like owner, or specific, like virtual machine reader.

Azure has **built-in roles** and you can define **custom roles**

	Read	Grant	Create, Update, Delete
Owner			
Contributor			
Reader			
User Access Administrator			

These are the four fundamental built-in role

Lock resources

As an admin, you may need to **lock a subscription, resource group, or resource** to **prevent other users from accidentally deleting or modifying critical resources.**

In the **Azure Portal** you can set the following lock levels.

CanNotDelete (Delete)
authorized users can still read and modify a resource, but they can't delete the resource.

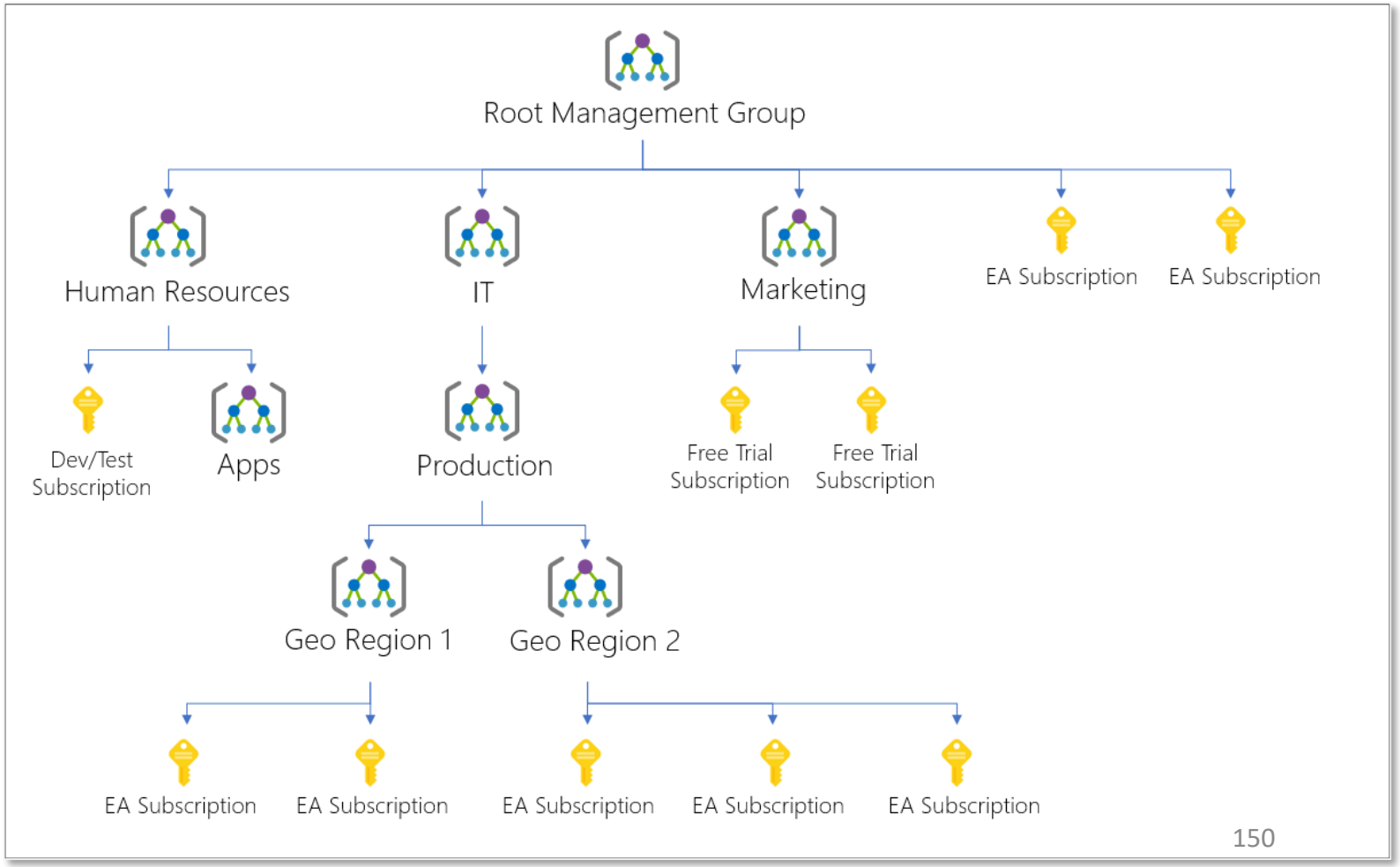
ReadOnly (Read-only)
authorized users can read a resource, but they can't delete or update the resource

Azure Management Groups

Managing multiple subscriptions (accounts) into a hierarchal structure.

Each directory is given a single top-level management group called the "Root" management group.

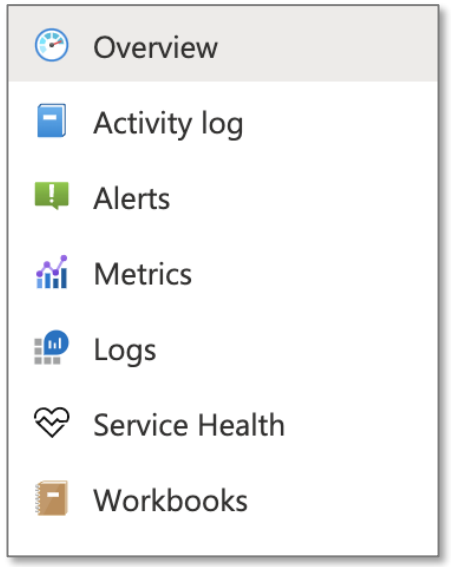
All subscriptions within a management group automatically inherit the conditions applied to the management group.

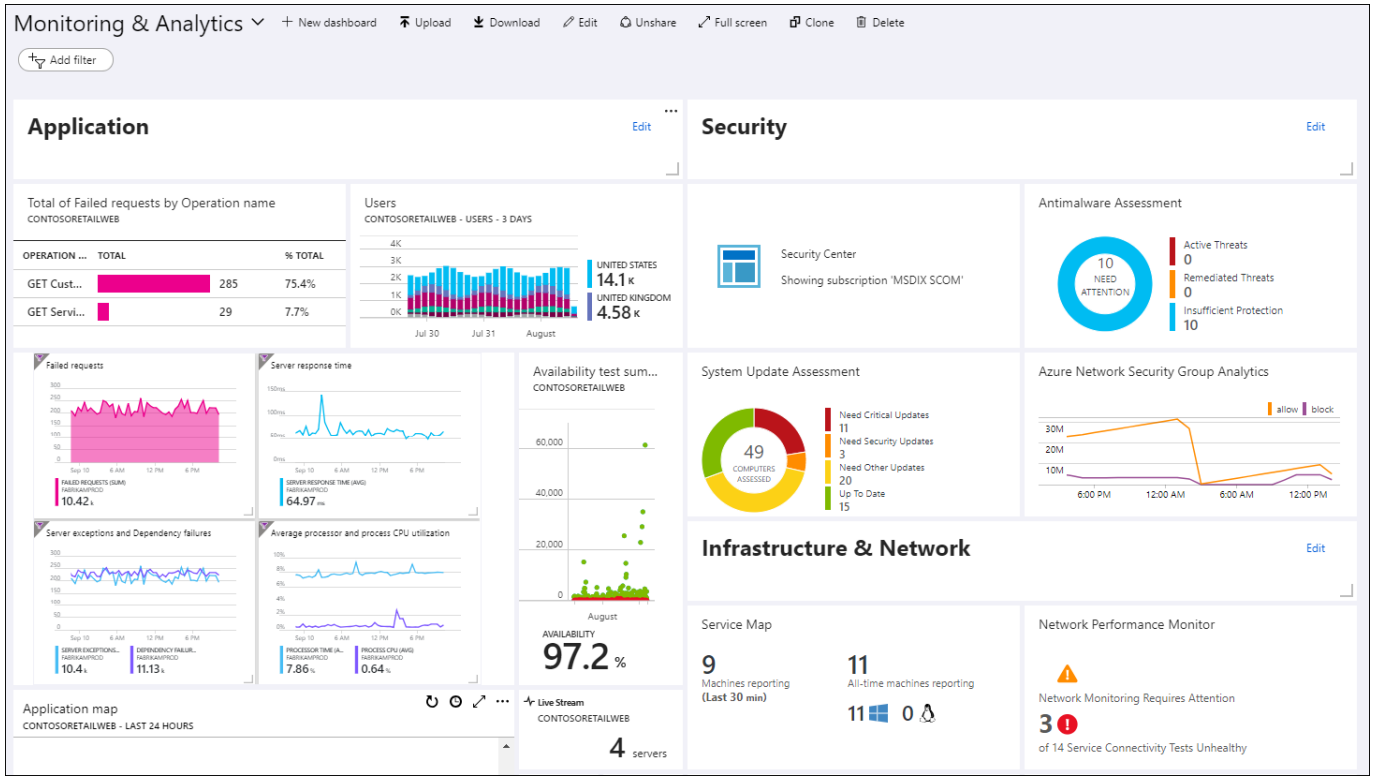


Azure Monitor

Cheat sheets, Practice Exams and Flash cards 👉 www.exampro.co/az-900

Azure Monitor comprehensive solution **for collecting, analyzing, and acting on telemetry** from your cloud and on-premises environments





- Create Visual Dashboards
- Smart Alerts
- Automated Actions
- Log Monitoring

Azure Service Health

Information about **current and upcoming issues** such as:

- service impacting events
- planned maintenance
- and other changes that may affect your availability.

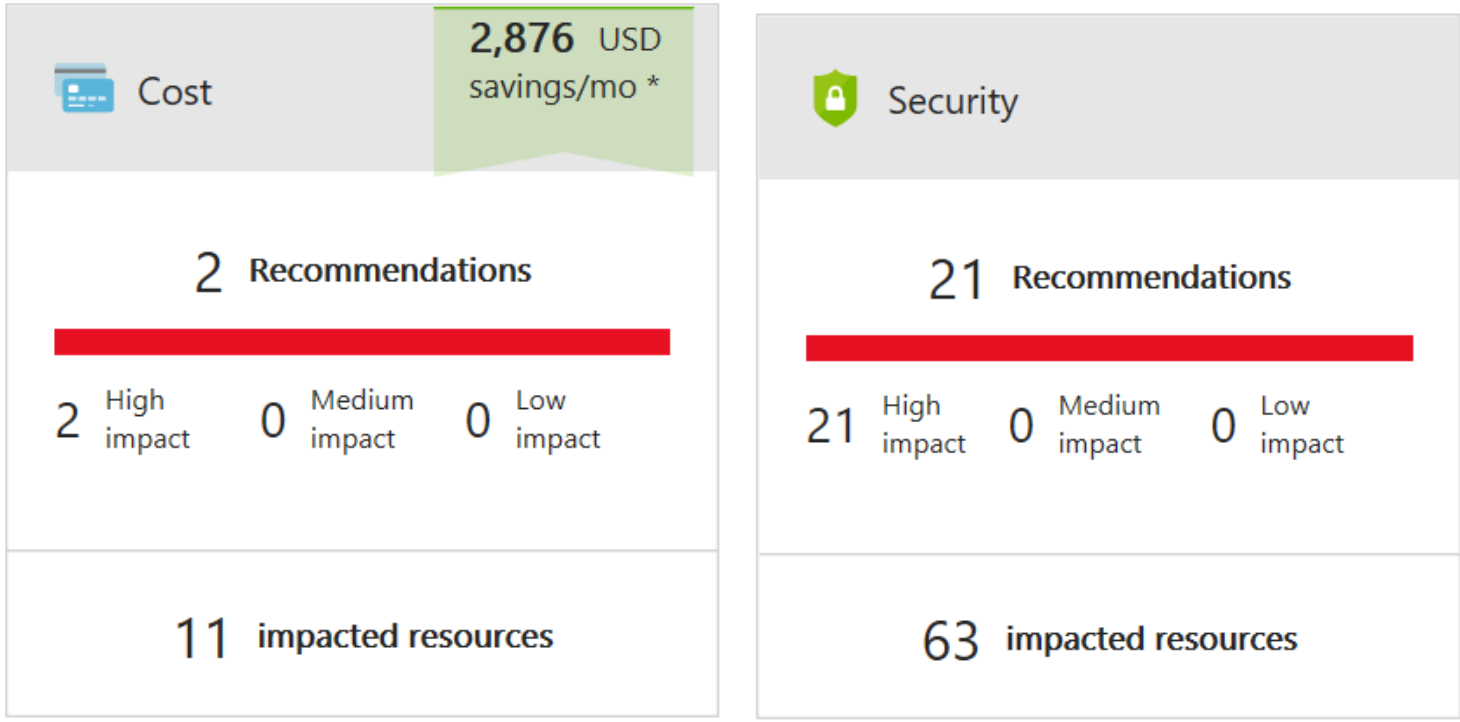
1. **Azure Status** informs you of service outages in Azure
2. **Azure service health** a personalized view of the health of the Azure services and regions you're using.
3. **Azure resource health** information about the health of your individual cloud resources eg. VM

Azure Advisor

Azure Advisor is a personalized cloud consultant that helps you follow best practices to optimize your Azure deployments.

The Advisor dashboard displays personalized recommendations for all your subscriptions for the following 5 categories:

1. High Availability
2. Security
3. Performance
4. Cost
5. Operational Excellence



Computing Services

Cheat sheets, Practice Exams and Flash cards 👉 www.exampro.co/az-900

Azure Virtual Machines

Windows or Linux virtual machines (VMs). The most common type of compute.
You choose your OS, Memory, CPU, Storage. You share hardware with other customers

Azure Container Instances

Docker as a Service Run containerized apps on Azure without provisioning servers or VMs

Azure Kubernetes Service (AKS)

Kubernetes as a Service. Easy to deploy, manage and scale containerized applications.
Uses the open source Kubernetes (K8) software.

Azure Service Fabric

Tier-1 Enterprise Containers as a Service

Distributed systems platform. Runs in Azure or on-premises.
Easy to package, deploy, and manage scalable and reliable **microservices**.

Azure Functions

Event-driven, serverless compute (functions) run code without provisioning or managing servers.
You pay only for the compute time you consume.

Azure Batch

Plans, schedules and executes your batch computer workloads across running 100+ jobs in parallel.
Use Spot VMs to save money (previously used Low-priority VMs to save on compute)

Storage Services

Cheat sheets, Practice Exams and Flash cards 👉 www.exampro.co/az-900

Azure Blob Storage

Object Serverless Storage. Store very large files and large amounts of unstructured files.
Pay for what you store, unlimited storage, no-resizing volumes, no filesystem protocols.

Azure Disk Storage

A virtual volume. Choose SSD or HDD, encryption by default, attach volume to VMs

Azure File Storage

A shared volume that you can access and manage like a file server. eg SMB

***Azure Queue Storage**

Messaging Queue A data store for queuing and reliably delivering messages between applications

***Azure Table Storage**

Wide-Column NoSQL Database A NoSQL store that hosts unstructured data independent of any schema

Azure Data Box / Azure Databox Heavy

A rugged briefcase computer and storage designed to move terabytes or petabytes of data

Azure Archive Storage

Long term cold storage for when you need to hold onto files for years on the cheapest storage options

Azure Data Lake Storage

A centralized repository that allows you to store all your structured and unstructured data at any scale.

Database Services

Cheat sheets, Practice Exams and Flash cards 👉 www.exampro.co/az-900

Azure Cosmos DB

A fully managed **NoSQL databases**. Designed for scale with guarantee of 99.999% availability

Azure SQL Database

Fully managed MS SQL database with auto-scale, integral intelligence, and robust security

Azure Database for MySQL / PSQL / MariaDB

Fully managed and scalable **MySQL / PostgreSQL / MariaDB database** with high availability and security

SQL Server on VMs

Host enterprise SQL Server apps in the cloud. Lift-and-shift MS SQL servers from on-premise to Azure Cloud.

Azure Synapse Analytics (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 Table Storage**

Wide-Column NoSQL Database A NoSQL store that hosts unstructured data independent of any schema

Application Integration Services

Cheat sheets, Practice Exams and Flash cards 👉 www.exampro.co/az-900

Azure Notifications Hub

Pub/Sub Send push notifications to any platform from any back end

Azure API Apps

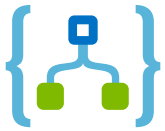
API Gateway Quickly build and consume APIs in the cloud. Route APIs to Azure Services

Azure Service Bus

Service Bus Reliable cloud messaging as a service (MaaS) and simple hybrid integration

Azure Stream Analytics

Serverless **real-time analytics**, from the cloud to the edge



Azure Logic Apps

Schedule, automate and orchestrate tasks, businesses processes and workflows.
Integration with Enterprise SaaS and Enterprise applications.

Azure API Management

Hybrid, multi-cloud management platform for APIs across all environments.
Put in-front of existing APIs to add additional functionality.

***Azure Queue Storage**

Messaging Queue A data store for queuing and reliably delivering messages between applications

Developer and Mobile Tools

Cheat sheets, Practice Exams and Flash cards 👉 www.exampro.co/az-900

Azure SignalR Service

Real-Time Messaging Easily add real-time web functionality to applications

Think of it like the Pusher for Azure

Azure App Service

Easy to use service for deploying and scaling web-applications with .Net, Node.js Java, Python and PHP

Developer focus on building their web-apps, and not worry about the underlying infrastructure

Think of it like Heroku for Azure

Visual Studio (Microsoft-owned)

Code Editor The integrated development environment (IDE) designed for creating powerful, scalable applications for Azure

Xamarin (Microsoft-owned)

Mobile-App Framework Create powerful and scalable native mobile apps with .NET and Azure

Azure DevOps Services

Cheat sheets, Practice Exams and Flash cards 👉 www.exampro.co/az-900

Azure DevOps

Plan smarter, collaborate , and ship faster with a set of modern dev services.

Azure Boards

Kanban Deliver value to your users faster using proven agile tools to plan, track, and discuss work across your teams.

Azure Pipelines

Build, test, and deploy with **CI/CD** that works with any language, platform, and cloud. Connect to GitHub or any other Git provider and deploy continuously.

Azure Repos

Get unlimited, cloud-hosted private **Git repos** and collaborate to build better code with pull requests and advanced file management.

Azure Test Plans

Test and ship with confidence using **manual and exploratory testing tools**.

Azure Artifacts

Create, host, and share packages with your team, and add artifacts to CI/CD pipelines with a single click.

Azure DevTest Labs

Fast, easy, and lean dev-test environments

Azure Resource Manager

What is Infrastructure as code (IaC)?

The process of managing and provisioning computer data centers through machine-readable definition files, rather than physical hardware configuration or interactive configuration tools.

Azure Resource Manager (ARM) allows you to programmatically create Azure resources via JSON template.

Launch VM

```
{
  "$schema": "https://schema.management.azure.com/schemas/2019-04-01/deploymentTemplate.json#",
  "resources": [{
    "type": "Microsoft.Compute/virtualMachines",
    "name": "MyServer",
    "properties": {
      "hardwareProfile": {
        "vmSize": "Standard_A4"
    }
  }]
}
```

Azure QuickStart Templates

Azure QuickStart is a library of a **pre-made ARM templates** provided by the community and partners to help you quickly launch new projects for a variety of stack scenarios:

Deploy a Django app

This template uses the Azure Linux CustomScript extension to deploy an application. This example creates an Ubuntu VM, does a silent install of Python, Django...


by Madhan Arumugam Ramakrishnan,

Last updated: 5/2/2019

Deploy an Ubuntu VM with Docker Engine

This template allows you to deploy an Ubuntu VM with Docker (using the Docker Extension). You can later SSH into the VM and run Docker containers.


by Corey Sanders,

Last updated: 12/11/2019

CI/CD & Containerized App Deploy Docker Enterpise & Jenkins

This quick start launches a stack that allows you to Build, Run & Ship Containerized Applications using Docker Enterprise Edition and CloudBees Jenkins. This integrated sta...


by Mazhar Hussain Warsi,

Last updated: 12/6/2019

Web App on Linux with PostgreSQL

This template provides a easy way to deploy Web App on Linux with Azure database for PostgreSQL.

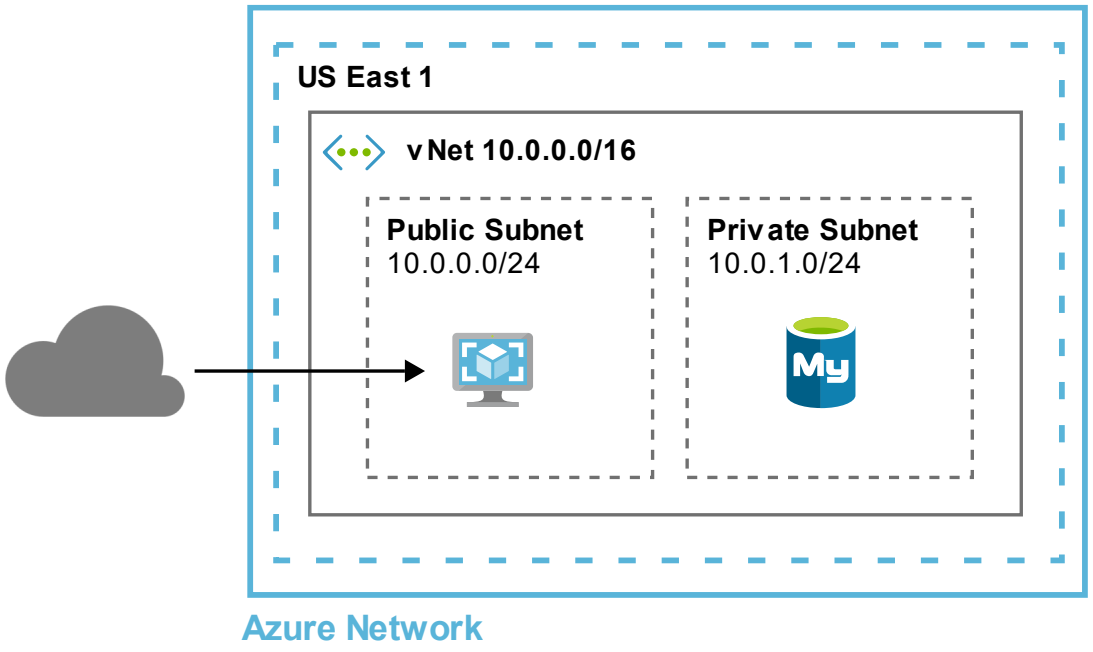

by Sunitha Muthukrishna,

Last updated: 5/5/2020

Azure Virtual Network (vNet) and Subnets

Virtual Network (vNet) is a logically isolated section of the Azure Network where you launch your Azure resources. You choose a **range of IPs using CIDR Range**

CIDR Range of **10.0.0.0/16 = 65,536** IP Addresses



Subnets a logical partition of an IP network into multiple smaller network segments. **You are breaking up your IP range for VNet** into smaller networks.

Subnets **need to have a smaller CIDR range than to the vNet** represent their portion.
eg Subnet CIDR Range 10.0.0.0/24 = 256 IP Addresses

A Public Subnet is one that can reach the internet

A Private Subnet is one that cannot reach the internet

Cloud-Native Networking Services

Azure DNS

Provides ultra-fast DNS responses and ultra-high domain availability

Azure Virtual Network (vNET)

A logical isolated section of the Azure network for customers to launch Azure resources within.

Azure Load Balancer

OSI Level 4 (Transport) Load Balancer

Azure Application Gateway

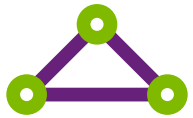
OSI Level 7 (HTTP) Load Balancer, can apply a Web Application Firewall

Network Security Groups

A virtual firewall at the subnet level

Enterprise/Hybrid Networking Services

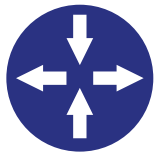
Azure Front Door
Scalable and secure entry point for fast delivery of your global applications



Azure Express Route
A connection between your on-premise to Azure cloud from 50 Mbps to 10 Gbps

Virtual WAN
a networking service that brings many networking, security, and routing functionalities together to provide a single operational interface

Azure Connection
A VPN connection securely connects two Azure local network via (IPsec).

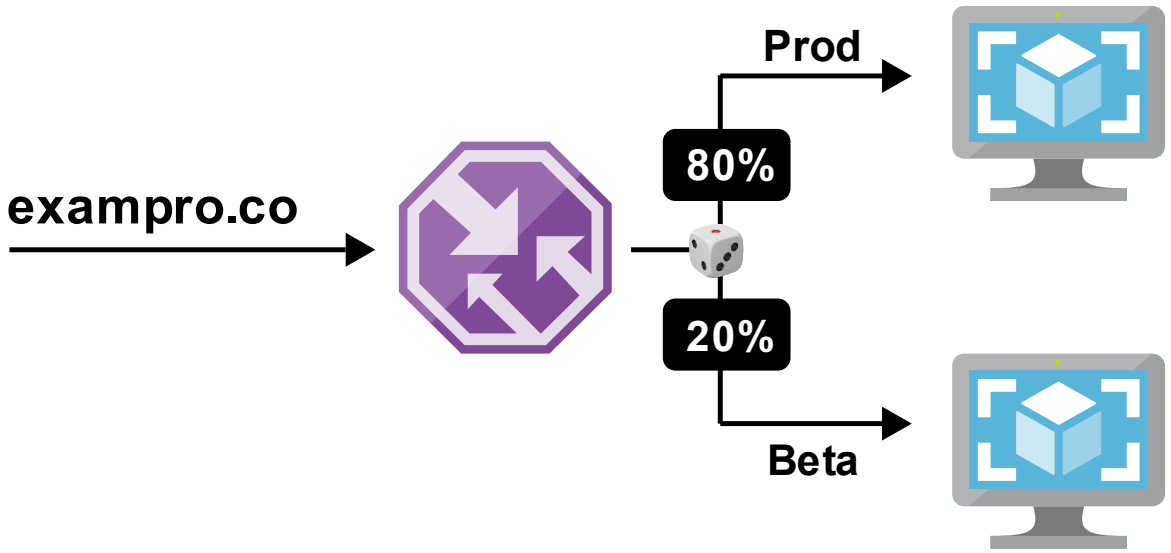


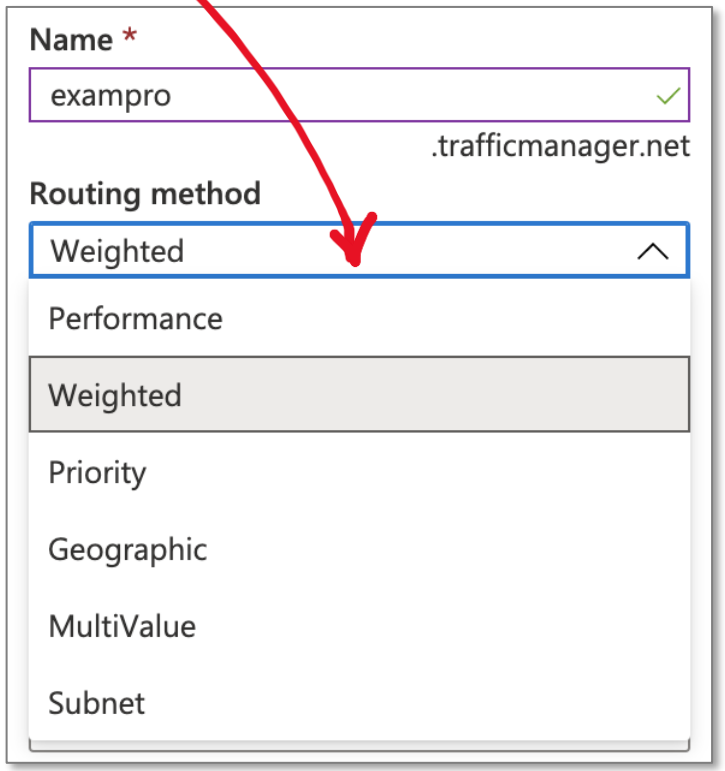
Virtual Network Gateway
A site-to-site VPN connection between an Azure virtual network and your local network

Azure Traffic Manager

Azure Traffic Manager operates at the **DNS layer** to quickly and efficiently direct incoming DNS requests based on the **routing method of your choice**.

- Route traffic to servers the geographically near by to reduce latency
- Fail-over to redundant systems in-case primary systems become unhealthy.
- Route to random VM to simulate A/B testing





Azure DNS

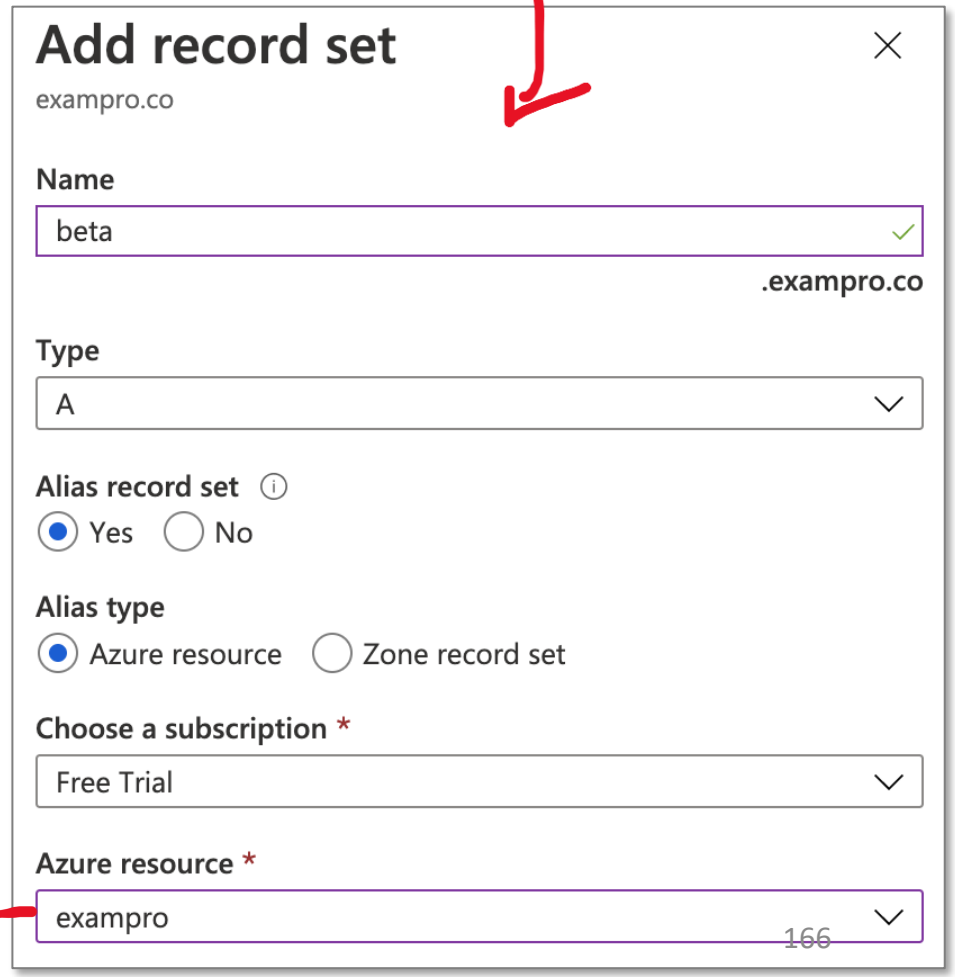
Cheat sheets, Practice Exams and Flash cards 👉 www.exampro.co/az-900

Azure DNS allows you to host your domains names on Azure.
You can create DNS Zones and **manage your DNS records**.

Azure DNS **does not allow you to purchase domains**.
Only the ability to manage DNS records.

Search record sets

Name	Type	TTL	Value
@	NS	172800	ns1-08.azure-dns.com. ns2-08.azure-dns.net. ns3-08.azure-dns.org. ns4-08.azure-dns.info.
@	SOA	3600	Email: azuredns-host... Host: ns1-08.azure-d... Refresh: 3600 Retry: 300 Expire: 2419200 Minimum TTL: 300 Serial number: 1



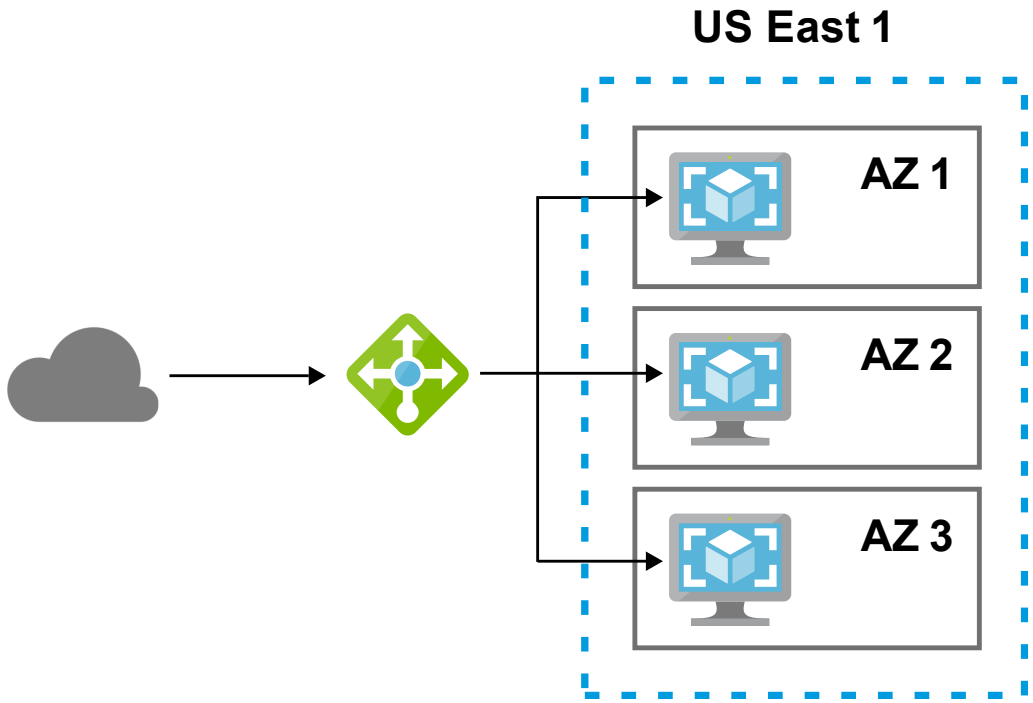
Azure Load Balancer

Azure Load Balancer is used for evenly distributing incoming network traffic across a group of backend resources or servers.

Azure Load Balancer operates on **OSI Layer 4 (Transport)**

You can create a:

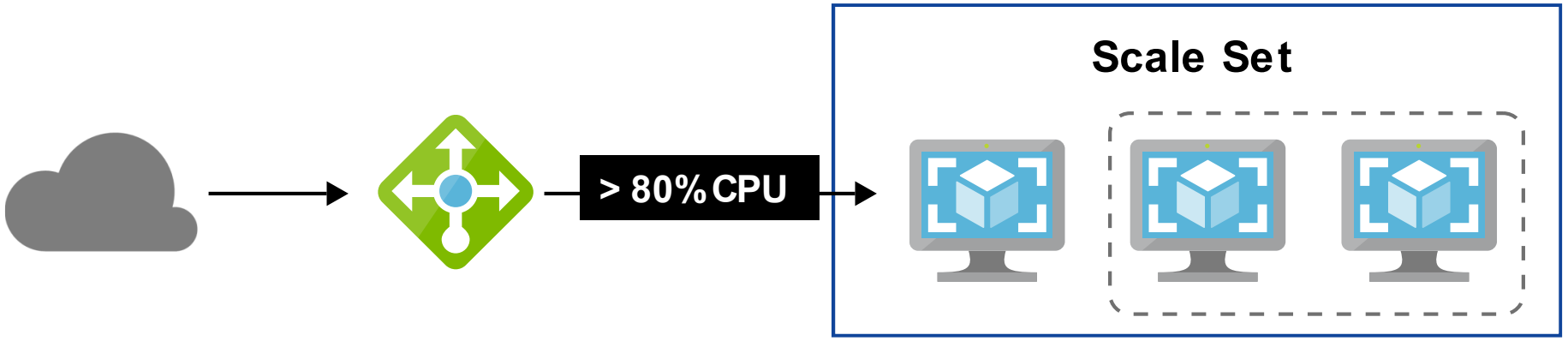
- **Public Load Balancer** incoming traffic from the internet **to public-facing servers** (Public IPs)
- **Internal (Private) Load Balancer** incoming internal network traffic to **private-facing servers** (Private IPs)



Scale Sets

Allows you group together identical Virtual Machines (VMs) and **automatically** **increase or decrease the amount of servers** based on:

- change in CPU, memory, disk, and network performance
- On a predefined schedule



IoT Services

What is Internet of Things (IoTs)?

A network of Internet connected objects (usually hardware) able to collect and exchange data.

- Smart Bulbs
- Smart Fridges
- Smart Light Switches
- Narrowband vs Wideband hardware
- Security Cameras
- Voice Command Speakers
- Temperature, Pressure or Humidity Sensors
- Drones
- Phones
- Buttons

IoT Services

IoT Central

Connects your IoT devices to the cloud

IoT Hub

Enable highly secure and reliable communication between your IoT application and the devices it manage

IoT Edge

A fully managed service built on Azure IoT Hub. It allows data processing and analysis nearest the IoT devices. Edge computing is when you offload compute from the cloud to local computing hardware such as IoT devices, phones or home computers

Azure IoT Edge strengthens privacy protection and security by enabling localized data processing. This approach minimizes the need to transmit sensitive data to remote servers, reducing the risk of data exposure during transit. With IoT Edge, you can implement robust security measures and enforce data access controls at the device level, ensuring sensitive information remains safeguarded, even in challenging or disconnected environments.

Windows 10 IoT Core Services

A cloud services subscription that provides the essential **services** needed to commercialize a device on **Windows 10 IoT Core.** Long-term OS support and services to manage device updates and assess device health

Big Data and Analytics Services

What is BigData?

A term used to describe **massive volumes of structured/unstructured data** that is so large it is difficult to **move and process** using traditional database and software techniques.

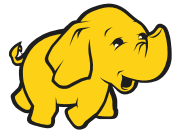
Azure Synapse Analytics *(formally known as SQL Data Warehouse)*

Enterprise **data warehousing and Big Data analytics**.

Intended to **run SQL queries** against large databases for things such as **reporting**.

HDInsight

Run **open-source analytics software** such as Hadoop, Kafka and Spark



Azure Databricks

An Apache Spark-based analytics platform optimized for the Microsoft Azure cloud services platform.

Third-Party Databricks cloud services supported within Azure.

Data Lake Analytics

An on-demand analytics job service that simplifies big data.

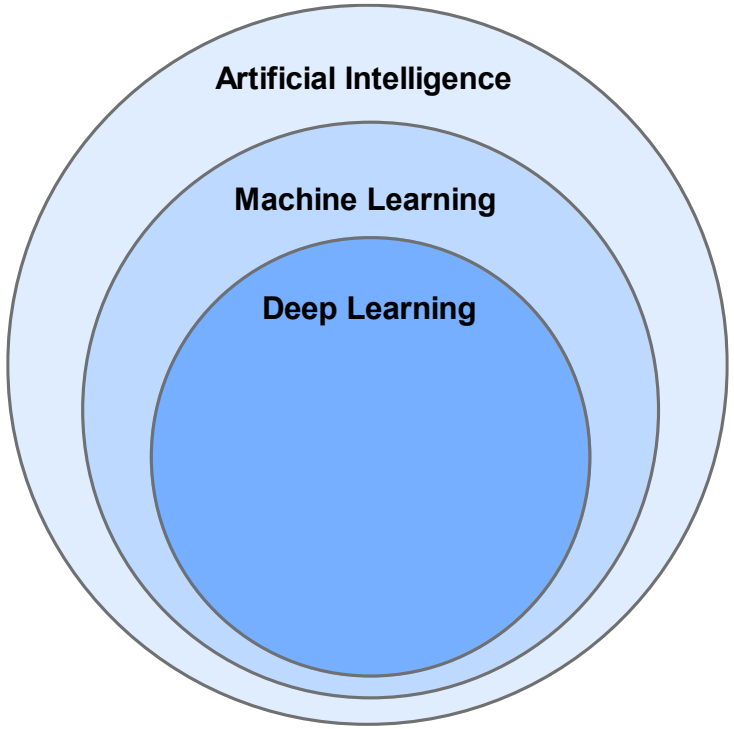
A **data lake** is a storage repository that holds a vast amount of raw **data** in its native format until it is needed.

AI/ML Services

What is Artificial Intelligence (AI)?
Machines that perform jobs that mimic human behavior

What is Machine Learning (ML)?
Machines that get better at a task without explicit programming

What is Deep Learning (DL)?
Machines that have an artificial neural network inspired by the human brain to solve complex problems.



Azure Machine Learning Service
A service for that simplifies running AI/ML related workloads allowing you to build flexible Pipelines to automate workflow. Use Python an R, Run DL workloads such as Tensorflow

Azure Machine Learning Studio (classic)
An older service that manages AI/ML workloads. Does not have a pipeline and other limitations. Workloads are not easily transferable to from classic to the new service.

AI/ML Services

Cheat sheets, Practice Exams and Flash cards 👉 www.exampro.co/az-900

Personalizer Deliver rich, personalised experiences for every user.

Translator Add real-time, multi-language text translation to your apps, website and tools.

Anomaly detector Detect anomalies in data to quickly identify and troubleshoot issues.

Azure Bot Service Intelligent, serverless bot service that scales on demand

Form Recogniser Automate the extraction of text, key/value pairs and tables from your documents.

Computer Vision Easily customise computer vision models for your unique use case.

Language Understanding Build natural language understanding into apps, bots and IoT devices.

AI/ML Services

QnA Maker Create a conversational question-and-answer bot from your existing content.

Text Analytics Extract information such as sentiment, key phrases, named entities and language from your text.

Content moderator Moderate text and images to provide a safer, more positive user experience.

Face Detect and identify people and emotions in images.

Ink Recogniser Recognise digital ink content, such as handwriting, shapes and document layout.

Serverless Services

What is Serverless?

When the underlying servers, infrastructure and OS is taken care of by the Cloud Service Provider (CSP) It will generally be highly available, scalable and cost-effective.

Event-Driven Scale

A serverless function can be triggered or trigger other events allowing you to compose complex applications and its just scales.

Abstraction of Servers

Servers are abstracted away. Your code is described as functions. These functions can be running on different compute instances.

Micro-Billing

Serverless compute could run for a fraction of a second.
Billing into micro-seconds will save you money.

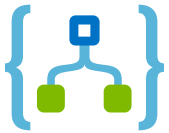
Serverless Services

Azure Functions

Run small amounts of code known as serverless functions in your favorite language: C#, Java, JavaScript, Python and PowerShell

Blob Storage

Serverless Object Storage. Just upload files, don't think about the underlying file-systems, resizing



Logic Apps

Allows you to build serverless workflows composed of Azure Functions Building a state machines for serverless compute.

Event Grid

Uses Pub/Sub messaging system to allow you react to events and trigger other Azure cloud services such as Azure Functions.

Pricing and Support – SLAs

Service Level Agreement (SLA) describes Azure's commitments for **uptime** and **connectivity**

SLA's are individualized per Azure service

Uptime and connectivity is described as **Performance Targets**

A Performance Target is represented as a **percentage %**.

- 99% (two nines)
- 99.9% (three nines)
- 99.999% (five nines)
- 99.9999999% (nine nines)

Azure not does provide SLAs for Free Tier or the shared tiers.

Pricing and Support – Service Credits

Service Credits

customers may **have a discount applied to their Azure bill**, **as compensation for an under-performing Azure product or service** based on the SLA.

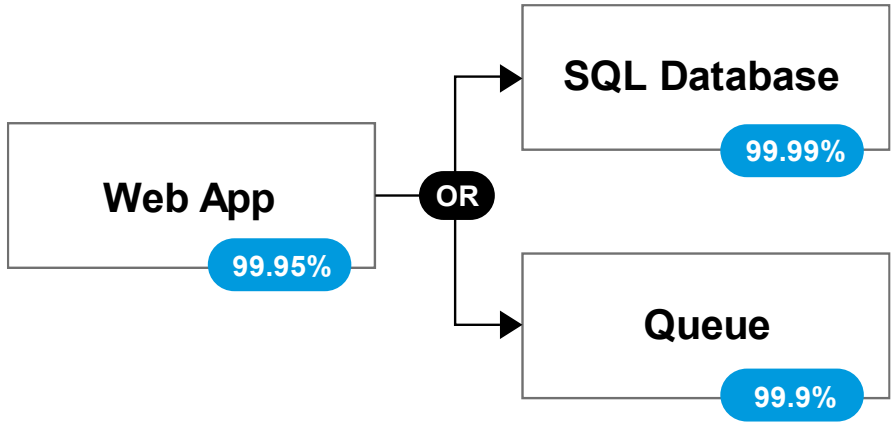
Azure Virtual Machine Service Credit Calculation

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

Pricing and Support – Composite SLA

Different services have different SLAs.

A Composite SLA is when you **combine** SLAs across different service offerings.



The real SLA for a Web-App + SQL Database would be:
99.95% × 99.99% = 99.94%.

Fallback systems will improve overall SLA.
Imagine SQL Database was down but you had a queue
Saving transactions attempts from Web App to Queue to write to DB.
Web app *and* (database *or* queue) = 99.95% × 99.99999% = ~99.95%

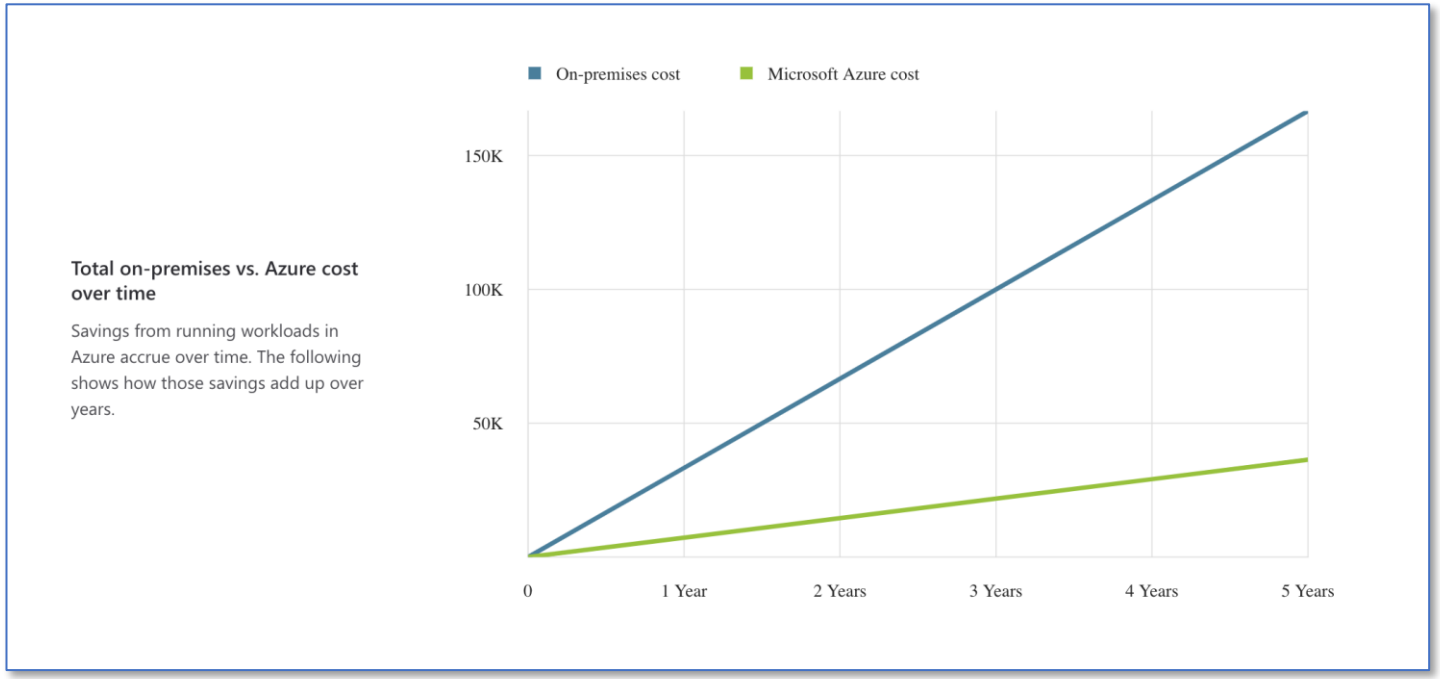
Pricing and Support – TCO Calculator

Estimate the cost savings you can realize by migrating your workloads to Azure

Generate out a detailed report and export as a PDF to send to decision makers.

azure.microsoft.com/pricing/calculator

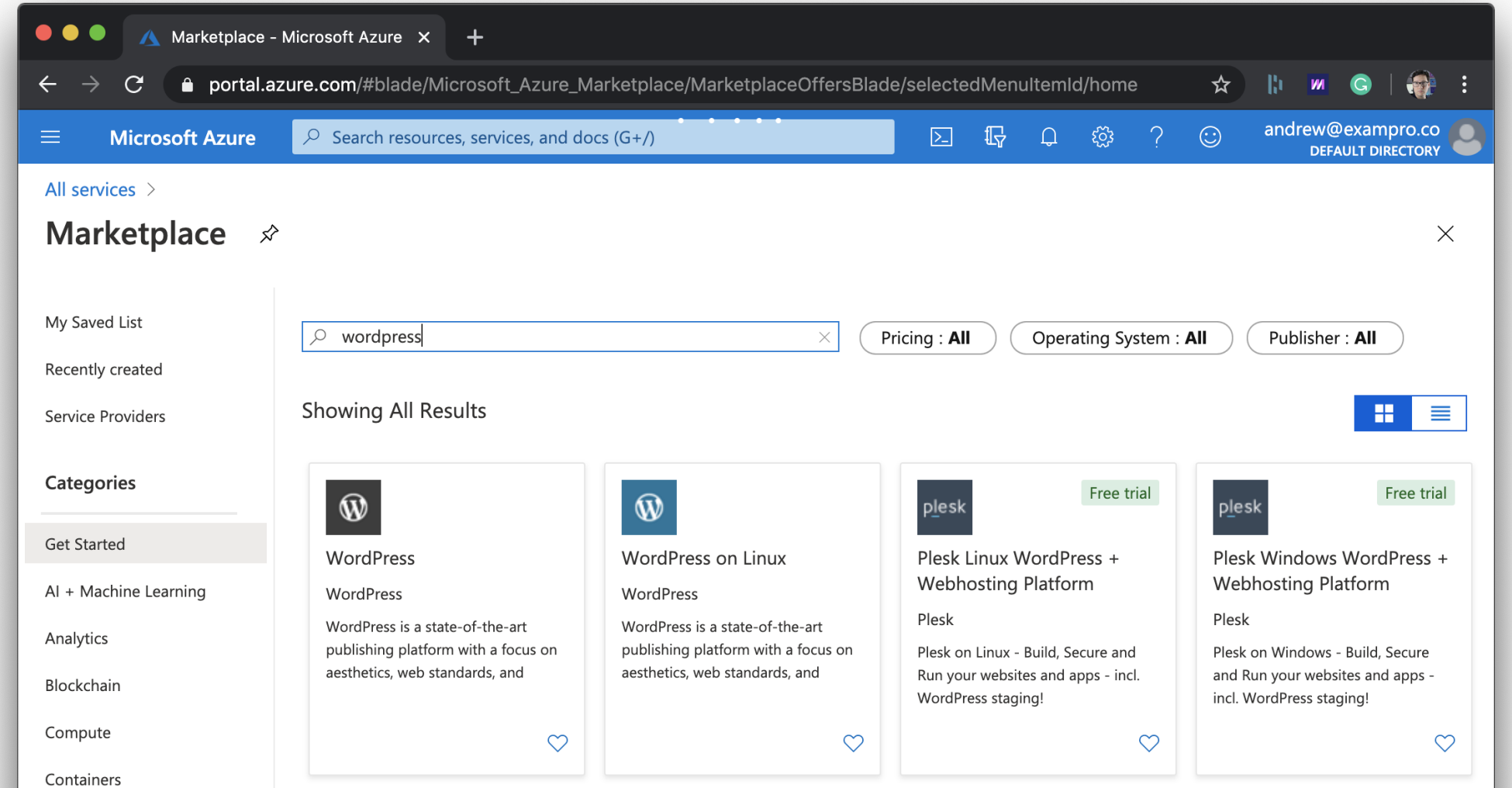
Over 5 year(s) with Microsoft Azure, your estimated cost savings could be as much as $130,191



Azure Marketplace

Cheat sheets, Practice Exams and Flash cards 👉 www.exampro.co/az-900

Azure Marketplace are **apps and services** made available by **third-party publishers** to quickly get started.
The available apps and services can be Free, Free-Trial, Pay-As-You-Go, Bring-Your-Own-License (BYOL)



Azure Support Plans

Cheat sheets, Practice Exams and Flash cards 👉 www.exampro.co/az-900

Basic	Developer	Standard	Professional Direct
Email Support only For **Billing and Account**	✉️ Email Tech Support		
	Reply during Business Hours	📞 24/7 Phone Support	
	Third Party Software Support		
	Minimal business impact (Sev C) < 8 hours		(Sev C) < 4 hours
		Moderate (Sev B) < 4 hours	(Sev B) < 2 hours
		Critical business impact (Sev A) < 1 hour	
Azure Advisor, Azure Health Status, Community Support, Azure Documentation			
	Architecture General Guidance		😎 Architecture, Operational Support and Proactive Guidance by pool **ProDirect** delivery managers
			👨‍🏫 Webinars led by Azure Engineers
$0 USD / month	**$29 USD / month**	**$100 USD / month**	**$1000 USD / month**

Azure Licensing – Azure Hybrid Benefit

Many customers have invested in **Windows Server licenses** and would like to **repurpose this investment** on Azure.

Azure Hybrid Use Benefit (HUB)

Gives customers the right to use these licenses for virtual machines on Azure.

- Windows Servers
- SQL Servers

  - HUB can be turned on and off at anytime for existing VMs
  - HUB can be applied at deployment time for new VMs

Bring your own license (BYOL)

Azure Subscriptions

An Azure Subscription is the same as saying our Azure Account.

There are **4 tiers** of Azure Subscriptions:

Free Subscription

- Credit Card Required
- $200 USD credits free for 30 days
- Certain Azure products free for 12 months

Pay-As-You-Go (PAYG) Subscription

- Credit Card Required
- Charged end at the of the month based on consumed cloud resources

Enterprise Agreement

- An Enterprise and Azure agree on receive discounted price for licenses and cloud services

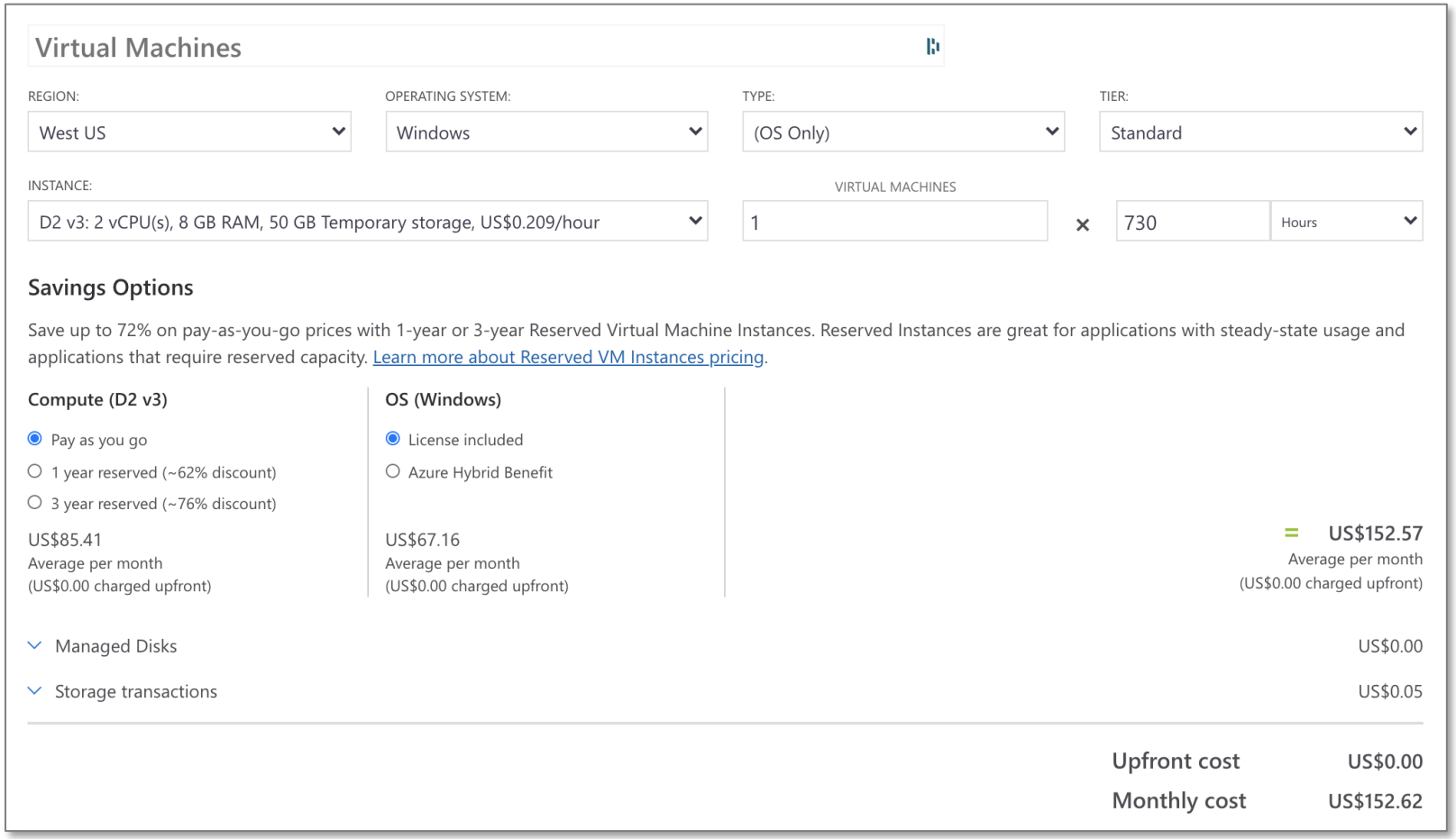
Student Subscription

- No Credit Card Required
- $100 USD credits for 12 months
- Requires valid student email

Azure Pricing Calculator

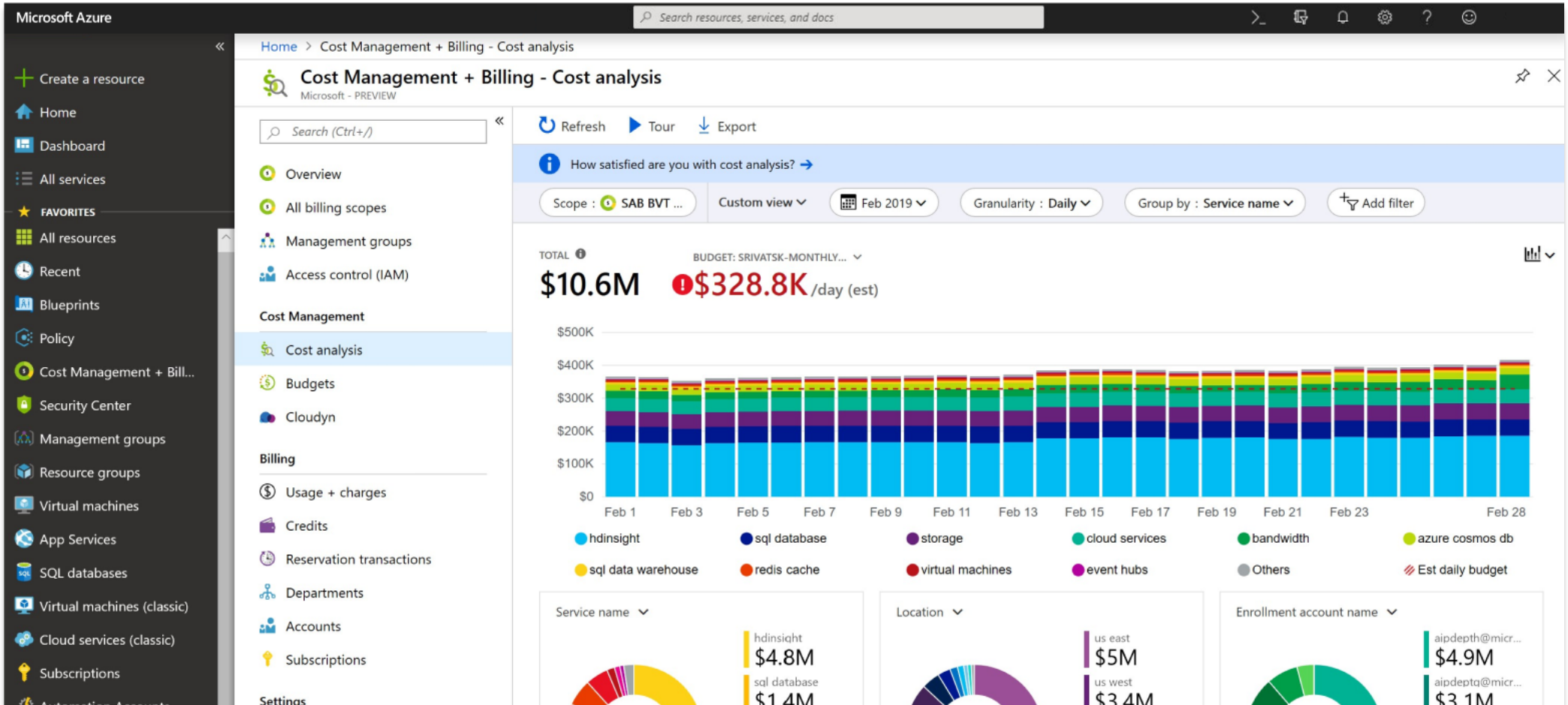
Configure and estimate the costs for Azure products. No Sign-in require.
Download an **Excel spreadsheet** and share with your boss.

azure.microsoft.com/pricing/calculator



Azure Cost Management

Perform **cost-analysis**, visualize the spending of your Azure cloud resources
Create **budgets**, set a budget threshold be alerted when approaching or exceeded

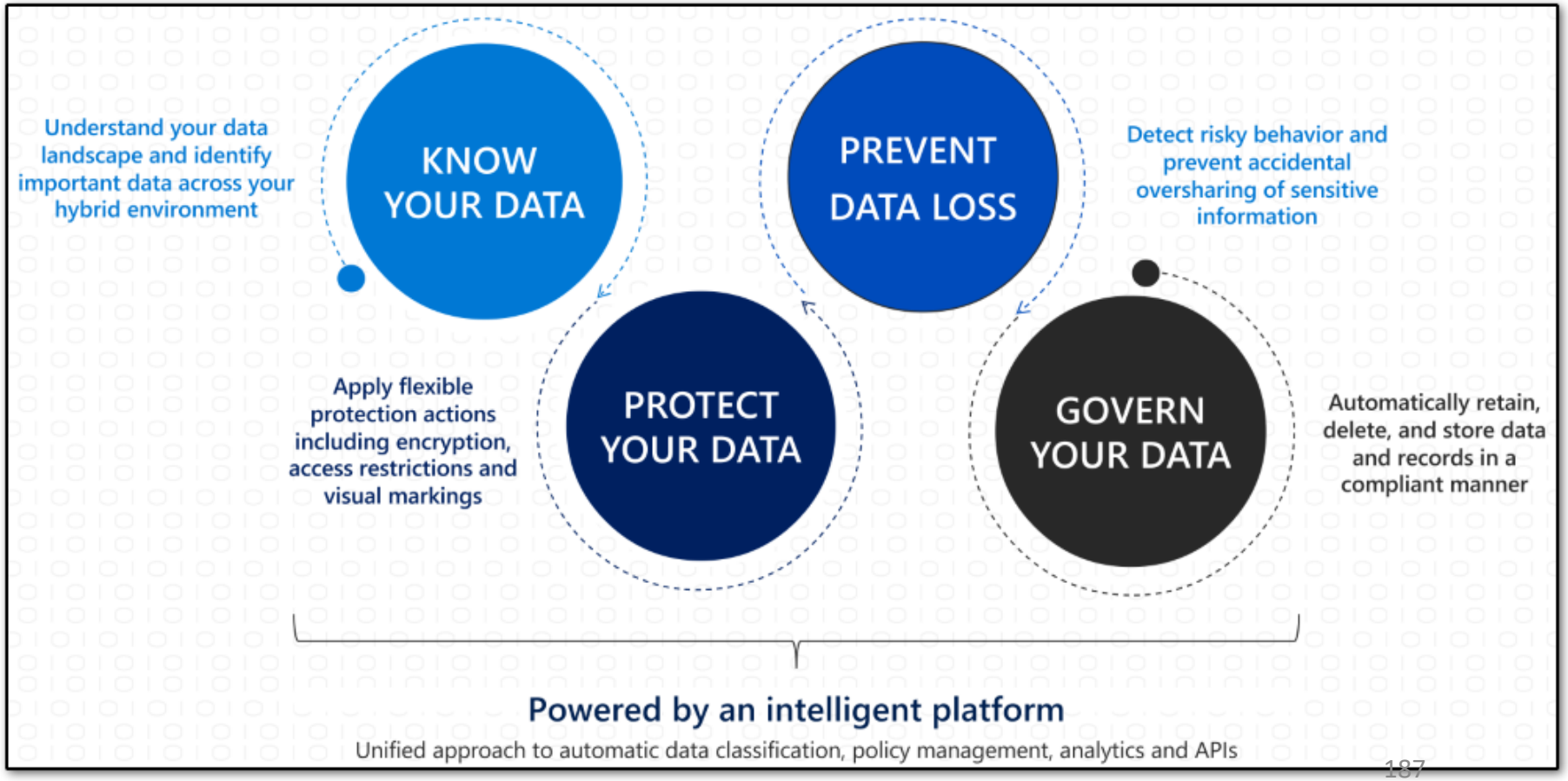


Microsoft Purview Information Protection

Microsoft Purview Information Protection (MPIP) is a collection of features within **Microsoft Purview** (formerly Microsoft 365 Compliance) to help **you discover, classify, and protect** sensitive information wherever it lives or travels.

MPIP capabilities:

- Know your data
- Protect your data
- Prevent Data Loss
- Govern your Data



MPIP – Know your data

Know your data

Understand your **data landscape** and identify important data across your hybrid environment

Sensitive information types

Identifies sensitive data by using **built-in or custom regular expressions** or a function.
Corroborative evidence includes keywords, confidence levels, and proximity.

- Built-in sensitive labels

Trainable classifiers

Identifies sensitive data by using examples of the data you're interested in rather than identifying elements in the item (pattern matching). You can use built-in classifiers or train a classifier with your own content.

- Trainable classifiers

Data classification

A **graphical identification of items** in your organization that have a sensitivity label, a retention label, or have been classified.
You can also use this information to gain insights into the actions that your users are taking on these items.

- Content explorer
- Activity explorer

MPIP – Protect your data

Protect your data

apply **flexible protection** actions that include encryption, access restrictions, and visual markings

- Sensitivity labels
- Azure Information Protection unified labeling client
- Double Key Encryption
- Office 365 Message Encryption (OME)
- Service encryption with Customer Key
- SharePoint Information Rights Management (IRM)
- Rights Management connector
- Azure Information Protection unified labeling scanner
- Microsoft Defender for Cloud Apps
- Microsoft Information Protection SDK

MPIP – Prevent data loss

Prevent data loss

prevent **accidental oversharing** of sensitive information

- Microsoft Purview Data loss prevention (DLP)
- Endpoint data loss prevention
- Microsoft Compliance Extension – Chrome Extension
- Microsoft Purview data loss prevention on-premises scanner
- Protect sensitive information in Microsoft Teams chat and channel messages

MPDLM – Govern Your Data

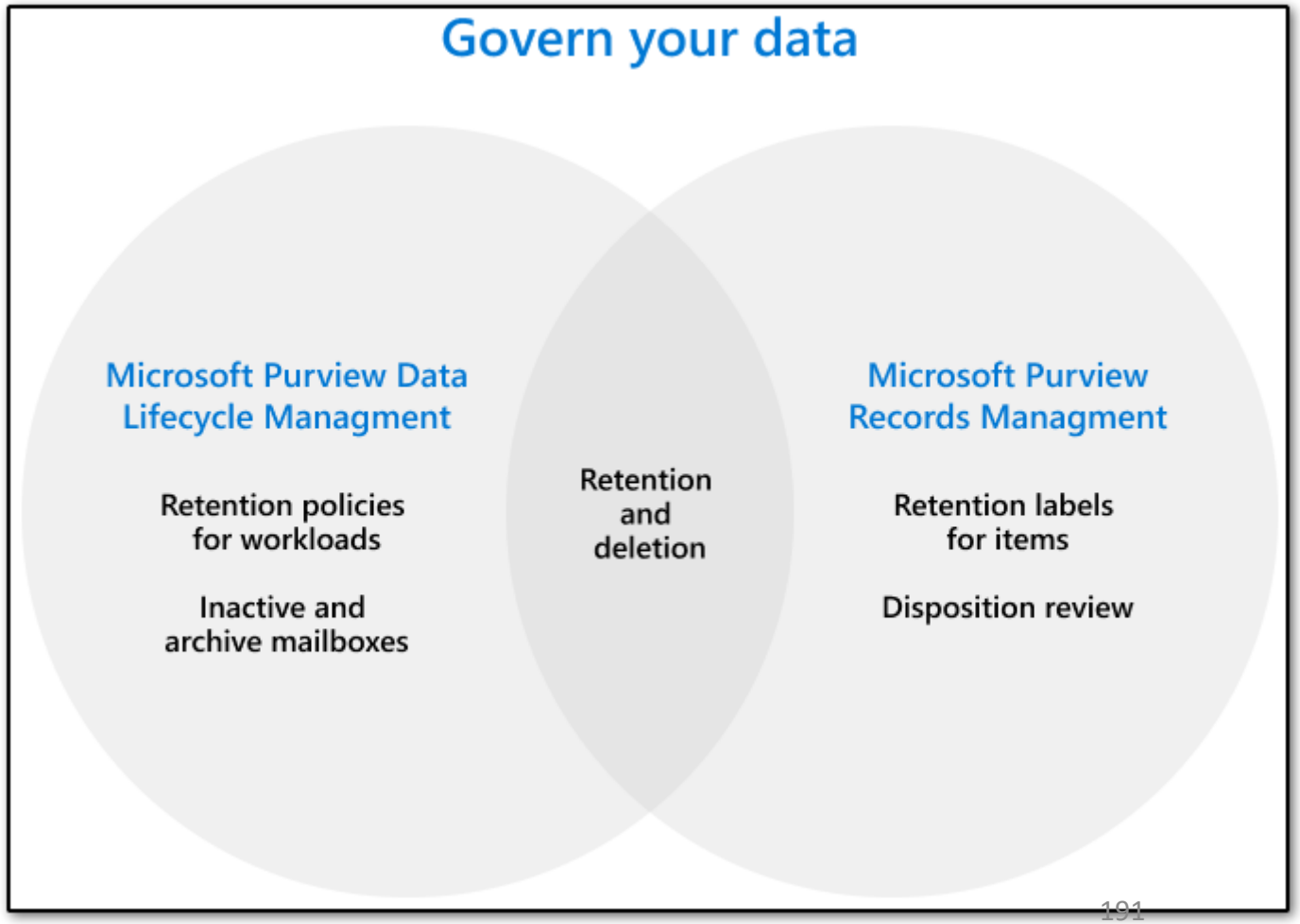
Microsoft Purview Data Lifecycle Management (formerly Microsoft Information Governance) is a collection of features to **govern your data for compliance** or regulatory

Microsoft Purview Data Lifecycle Management
To keep what you need and delete what you don't

- Retention policies and retention labels
- Inactive mailboxes
- Archive mailboxes
- Import service for PST files

Microsoft Purview Records Management
Manage high-value items for business, legal, or regulatory record-keeping requirements

- File plan
- Retention labels for individual items, retention policies if needed for baseline retention
- Disposition review and proof of disposition



Introduction to Azure Policies

Azure Policy enforce organizational standards and to assess **compliance** at-scale
Policies do not restrict access, they only observe for compliance.

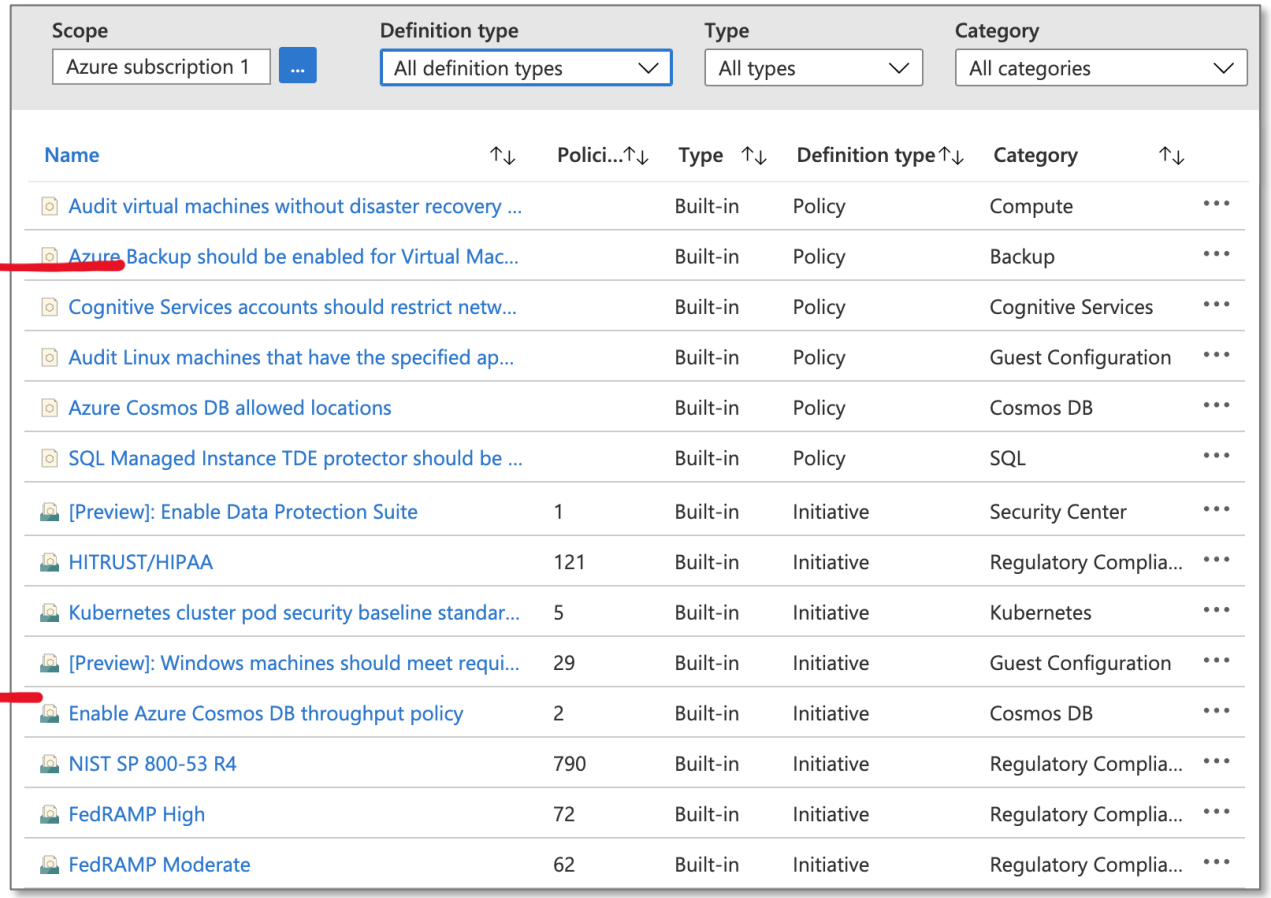
Azure has "built-in" policies you can used right away

Policy Definitions
A policy definition is a **JSON** file used to describe business rules to control access to resources.

Policy Assignment
The scope of a policy can effect. Assigned to a user, a resource group or management group.

Policy Parameters
Values you can pass into your Policy definition so your Policies are more flexible for re-use.

Initiative Definitions
An initiative definition is a collection of policy definitions, that you can assign. eg. A group of policies to enforce **PCI-DSS compliance**



Name	Polici...	Type	Definition type	Category
Audit virtual machines without disaster recovery ...		Built-in	Policy	Compute
Azure Backup should be enabled for Virtual Mac...		Built-in	Policy	Backup
Cognitive Services accounts should restrict netw...		Built-in	Policy	Cognitive Services
Audit Linux machines that have the specified ap...		Built-in	Policy	Guest Configuration
Azure Cosmos DB allowed locations		Built-in	Policy	Cosmos DB
SQL Managed Instance TDE protector should be ...		Built-in	Policy	SQL
[Preview]: Enable Data Protection Suite	1	Built-in	Initiative	Security Center
HITRUST/HIPAA	121	Built-in	Initiative	Regulatory Complia...
Kubernetes cluster pod security baseline standar...	5	Built-in	Initiative	Kubernetes
[Preview]: Windows machines should meet requi...	29	Built-in	Initiative	Guest Configuration
Enable Azure Cosmos DB throughput policy	2	Built-in	Initiative	Cosmos DB
NIST SP 800-53 R4	790	Built-in	Initiative	Regulatory Complia...
FedRAMP High	72	Built-in	Initiative	Regulatory Complia...
FedRAMP Moderate	62	Built-in	Initiative	Regulatory Complia...

Resource Locks

As an admin, you may need to **lock a subscription, resource group, or resource** to **prevent other users from accidentally deleting or modifying critical resources.**

In the **Azure Portal** you can set the following lock levels.

CanNotDelete (Delete)
authorized users can still read and modify a resource, but they can't delete the resource.

ReadOnly (Read-only)
authorized users can read a resource, but they can't delete or update the resource

Azure Blueprints

Azure Blueprints enable **quick creation** of **governed subscriptions**.
Compose artifacts based on common or organization-based patterns into re-usable blueprints.
The service is designed to help with *environment setup*

Blueprints are a declarative way to orchestrate the deployment of various resource templates and other artifacts such as:

- Role Assignments
- Policy Assignments
- Azure Resource Manager templates (ARM templates)
- Resource Groups

The Azure Blueprints service is backed by the globally distributed **Azure Cosmos DB**
Blueprint objects are replicated to multiple Azure regions.

ARM Templates vs Azure Blueprints

Nearly everything that you want to include for deployment in Azure Blueprints can be accomplished with an ARM template.

ARM Template

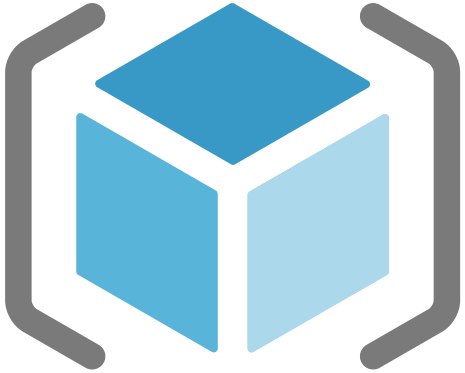
- ARM templates are stored either locally or in source control.
- There's no active connection or relationship to the ARM template

Azure Blueprints

- relationship between the blueprint definition (what *should be* deployed) and the blueprint assignment (what *was* deployed)
- can also upgrade several subscriptions at once that are governed by the same blueprint

Azure Blueprints supports **improved tracking and auditing of deployments**

Azure Resource Manager

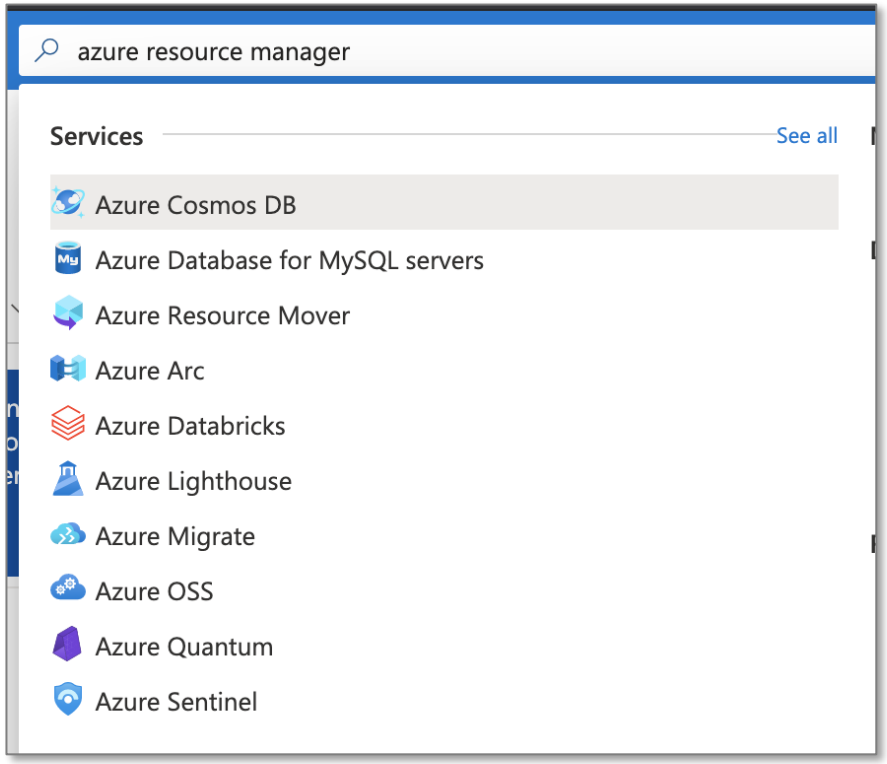


A **deployment and management service** for Azure
Enables you to **create**, **update**, and **delete** resources in your Azure account

Introduction to Azure Resource Manager

Azure Resource Manager (ARM) is a service that allows you to **manage** Azure resources.

Azure Resource Manager is a collection of services in the Azure Portal, **so you can't simply type** in "Azure Resource Manager"



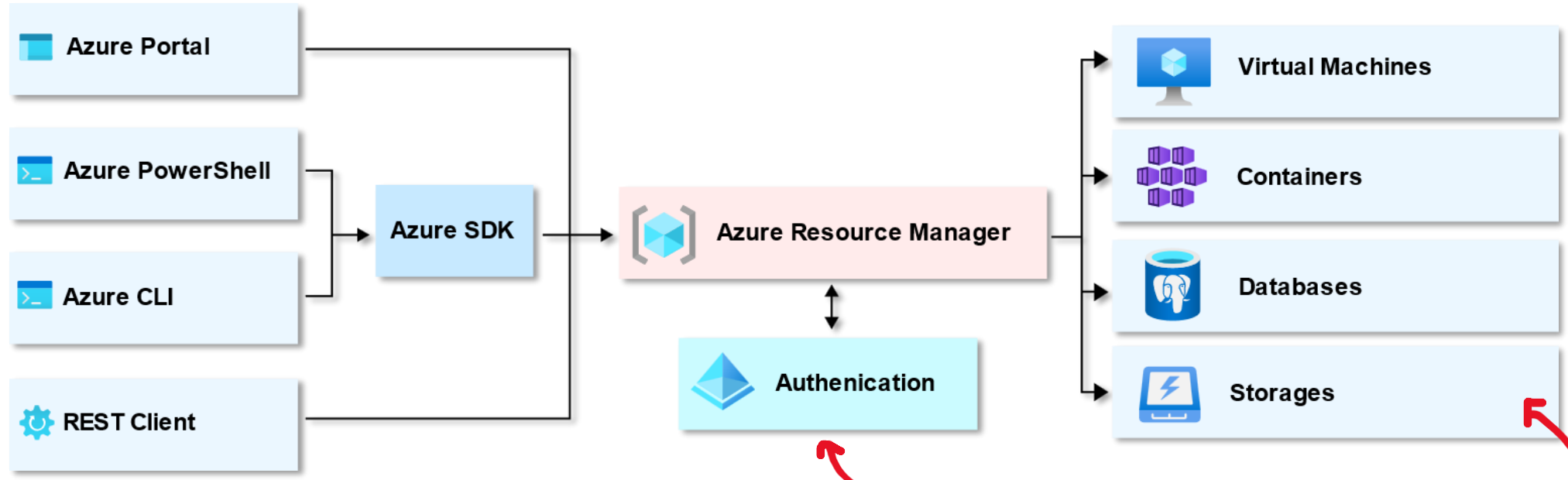
It is a management layer that allows you to:

- Create, Update, Delete Resources
- Apply Management features e.g., Access Controls, Locks, Tags
- Write Infrastructure as Code (IaC) via JSON templates.

We will be examining the following key components that form the **Azure Resource Manager (ARM) layer**:

- Subscriptions
- Management Groups
- Resource Groups
- Resource Providers
- Resource Locks
- Azure Blueprints
- Resource Tags
- Access Control (IAM)
- Role-Based Access Controls (RBAC)
- Azure Policies
- ARM Templates

Azure Resource Manager – Use Case



Think of Azure Resource Manager (ARM) as a **"gatekeeper"**.

All **requests** flow through ARM, and it decides whether that request can be performed on a **resource**

E.g., creation, updating, and deletion of a virtual machine

ARM uses **Azure's RBAC** to determine whether a user has the necessary permissions to carry out a request. When a request is made, ARM checks the user's assigned roles and the permissions associated with those roles. If the user has the necessary permissions, the request is **allowed**; otherwise, it is **denied**.

Azure Resource Manager – Scope

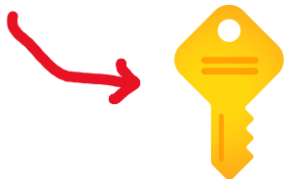
What is scope?

Scope is a **boundary of control** for azure resources. It is a way to **govern** your resource by placing resources

- within a logical grouping
- and applying logical restrictions in the form of rules.

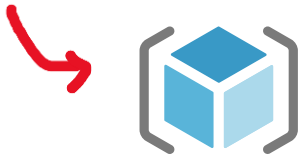
Management Groups

A logical grouping of multiple subscriptions



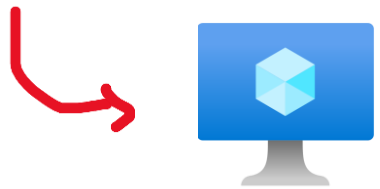
Subscriptions

Grants you access to Azure services based on a billing and support agreement



Resource Groups

A logical grouping of multiple resources



Resources

An azure service e.g., Azure VMs

ARM Templates

What is Infrastructure As Code? (IaC)
The process of **managing and provisioning** computer data centers (e.g., Azure) through machine-readable **definition files** (e.g., JSON files) rather than physical hardware configuration or interactive configuration tools.

You write a script that will setup cloud services for you.

IaCs can either be:

- **Declarative** — You describe your desired outcome, and the system figures out how to achieve it.
- **Imperative** — You provide specific instructions, detailing exactly how to reach the desired state.

ARM templates are **JSON files that define azure resources** you want to provision and azure services you want to configure.

With ARM templates you can:

- **ARM templates** are declarative. (You just outline your desired setup, and the system takes care of the rest)
- Build, remove, or share entire architectures in minutes
- Reduce configuration mistakes
- Know exactly what you have defined for a stack to establish an architecture baseline for compliance

ARM Templates

With ARM templates you can:

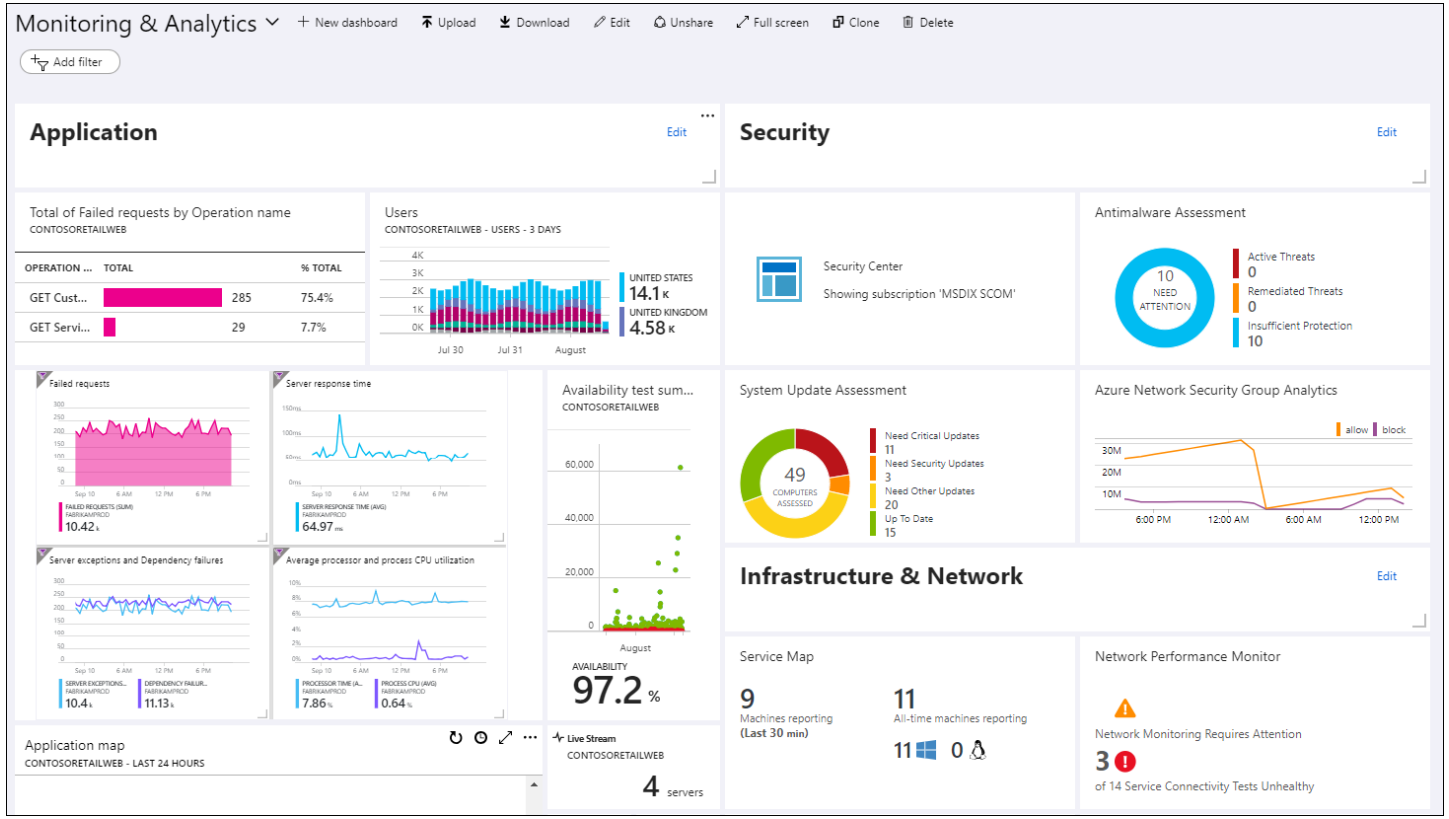
- Establish an architecture baseline for compliance
- **Modularity** Break up your architecture in multiple files and reuse them
- **Extensibility** Add PowerShell and Bash scripts to your templates
- **Testing** You can use the ARM template tool kit (arm-ttk)
- **Preview Changes** Before you create infrastructure via template, see what it will create
- **Built-In Validation** Will only deploy your template if it passes
- **Tracked Deployments** Keep track of changes to architecture over time
- **Policy as Code** Apply Azure policies to ensure you remain compliant
- **Microsoft Blueprints** (establishes relationship between resource and the template)
- **CI/CD integration**
- **Exportable Code** (exporting the current state of a resource groups and resources)
- **Authoring Tools** Visual Studio Code has advanced features for authoring ARM templates

Introduction to Azure Monitor

Azure Monitor comprehensive solution **for collecting, analyzing, and acting on telemetry** from your cloud and on-premises environments

Key Features:
Visual Dashboards: A visual representation of your data.
Smart Alerts: Intelligent notifications based on specific conditions.
Automated Actions: Set automation based on certain triggers.
Log Monitoring: Track and analyze event logs.

Many Azure services by default are already sending telemetry data to Azure Monitor



The Pillars of Observability

What is Observability?
The ability to measure and understand how internal systems work in order to answer questions regarding performance, tolerance, security and faults with a system / application.

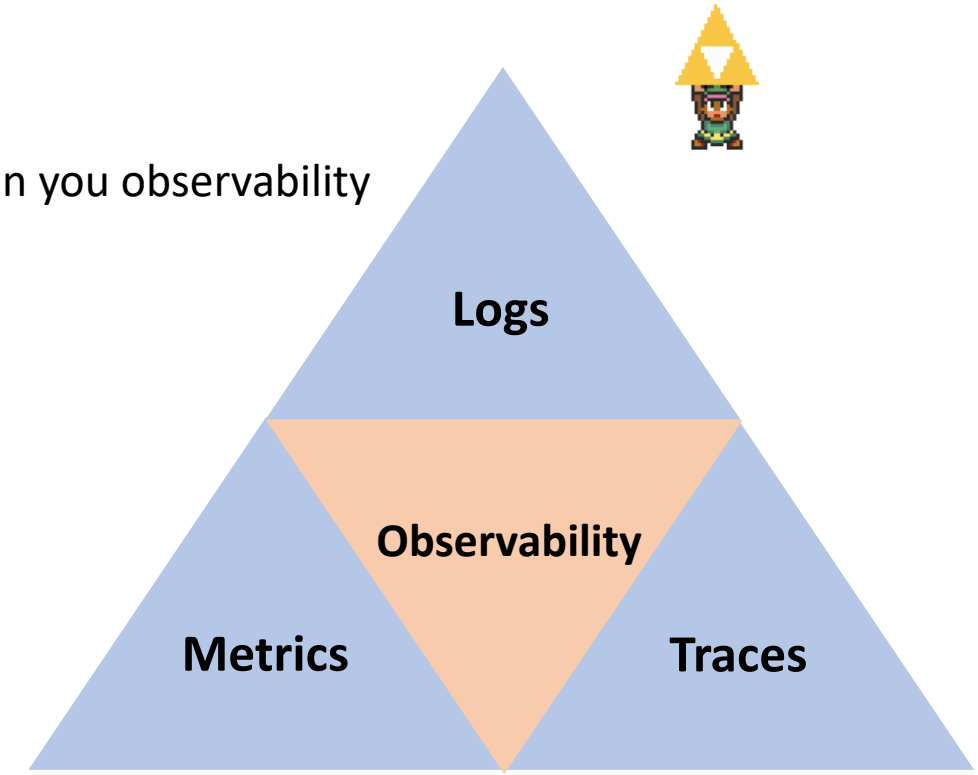
To obtain observability you need to use **Metrics**, **Logs** and **Traces**.
You have to use them together, using them in isolation does not gain you observability

Metrics
A number that is measured over a period of time
e.g., If we measured the CPU usage and aggerated it over a period of time, we could have an **Average CPU metric**

Logs
A text file where each line contains event data about what happened at a certain time.

Traces
A history of request that travels through multiple Apps/services so we can pinpoint performance or failure.

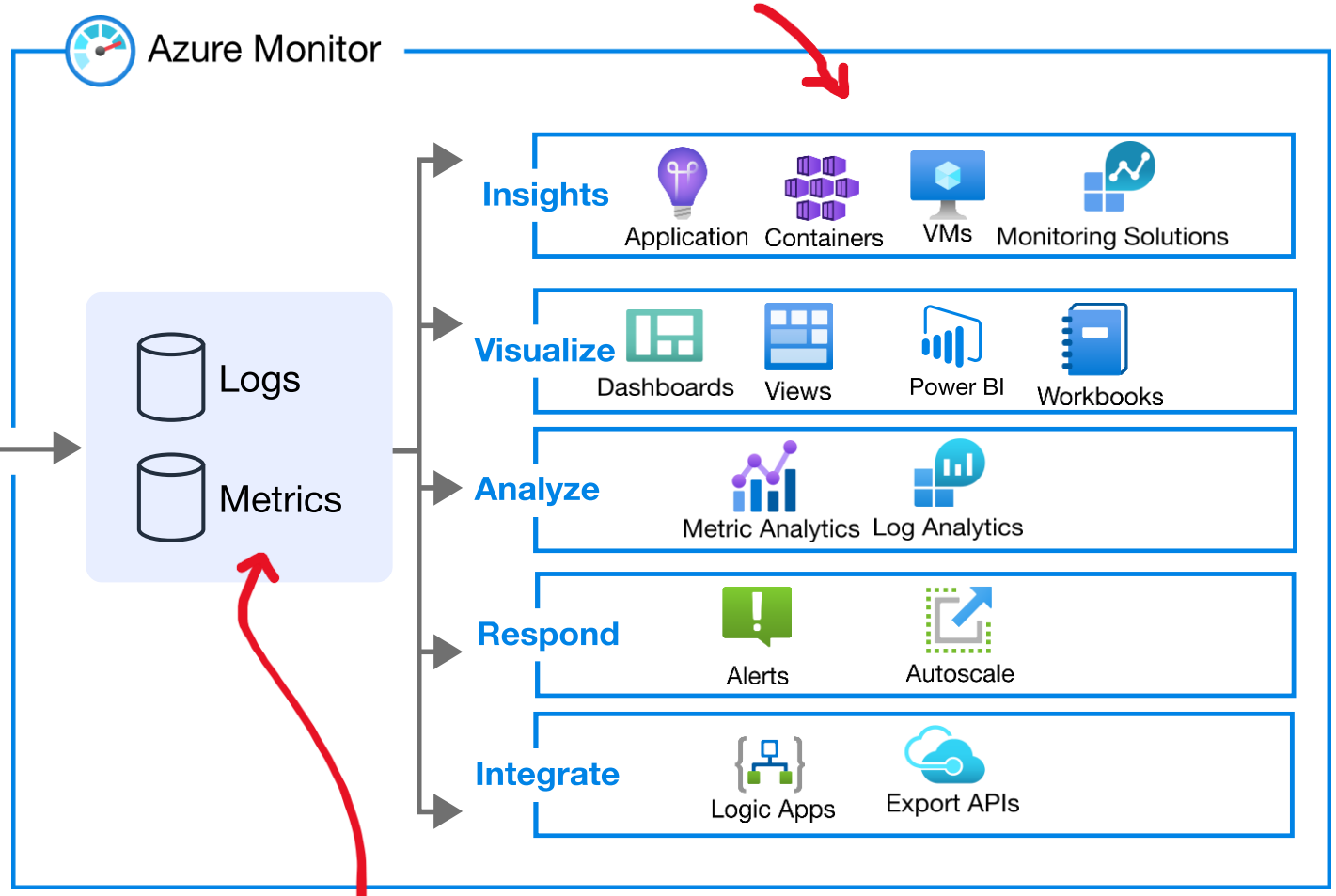
Looks like they should have called it the Triforce of Observability



Anatomy of Azure Monitor

The **sources of common monitoring data** to populate datastores
Order by (Highest to Lowest)

- Application
- Operating System
- Azure Resources
- Azure Subscription
- Azure Tenant
- Custom Sources



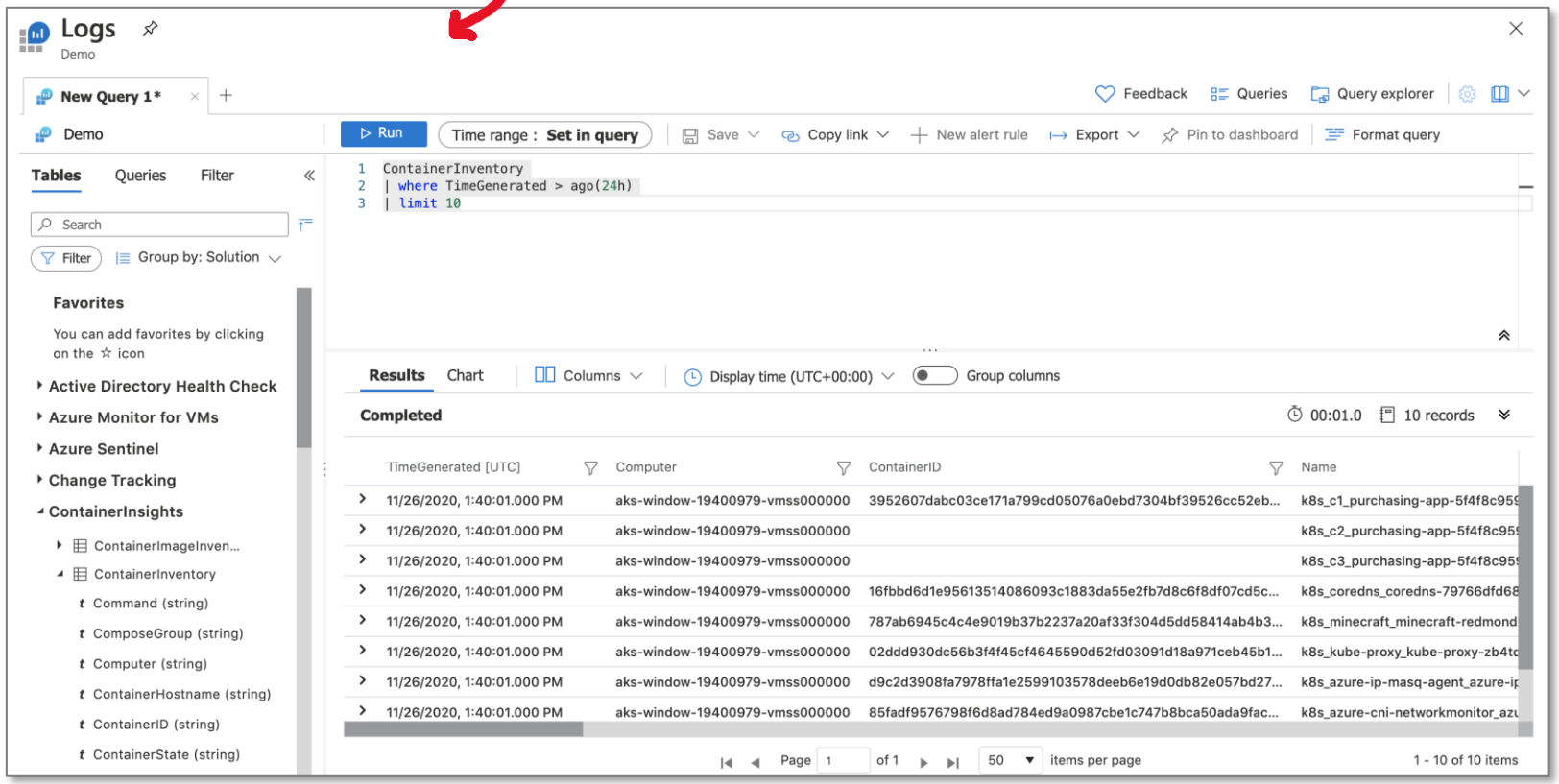
The **functions** that Azure monitor can perform

The two fundamental data stores are **Metrics** and **Logs**

Log Analytics

Log Analytics is a tool in the Azure portal used **to edit and run log queries** with data in **Azure Monitor Logs.**

- Log Analytics processes data from various sources and transforms it into actionable insights.
- It ingests data from **Azure Monitor**, **Windows**, and **Linux agents**, **Azure services**, and other sources.
- Once the data is collected, you can use **Log Analytics query language** to retrieve, consolidate, and analyze the data.



Log Analytics uses a query language called **KQL**

Log Analytics

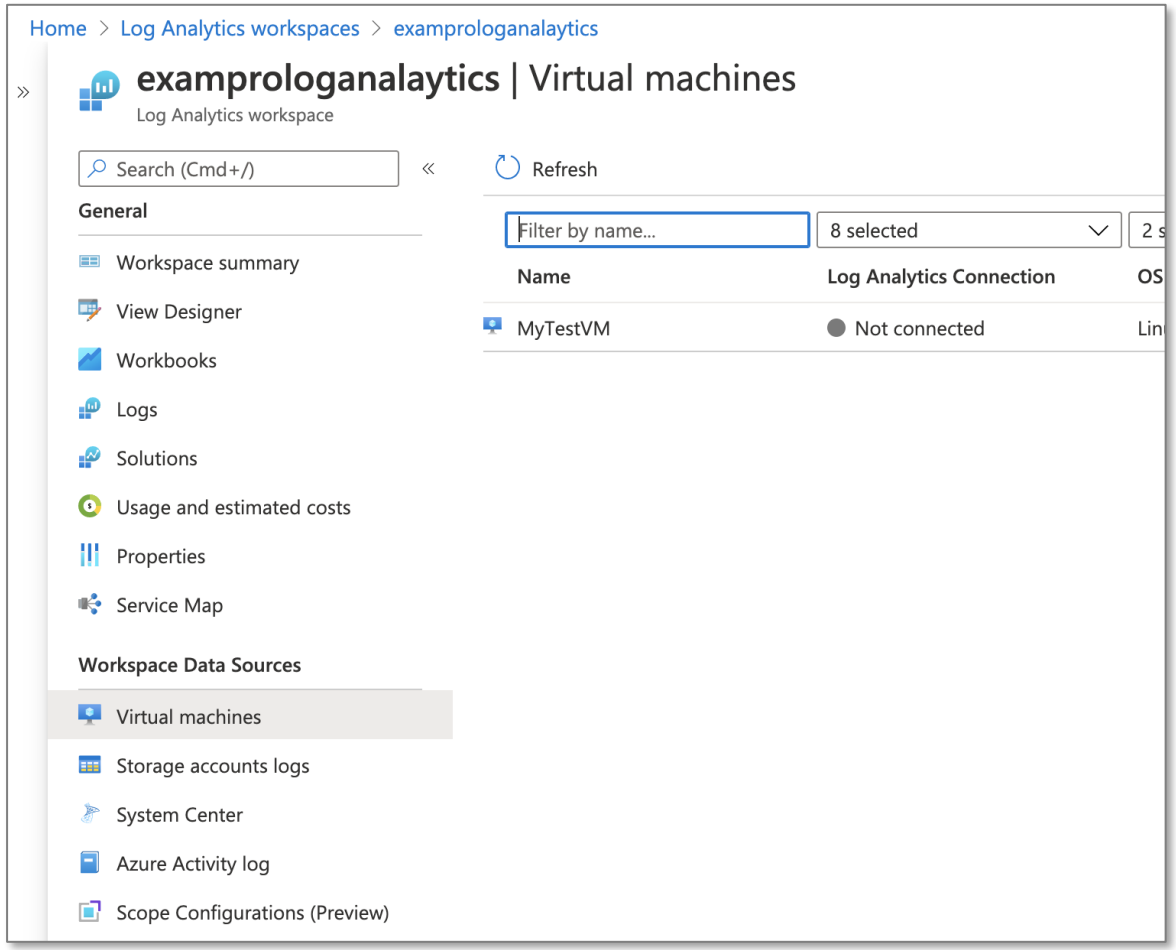
Benefits

1. **Centralized Log Management:** Collect and analyze data from multiple sources, both on-premises and in the cloud, in a centralized location.
2. **Powerful Analytics:** Utilize the Kusto Query Language (KQL) to run advanced analytics on large amounts of fast-streaming data in real time.
3. **Custom Dashboards:** Create custom dashboards and visualizations to display real-time data and trends.
4. **Integration:** Seamless integration with other Azure services and Microsoft solutions, such as Power BI and Azure Automation.
5. **Alerting:** Set up alerts based on specific criteria to proactively identify and respond to potential issues before they affect your users.

Log Analytics Workspaces

Log Analytics workspace is a unique environment for Azure Monitor log data

Each **workspace** has its own data repository and configuration, and data sources and solutions are configured to store their data in a particular **workspace**



Azure Alerts

Alerts notify you when issues are found with your infrastructure or application
They allow you to **identify** and **address** issues before the users of your system notice them.

Azure has 3 kinds of Alerts

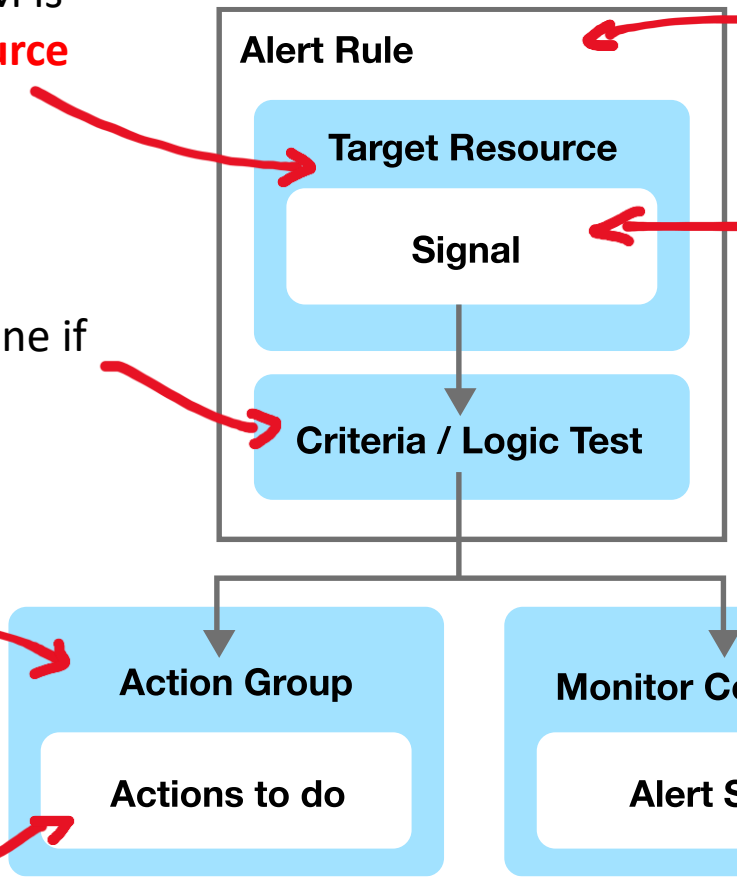
1. Metric Alerts
2. Log Alerts
3. Activity Log Alerts

When an alert is triggered you can be notified and have it take action

Azure Alerts

A resource such as an Azure VM is designated as the **Target Resource** and it omits a **signal**

The signal is evaluated against a **criteria or logical test** to determine if the alert has been triggered
eg. Percentage CPU > 70%



The **Alert Rule** defines who should we monitor and when should we react

The **Signal** is a data payload emitted from the resource that could be the following types:

- Metric
- Log
- Activity log
- Application Insights

An **action group** contains actions to be that will be performed when alert is triggered

The current state of your alert
Monitor Condition is set by the system
Alert state is set by the user

An **action** could be a:
Automation runbook, Azure Function, ITSM, Logic App, Webhooks or Secure Webhooks

Application Insights

Application Insights is an **Application Performance Management (APM)** service
It is a sub-service of Azure Monitor.

What is an APM?

Monitoring and management of **performance and availability** of software apps. APM strives to detect and diagnose complex application performance problems to maintain an expected level of service.

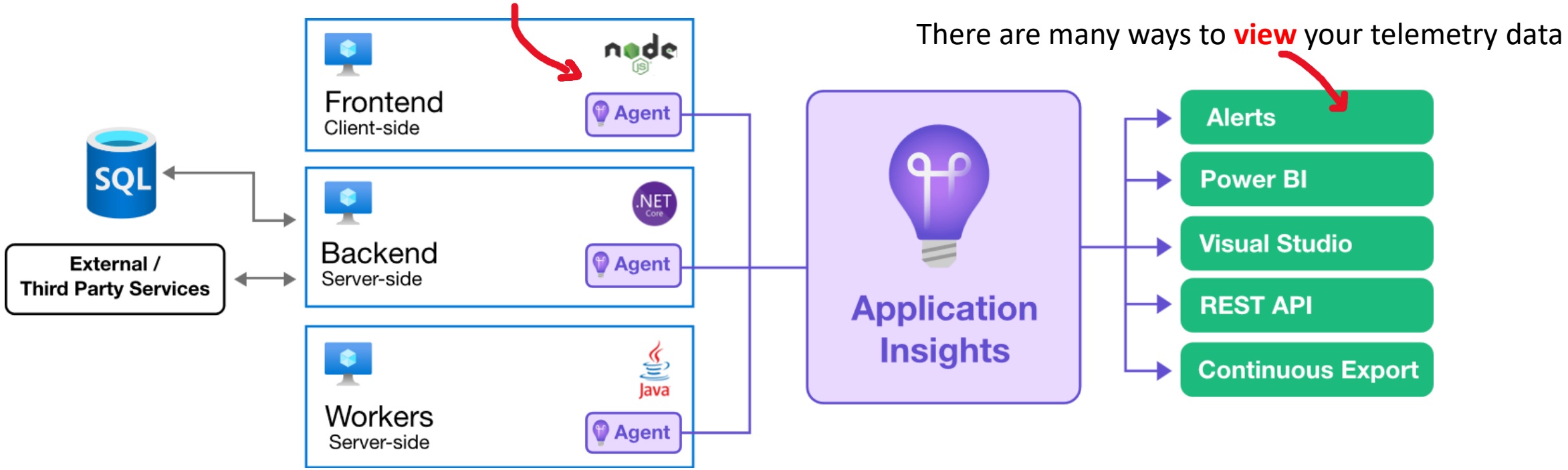
Why use Application Insights?

- **Automatic Detection of Performance Anomalies**: Application Insights automatically identifies performance anomalies in your system.
- **Powerful Analytics Tools**: It comes with robust analytics tools to help you diagnose issues and understand what users do with your app.
- **Continuous Improvement**: It is designed to help you continuously improve performance and usability of your applications.
- **Platform Agnostic**: It works for apps on .NET, Node.js, Java, and Python, hosted on-premises, hybrid, or any public cloud.
- **DevOps Integration**: It can be integrated into your DevOps process.
- **Mobile App Monitoring**: It can monitor and analyze telemetry from mobile apps by integrating with Visual Studio App Center.

Application Insights

To use Application Insights, **you need to instrument your application**.

- This involves installing the **instrument package (SDK)**, or enabling Application Insights using the **Application Insights Agents**, where supported.



- Apps can be instrumented from anywhere
- When you set up Application Insights monitoring for your web app, you create an Application Insights *resource* in Microsoft Azure.
- You open this resource in the Azure portal to see and analyze the telemetry collected from your app.
- The resource is identified by an instrumentation key (ikey)

Application Insights

What does Application Insights Monitor?

- Request rates, response times, and failure rates
- Dependency rates, response times, and failure rates
- Exceptions
- Page views and load performance
- AJAX calls
- User and session counts
- Performance counters
- Host diagnostics
- Diagnostic trace logs
- Custom events and metrics

Where do I see my telemetry?

- Smart detection and manual alerts
- Application map
- Profiler
- Usage Analysis
- Diagnostic search for instance data
- Metrics Explorer for aggerated data
- Dashboards
- Live Metrics Stream
- Analytics
- Visual Studio
- Snapshot debugger
- Power BI
- REST API
- Continuous Export