

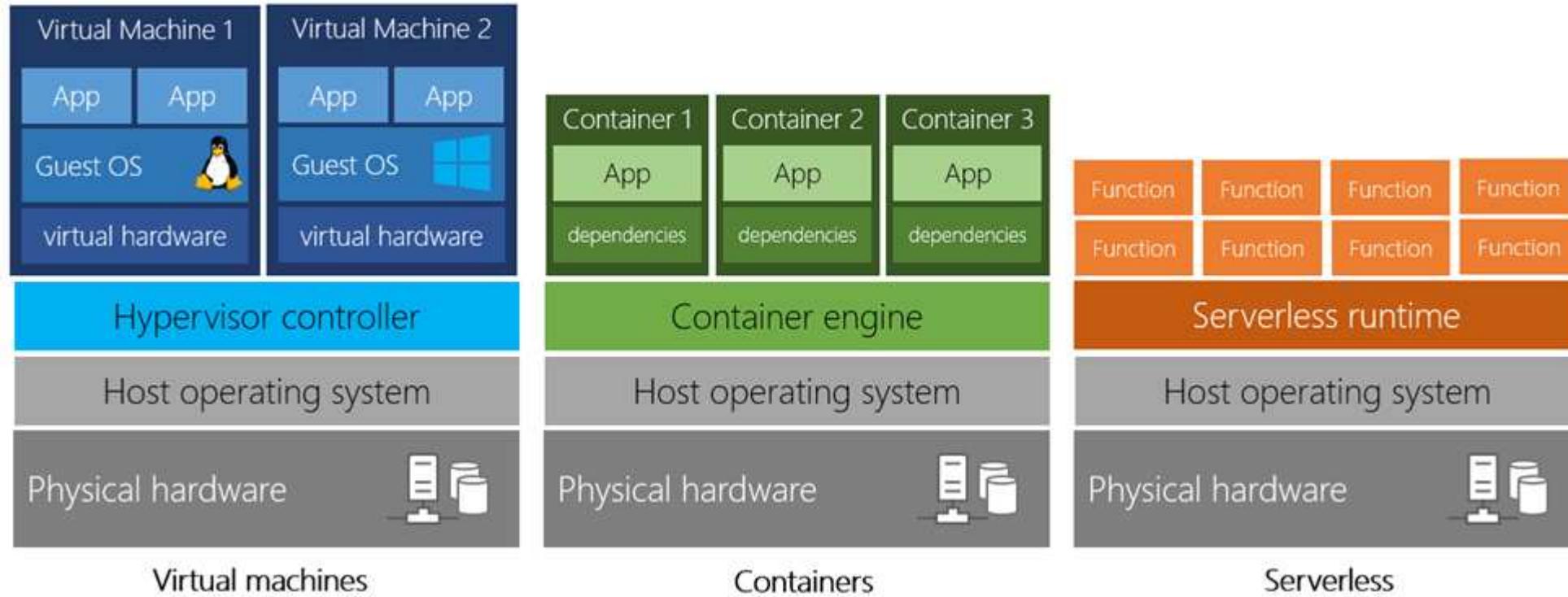
## What is cloud computing?

Cloud computing is renting resources, like storage space or CPU cycles, on another company's computers. You only pay for what you use. The company providing these services is referred to as a cloud provider. Some example providers are Microsoft, Amazon, and Google.

The cloud provider is responsible for the physical hardware required to execute your work, and for keeping it up-to-date. The computing services offered tend to vary by cloud provider. However, typically they include:

- **Compute power** - such as Linux servers or web applications
- **Storage** - such as files and databases
- **Networking** - such as secure connections between the cloud provider and your company
- **Analytics** - such as visualizing telemetry and performance data

# Cloud Computing Services



**Every business has different needs and requirements. Cloud computing is flexible and cost-efficient, which can be beneficial to every business, whether it's a small start-up or a large enterprise.**

### Compute Power

The difference is that you don't have to buy any of the hardware or install the OS. The cloud provider runs your virtual machine on a physical server in one of their datacenters - often sharing that server with other VMs (isolated and secure). With the cloud, you can have a VM ready to go in minutes at less cost than a physical computer.

### What are containers?

**Containers** provide a consistent, isolated execution environment for applications. They're similar to VMs except they don't require a guest operating system. Instead, the application and all its dependencies is packaged into a "container" and then a standard runtime environment is used to execute the app. This allows the container to start up in just a few seconds, because there's no OS to boot and initialize. You only need the app to launch. The open-source project, Docker, is one of the leading platforms for managing containers. Docker containers provide an efficient, lightweight approach to application deployment because they allow different components of the application to be deployed independently into different containers. Multiple containers can be run on a single machine, and containers can be moved between machines. The portability of the container makes it easy for applications to be deployed in multiple environments, either on-premises or in the cloud, often with no changes to the application.

### What is serverless computing?

**Serverless computing** lets you run application code without creating, configuring, or maintaining a server. The core idea is that your application is broken into separate *functions* that run when triggered by some action. This is ideal for automated tasks - for example, you can build a serverless process that automatically sends an email confirmation after a customer makes an online purchase.

The serverless model differs from VMs and containers in that you only pay for the processing time used by each function as it executes. VMs and containers are charged while they're running - even if the applications on them are idle. This architecture doesn't work for every app - but when the app logic can be separated to independent units, you can test them separately, update them separately, and launch them in microseconds, making this approach the fastest option for deployment.

## Storage

Most devices and applications read and/or write data. Here are some examples:

- Buying a movie ticket online
- Looking up the price of an online item
- Taking a picture
- Sending an email
- Leaving a voicemail

In all of these cases, data is either *read* (looking up a price) or *written* (taking a picture). The type of data and how it's stored can be different in each of these cases.

Cloud providers typically offer services that can handle all of these types of data. For example, if you wanted to store text or a movie clip, you could use a file on disk. If you had a set of relationships such as an address book, you could take a more structured approach like using a database.

The advantage to using cloud-based data storage is you can scale to meet your needs. If you find that you need more space to store your movie clips, you can pay a little more and add to your available space. In some cases, the storage can even expand and contract automatically - so you pay for exactly what you need at any given point in time.

High Availability, Fault Tolerance, and Disaster Recovery

Scalability and Elasticity

Business Agility

Economies of Scale

Capital Expenditure (CapEx) and Operational Expenditure (OpEx)

The Consumption-Based Model

### High Availability

High Availability Maintaining **acceptable continuous performance** despite temporary load fluctuations or failures in services, hardware, or datacentres.

#### Data Center Redundancies

- Power
- Cooling
- Networking - Etc.

#### Availability Zone Redundancies

- One or more data centers

#### Region Redundancies

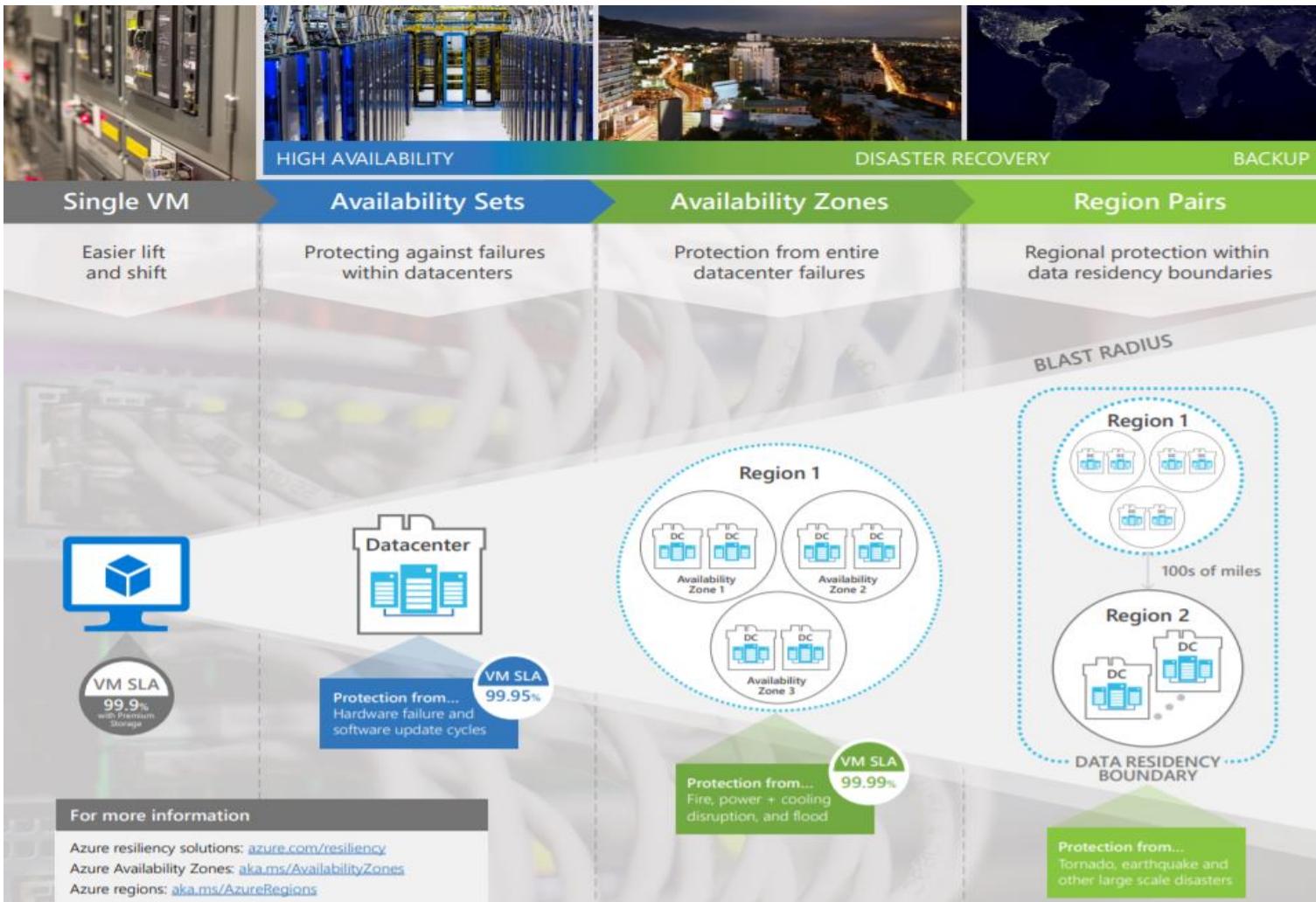
- Multiple availability zones

## Achieve High Availability faster in the cloud

As soon as you sign up, access the tools, the infrastructure, and the guidance you need to deploy your applications in the cloud. Support your most demanding mission-critical applications to build always-available sites cost-effectively. And take advantage of an SLA of up to 99.99 percent for your virtual machines.

### High-availability solutions

- **Availability Zones**
- **Availability sets**
- **Virtual Machine Scale Sets (VMSS)**
- An Availability Set is a logical grouping capability for isolating VM resources from each other when they're deployed. Azure makes sure that the VMs you place within an Availability Set run across multiple physical servers, compute racks, storage units, and network switches. If a hardware or software failure happens, only a subset of your VMs are impacted and your overall solution stays operational. Availability Sets are essential for building reliable cloud solutions.



## **Understand Azure global infrastructure**

### **Regions**

A region is a set of datacenters deployed within a latency-defined perimeter and connected through a dedicated regional low-latency network.

With more global regions than any other cloud provider, Azure gives customers the flexibility to deploy applications where they need to. Azure is generally available in 52 regions around the world, with plans announced for 3 additional regions.

### **Geographies**

A geography is a discrete market, typically containing two or more regions, that preserves data residency and compliance boundaries.

Geographies allow customers with specific data-residency and compliance needs to keep their data and applications close. Geographies are fault-tolerant to withstand complete region failure through their connection to our dedicated high-capacity networking infrastructure.

### **Availability Zones**

Availability Zones are physically separate locations within an Azure region. Each Availability Zone is made up of one or more datacenters equipped with independent power, cooling, and networking.

Availability Zones allow customers to run mission-critical applications with high availability and low-latency replication.

### Fault Tolerance

Redundancy is often built into cloud services architecture so if one component fails, a backup component takes its place. This is referred to as fault tolerance and it ensures that your customers aren't impacted when an unexpected accident occurs.

#### Proactive

- Regularly backup Data / app/Resources
- Deploy to multiple Availability zones or Regions
- Load balance across multiple availability zones or regions
- Monitor health of data /apps / resources

#### Reactive

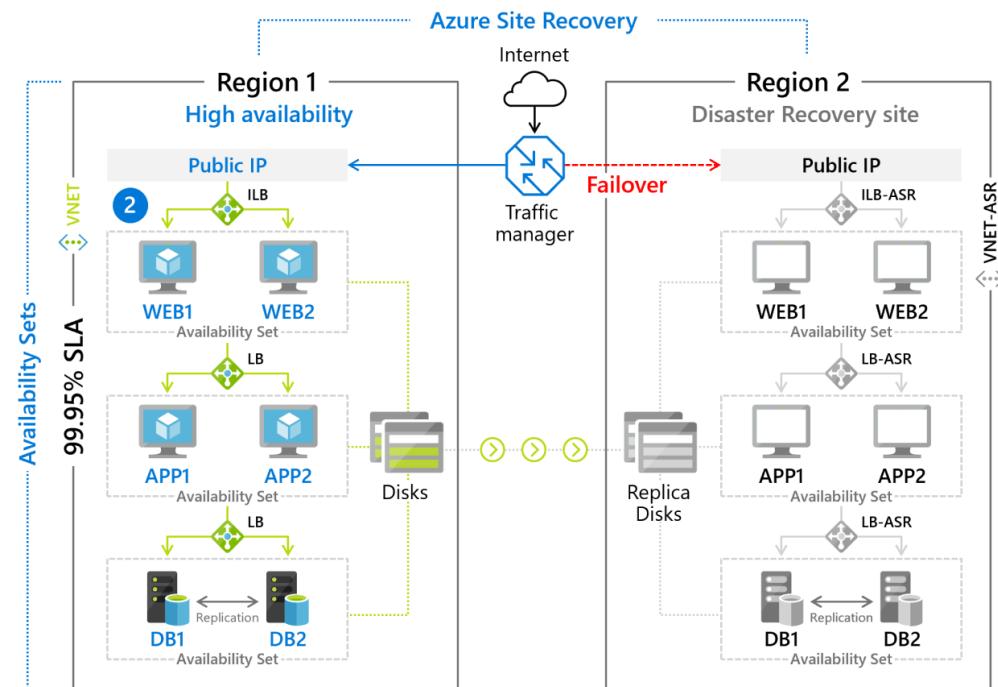
Restore data/apps/Resources to different availability zones or regions

Deploy to different Availability zones or regions

## Disaster Recovery

### Disaster Recovery

The ability to recover from rare but major incidents: non-transient, wide-scale failures, such as service disruption that affects an entire region. Disaster recovery includes data backup and archiving, and may include manual intervention, such as restoring a database from backup.



- On-Premises to On-Premises
- On-Premises to Azure
- other Cloud to Azure
- Azure to Azure

The ability to increase the instance count or size of existing resources.

## Scaling Out

- Increase instance count of existing resources
- Non-disruptive

<https://docs.microsoft.com/en-us/azure/azure-monitor/platform/autoscale-overview>

## Scaling Up

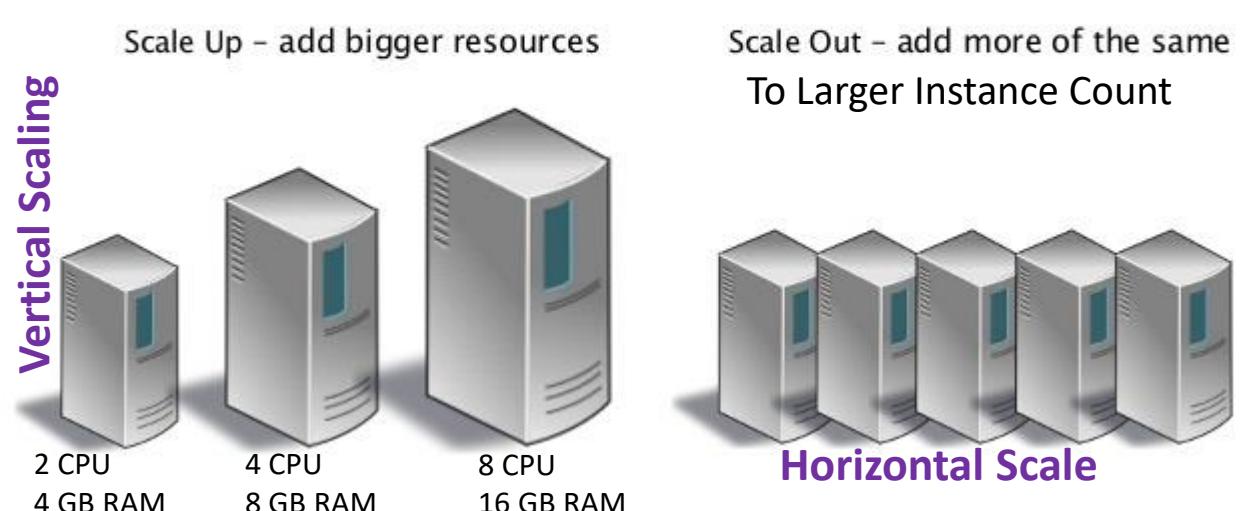
- Increase instance size of existing resources
- Disruptive

## Elasticity

The Ability to Increase or decrease the instance count or Size of existing resources based on fluctuations in traffic or load or in resource workload.

- Ability to scale in both Directions Up and Down
- Can be manual or automatic
- Based on Changes in load or workload
- Pay only for what you use

## SCALE UP VS SCALE OUT



## Business Agility

An organization's ability to **rapidly adapt** to market and environmental changes in productive and cost-effective ways and take advantage of available resources to meet customer demands.



## Economies of Scale

### Supply-side savings

- ▶ Lower costs of land, servers, power, labor, etc.
- ▶ Higher buying power, security, reliability, etc.

### Demand-side savings

- ▶ Serving more customers allows for higher server utilization rates
- ▶ Higher server utilization rates allow for lower costs

### Multi-tenancy savings

- ▶ More tenants (customers or users) lowers the cost of servers and management per tenant

## On-Premises

### Capital Expenditure (CapEx) and Operational Expenditure (OpEx)



#### Ongoing Costs

- ♦ Apply patches, upgrades
- ♦ Downtime
- ♦ Performance tuning
- ♦ Rewrite customizations
- ♦ Rewrite integrations
- ♦ Upgrade dependent applications
- ♦ Ongoing burden on IT (hardware)
- ♦ Maintain/upgrade network
- ♦ Maintain/upgrade security
- ♦ Maintain/upgrade database

## Cloud Computing

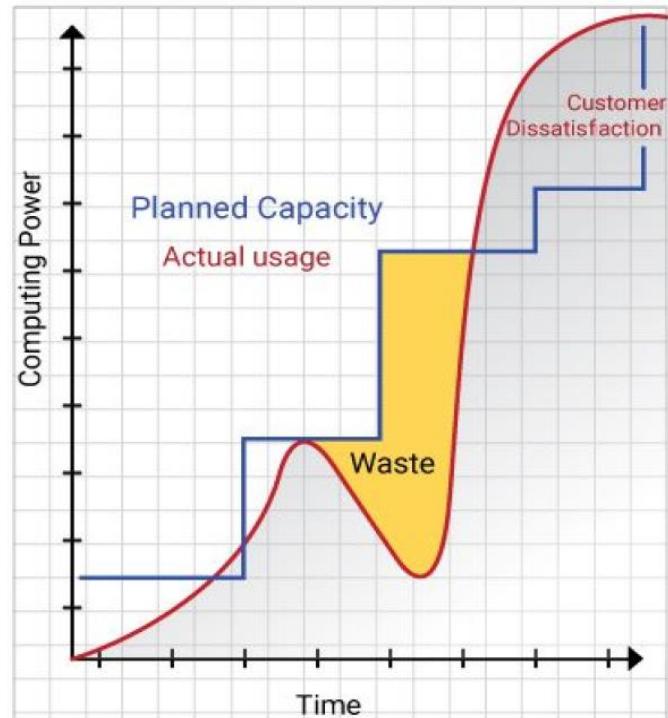


#### Ongoing Costs

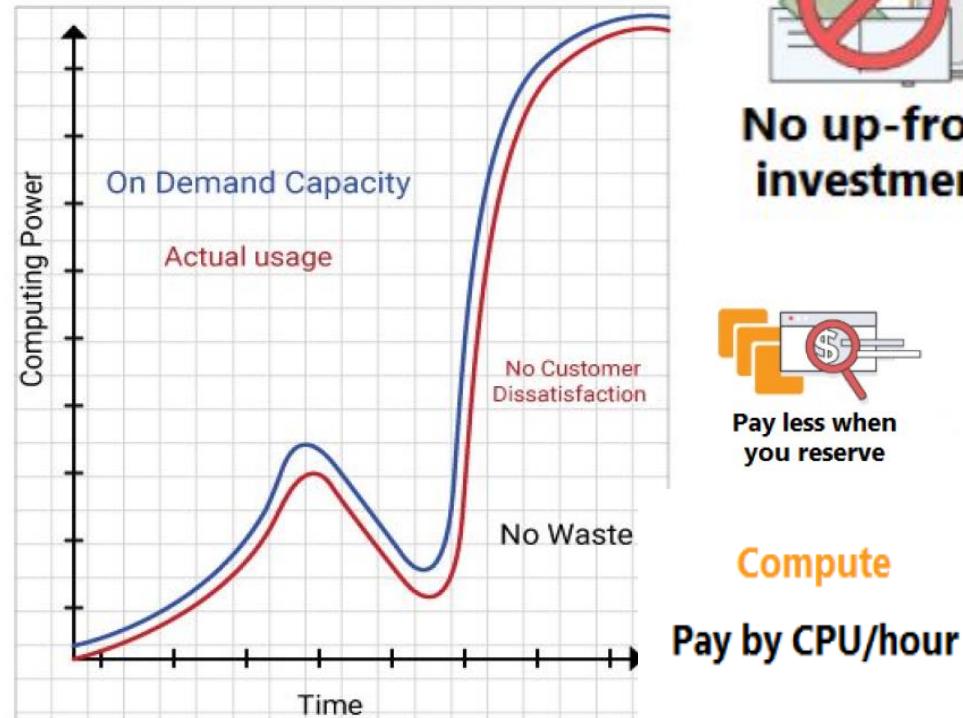
- ♦ Subscription fees
- ♦ Training
- ♦ Configuration
- ♦ System Administration

## Consumption Based Model

Traditional Data Center



Azure



**No up-front investment**



Pay less when you reserve

**Compute**

Pay by CPU/hour



**Pay as you go**



Pay per use



Pay less when Azure grows

**Data Transfer**

Pay by GB for data out, not in

Applications

Middleware/OS

Servers

**IaaS**  
host



Applications

Middleware/OS

Servers

**PaaS**  
build



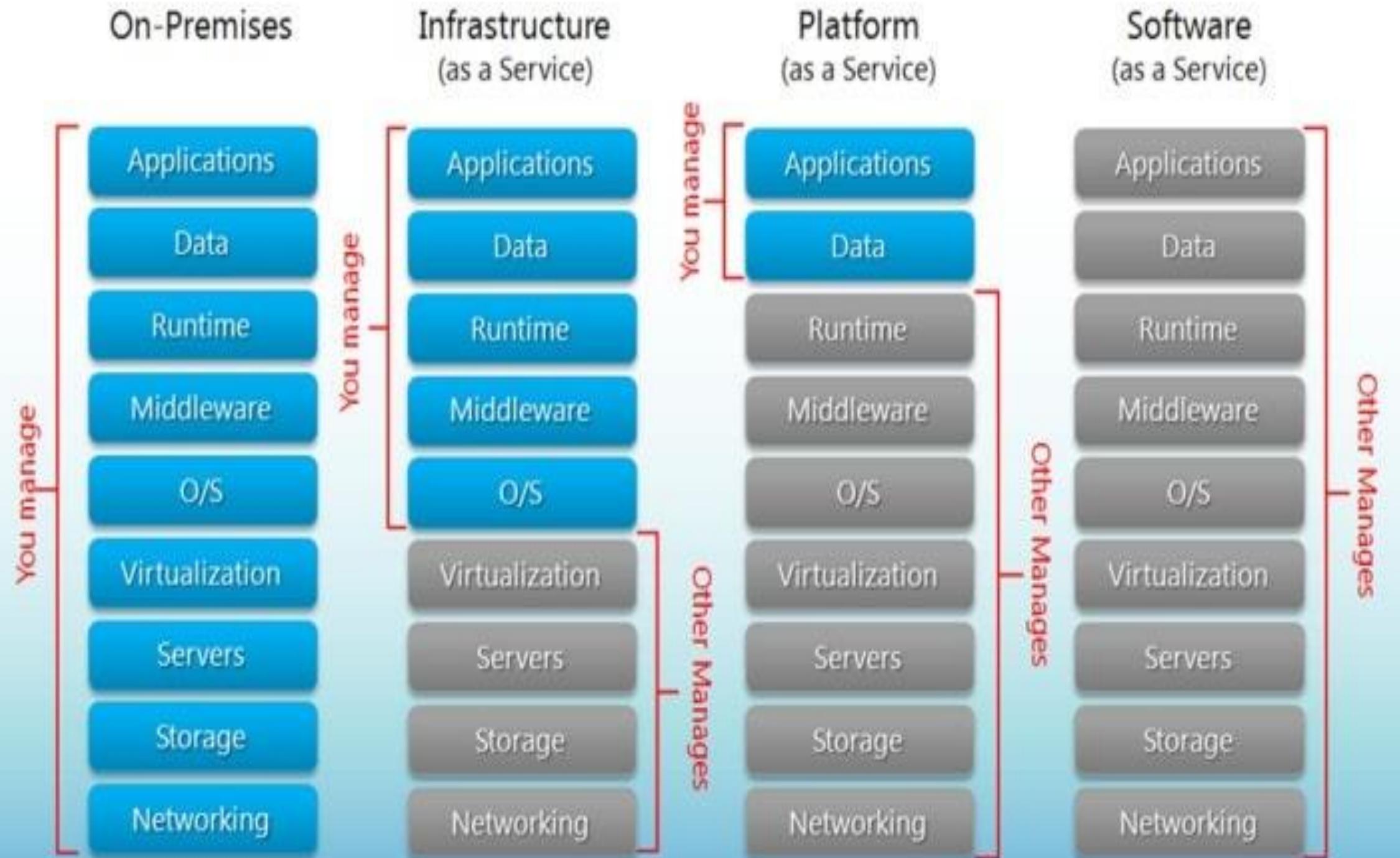
Applications

Middleware/OS

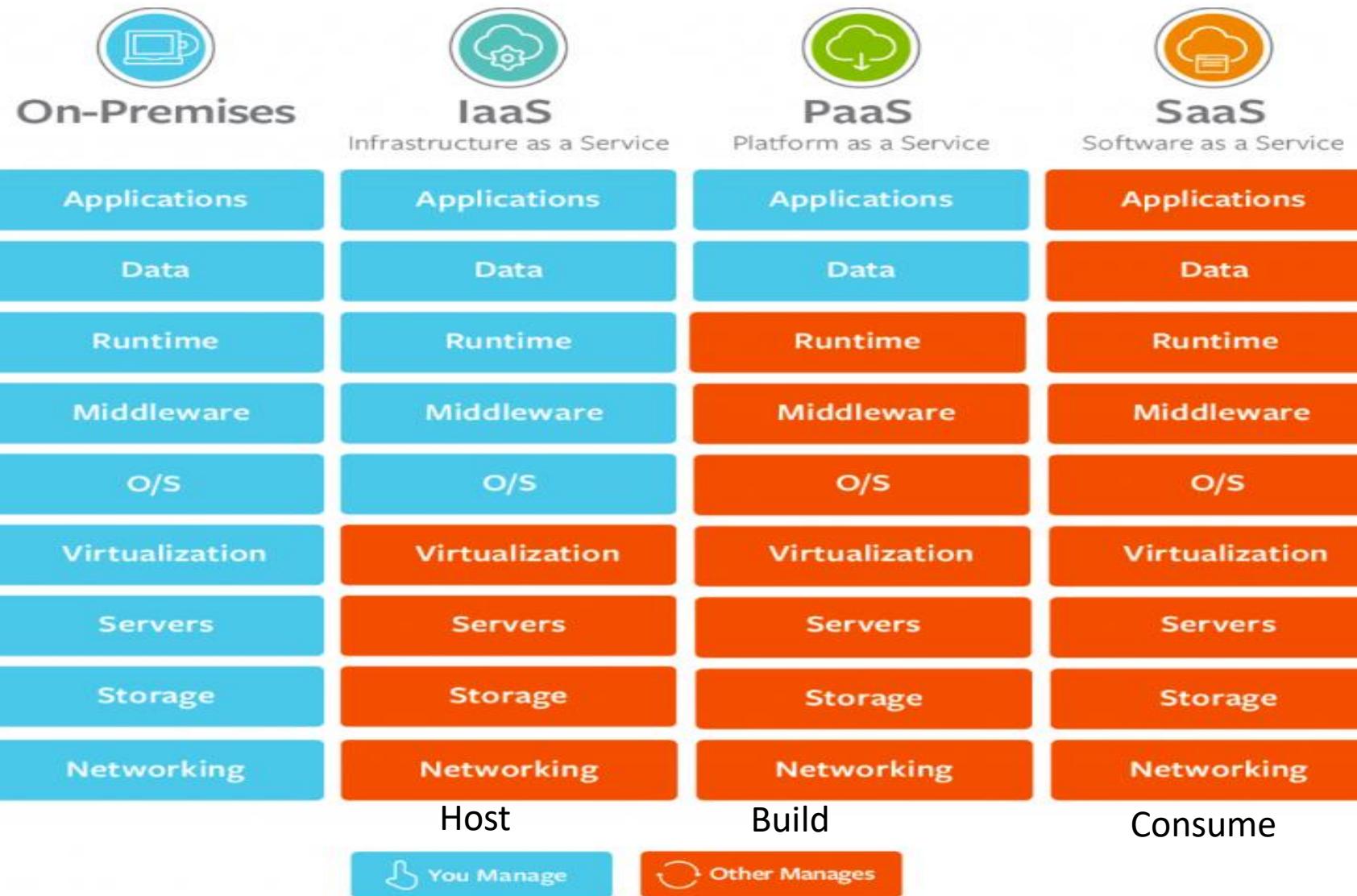
Servers

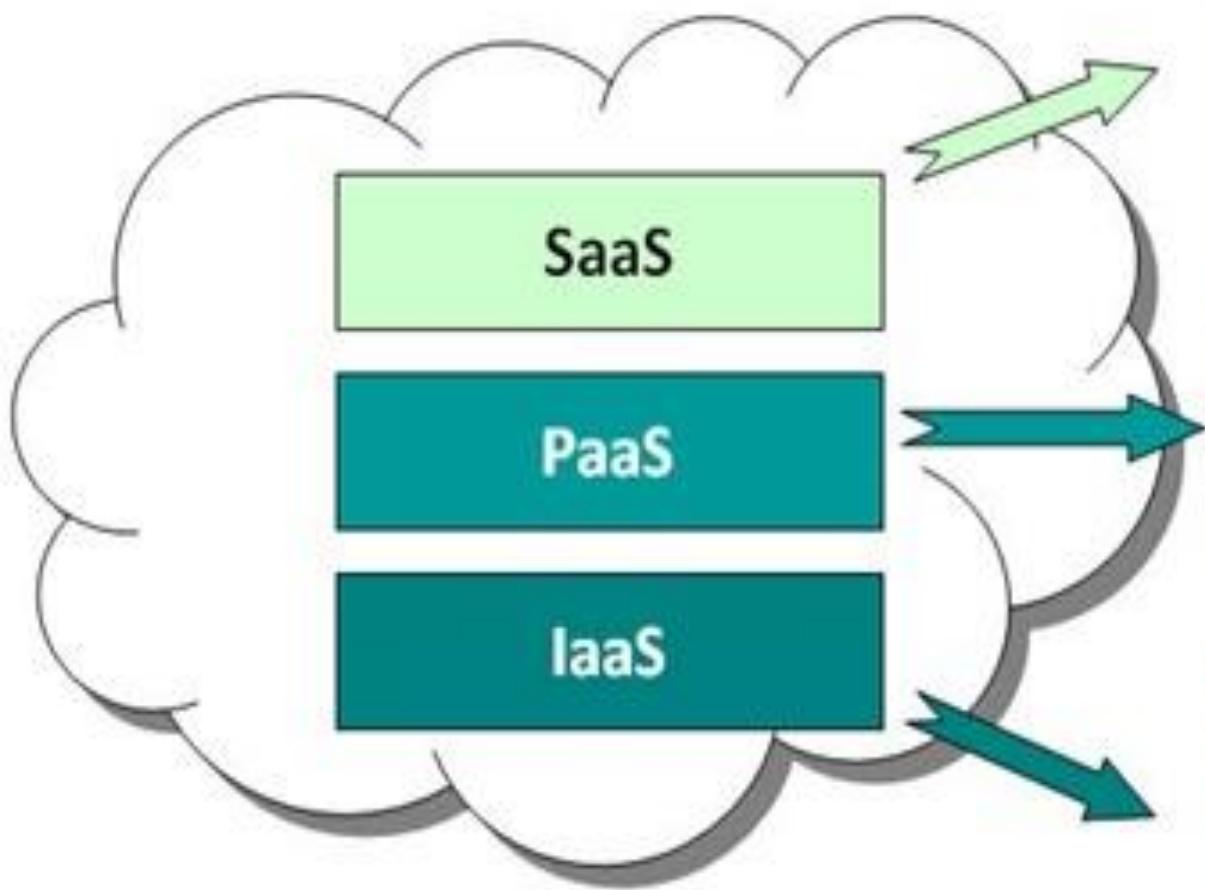
**SaaS**  
Consume





# Key Differences





Who Uses It	What Services are available	Why use it?
Business Users	EMail, Office Automation, CRM, Website Testing, Wiki, Blog, Virtual Desktop ...	To complete business tasks
Developers and Deployers	Service and application test, development, integration and deployment	Create or deploy applications and services for users
System Managers	Virtual machines, operating systems, message queues, networks, storage, CPU, memory, backup services	Create platforms for service and application test, development, integration and deployment

# Common Examples of SaaS, PaaS, & IaaS

Platform Type	Common Examples
<b>SaaS</b>	Google Apps, Dropbox, Salesforce, Cisco WebEx, Concur, GoToMeeting
<b>PaaS</b>	AWS Elastic Beanstalk, Windows Azure, Heroku, Force.com, Google App Engine, Apache Stratos, OpenShift
<b>IaaS</b>	DigitalOcean, Linode, Rackspace, Amazon Web Services (AWS), Cisco Metapod, Microsoft Azure, Google Compute Engine (GCE)

## Multi-Tenant Implementation

Owned and Operated by service provider

Bound by multi-tenant Data management policies

Similar self service and automation capabilities as Private Cloud

## Pros

- No Up-Front Capital expenses
- No Maintenance
- High Reliability
- Easy Scalability

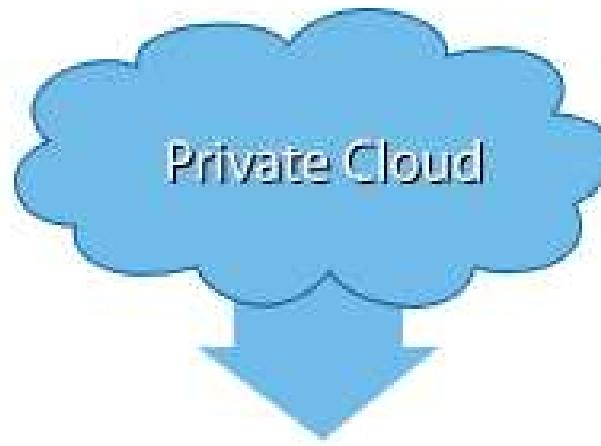
## Cons

- Less Customizable
- Potential latency
- Potential governance issues



## Public Cloud

- ✓ Hosted at a Service Provider Site
- ✓ Supports multiple customers
- ✓ Often utilises shared infrastructure
- ✓ Supports connectivity over the internet
- ✓ Suited for information that is not sensitive
- ✓ Can be cheaper than Private Cloud



## Private Cloud

- ✓ Hosted at an Enterprise or a Service Provider site
- ✓ Supports one customer
- ✓ Does not utilise shared infrastructure
- ✓ Connectivity over private network/fiber or the internet
- ✓ Suited for information that requires a high level of security

## What is a private cloud?



A private cloud consists of computing resources used exclusively by one business or organization. The private cloud can be physically located at your organization's on-site datacenter or it can be hosted by a third-party service provider. But in a private cloud, the services and infrastructure are always maintained on a private network and the hardware and software are dedicated solely to your organization. In this way, a private cloud can make it easier for an organization to customize its resources to meet specific IT requirements. Private clouds are often used by government agencies, financial institutions, any other mid- to large-size organizations with business-critical operations seeking enhanced control over their environment.

### **Advantages of a private clouds:**

- More flexibility—your organization can customize its cloud environment to meet specific business needs.
- Improved security—resources are not shared with others, so higher levels of control and security are possible.
- High scalability—private clouds still afford the scalability and efficiency of a public cloud.

## What is a private cloud?

- Single Tenant Implementation
- Owned and operated by IT organisation
- Define your own data management policies
- Self-Service and automated Capabilities provide new agility



### Pros

Fully Customizable

Higher level of security

Better Performance

### Cons

Higher up-front capital expense

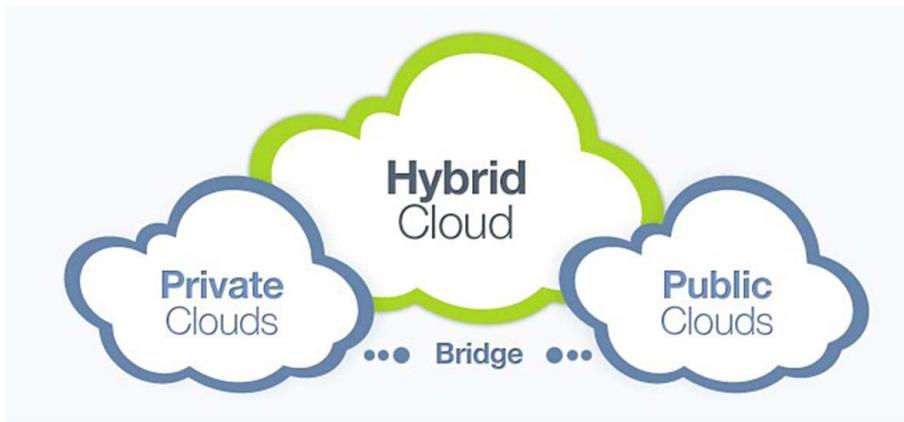
Risk under-utilization of resources

Higher ongoing costs

More maintenance







- ✓ Combination for Private and One or more Public clouds
- ✓ Allows IT organizations to become brokers of services

#### Pros:

- Greater Flexibility
- Resilience to outages
- No capacity ceiling
- Manageable security

#### Cons:

- Higher up-front capital expenses
- Risk under-utilization of resources
- Higher ongoing costs
- More maintenance
- Risk of less compatibility

## Comparing Three Cloud Models

### Public Cloud

#### Best Use case

- Transitioning to the cloud
- New applications or systems
- Standard workloads
- Systems that don't need much customization

- Multi-Tenant Implementation
- Owned and Operated by service provider
- Bound by multi-tenant Data management policies
- Similar self service and automation capabilities as Private Cloud

### Private Cloud

#### Best Use case

- Transitioning to the cloud
- Systems that need enhanced security
- Systems that need some data, apps, or systems on-premises

- Single Tenant Implementation
- Owned and operated by IT organisation
- Define your own data management policies
- Self-Service and automated Capabilities provide new agility

### Hybrid Cloud

#### Best Use case

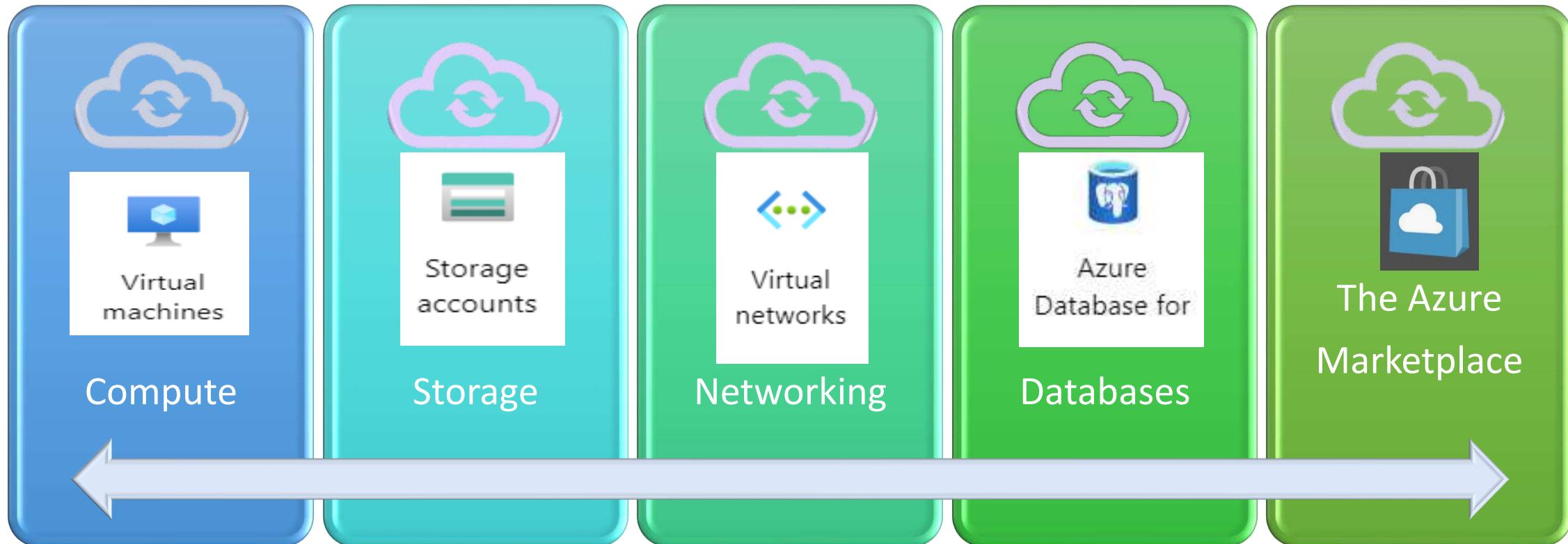
- Highly secure applications or systems
- Systems that need some customization

- Combination for Private and One or more Public clouds
- Allows IT organizations to become brokers of services

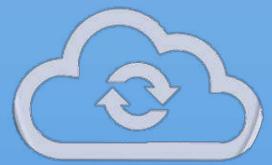
# Azure Architecture



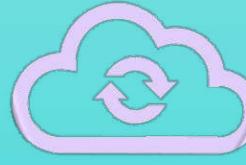
# Azure Products and Services



# Azure Solutions



Internet of  
Things - IoT



Artificial  
Intelligence  
- AI



Big Data and  
Analytics



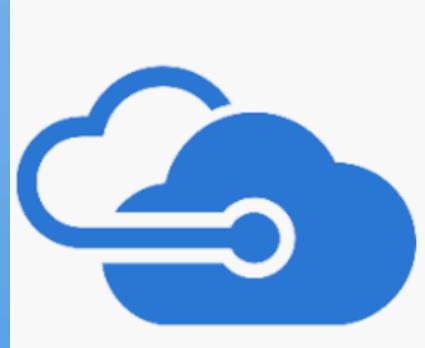
Server less  
Computing



Azure  
Solutions  
Benefits



# Azure Management Tools



Azure CLI



Azure  
PowerShell



Azure Portal



A region is a set of datacenters deployed within a latency-defined perimeter and connected through a dedicated regional low-latency network.

Deploying your applications / systems to multiple regions allows for **resiliency to region-wide outages**.

## Multi-Region Failover (Active/Passive):

- ✓ Failover across regions instantly
- ✓ Resiliency to region wide outages
- ✓ Best when all users are in the same region

## Multi-Region Deployments(Active/Active):

- ✓ Distribute traffic/ load across regions
- ✓ Resiliency to region wide outages
- ✓ Best when all users are in different regions

## Multi-Region Failover (Active/Passive)

### Passive Azure Region - West

- Failover across regions instantly
- Resiliency to region wide outages
- Best when all users are in the same region

**Failover only**

Web App  
Service



www.contoso.com

Traffic  
Manager



### Active Azure Region - East

Web App  
Service



## Multi-Region Deployments (Active/Active)

### Active Azure Region - West

- Distribute traffic/ load across regions
- Resiliency to region wide outages
- Best when all users are in different regions

Web App  
Service



www.contoso.com

Traffic  
Manager



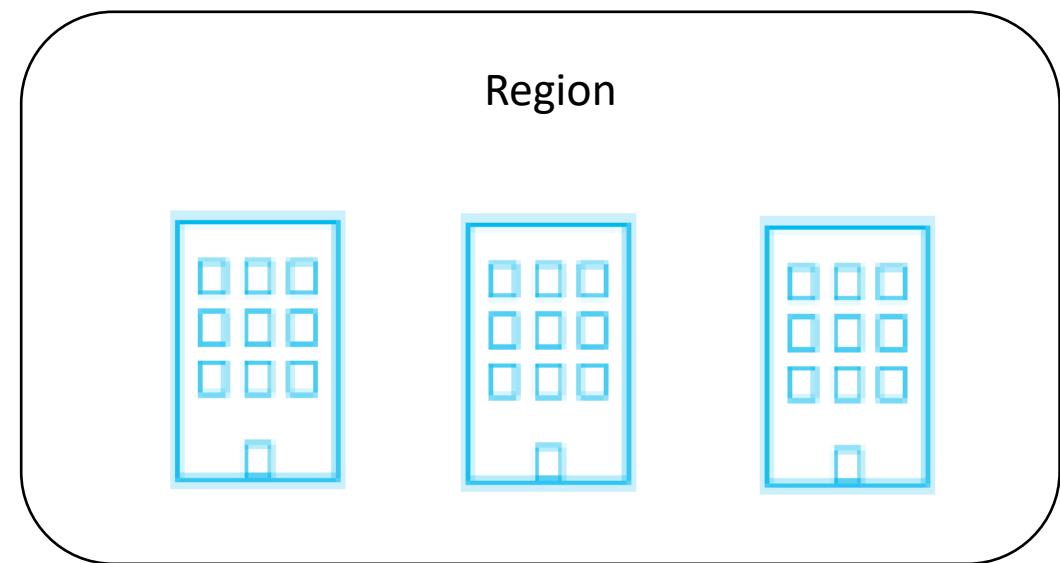
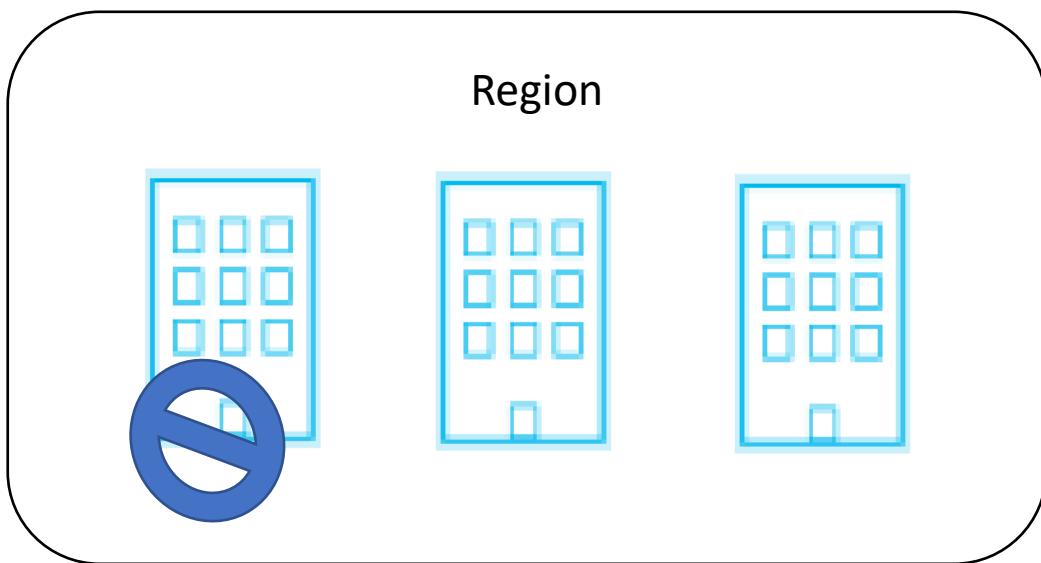
### Active Azure Region - East

Web App  
Service



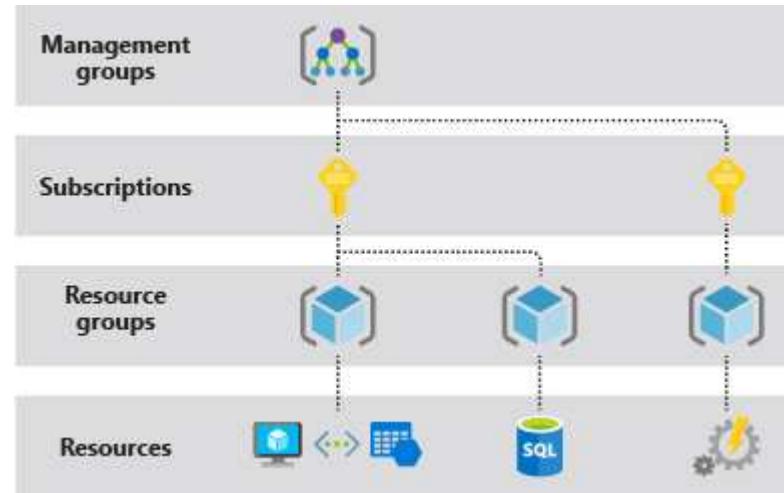
## Availability Zones

- ✓ Unique physical locations within an Azure region made up of one or more data centers.
- ✓ Allow for high availability by protecting your applications and data from data center failures
- ✓ Some Azure services can be deployed to two or more Availability Zones within an Azure region.



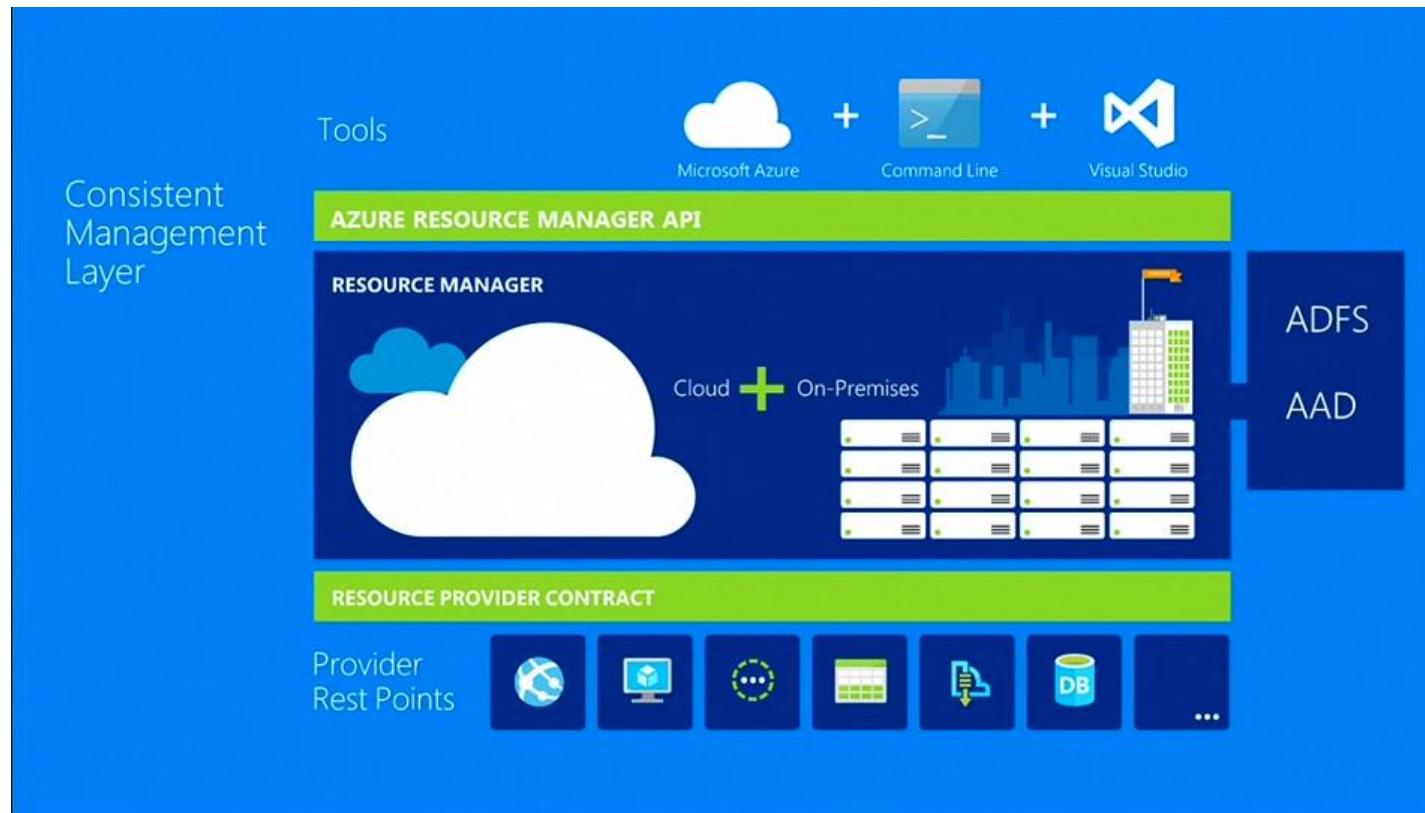
## Azure Resource Groups

- Containers of **related Azure Services** grouped together.
- All the resources in the group should share the same lifecycle
- They should be deployed, updated, and deleted together.
- A resource can only exist in **one** resource group.
- A resource group can contain resources that are located in different regions.
- A resource group can be used to scope access control for administrative actions.
- A resource can interact with resources in other resource groups.  
(When two resources are related but don't share the same lifecycle; for example, web apps connecting to a database.)



## Azure Resource Manager - ARM

- The Azure deployment and management service.
- Provides a consistent management layer that enables you to create, update, and delete resources in your Azure subscription, including with templates (ARM).
- You can use its access control, auditing, and tagging features to secure and organize your resources after deployment.



# Azure Architecture



### Regions

- Deploying your applications / systems to multiple regions allows for high availability and resiliency to region-wide outages

### Availability Zones

- Allow for high availability by protecting your applications and data from data center failures

### Resource Groups

- Containers of related azure services grouped together for administrative and access control actions

### Azure Resource Manager

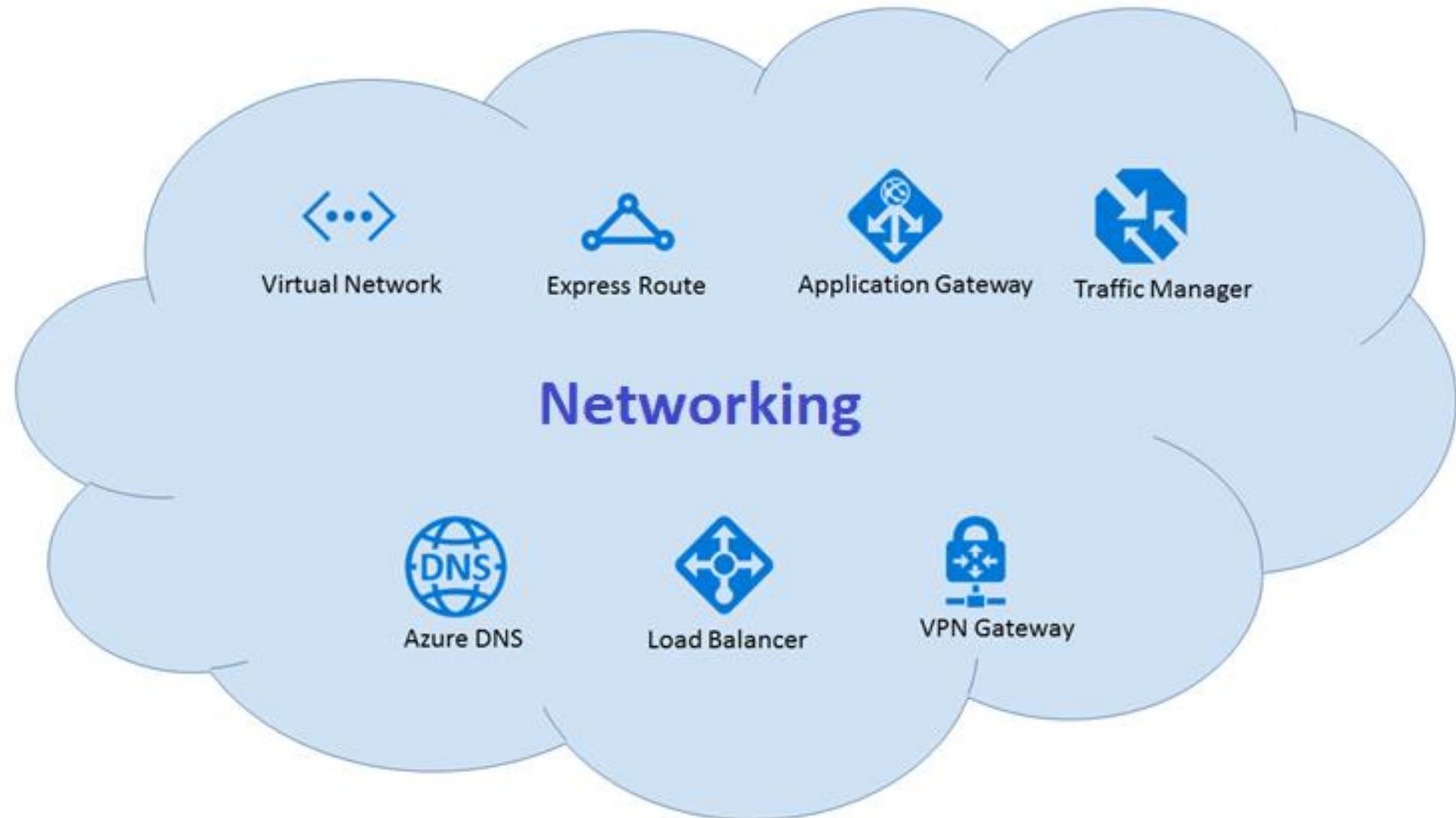
- Single centralized deployment and management service that enables you to create, update and delete resources in your Azure subscription

1. Azure Products and Services
2. Azure Solutions
3. Azure Management Tools
4. Security, Privacy, Compliance, and Trust
5. Azure Identity Services
6. Azure Security Tools and Features
7. Azure Governance
8. Monitoring and Reporting in Azure
9. Azure Privacy, Compliance, and Data Protection Standards
10. Azure Subscriptions
11. Planning and Managing Azure Costs
12. Azure Support Options
13. Azure Service Level Agreements (SLAs)
14. The Azure Service Lifecycle
15. Course Conclusion

# Networking

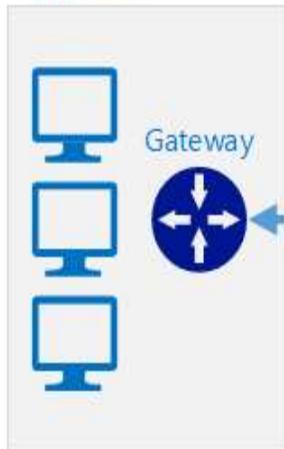
NETWORKING (31)		
 Virtual networks	 Virtual networks (classic)	 Load balancers
 Application Gateways	 Virtual network gateways	 Local network gateways
 DNS zones	 CDN profiles	 Traffic Manager profiles
 ExpressRoute circuits	 Network Watcher	 Network security groups
 Network security groups (classic)	 Network interfaces	 Public IP addresses
 Public IP Prefixes	 Reserved IP addresses (classic)	 Connections
 On-premises Data Gateways	 Route tables	 Route filters
 Application security groups	 DDoS protection plans	 Front Doors
 Service endpoint policies	 Private DNS zones	 WAF policies
 Private Link	 WAF policies	 Virtual WANs
 Bastions	PREVIEW	PREVIEW

# Networking

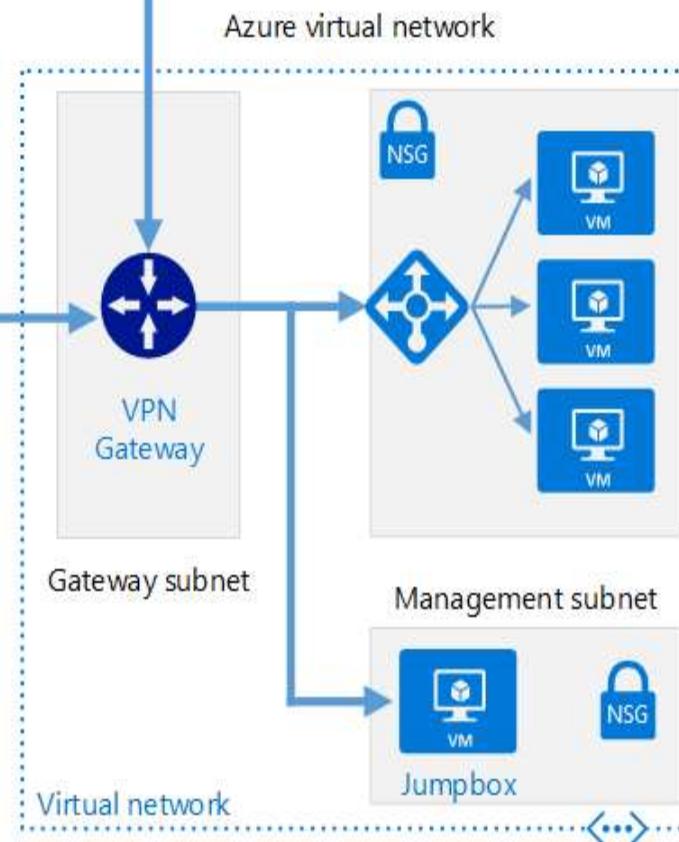
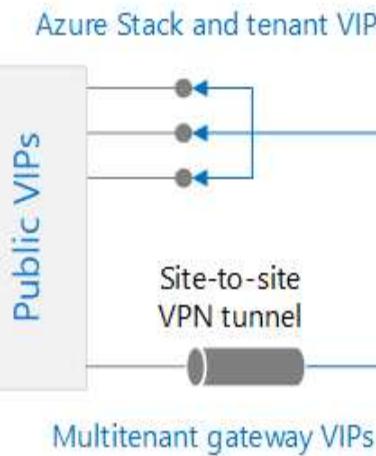
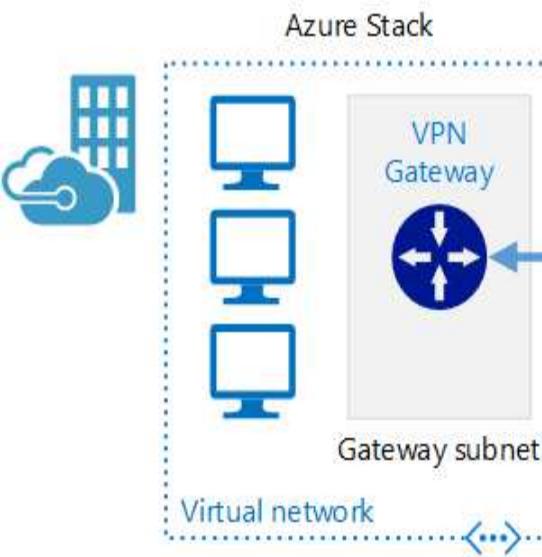


# Networking

On-premises network



Enables Azure resources, such as Azure Virtual Machines (VMs), to securely communicate with each other, the internet, and on-premises networks.



<...> VNET



VM



VM



VM



WEB APPS

Subnet 1 10.1.0.0/24



VM



VM



VM



WEB APPS

Subnet 2 10.1.1.0/24

## What is VPN Gateway?

A VPN gateway is a specific type of virtual network gateway that is used to send encrypted traffic between an Azure virtual network and an on-premises location over the public Internet.

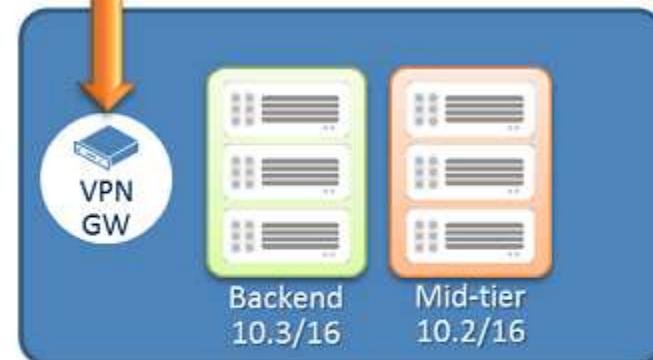
## Azure VPN Gateway

### On Premises

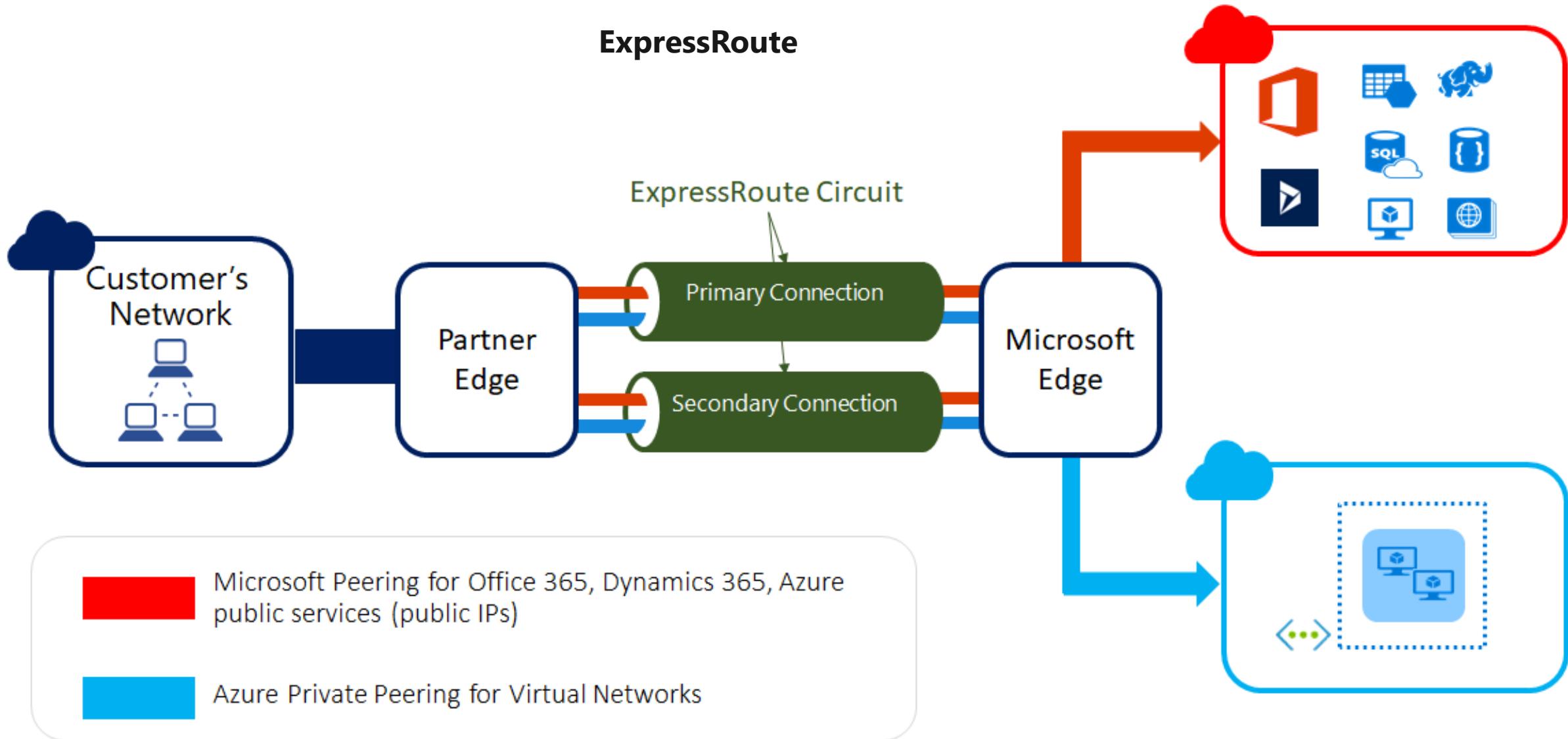


Used to send encrypted traffic between an Azure virtual network and an on-premises location over the public internet or between Azure virtual networks over the Microsoft network.

### Site to Site VPN



## ExpressRoute



ExpressRoute lets you extend your on-premises networks into the Microsoft cloud over a private connection facilitated by a connectivity provider

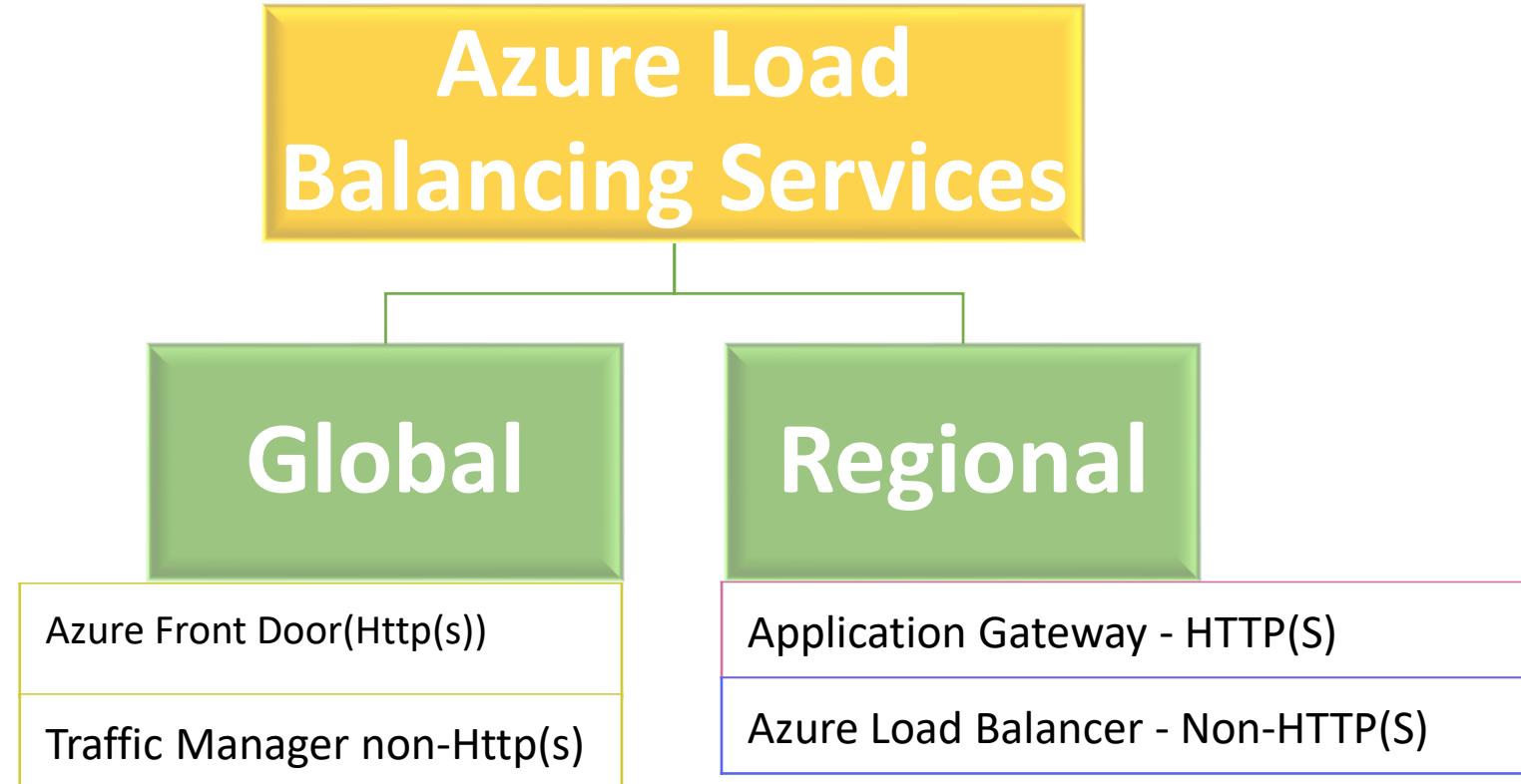
ExpressRoute connections do not go over the public Internet.

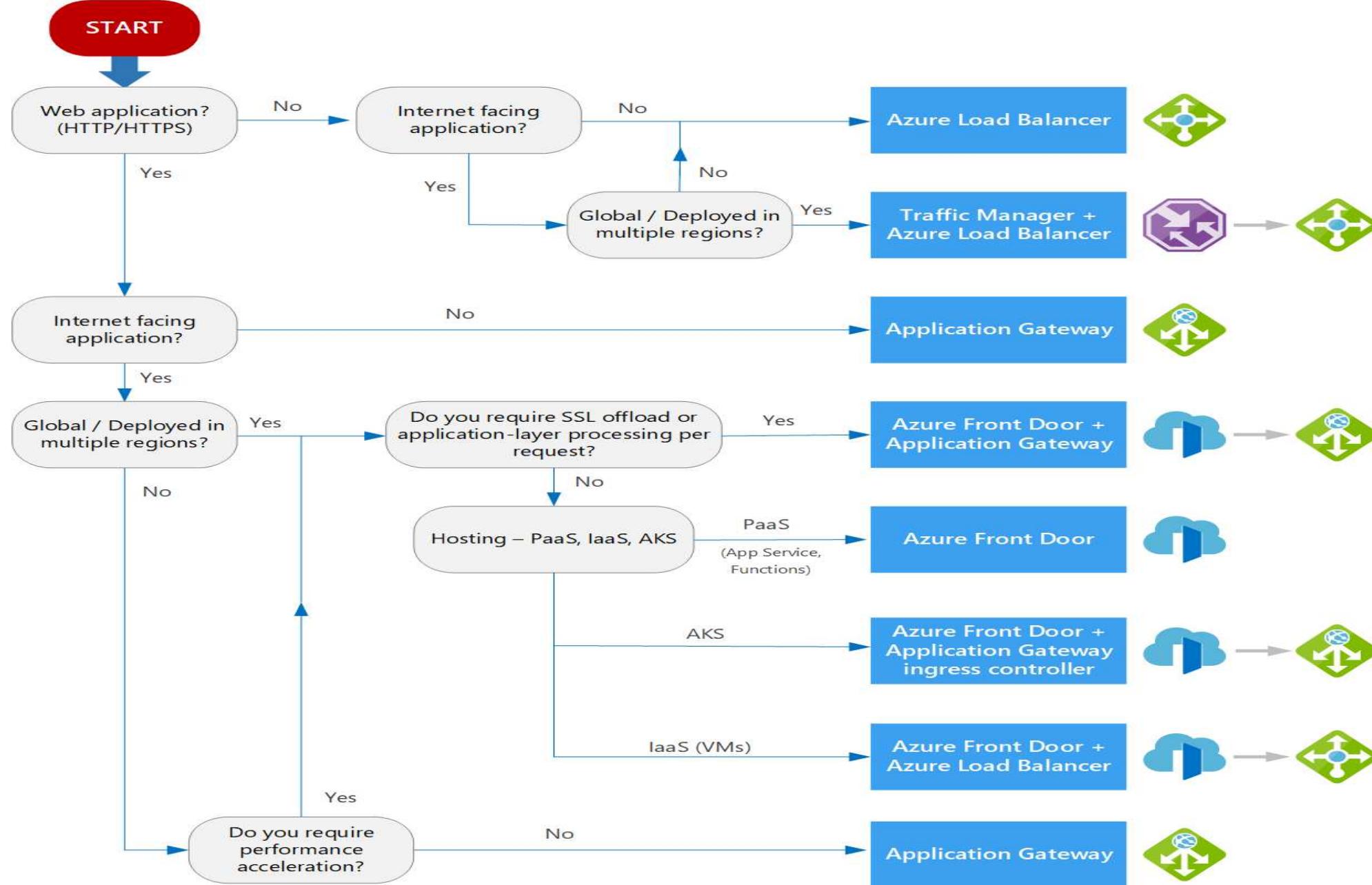
This allows ExpressRoute connections to offer more reliability, faster speeds, consistent latencies, and higher security than typical connections over the Internet.

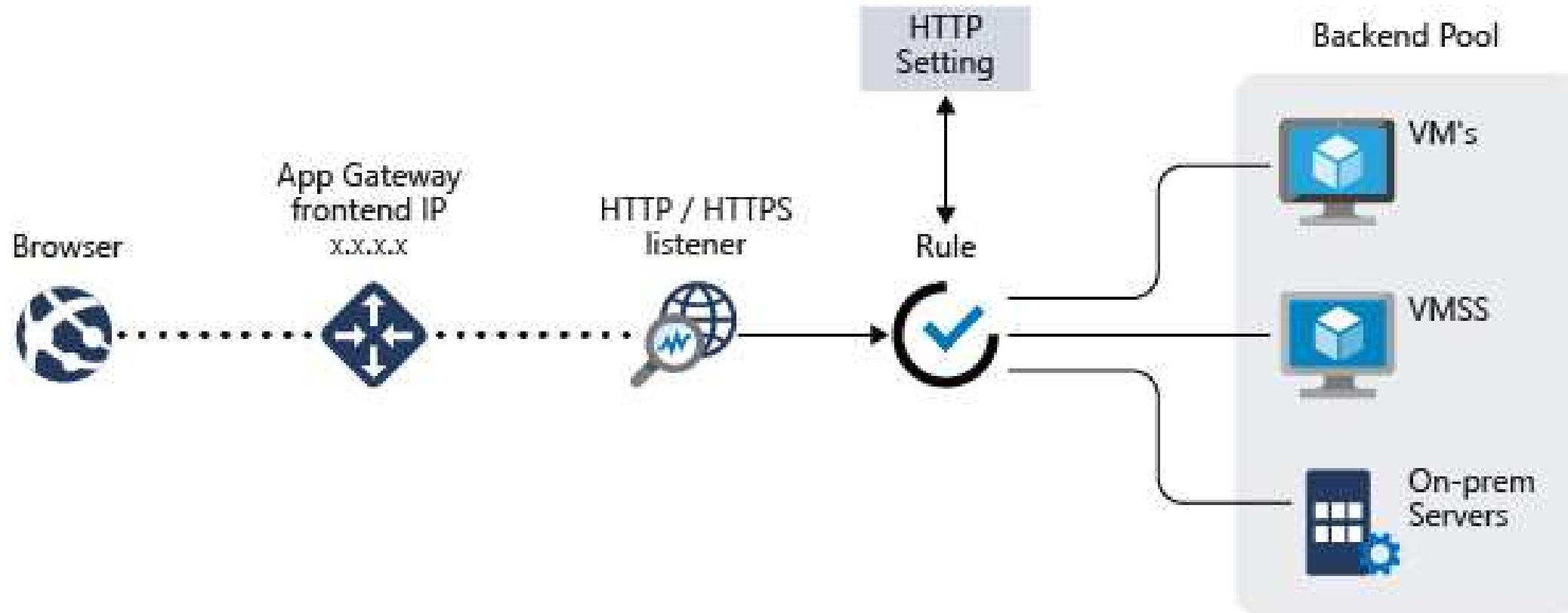
- Layer 3 connectivity between your on-premises network and the Microsoft Cloud through a connectivity provider. Connectivity can be from an any-to-any (IPVPN) network, a point-to-point Ethernet connection, or through a virtual cross-connection via an Ethernet exchange.
- Connectivity to Microsoft cloud services across all regions in the geopolitical region.
- Global connectivity to Microsoft services across all regions with the ExpressRoute premium add-on.
- Dynamic routing between your network and Microsoft via BGP.
- Built-in redundancy in every peering location for higher reliability.
- Connection uptime SLA.
- QoS support for Skype for Business.

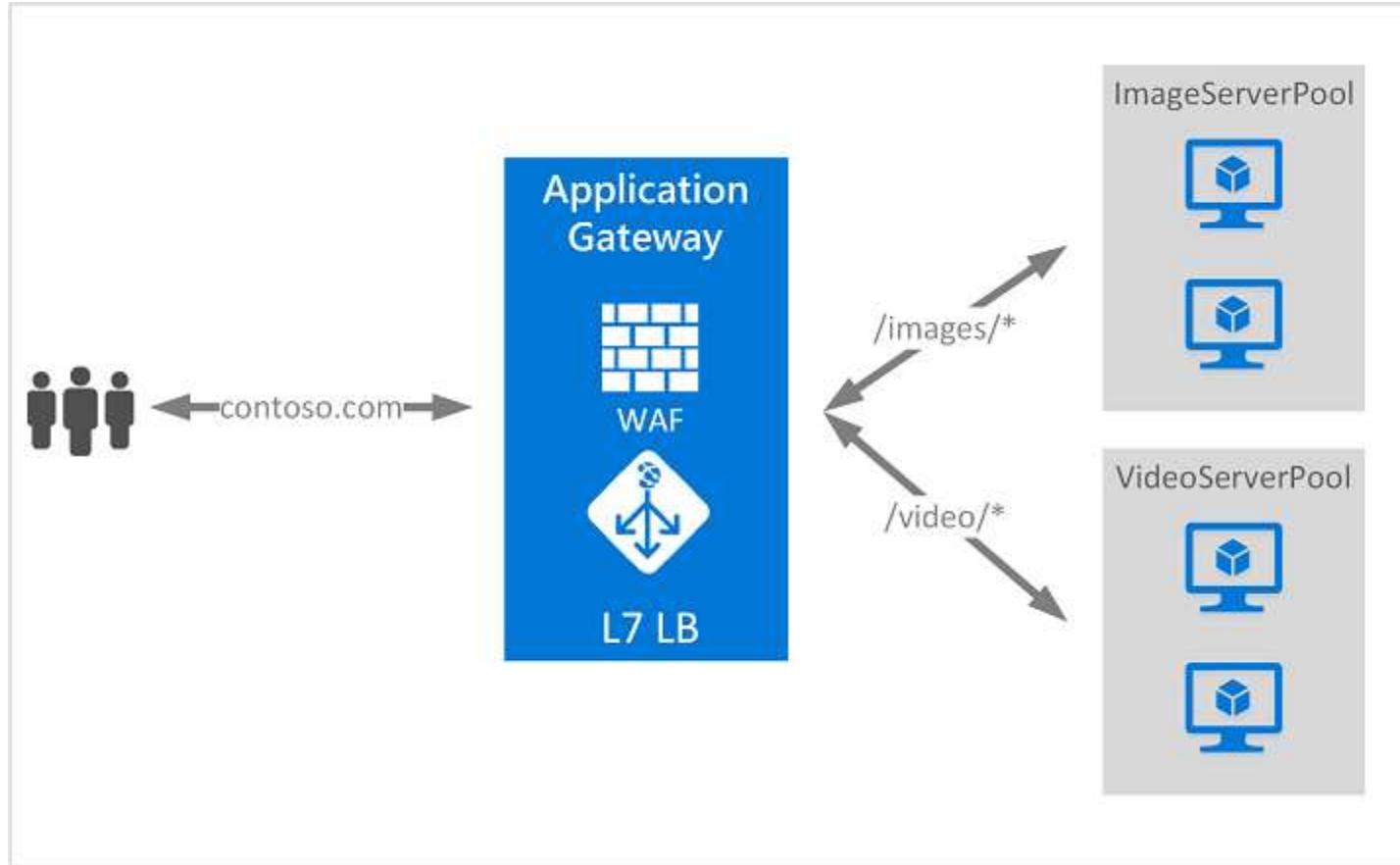
## Azure Load Balancing Services

*Load balancing* refers to efficiently distributing load or incoming network traffic across a group of backend resources or servers.









## IaaS

## DISKS

- ✓ Persistent Disks for Azure IaaS VM's.
- ✓ Premium Storage Disks
  - ✓ SSD based, High IOPS, Low latency

## FILES

- ✓ Fully Managed File Shares in the Cloud
- ✓ SMB and REST access

## PaaS

## Blobs

- ✓ Highly scalable, REST based object store
- ✓ Unstructured Data

## TABLES

- ✓ Massive Auto-Scaling NoSQL Store
- ✓ Dynamic Scaling Based on Load
- ✓ Scale to PB's of the Table Data
- ✓ Fast key/Value lookups

## Queues

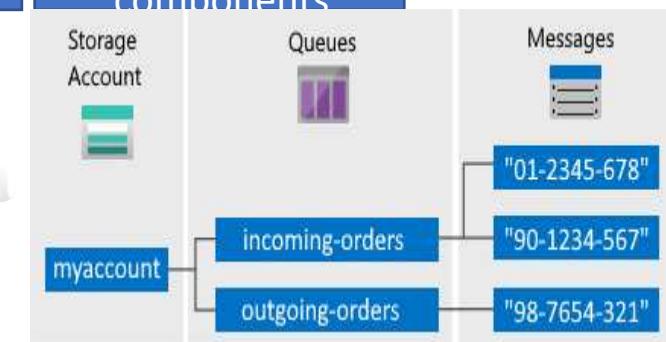
- ✓ Reliable queues at scale for cloud services
- ✓ Decouple and scale components

## Storage Tiers

- Hot Tier
- Cool Tier
- Archive Tier

## Storage Tiers

- Replication



## IaaS

**DISKS**

- ✓ Persistent Disks for Azure IaaS VM's.
- ✓ Premium Storage Disks
  - ✓ SSD based, High IOPS, Low latency

**FILES**

- ✓ Fully Managed File Shares in the Cloud
- ✓ SMB and REST access

## PaaS

**Blobs**

- ✓ Highly scalable, REST based object store
- ✓ Unstructured Data

**TABLES**

- ✓ Massive Auto-Scaling NoSQL Store
- ✓ Dynamic Scaling Based on Load
- ✓ Scale to PB's of the Table Data
- ✓ Fast key/Value lookups

**Queues**

- ✓ Reliable queues at scale for cloud services
- ✓ Decouple and scale components

## Storage Tiers

- Hot Tier
- Cool Tier
- Archive Tier

**SetBlobTier  
Direction****Write Charges (Operation + Access)**

hot->cool,  
hot->archive,  
cool->archive

**Read Charges (Operation + Access)**

archive->cool,  
archive->hot,  
cool->hot

## IaaS

**DISKS**

- ✓ Persistent Disks for Azure IaaS VM's.
- ✓ Premium Storage Disks
  - ✓ SSD based, High IOPS, Low latency

**FILES**

- ✓ Fully Managed File Shares in the Cloud
- ✓ SMB and REST access

## PaaS

**Blobs**

- ✓ Highly scalable, REST based object store
- ✓ Unstructured Data

**TABLES**

- ✓ Massive Auto-Scaling NoSQL Store
- ✓ Dynamic Scaling Based on Load
- ✓ Scale to PB's of the Table Data
- ✓ Fast key/Value lookups

**Queues**

- ✓ Reliable queues at scale for cloud services
- ✓ Decouple and scale components

## Storage Tiers

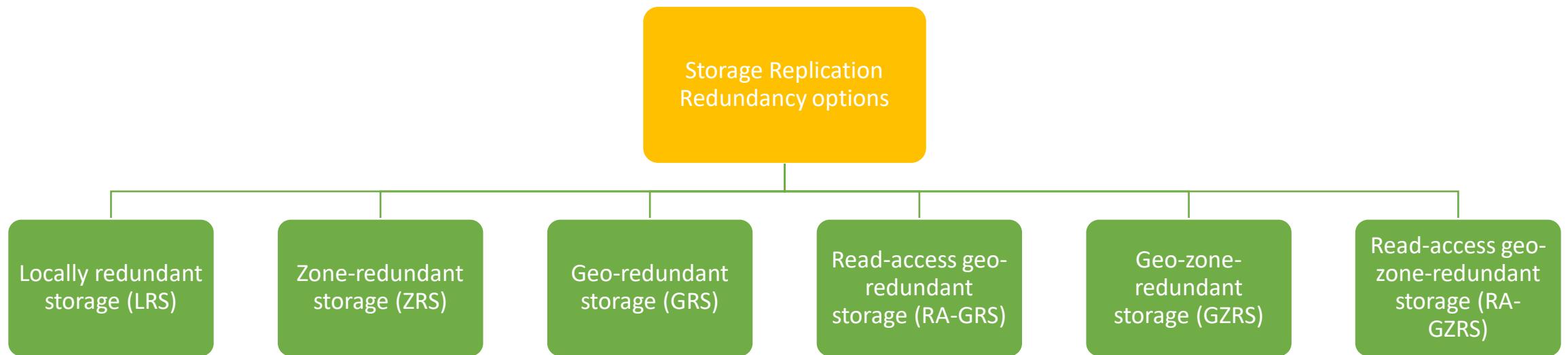
- Hot Tier
- Cool Tier
- Archive Tier

## Storage Tiers

- Replication

		Premium	Replication	Access Tier
	Standard			
Account Kind	Storage V2 - General Purpose V2	Yes	LRS,ZRS,GRS,RA-GRS,GZRS,RA-GZRS	Cool and Hot
	Storage - General Purpose V1	Yes	LRS, GRS and RA- GRS	NA
	Blog Storage	No	LRS, GRS and RA- GRS	Cool and Hot
	Premium			
Account Kind	Storage V2 - General Purpose V2	Yes	LRS	NA
	Storage - General Purpose V1	Yes	LRS	NA
	Block Blob Storage	Yes	LRS	NA
	File Storage	Yes	LRS	NA

Scenario	LRS	ZRS	GRS/RA-GRS	GZRS/RA-GZRS (preview)
Node unavailability within a data center	Yes	Yes	Yes	Yes
An entire data center (zonal or non-zonal) becomes unavailable	No	Yes	Yes	Yes
A region-wide outage	No	No	Yes	Yes
Read access to your data (in a remote, geo-replicated region) in the event of region-wide unavailability	No	No	Yes (with RA-GRS)	Yes (with RA-GZRS)
Designed to provide __ durability of objects over a given year <sup>1</sup>	At least 99.999999999% (11 9's)	At least 99.999999999% (12 9's)	At least 99.99999999999999% (16 9's)	At least 99.99999999999999% (16 9's)
Supported storage account types	GPv2, GPv1, BlockBlobStorage, BlobStorage, FileStorage	GPv2, BlockBlobStorage, FileStorage	GPv2, GPv1, BlobStorage	GPv2
Availability SLA for read requests	At least 99.9% (99% for cool access tier)	At least 99.9% (99% for cool access tier)	At least 99.9% (99% for cool access tier) for GRS At least 99.99% (99.9% for cool access tier) for RA-GRS	At least 99.9% (99% for cool access tier) for GZRS At least 99.99% (99.9% for cool access tier) for RA-GZRS
Availability SLA for write requests	At least 99.9% (99% for cool access tier)	At least 99.9% (99% for cool access tier)	At least 99.9% (99% for cool access tier)	At least 99.9% (99% for cool access tier)



## Locally redundant storage (LRS): Low-cost data redundancy

Locally redundant storage (LRS) replicates your data three times within a single data center

LRS provides at least 99.99999999% (11 nines) durability of objects over a given year

### Scenario Based example

If a datacenter-level disaster (for example, fire or flooding) occurs, all replicas in a storage account using LRS may be lost or unrecoverable. To mitigate this risk, Microsoft recommends using zone-redundant storage (ZRS), geo-redundant storage (GRS), or geo-zone-redundant storage (GZRS).

A write request to an LRS storage account returns successfully only after the data is written to all three replicas.

### Use Cases

If your application stores data that can be easily reconstructed if data loss occurs, you may opt for LRS.

Some applications are restricted to replicating data only within a country/region due to data governance requirements. In some cases, the paired regions across which the data is replicated for GRS accounts may be in another country/region

## ZONE-REDUNDANT STORAGE

Zone-redundant storage (ZRS) replicates your data synchronously across three storage clusters in a single region.

Each storage cluster is physically separated from the others and is located in its own availability zone (AZ)

Each availability zone—and the ZRS cluster within it—is autonomous and includes separate utilities and networking features.

A write request to a ZRS storage account returns successfully only after the data is written to all replicas across the three clusters.

### **What happens when a zone becomes unavailable?**

Your data is still accessible for both read and write operations even if a zone becomes unavailable. Microsoft recommends that you continue to follow practices for transient fault handling. These practices include implementing retry policies with exponential back-off.

ZRS may not protect your data against a regional disaster where multiple zones are permanently affected. Instead, ZRS offers resiliency for your data if it becomes temporarily unavailable. For protection against regional disasters, Microsoft recommends using geo-redundant storage (GRS)

## Geo-redundant storage (GRS)

### Cross-regional replication for Azure Storage

Geo-redundant storage (GRS) is designed to provide at least 99.9999999999999% (16 9's) durability of objects over a given year by replicating your data to a secondary region that is hundreds of miles away from the primary region. If your storage account has GRS enabled, then your data is durable even in the case of a complete regional outage or a disaster in which the primary region isn't recoverable.

If you opt for GRS, you have two related options to choose from:

GRS replicates your data to another data center in a secondary region, but that data is available to be read only if Microsoft initiates a failover from the primary to secondary region.

Read-access geo-redundant storage (RA-GRS) is based on GRS. RA-GRS replicates your data to another data center in a secondary region, and also provides you with the option to read from the secondary region. With RA-GRS, you can read from the secondary region regardless of whether Microsoft initiates a failover from the primary to secondary region

## Build highly available Azure Storage applications with geo-zone-redundant storage (GZRS)

Geo-zone-redundant storage (GZRS) marries the high availability of zone-redundant storage (ZRS) with protection from regional outages as provided by geo-redundant storage (GRS). Data in a GZRS storage account is replicated across three Azure availability zones in the primary region and also replicated to a secondary geographic region for protection from regional disasters. Each Azure region is paired with another region within the same geography, together making a regional pair

- ✓ With a GZRS storage account, you can continue to read and write data if an availability zone becomes unavailable or is unrecoverable.
- ✓ Additionally, your data is also durable in the case of a complete regional outage or a disaster in which the primary region isn't recoverable.
- ✓ GZRS is designed to provide at least 99.9999999999999% (16 9's) durability of objects over a given year. GZRS also offers the same scalability targets as LRS, ZRS, GRS, or RA-GRS. You can optionally enable read access to data in the secondary region with read-access geo-zone-redundant storage (RA-GZRS) if your applications need to be able to read data in the event of a disaster in the primary region.
- ✓ Microsoft recommends using GZRS for applications requiring consistency, durability, high availability, excellent performance, and resilience for disaster recovery
- ✓ For the additional security of read access to the secondary region in the event of a regional disaster, enable RA-GZRS for your storage account

## How GZRS and RA-GZRS work

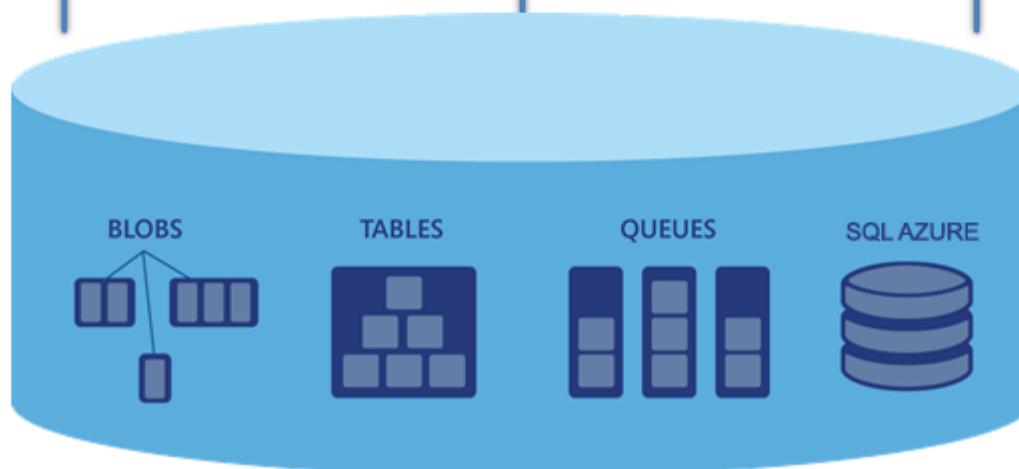
When data is written to a storage account with GZRS or RA-GZRS enabled, that data is first replicated synchronously in the primary region across three availability zones. The data is then replicated asynchronously to a second region that is hundreds of miles away. When the data is written to the secondary region, it's further replicated synchronously three times within that region using [locally redundant storage \(LRS\)](#).

**TABLES:**  
Provide structured storage. A table is a set of entities which contain a set of properties.

**BLOBS:**  
Provide a simple interface for storing named files along with metadata for the file.

**QUEUES:**  
Provide reliable storage and delivery of messages for an application.

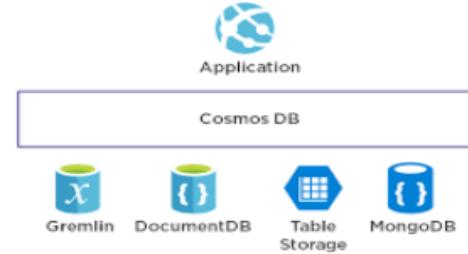
**SQL Azure:**  
A relational database hosted in a MS data center, triply replicated.



## Databases

### Azure Cosmos DB

- Globally distributed, multi-Model NoSQL database Service
- Paas Service – Auto-Scalable Across multiple regions
- Supports API, Including SQL, MongoDB, Cassandra, Tables & Gremlin



### Azure Sql Database

IaaS

- SQL Server on Azure VMs
- Pay-As-You-Go for SQL server license or use an existing licenses

Paas

- Fully Managed SQL database Engine
- Available as Single Database, Elastic pool and Managed instances

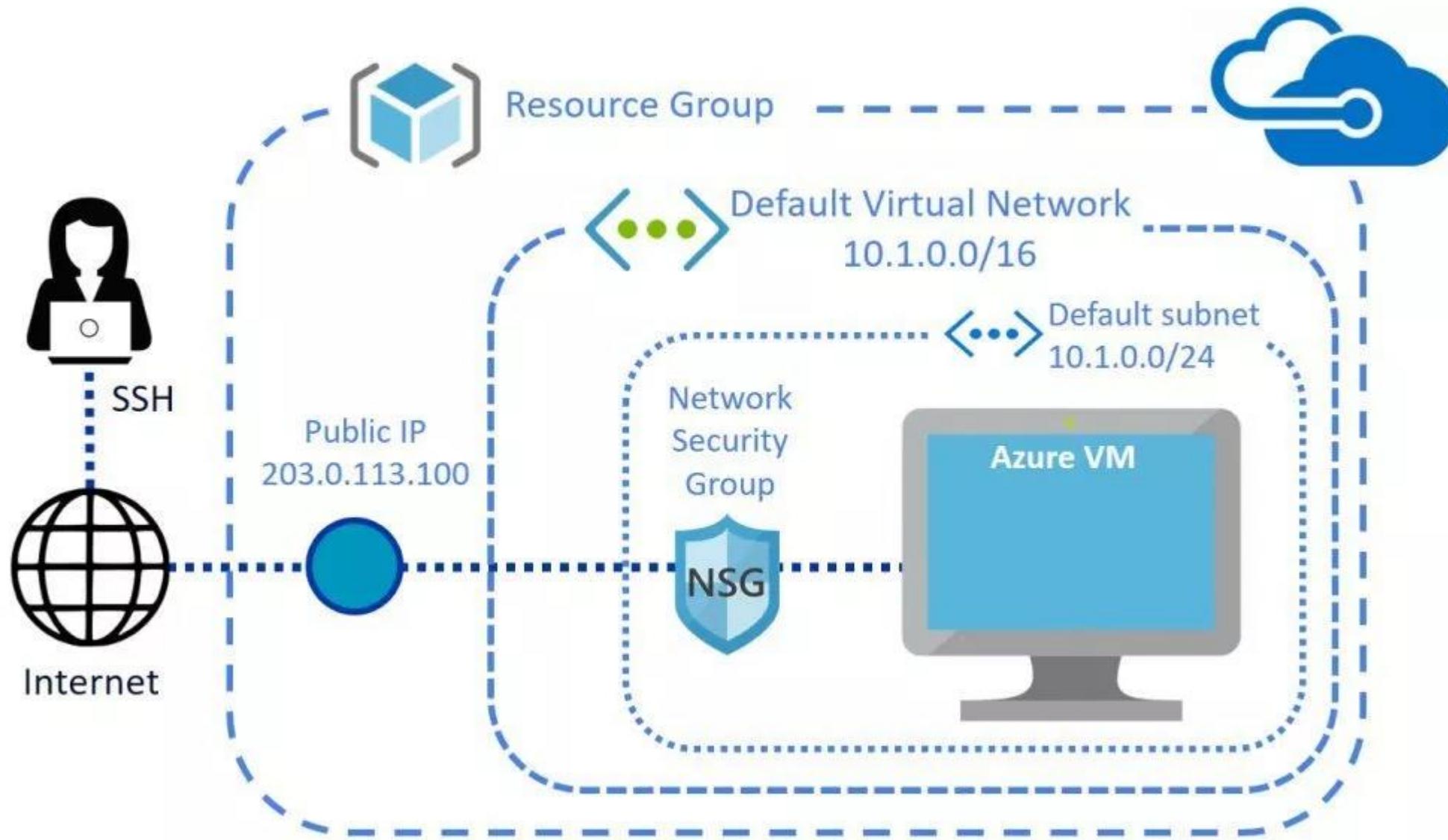
### Azure SQL Data Warehouse

- Cloud Based Enterprise Data Warehouse – EDW
- Leverages massively parallel processing (MPP) to Quickly run complex queries across petabytes of Data
- Key component of a Big Data Solution

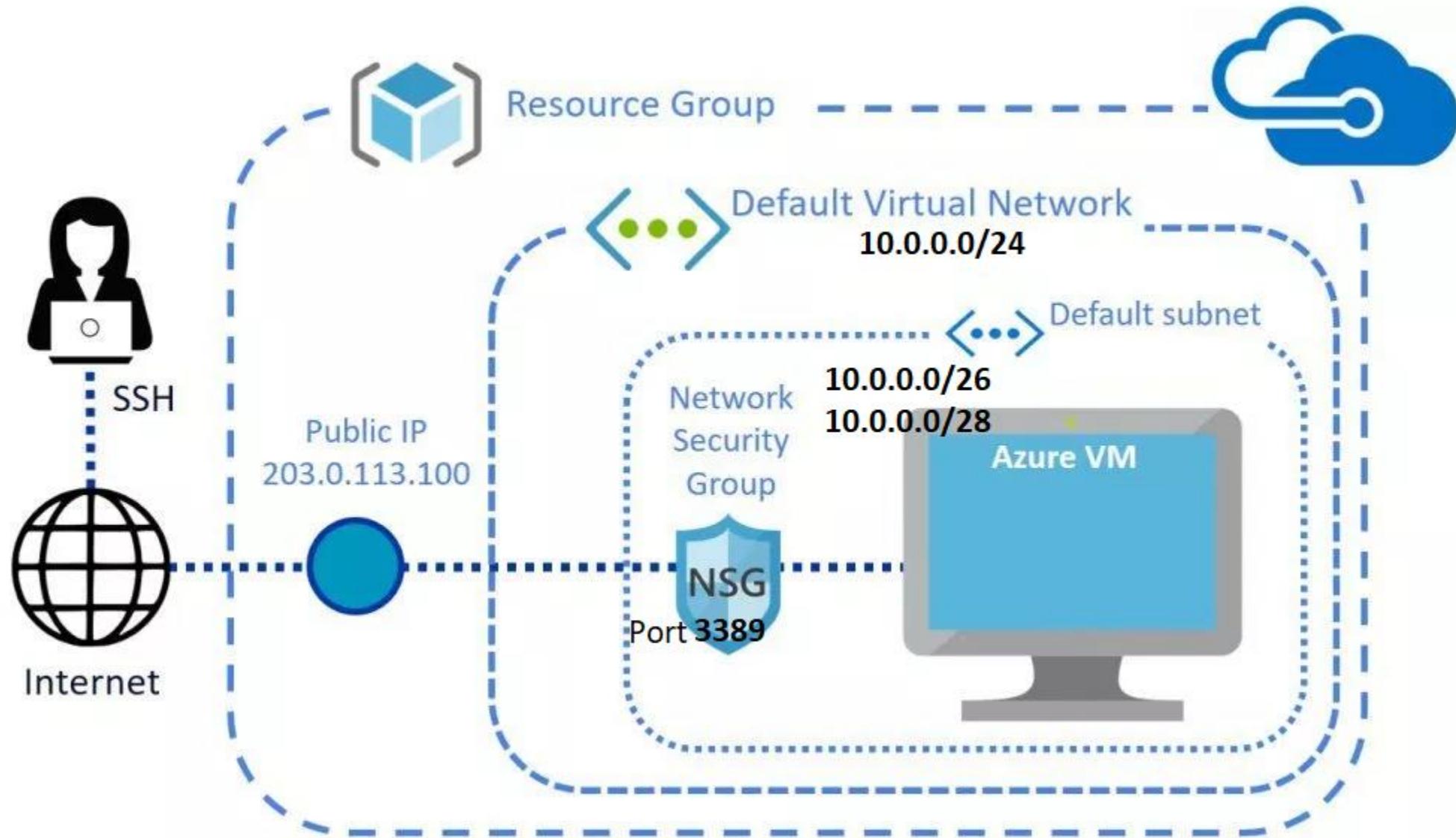
### Azure Database Migration services

- Enables seamless migration from multiple databases sources to Azure Data platforms with minimal downtime
- Offline migration: Application downtime starts when the migration starts
- Online Migration: Downtime is limited to the time to cur over at the end of the migration

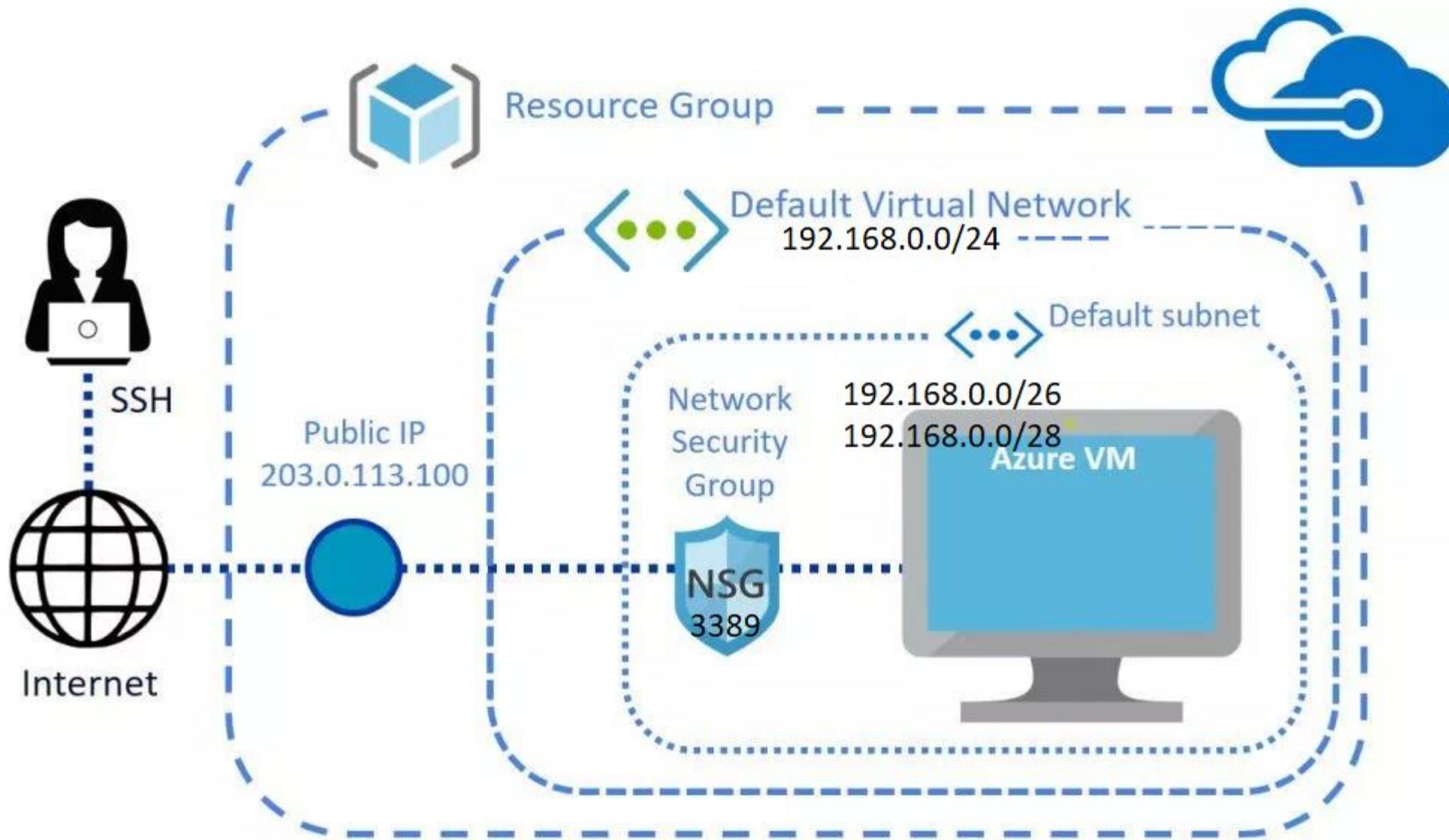
## Creating Your First Azure Virtual Machine -Step By Step – Try Yourself



## LAB Demo - Creating Azure Virtual Networks



## LAB Demo - Creating Azure Virtual Networks



## Intro to Using Azure Blob Storage

Internet of  
Things – IoT

BigData And  
Analytics

Artificial  
Intelligence – AI

Serverless  
Computing

Azure Solitons  
Benefits

## Internet of Things (IoT)

- An IoT Solution is made up of one or more IoT devices and one or more back0end services running in the cloud that communicate with each other
- Devices usually have sensors and connect to the internet



## Internet of Things (IoT)

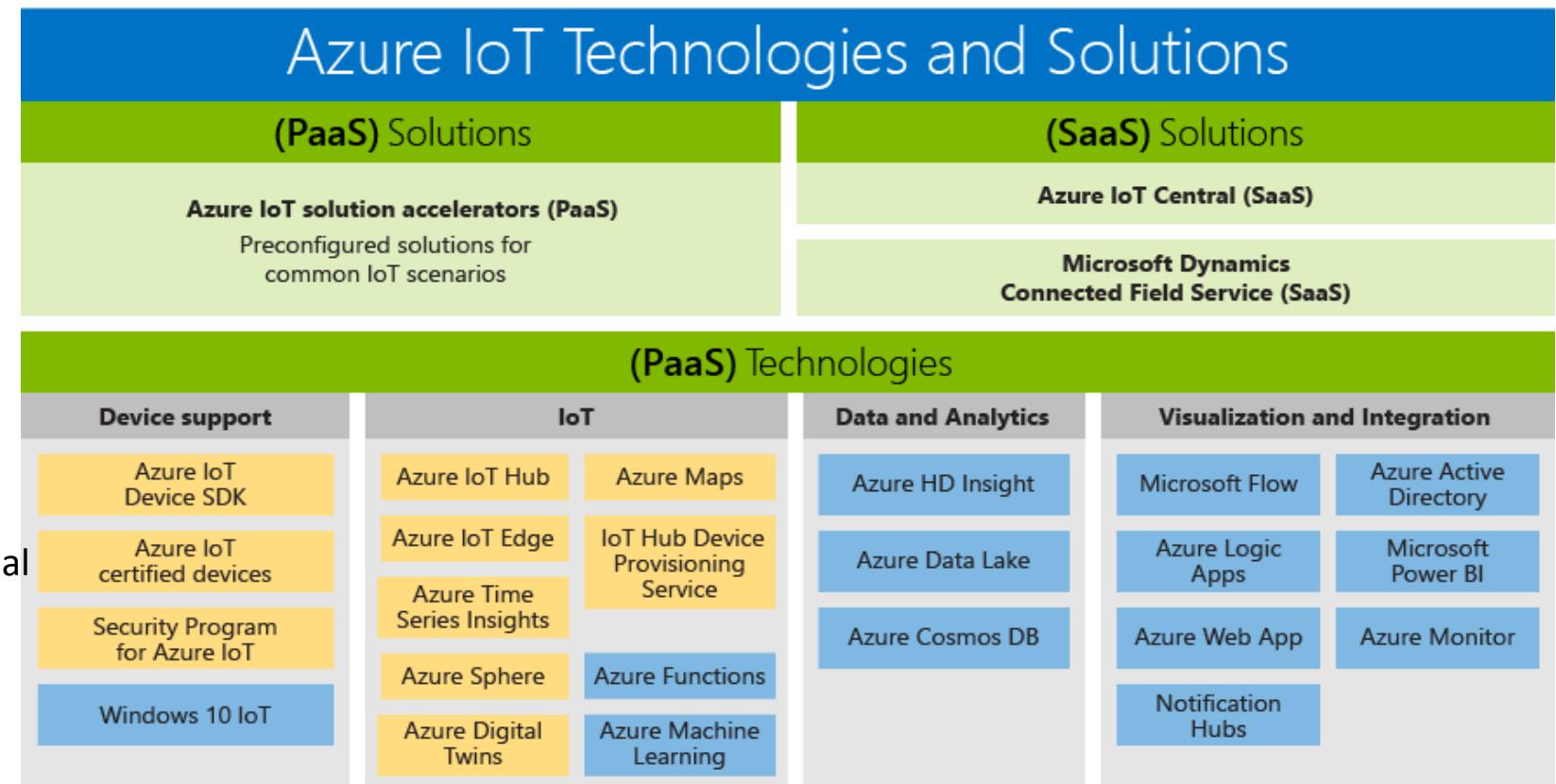
- An IoT Solution is made up of one or more IoT devices and one or more back-end services running in the cloud that communicate with each other
- Devices usually have sensors and connect to the internet

### IOC Central

- Fully managed SaaS Solution
- Easily connect, Monitor and manager your IoT Devices / Assists at scale.
- Collaborative drag and Drop visual workspace where you can build test and deploy IOT Solutions without needing to write code

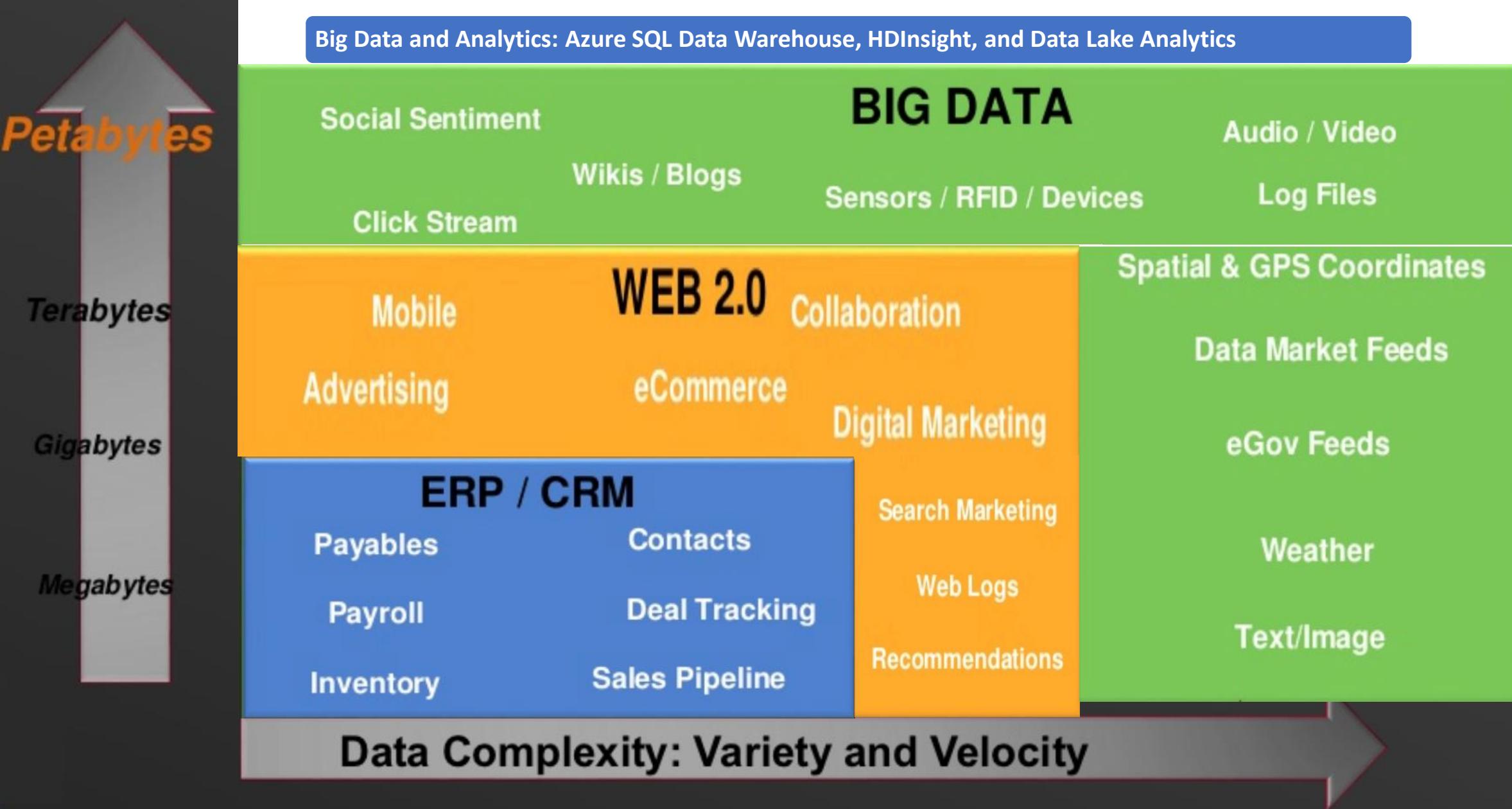
### IOT Hub

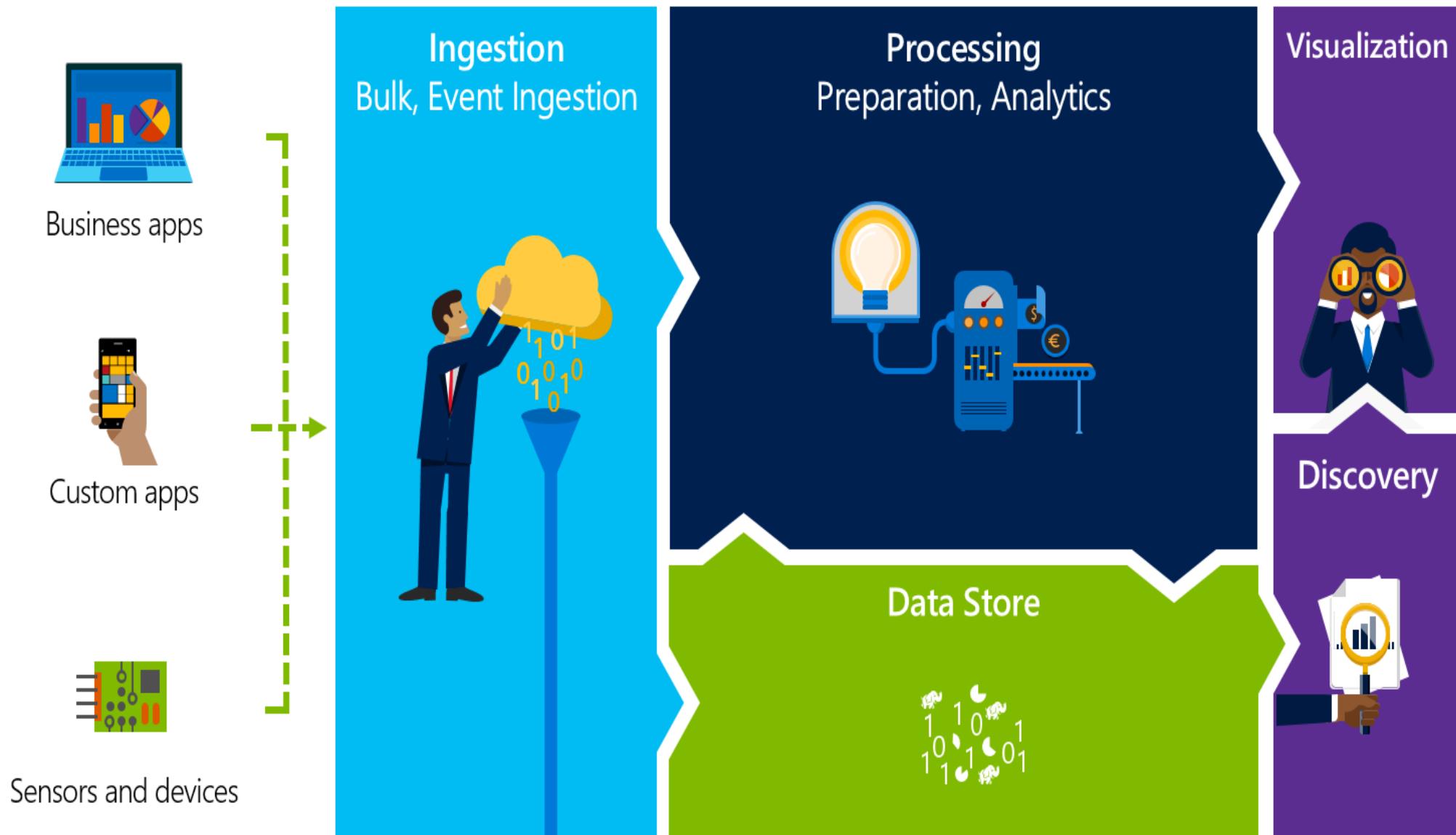
- Core Azure PaaS Messaging Service used by Azure IOT Central
- Enables reliable and secure bidirectional communications between millions of IoT Devices and a Cloud Solution

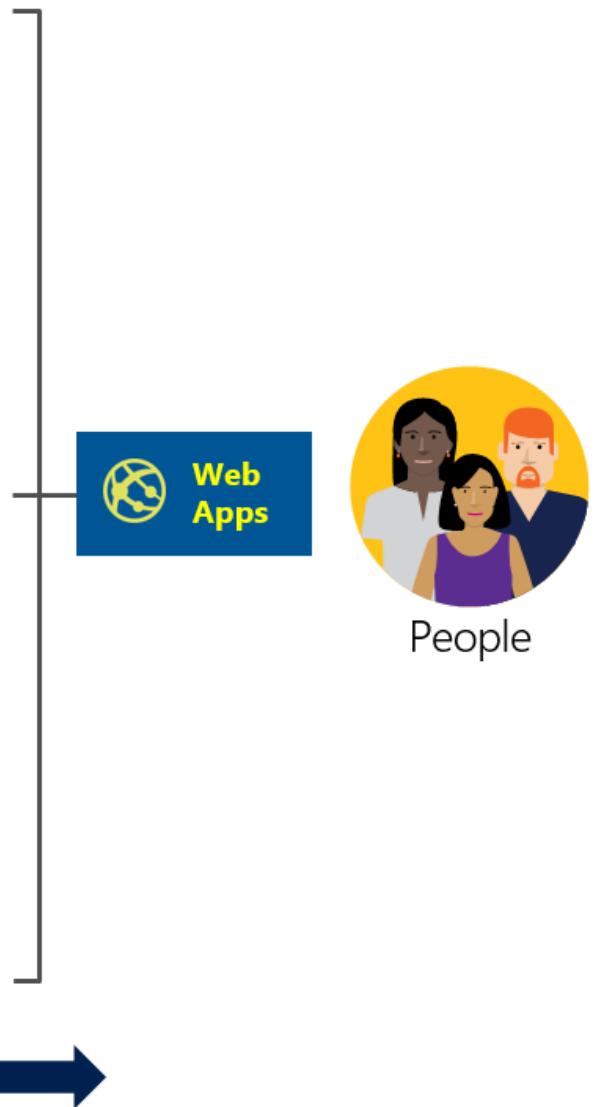
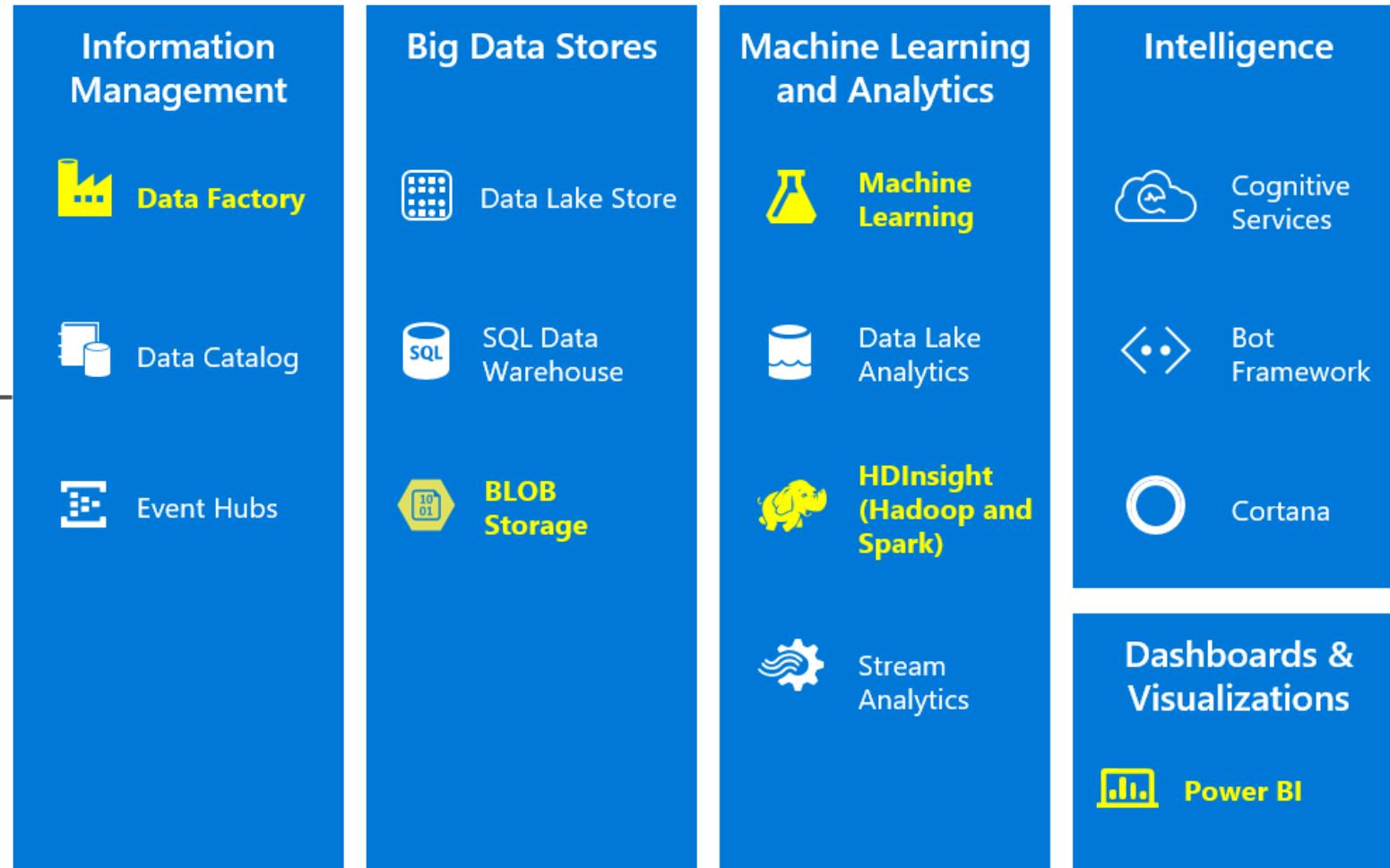




Big Data and Analytics: Azure SQL Data Warehouse, HDInsight, and Data Lake Analytics

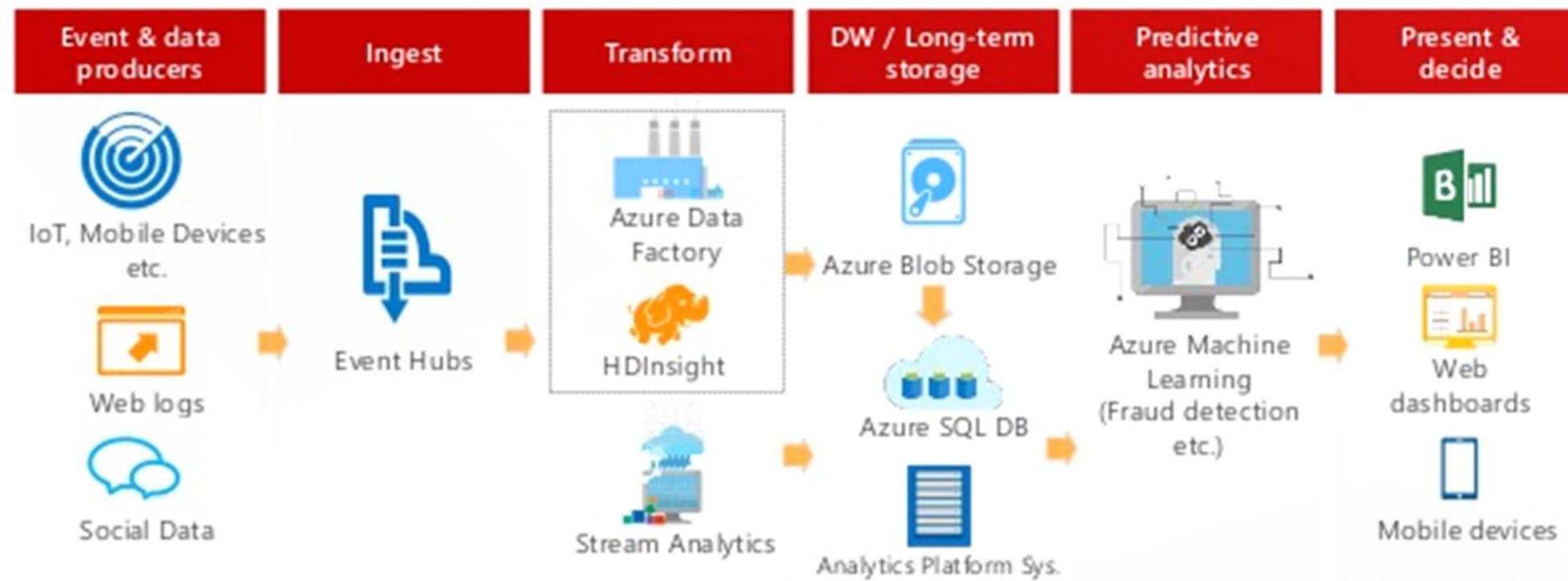




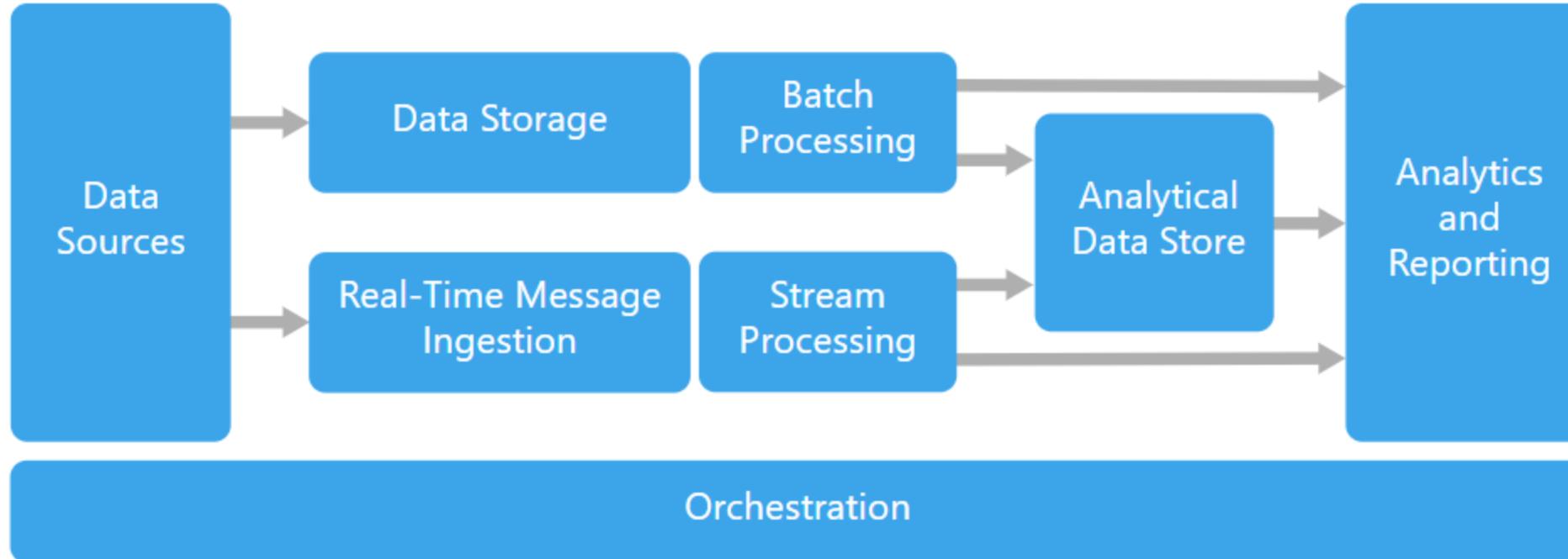


INTELLIGENCE

# Example overall data flow and Architecture

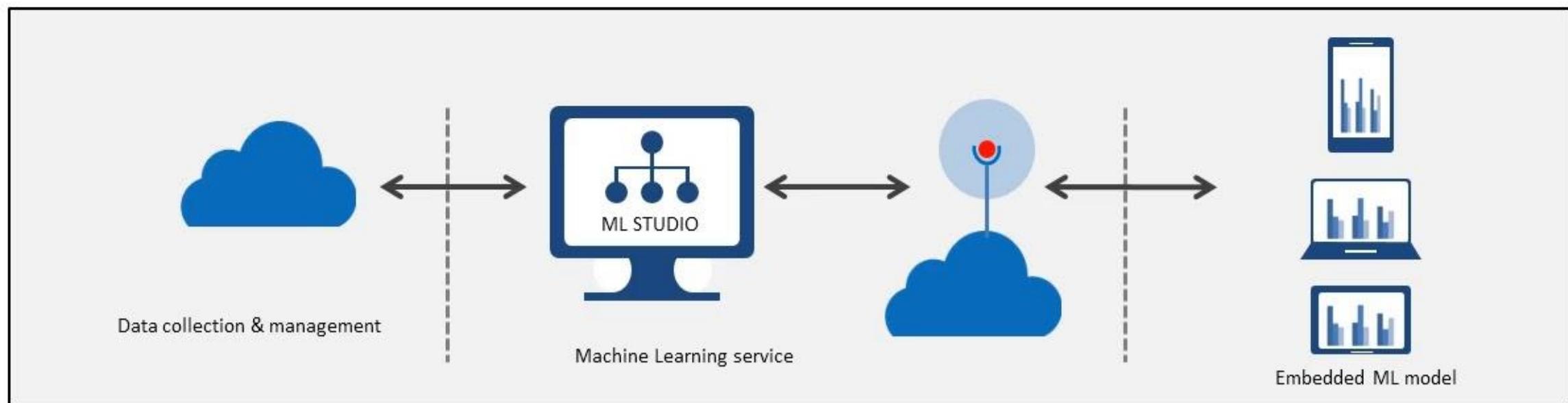


## BIG DATA ARCHITECTURE STYLE



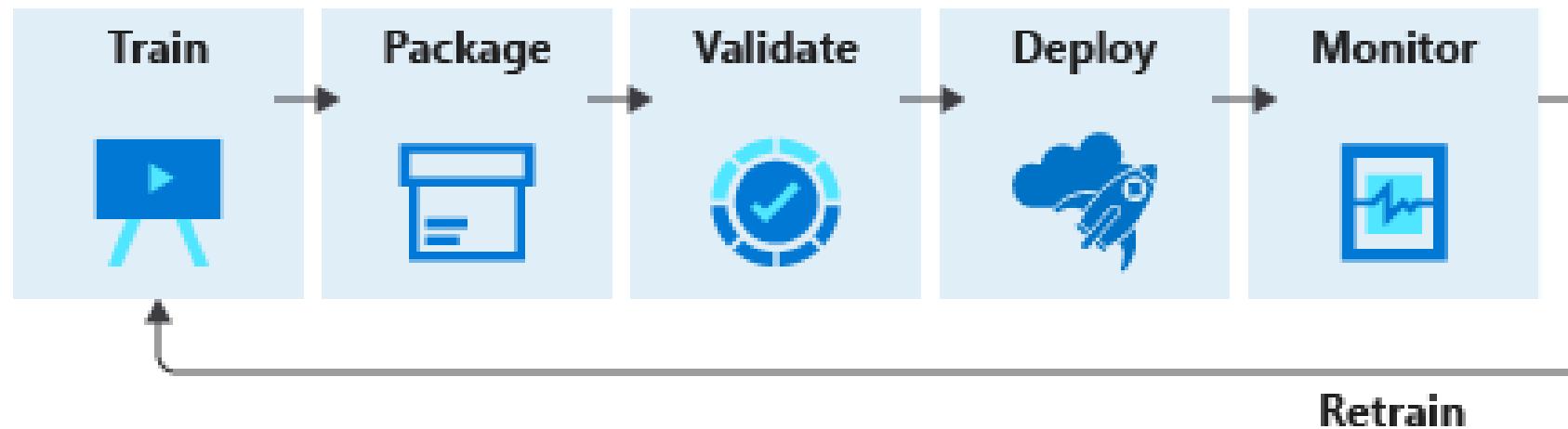
# Azure Machine Learning Workflow

- Data collection and management using database applications
  - Massive data stores (Azure Data Lake)
  - Relational data (Azure SQL database)
  - Blobs and tables (Azure Storage)
  - Hadoop (Azure)



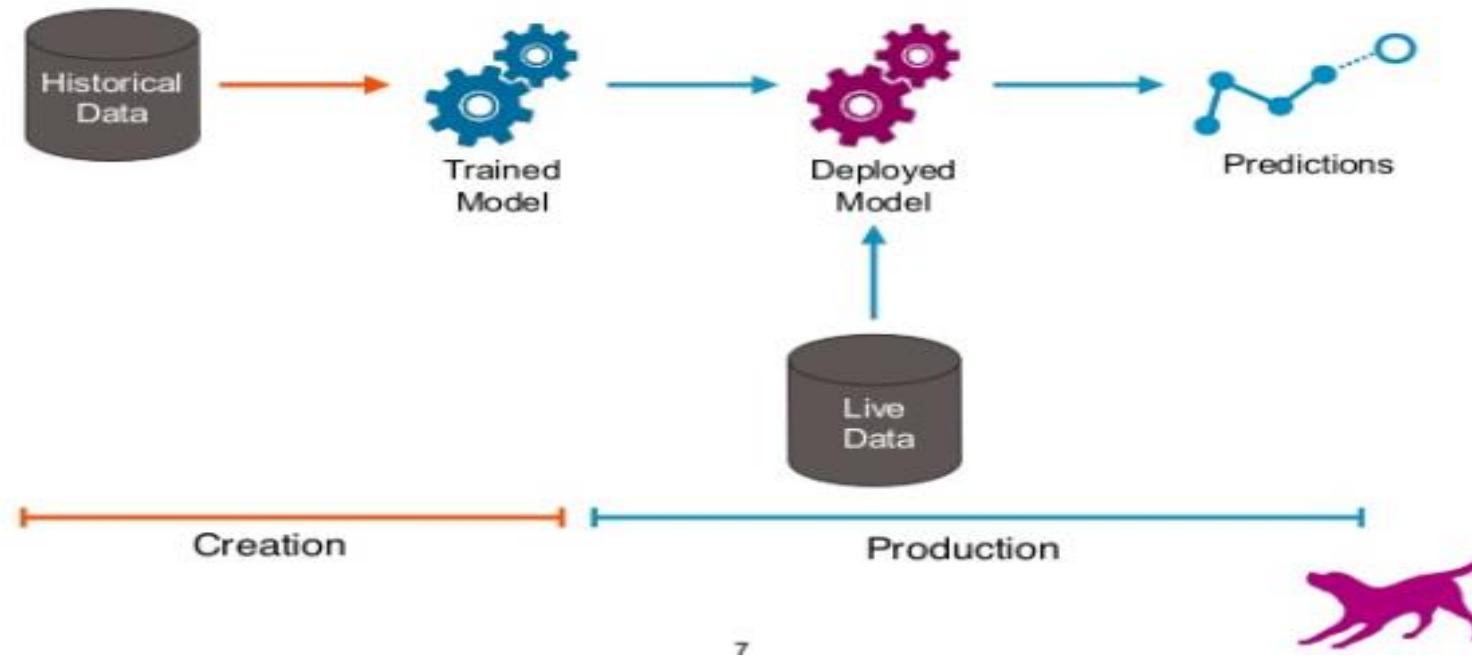
# Azure Machine Learning

## Azure Machine Learning Model Workflow



# Azure Machine Learning

## ML in Production - 101



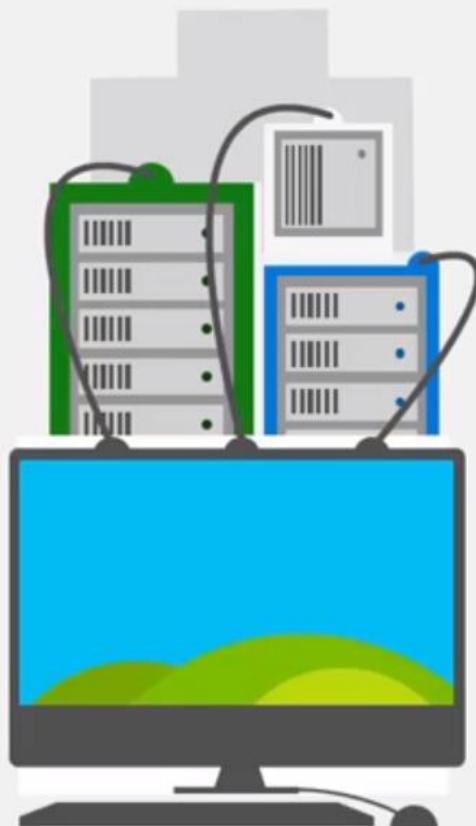
7

# Azure Machine Learning

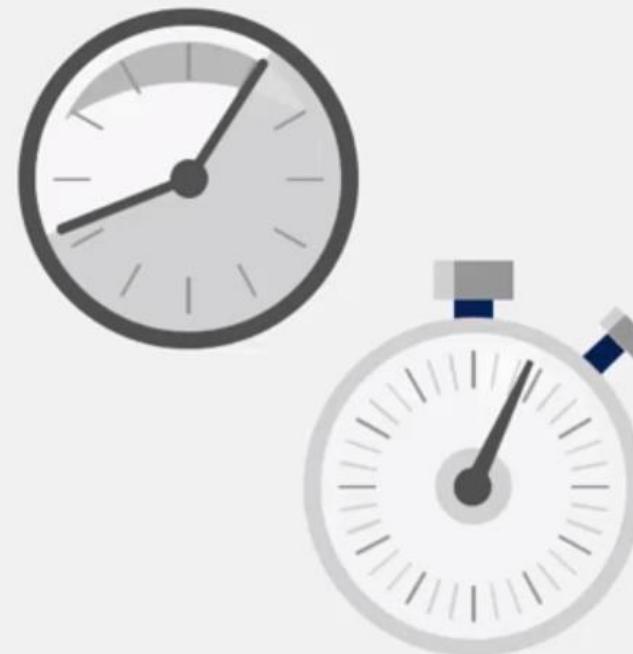
Machine  
Learning Service

Machine  
Learning Studio

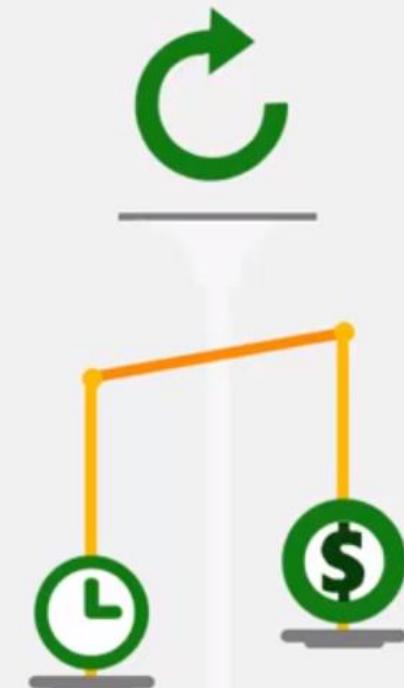
# Serverless Technologies



Reduced  
devops



Reduced time  
to market



Per action billing

# Azure serverless Computing



Azure Functions



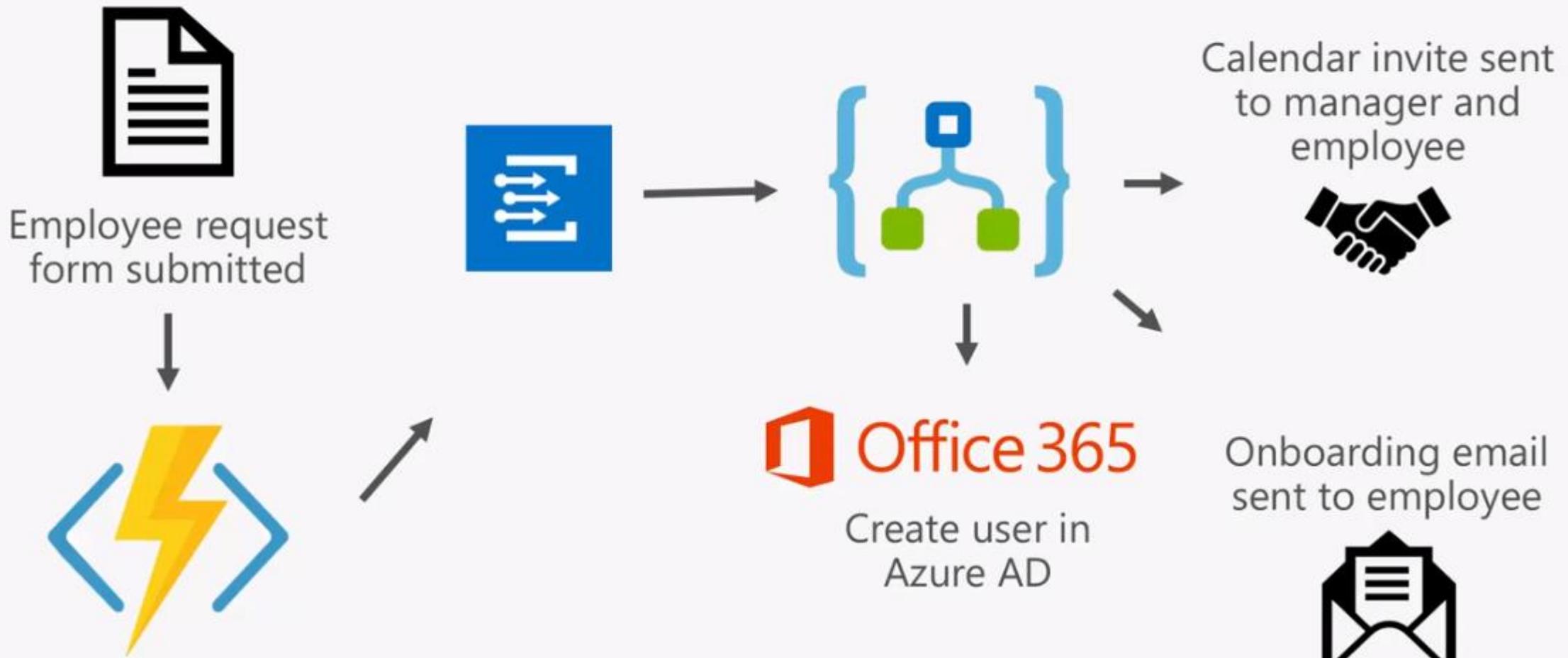
Azure logic Apps



Azure Event Grid



# Employee Onboarding



# Azure Solutions



## Azure Management Tools

Azure  
PowerShell

Azure  
Portal

Azure CLI

# Azure CLI

The Azure CLI is a command-line tool providing a great experience for managing Azure resources. The CLI is designed to make scripting easy, query data, support long-running operations, and more

Windows <https://aka.ms/installazurecliwindows>

macOS

Linux

## Steps to Create a VM

```
az group create --name myResourceGroup --location eastus
```

```
az vm create \  
  --resource-group myResourceGroup \  
  --name myVM \  
  --image win2016datacenter \  
  --admin-username azureuser \  
  --admin-password myPassword
```

```
az vm open-port --port 80 --resource-group myResourceGroup --name myVM
```

```
  Install-WindowsFeature -name Web-Server -IncludeManagementTools
```

```
az group delete --name myResourceGroup
```

# Azure PowerShell

Azure PowerShell works with

- PowerShell 5.1 or higher on Windows
- PowerShell Core 6.x and later on all platforms

Find Version

- `$PSVersionTable.PSVersion`

If you're on Windows 10, you already have PowerShell 5.1 installed

- `Install-Module -Name Az -AllowClobber -Scope AllUsers`

For Offline save and Install

- `Save-Module -Name Az -Path '\\someshare\PowerShell\modules' -Force`

To login with Azure from Powershell

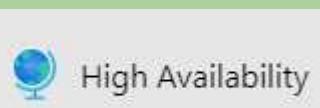
- `Connect-AzAccount`

Update the Azure PowerShell module

- `Install-Module -Name Az -AllowClobber -Force`

Azure  
Portal

# Azure Advisor



High Availability



Security



Performance

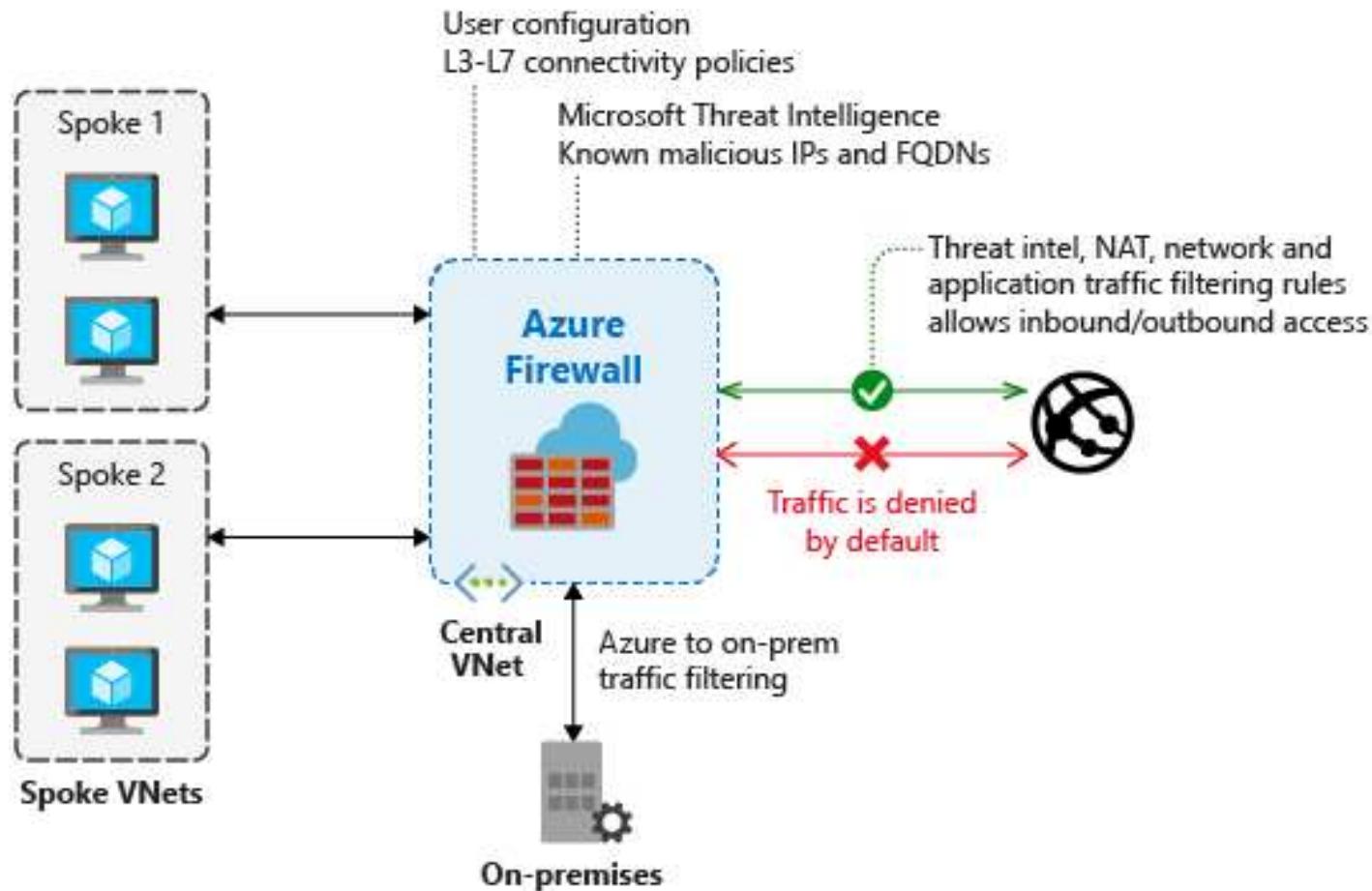


Operational Excellence

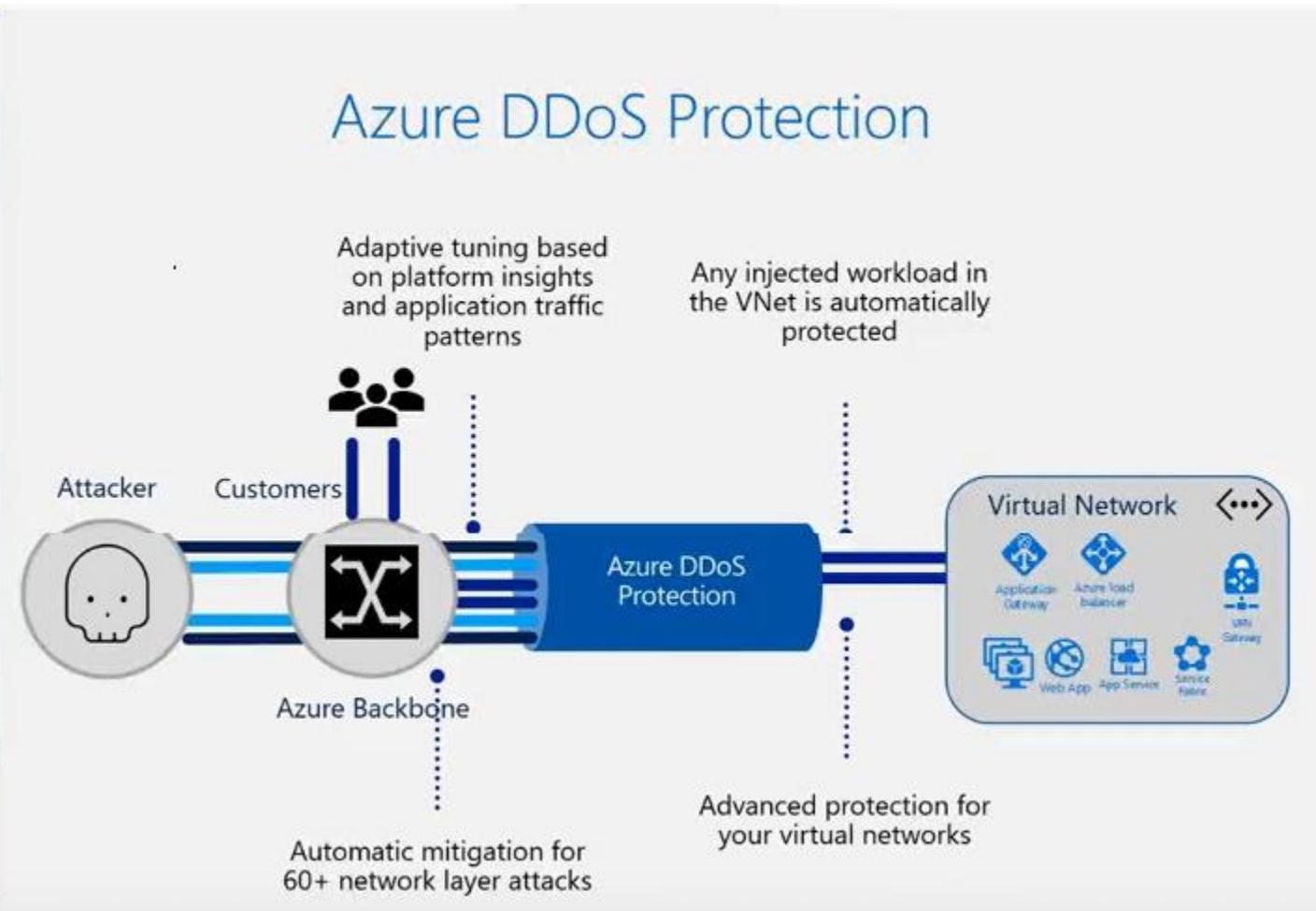
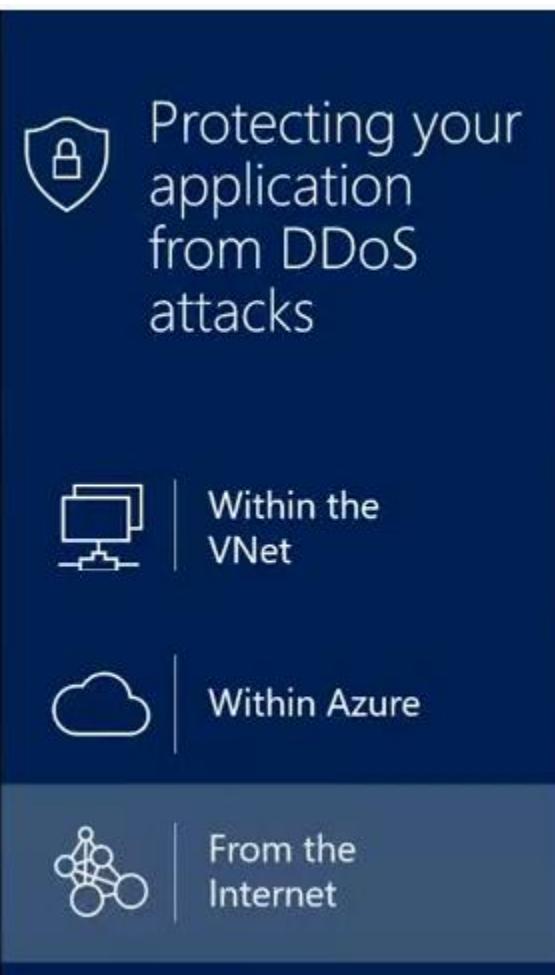


Cost

## Azure Firewall



## Azure DDoS Protection



Reliable  
proven success



Scalable  
global capacity

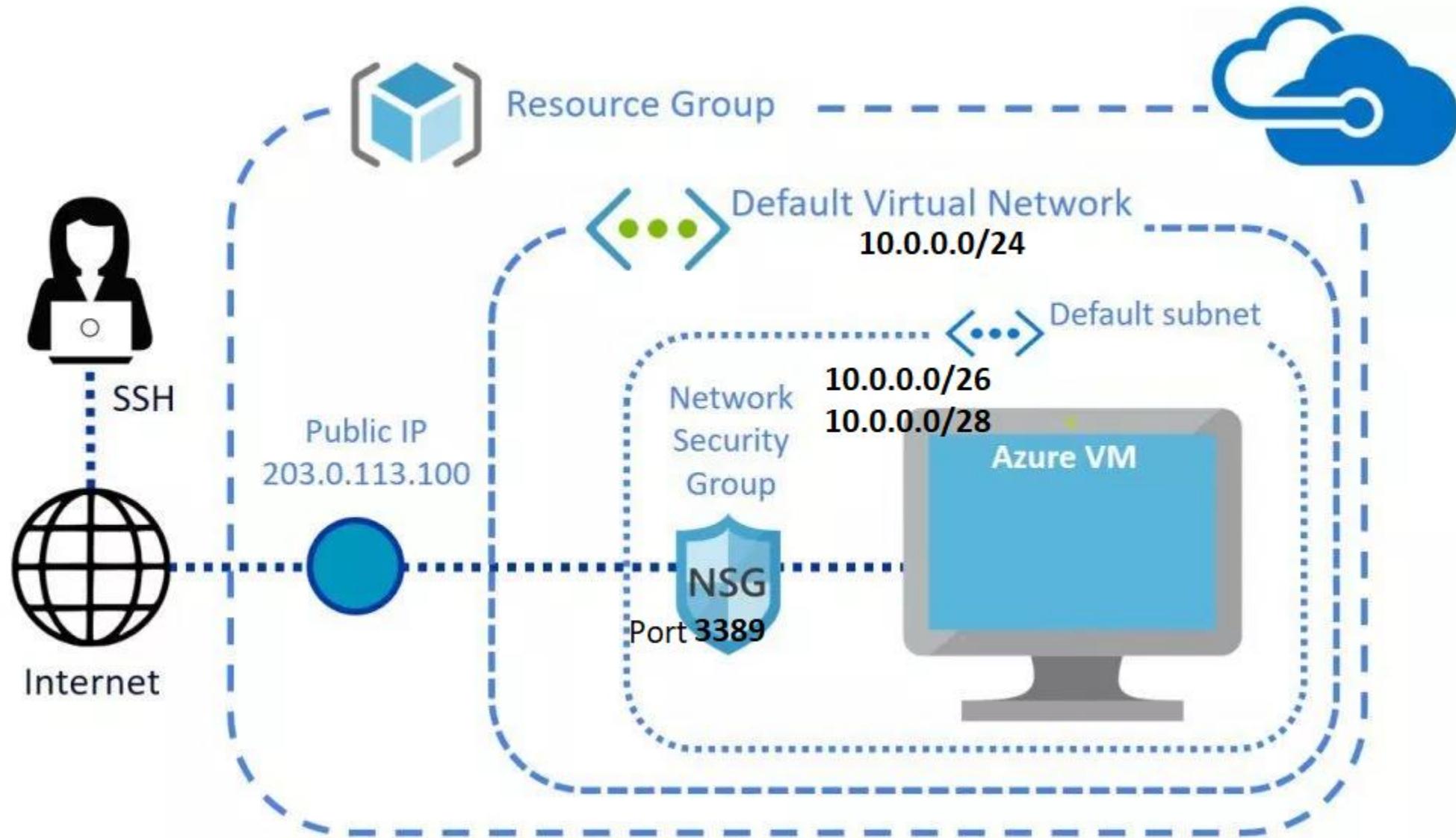


Automatic  
simple, automated



Adaptive  
real time tuning

## LAB Demo - Creating Azure Virtual Networks



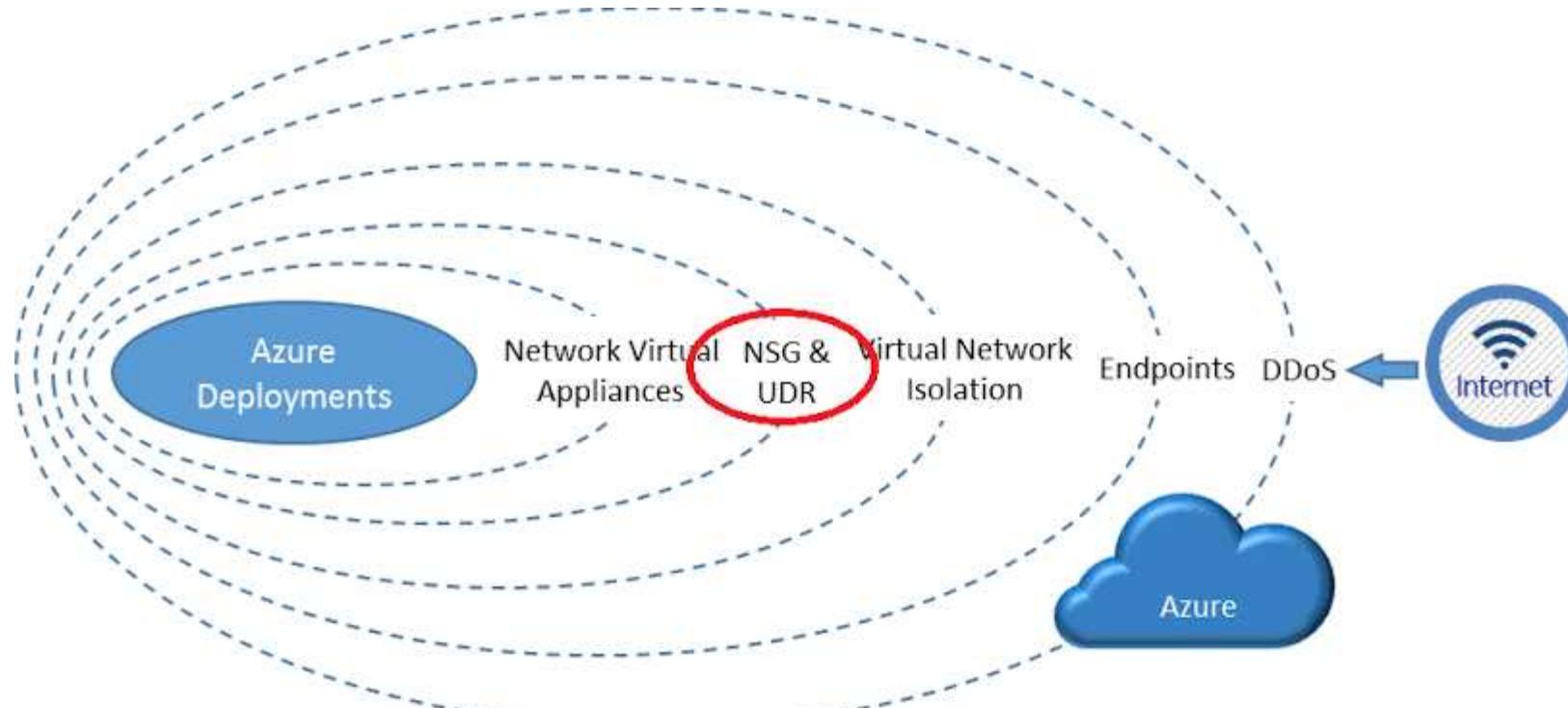


### Inbound security rules

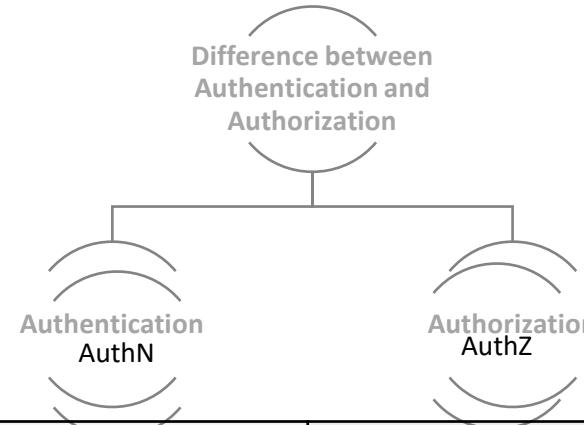
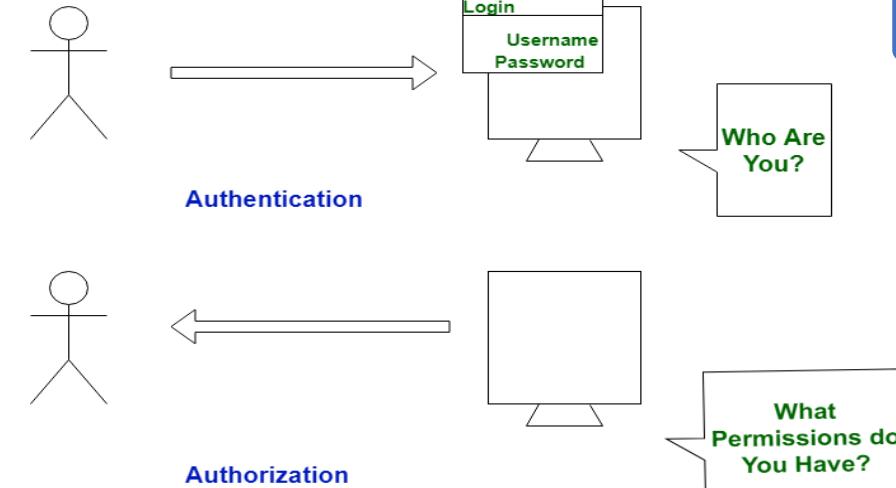
Priority	Name	Port	Protocol	Source	Destination	Action
101	⚠ Port_8080	81	Any	Any	Any	✓ Allow
102	⚠ Port_80	80	Any	Any	Any	✓ Allow
1000	⚠ default-allow-rdp	3389	TCP	Any	Any	✓ Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	✓ Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	✓ Allow
65500	DenyAllInBound	Any	Any	Any	Any	✗ Deny

### Outbound security rules

Priority	Name	Port	Protocol	Source	Destination	Action
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	✓ Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	✓ Allow
65500	DenyAllOutBound	Any	Any	Any	Any	✗ Deny

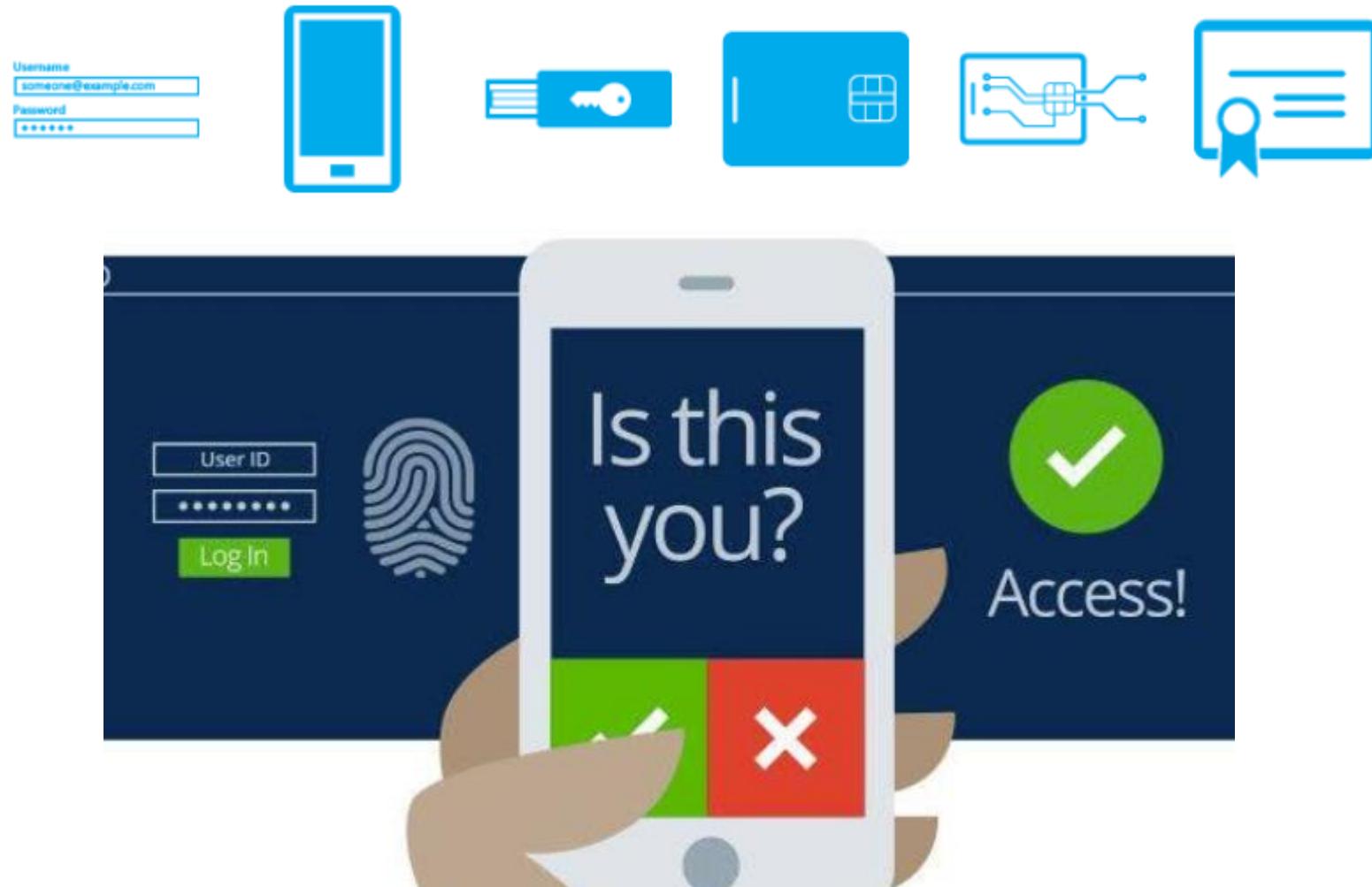


## Security Privacy compliance and Trust



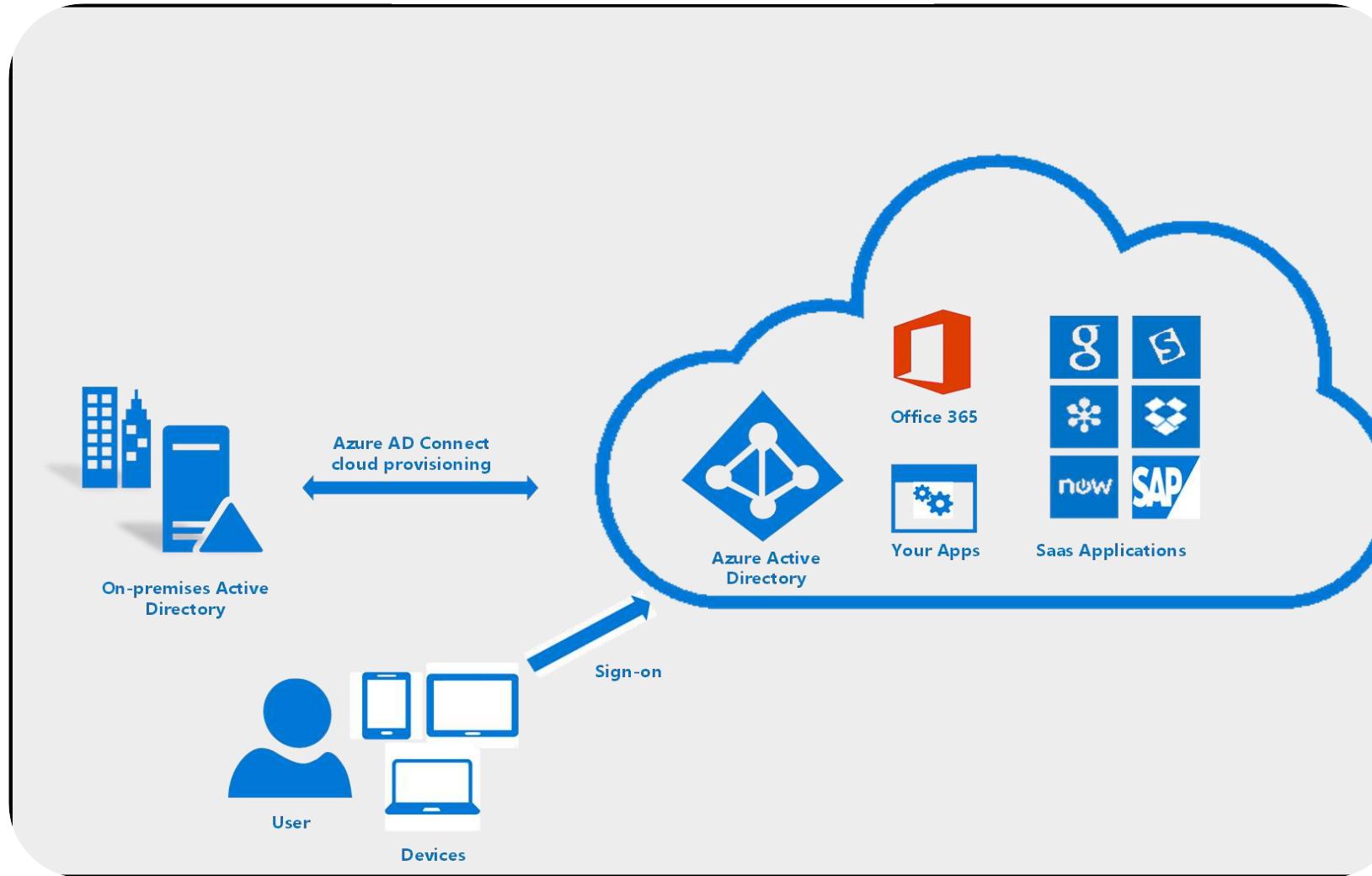
Authentication	Authorization
Authentication confirms your identity to grant access to the system.	Authorization determines whether you are authorized to access the resources.
It is the process of validating user credentials to gain user access.	It is the process of verifying whether access is allowed or not.
It determines whether user is what he claims to be.	It determines what user can and cannot access.
Authentication usually requires a username and a password.	Authentication factors required for authorization may vary, depending on the security level.
Authentication is the first step of authorization so always comes first.	Authorization is done after successful authentication.
For example, students of a particular university are required to authenticate themselves before accessing the student link of the university's official website. This is called authentication.	For example, authorization determines exactly what information the students are authorized to access on the university website after successful authentication.

## Azure Multi-Factor Authentication





## Azure Active Directory



Azure Security Tools  
and Features

Security in Azure

Azure Key Vault

Azure Security  
Center

Azure Information  
Protection – AIP

Azure Advanced  
Threat Protection -  
ATP

## Azure Security Tools and Features

Security in Azure

Azure Key Vault

Azure Security  
Center

Azure Information  
Protection – AIP

Azure Advanced  
Threat Protection -  
ATP

# Security Services and Technologies available on Azure

## General Azure security

- Azure Security Center
- Azure Key Vault
- Azure Monitor logs
- Azure Dev/Test Labs

## Storage security

- Azure Storage Service Encryption
- StorSimple Encrypted Hybrid Storage
- Azure Client-Side Encryption
- Azure Storage Shared Access Signatures
- Azure Storage Account Keys
- Azure File shares with SMB 3.0 Encryption
- Azure Storage Analytics

## Database security

- Azure SQL Firewall
- Azure SQL Cell Level Encryption
- Azure SQL Connection Encryption
- Azure SQL Always Encryption
- Azure SQL Transparent Data Encryption
- Azure SQL Database Auditing

## Identity and Access Management

- Azure Role Based Access Control
- Azure Active Directory
- Azure Active Directory B2C
- Azure Active Directory Domain Services
- Azure Multi-Factor Authentication

## Backup and Disaster Recovery

- Azure Backup
- Azure Site Recovery

## Networking

- Network Security Groups
- Azure VPN Gateway
- Azure Application Gateway
- Web application firewall (WAF)
- Azure Load Balancer
- Azure ExpressRoute
- Azure Traffic Manager
- Azure Application Proxy
- Azure Firewall
- Azure DDoS protection
- Virtual Network service endpoints

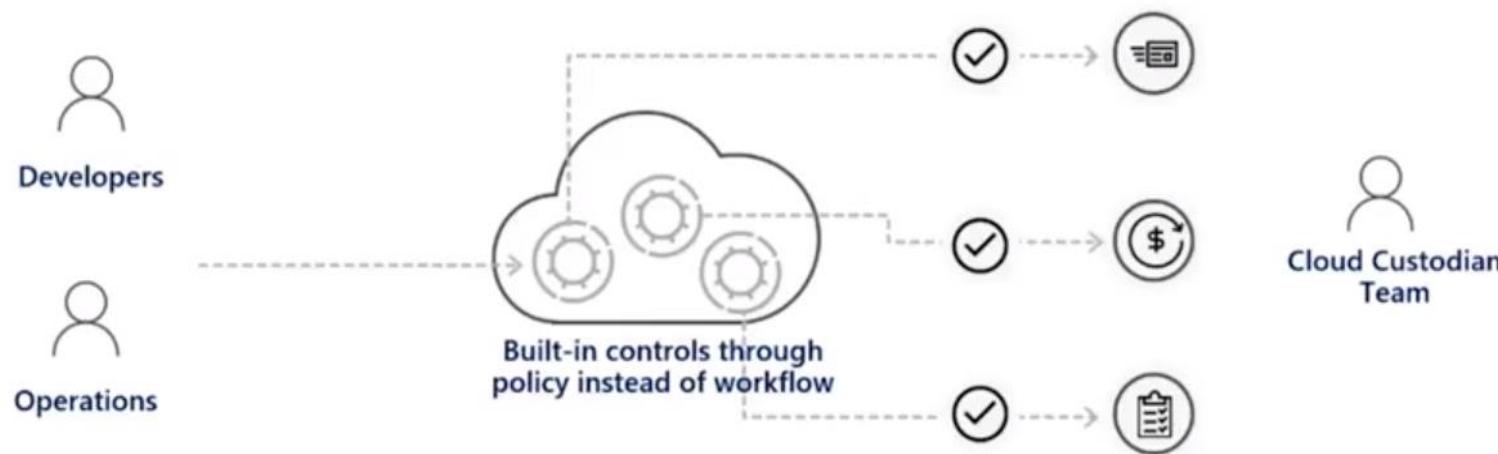
# Need to Govern

Your team runs an Azure Environment with:

- Multiple Engineering Teams (deploying to & operating in)
- Multiple Subscriptions
- Need to standardize/enforce how cloud resources are configured
- Due to regulatory compliance, cost control, security or design consistency

# Cloud-native governance

Removing barriers to compliance and enabling velocity



# Azure policy for enterprise-level compliance



- Turn on built-in policies or build custom ones for all resource types
- Real-time policy evaluation and enforcement
- Periodic & on-demand compliance evaluation

## Enforcement & Compliance



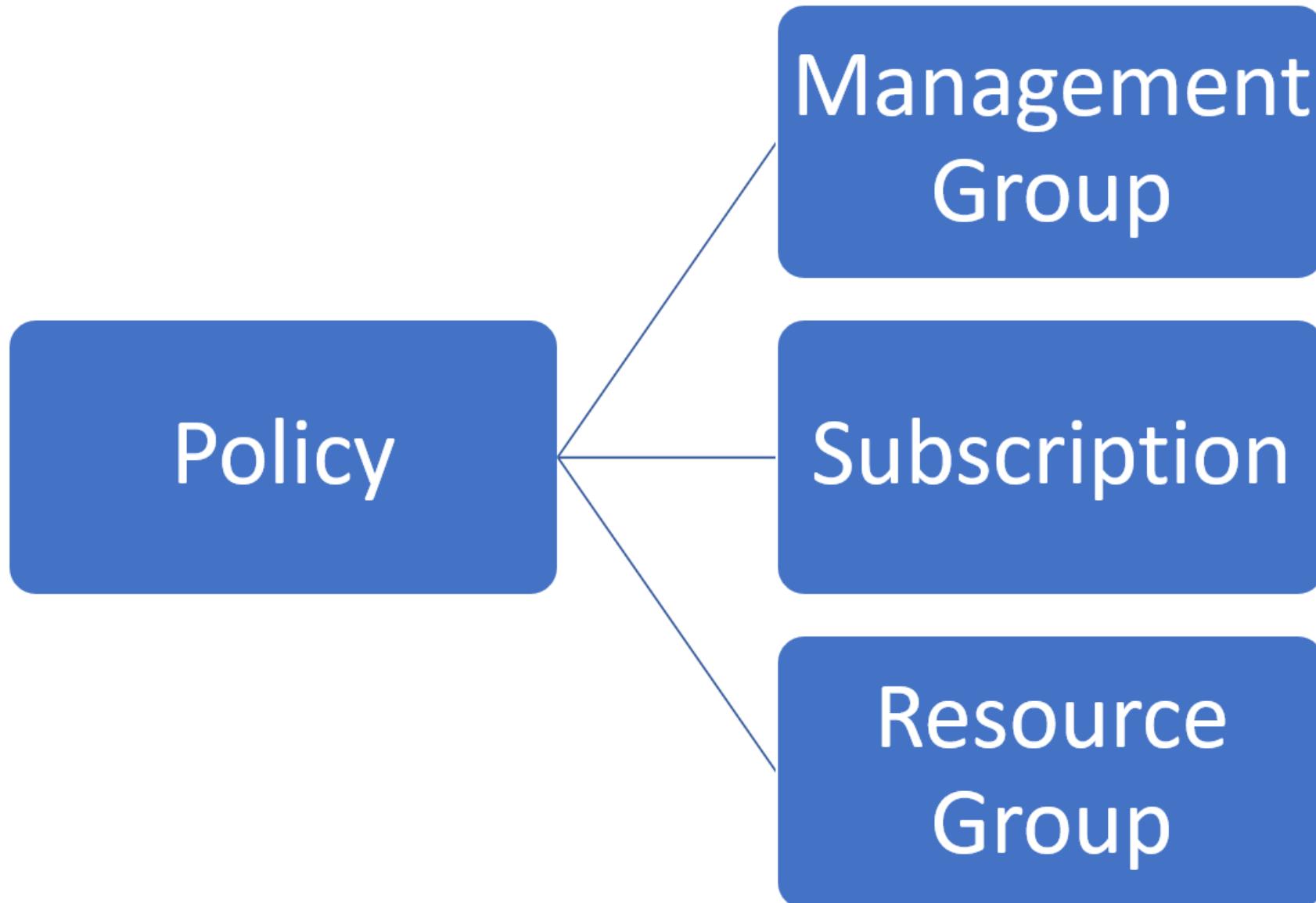
- Apply policies to a Management Group with control across your entire organization
- Apply multiple policies and & aggregate policy states with policy initiative
- Exclusion Scope

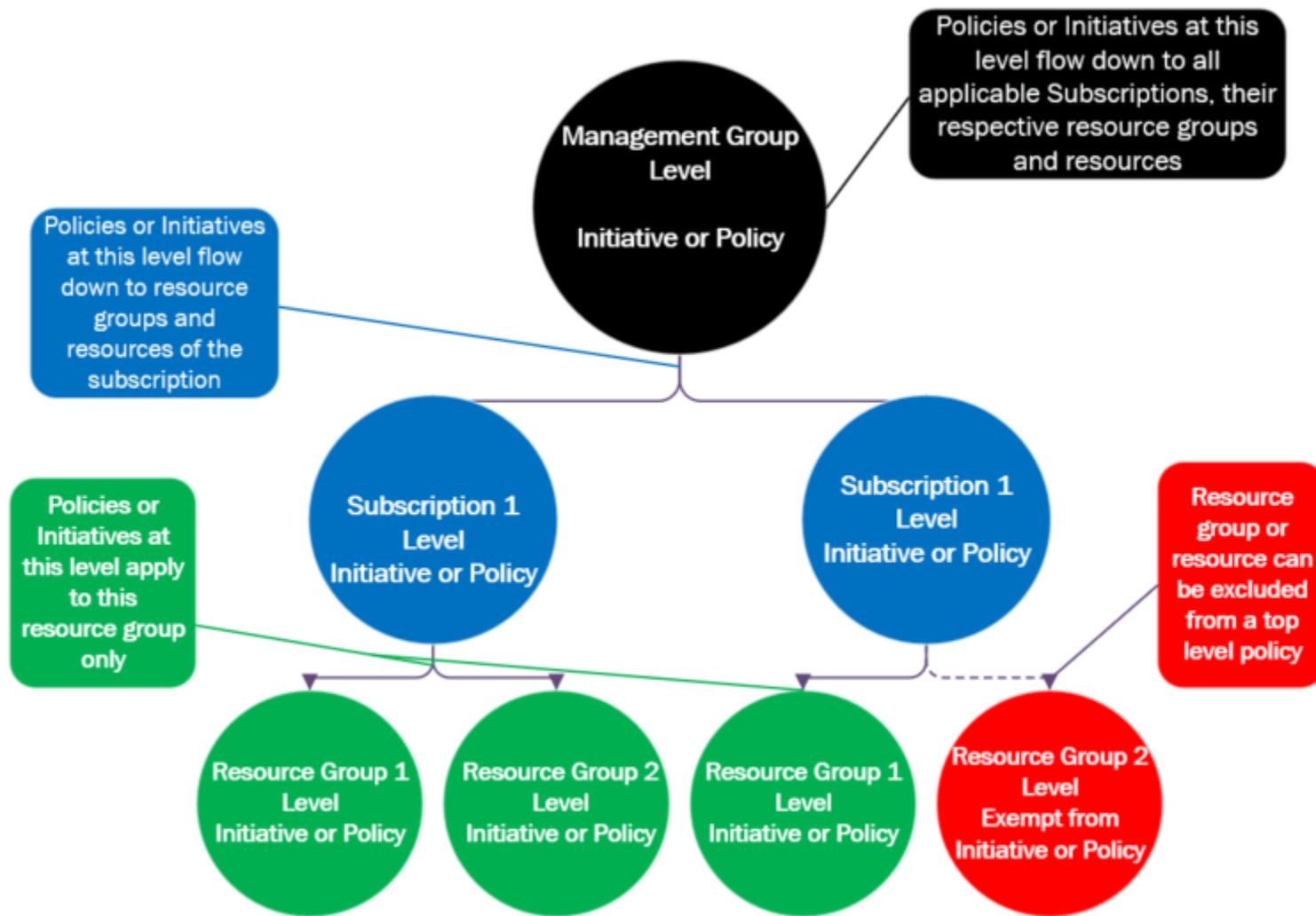
## Apply policies at scale

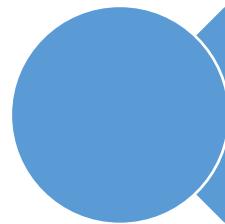


- Real time remediation
- Remediation on existing resources

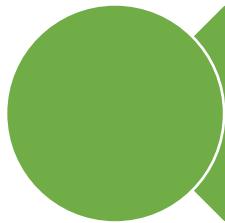
## Remediation







Access management for cloud resources is a critical function for any organization that is using the cloud. Role-based access control (RBAC) helps you manage who has access to Azure resources, what they can do with those resources, and what areas they have access to.



RBAC is an authorization system built on [Azure Resource Manager \(ARM\)](#) that provides fine-grained access management of Azure resources.

### What can I do with RBAC?

- ✓ Allow one user to manage virtual machines in a subscription and another user to manage virtual networks
- ✓ Allow a DBA group to manage SQL databases in a subscription
- ✓ Allow a user to manage all resources in a resource group, such as virtual machines, websites, and subnets
- ✓ Allow an application to access all resources in a resource group

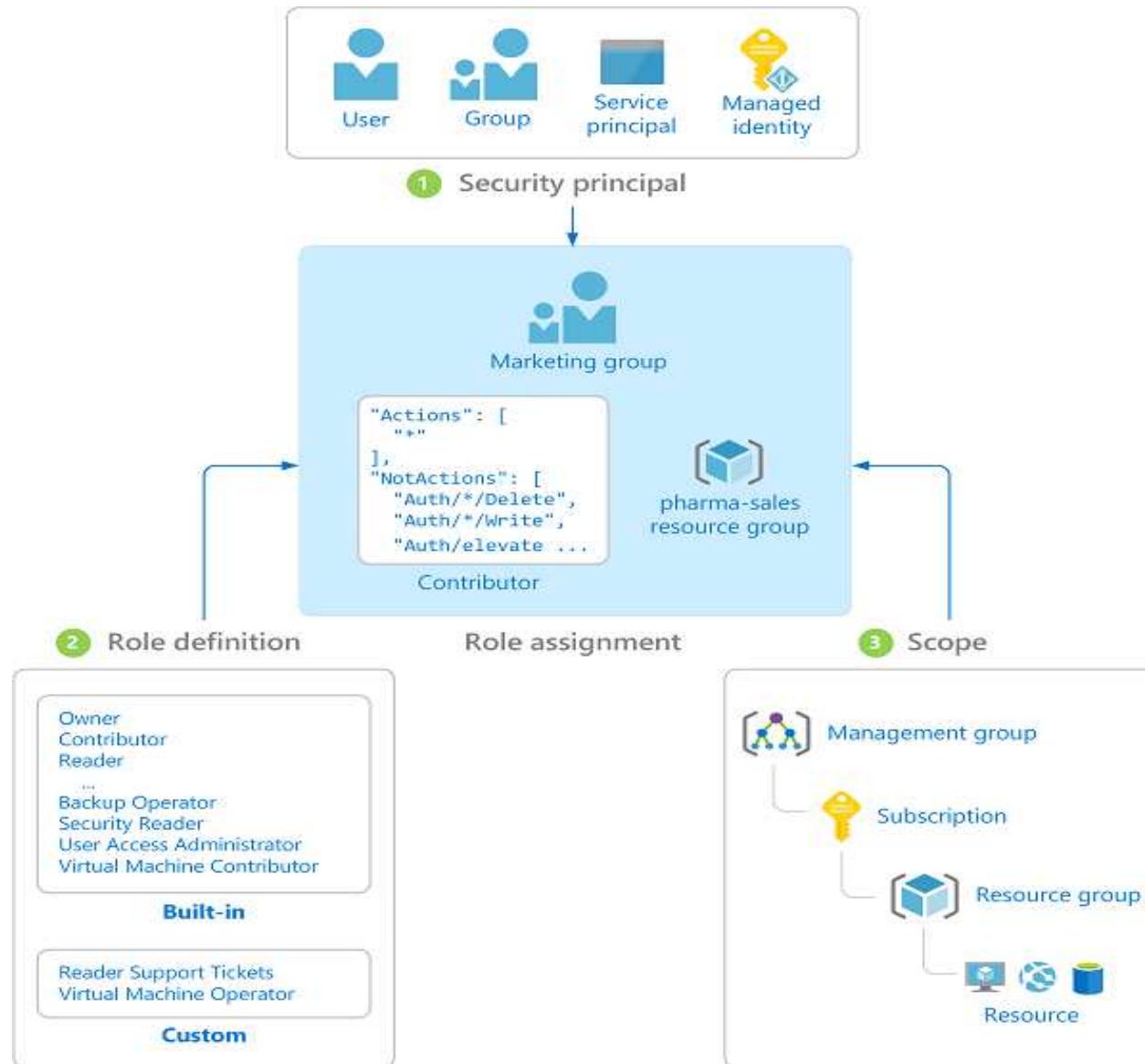
## Best practice for using RBAC

Using RBAC, you can segregate duties within your team and grant only the amount of access to users that they need to perform their jobs. Instead of giving everybody unrestricted permissions in your Azure subscription or resources, you can allow only certain actions at a particular scope.

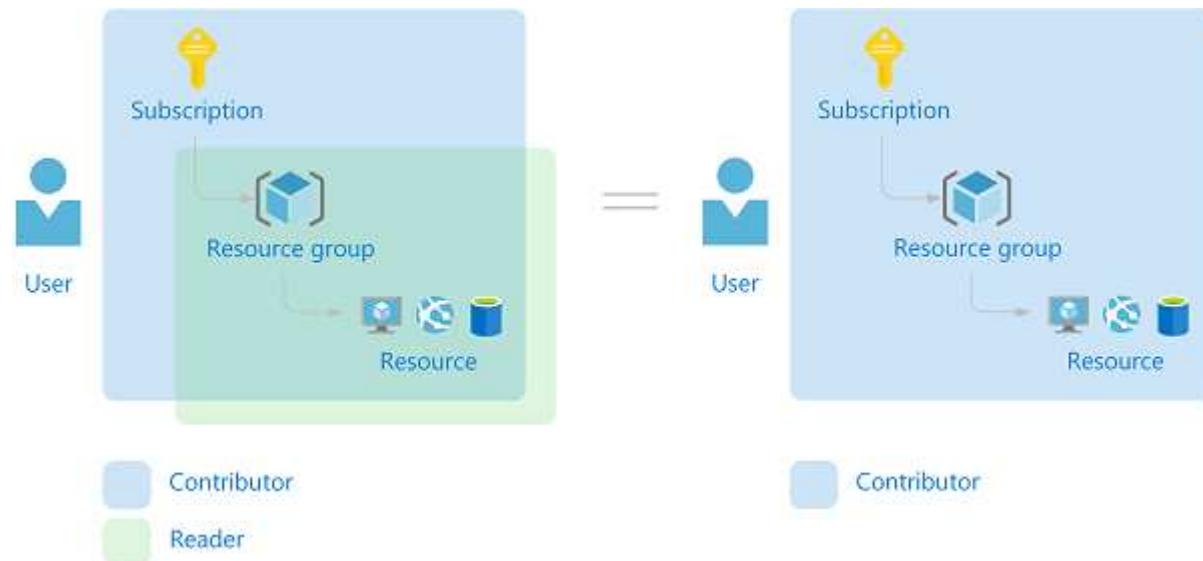
		Role		
		Reader	Resource-specific or custom role	Contributor
Scope	Subscription	Observers	Users managing resources	Admins
	Resource group			
	Resource	Automated processes		

- **Owner** - Has full access to all resources including the right to delegate access to others.
- **Contributor** - Can create and manage all types of Azure resources but can't grant access to others.
- **Reader** - Can view existing Azure resources.
- **User Access Administrator** - Lets you manage user access to Azure resources.

# RBAC



## Multiple role assignments



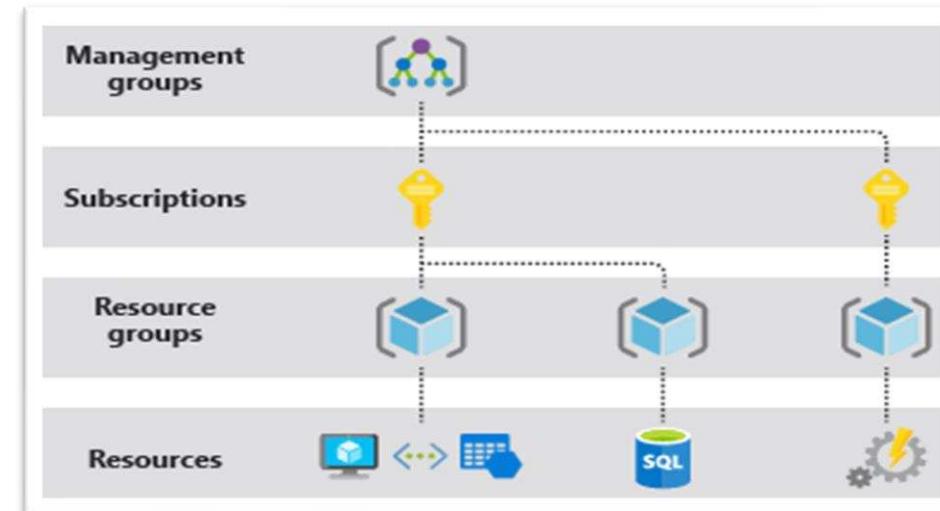
## Lock resources to prevent unexpected changes

As an administrator, you may need to lock a subscription, resource group, or resource to prevent other users in your organization from accidentally deleting or modifying critical resources.

You can set the lock level to **CanNotDelete** or **ReadOnly**. In the portal, the locks are called **Delete** and **Read-only** respectively.

**CanNotDelete** means authorized users can still read and modify a resource, but they can't delete the resource.

**ReadOnly** means authorized users can read a resource, but they can't delete or update the resource. Applying this lock is similar to restricting all authorized users to the permissions granted by the **Reader** role.



# Security Center VS Azure Advisor

Advisor recommendations

[Download as CSV](#) [Download as PDF](#) [Configure](#)

Subscriptions: 1 of 14 selected –

Contoso IT - demo All types Active No group

Overview [High Availability \(5\)](#) [Security \(20\)](#) [Performance \(1\)](#) [Cost \(2\)](#) [All \(28\)](#)

Category	Recommendations	Impact	Impact	Impact
High Availability	5	1	4	0
Security	20	20	0	0
Performance	1	1	0	0
Cost	2	2	0	0

Category	Impacted Resources
High Availability	44
Security	69
Performance	2
Cost	24

[Tips & tricks](#)

- 1 You can customize Advisor to process recommendations for resources that matter to you the most.
- 1 You can create elastic database pools to reduce your monthly Azure spend.
- 1 You can improve the performance of your SQL Azure databases.
- 1 You can enable virtual machine backup to protect your data from corruption or accidental deletion.

[Download recommendations as PDF](#)

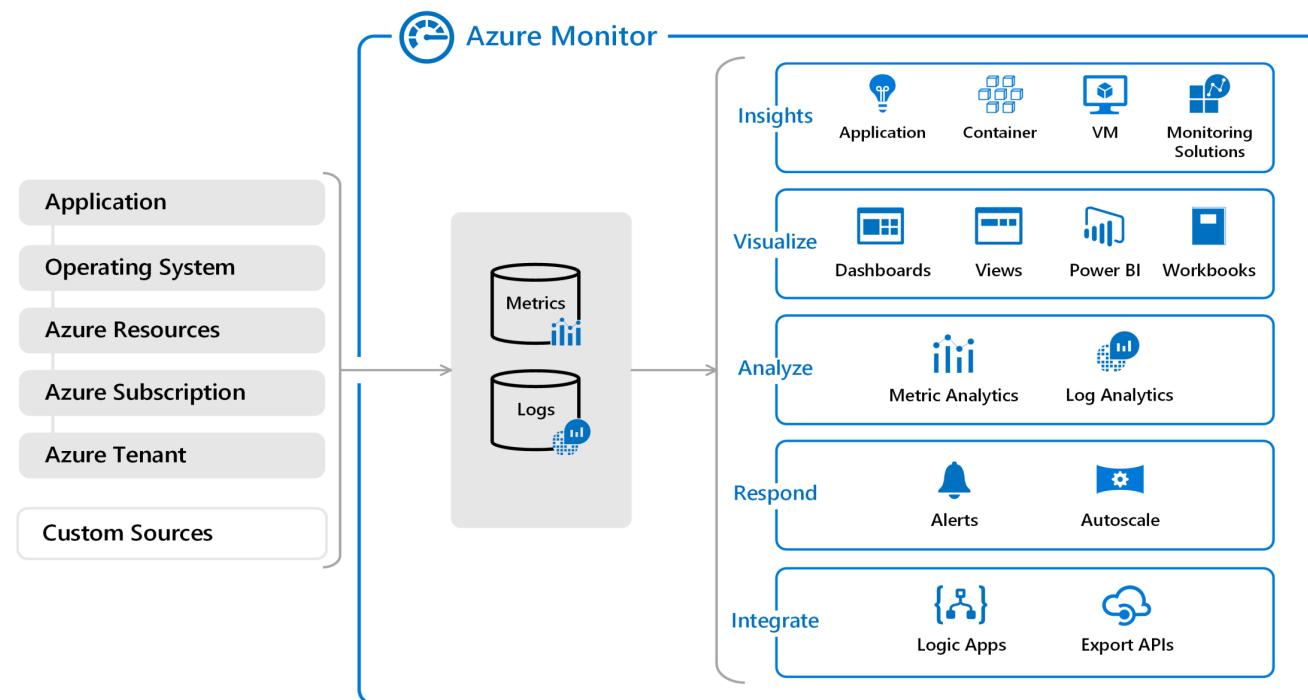
[Download recommendations as CSV](#)

# Azure Monitor

Azure Monitor maximizes the availability and performance of your applications and services by delivering a comprehensive solution for collecting, analyzing, and acting on telemetry from your cloud and on-premises environments. It helps you understand how your applications are performing and proactively identifies issues affecting them and the resources they depend on.

## Examples

- ✓ Detect and diagnose issues across **applications** and **dependencies** with **Application Insights**.
- ✓ Correlate infrastructure issues with Azure Monitor **for VMs** and Azure Monitor **for Containers**.
- ✓ Drill into your monitoring data with **Log Analytics** for troubleshooting and **deep diagnostics**.
- ✓ Support operations at scale with **smart alerts** and **automated actions**.
- ✓ Create visualizations with Azure **dashboards** and **workbooks**.

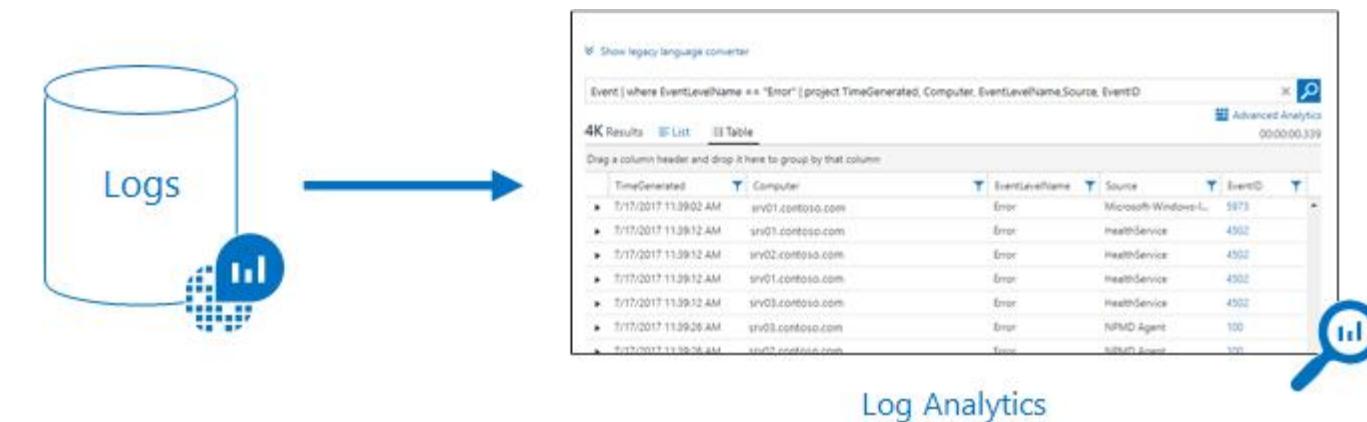


## What data does Azure Monitor collect?

Azure Monitor can collect data from a variety of sources. You can think of monitoring data for your applications in tiers ranging from your application, any operating system and services it relies on, down to the platform itself. Azure Monitor collects data from each of the following tiers:

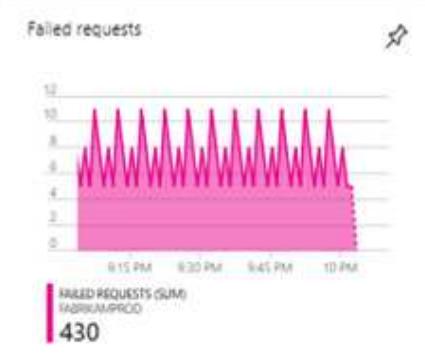
- **Application monitoring data:** Data about the performance and functionality of the code you have written, regardless of its platform.
- **Guest OS monitoring data:** Data about the operating system on which your application is running. This could be running in Azure, another cloud, or on-premises.
- **Azure resource monitoring data:** Data about the operation of an Azure resource.
- **Azure subscription monitoring data:** Data about the operation and management of an Azure subscription, as well as data about the health and operation of Azure itself.
- **Azure tenant monitoring data:** Data about the operation of tenant-level Azure services, such as Azure Active Directory.
- **Custom sources**
  - Azure Monitor can collect log data from any REST client

## Monitoring data platform



Show data for last: 30 minutes 1 hour 6 hours 12 hours 1 day 3 days 7 days 30 days

# Application Insights



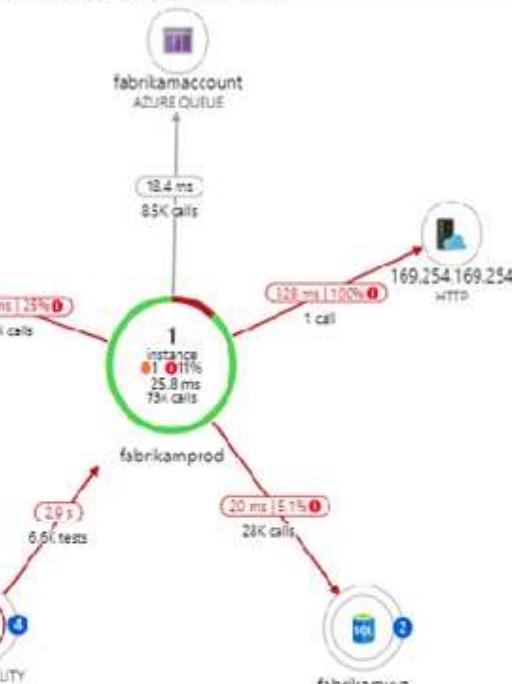
## App Service Home Page

Last 24 hours (30-minute granular) - fabrikamprod

EDIT TEST  Time range  Refresh

Download web test  Enable  Disable  Delete

### App Service Home Page test summary



Set time range or select a specific location. To see all the results, use Search by name or location.



South Central US	100%	100%	100%	100%
UK West	100%	100%	100%	100%
West US	100%	100%	100%	100%

# Monitoring solutions

Last 24 hours

Filter by name...

Active Directory Health Check

**2**Servers Assessed  
in last 21 days**0**

High Priority Recommendations

**2**

Low Priority Recommendations

**106**

Passed checks

AD Replication Status

**0**

Critical Replication Errors

**0**

Total Replication Errors

Agent Health

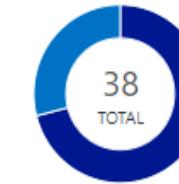
**38**

Total count of agents

**0**

Count of unresponsive agents in the last 24 hours

Agents



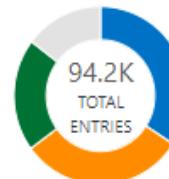
Windows  
27  
Linux  
11

Antimalware Assessment

**13**NEED  
ATTENTION

Active Threats  
0  
Remediated Threats  
0  
Insufficient Protection  
13

Application Insights



Request  
32.2K  
PageView  
29K  
Availability  
19.3K

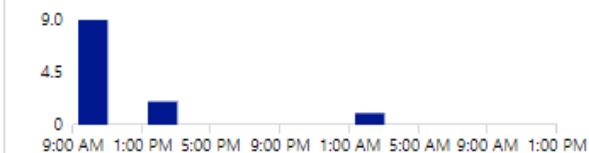
Azure Activity Logs

**40.9K**

Number of Activity Records

Azure Application Gateway Analytics

**9** CLIENT ERRORS **1** SERVER ERRORS



Azure Backup Monitoring Solution

**14**

TOTAL

Completed  
12  
Failed  
2

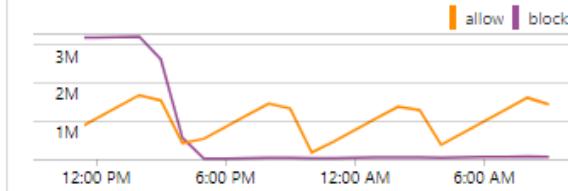
Azure Backup Monitoring Solution Copy

**14**

TOTAL

Completed  
12  
Failed  
2

Azure Network Security Group Analytics



Azure SQL Analytics (Preview)

**2**

Total Azure SQL Databases

**0**

Total Azure SQL Elastic Pools

Monitoring & Analytics + New dashboard Upload Download Edit Unshare Full screen Clone Delete

Add filter

# Dashboards

## Application

Edit

...

Total of Failed requests by Operation name  
CONTOSORETAILWEB

OPERATION ...	TOTAL	% TOTAL
GET Cust...	285	75.4%
GET Servi...	29	7.7%

Users  
CONTOSORETAILWEB - USERS - 3 DAYS

UNITED STATES **14.1k**  
UNITED KINGDOM **4.58k**

Failed requests

FAILED REQUESTS (SUM)  
FABRIKAMF900  
**10.42k**

Server response time

SERVER RESPONSE TIME (AVG)  
FABRIKAMF900  
**64.97 ms**

Server exceptions and Dependency failures

SERVER EXCEPTIONS...  
FABRIKAMF900  
**10.4k**

DEPENDENCY FAILUR...  
FABRIKAMF900  
**11.13k**

Average processor and process CPU utilization

PROCESSOR TIME (A...  
FABRIKAMF900  
**7.86%**

PROCESS CPU (AVG)  
FABRIKAMF900  
**0.64%**

Application map  
CONTOSORETAILWEB - LAST 24 HOURS

...

Live Stream  
CONTOSORETAILWEB

4 servers

## Security

Edit

Security Center

Showing subscription 'MSDIX SCOM'

Antimalware Assessment

10  
NEED ATTENTION

Active Threats	0
Remediated Threats	0
Insufficient Protection	10

System Update Assessment

49  
COMPUTERS ASSESSED

Need Critical Updates	11
Need Security Updates	3
Need Other Updates	20
Up To Date	15

Azure Network Security Group Analytics

allow  
block

## Infrastructure & Network

Edit

Service Map

9

Machines reporting  
(Last 30 min)

11

All-time machines reporting

11 0

Network Performance Monitor

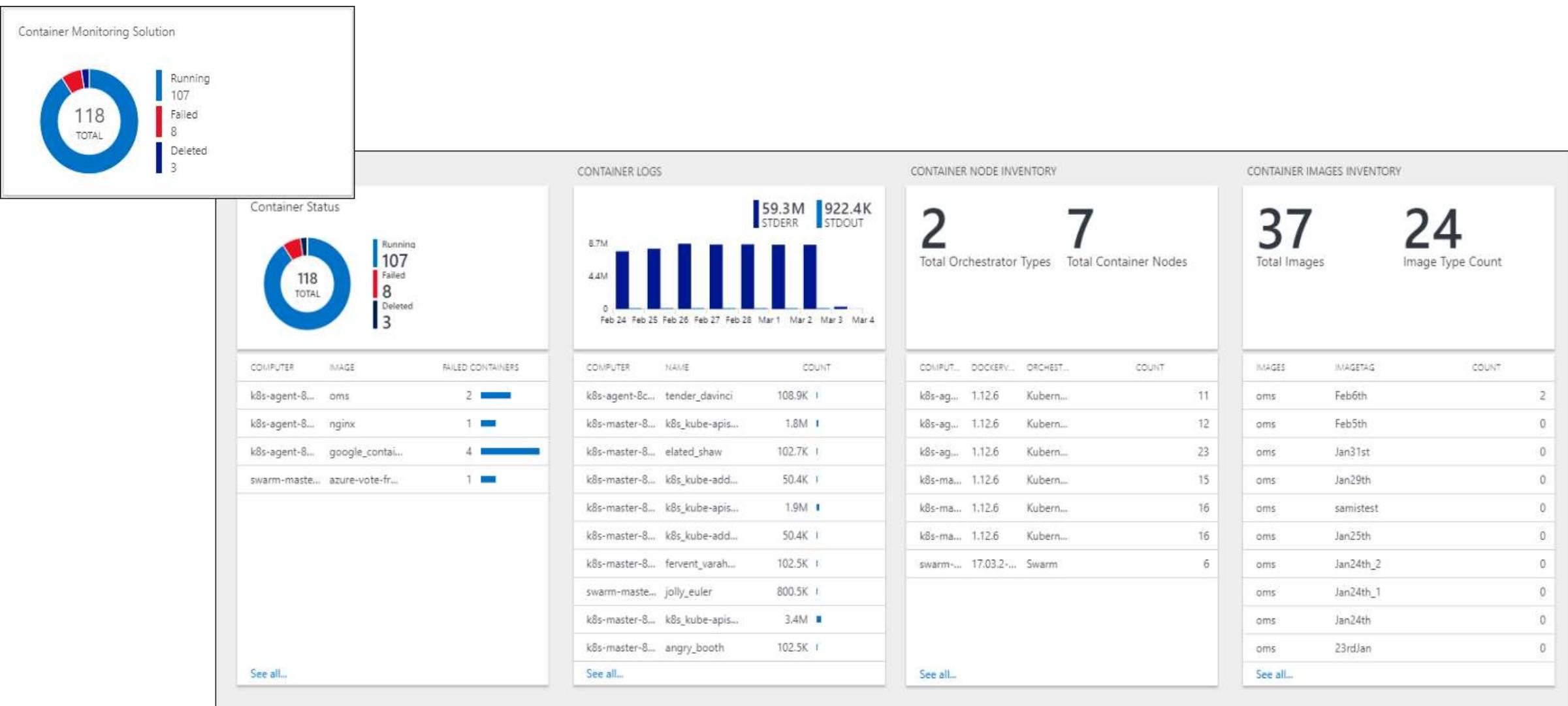
Network Monitoring Requires Attention

3

of 14 Service Connectivity Tests Unhealthy

laddy.com  
dy

# View S



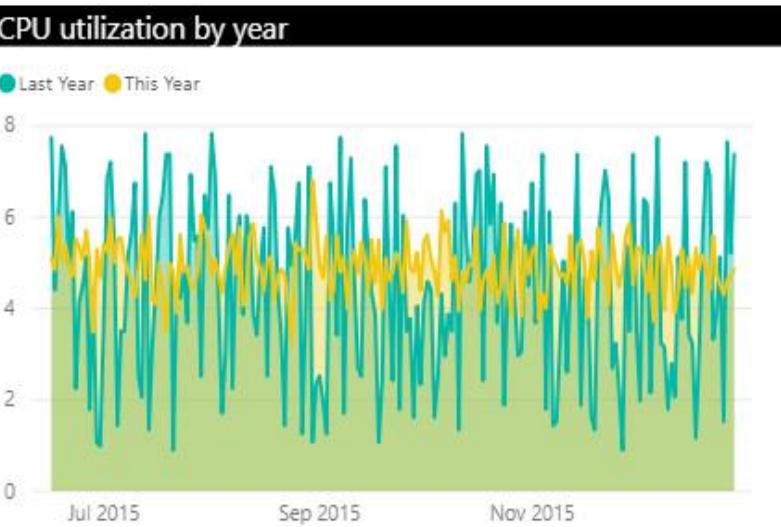
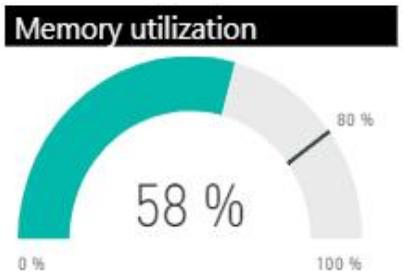
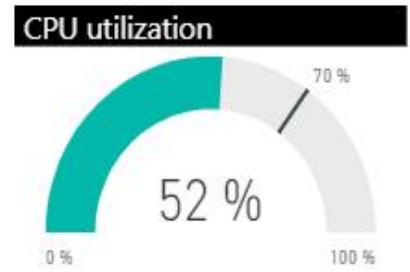
# IT Operations

## Power BI

Resource usage and availability

### Server

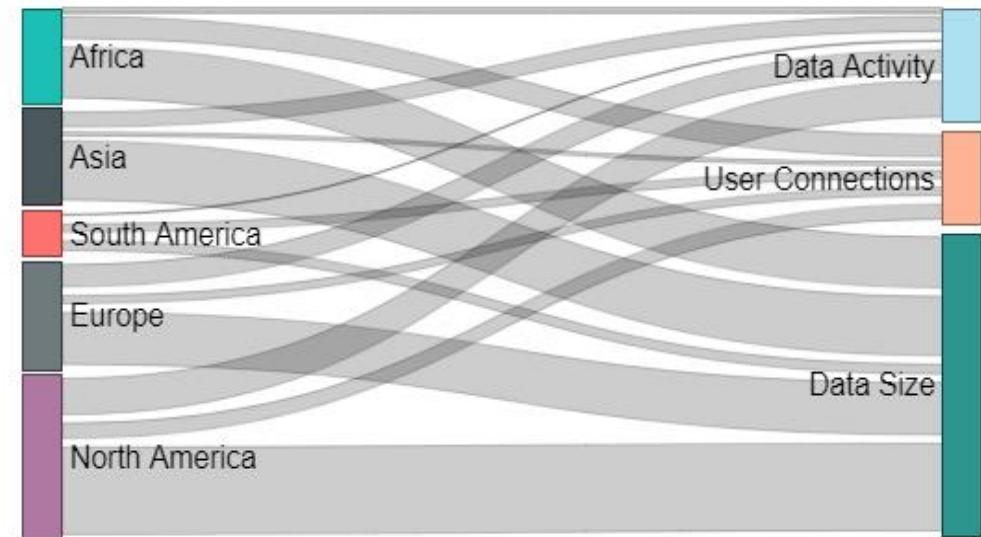
- DBServer-1
- DBServer-2
- DBServer-3
- DBServer-4
- WebApp-1
- WebApp-2
- WebApp-3
- WebApp-4
- WebApp-5



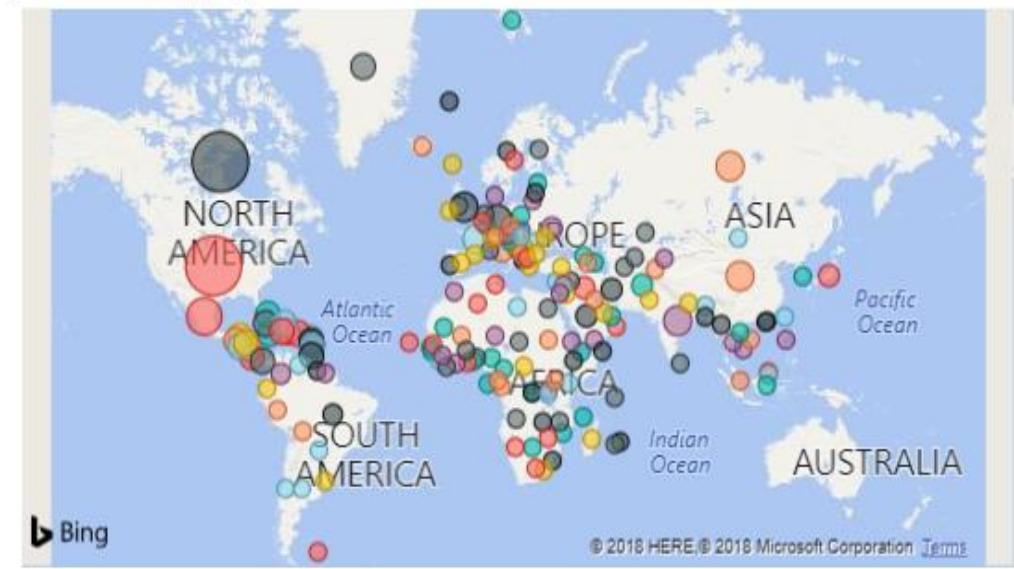
### Usage Type

- Data Activity
- Data Size
- User Conne...

### Usage by type and region



### Network usage by location



Service Health provides you with a customizable dashboard which tracks the health of your Azure services in the regions where you use them. In this dashboard, you can track active events like ongoing service issues, upcoming planned maintenance, or relevant health advisories. When events become inactive, they get placed in your health history for up to 90 days. Finally, you can use the Service Health dashboard to create and manage service health alerts which proactively notify you when service issues are affecting you.

Service Health tracks three types of health events that may impact your resources:

**Service issues** - Problems in the Azure services that affect you right now.

**Planned maintenance** - Upcoming maintenance that can affect the availability of your services in the future.

**Health advisories** - Changes in Azure services that require your attention. Examples include when Azure features are deprecated or if you exceed a usage quota.



### GDPR

#### General Data Protection Regulation

A regulation in EU law on data protection and privacy for all individuals within the European Union and the European Economic Area

Aims to give control to individuals over their personal data

Addresses the export of personal data outside the EU and the security of personal data saved



### ISO

#### International Organization for Standardization

International standard-setting body composed of representatives from various national standards organizations

ISO 27001 - framework of policies and procedures that includes all legal, physical and technical controls involved in an organisation's information risk management processes



### NIST

#### National Institute of Standards and Technology

Provides the set of standards for recommended security controls for information systems at federal agencies

In many cases, complying with NIST guidelines and recommendations will help federal agencies ensure compliance with other regulations, such as HIPAA, FISMA, or SOX

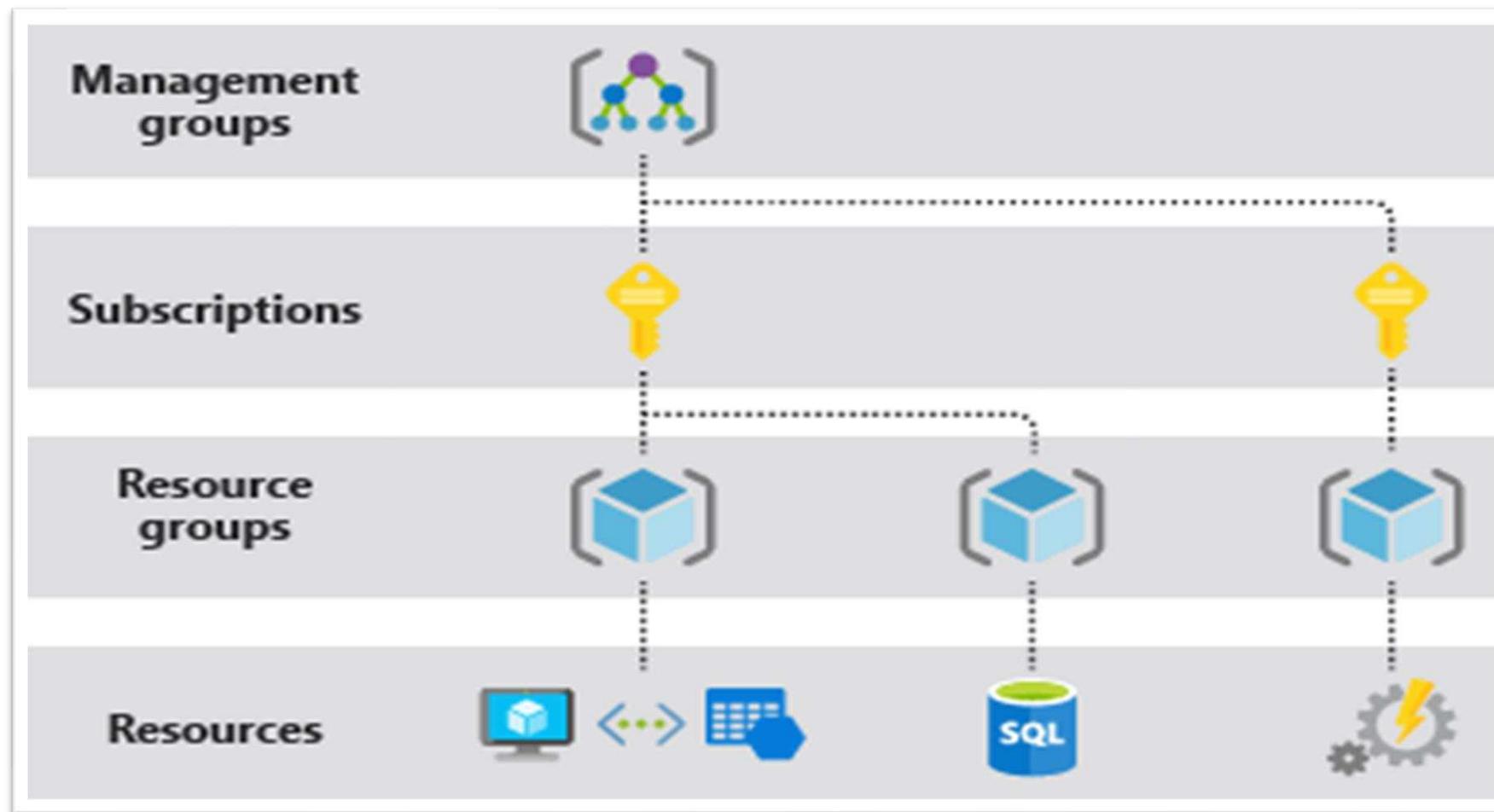
## The Microsoft Privacy Statement

Here's what you find at the Microsoft Trust Center:

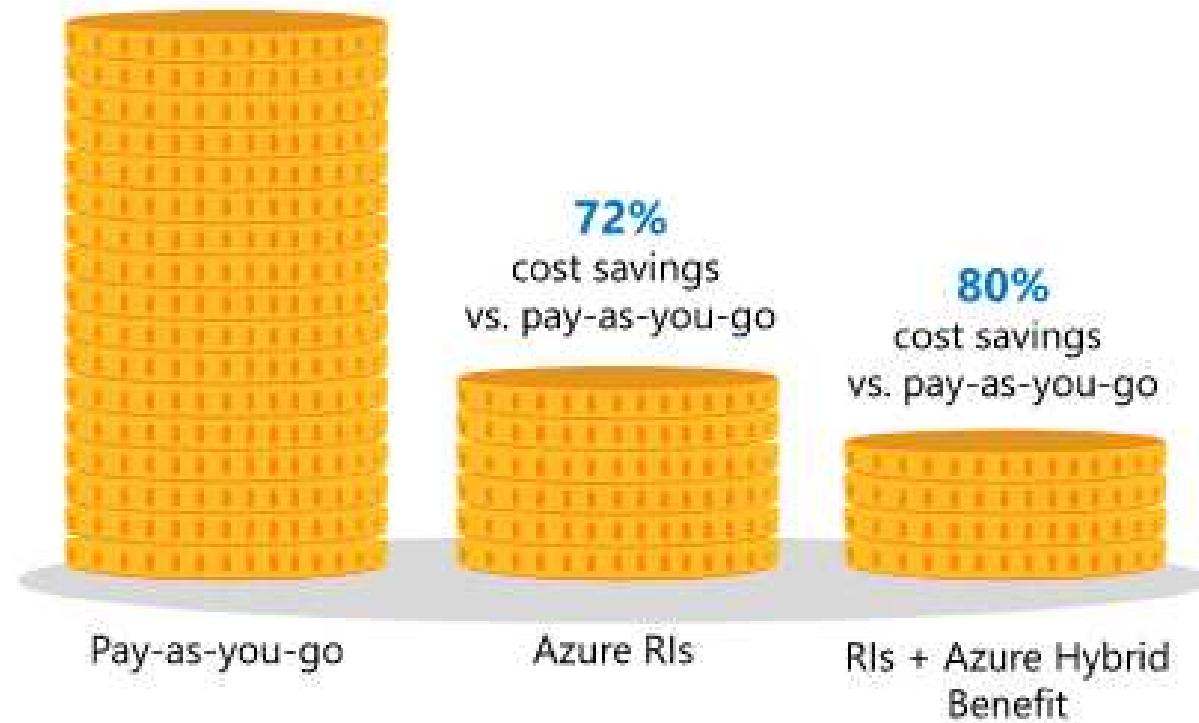
- [Security](#) – Learn how all the Microsoft Cloud services are secured.
- [Privacy](#) – Understand how Microsoft ensures privacy of your Data in the Microsoft cloud.
- [Compliance](#) – Discover how Microsoft helps organizations comply with national, regional, and industry-specific requirements governing the collection and use of individuals' data.
- [Transparency](#) – View how Microsoft believes that you control your data in the cloud and how Microsoft helps you know as much as possible about how that data is handled.
- [Products and Services](#) – See all the Microsoft Cloud products and services in one place
- [Service Trust Portal](#) – Obtain copies of independent audit reports of Microsoft cloud services, risk assessments, security best practices, and related materials.
- [What's New](#) – Find out what's new in Microsoft Cloud Trust
- [Resources](#) – Investigate white papers, videos, and case studies on Microsoft Trusted Cloud

## Microsoft Service Trust Portal

- Part of the Microsoft Trust Center
- Provides a variety of content, tools, and other resources about Microsoft security, privacy and compliance practices
- Obtain copies of independent audit reports of Microsoft cloud services, risk assessments, security best practices, and related materials
- Contains details about Microsoft's implementation of controls and processes that protect cloud services and the customer data therein



Save up to **80%** with RIs and Azure Hybrid Benefit



## Minimizing Azure Costs



## Cost Management: Trey Research - Cost analysis



## Cost Management: Trey Research - Cost analysis



Search (Ctrl+ /)



Refresh



Export

How satisfied are you with cost analysis? →

Scope : [Trey Res...](#)

Custom view

Feb 2019

Granularity : Daily

Group by : Provider

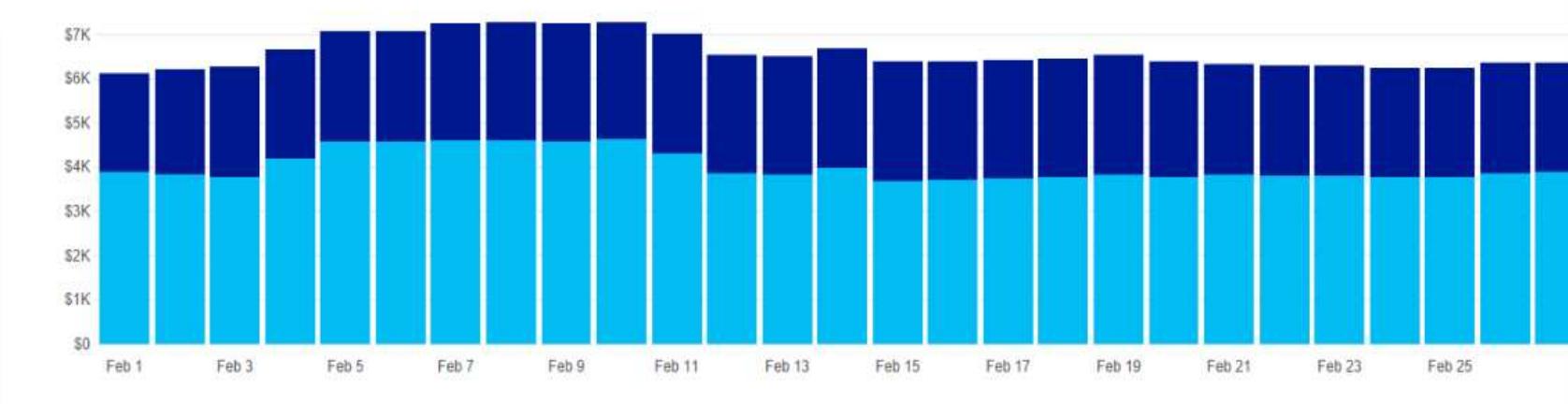
Add filter

TOTAL

BUDGET: NONE

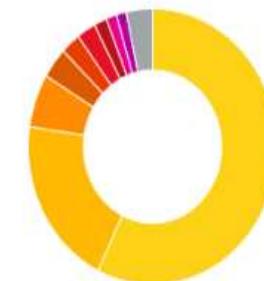
\$184.7K --

\$8K



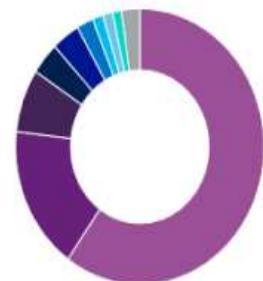
aws      azure

Service name



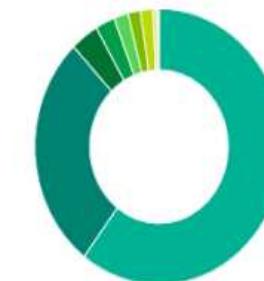
amazon elastic com...	\$105.7K
virtual machines	\$37,082
expressroute	\$11,558
hdinsight	\$6,724
storage	\$4,706
azure app service	\$4,706

Location



us-east-1	\$110.5K
br south	\$31,225
us west	\$13,752
us central	\$7,008
eu west	\$6,752
us west 2	\$3,440

Subscription name



i00000000-0000-0000-0000-000000000000	\$111.4K
trey research finance	\$50,999
trey research delta	\$6,725
trey research itied3	\$4,703
trey research alpha	\$3,440
trey research corp	\$3,440

## Subscriptions

Microsoft



Showing subscriptions in Microsoft. Don't see a subscription?  
Switch directories

My role ?Status ?8 selected ▼ 3 selected ▼

Apply

 Show only subscriptions selected in the global subscriptions filter ?

Search to filter items...

SUBSCRIP... ▼ SUBSCRIPTION ID ▼

Trey Resear... 586ftd47-9dd9-4...

Trey Resear... ed570627-0265-4...

Trey Resear... 73c0021f-a37d-43...

Trey Resear... 9ec51cf8-5ca7-4d...

Trey Resear... d08df488-ca06-4...

Cost Manag... 1caa5a3-2b66-4...

Trey Resear... 64e355d7-997c-4...

Contoso IT ... e4272367-5645-4...

CloudOps G... a6383be3-f0e8-4...

## Cost Management Research - Cost analysis

Subscription



Refresh



Tour



Export Cost by resource

Scope : Cost Man...

Custom view ▼Feb 2019 ▼Granularity : Accumulated ▼Group by : None ▼

Add filter

TOTAL 1  
**\$3,171**BUDGET: GARDA ▼  
**\$3,000** /mo

Last month	Feb 2019
This month	Mar 2019
This quarter	Jan-Mar 2019
This year	2019
Custom >	

\$3.5K

\$3K

\$2.5K

\$2K

\$1.5K

\$1K

\$500

\$0

Feb 1

Feb 3

Feb 5

Feb 7

Feb 9

Feb 11

Feb 13

Feb 15

Feb 17

Feb 19

Feb 21

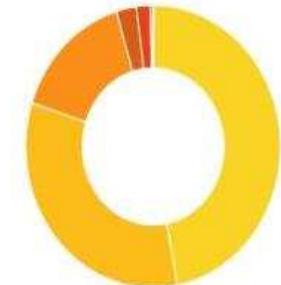
Feb 23

Feb 25

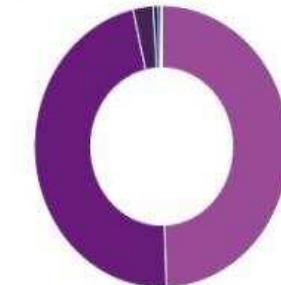
Accumulated cost

Monthly budget

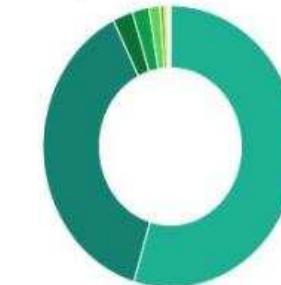
Overage

Service name ▼

starsimple	\$1,489
virtual machines (ice...	\$1,048
virtual machines	\$485.91
security center	\$80.64
storage	\$55.54

Location ▼

us north central	\$1,567
us east 2	\$1,489
us east	\$80.64
us west	\$20.22
us central	\$13.31

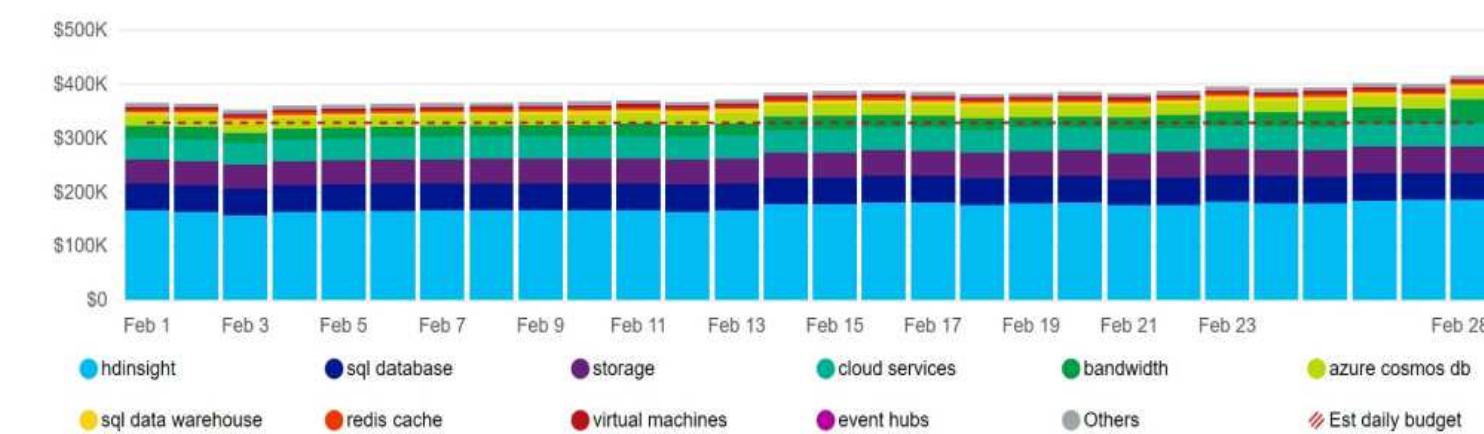
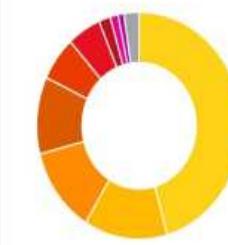
Resource group name ▼

carda1hourbill	\$1,732
formatica	\$1,205
defaultresource	\$80.64
moderntm	\$67.13
mar-ccm	\$43.89

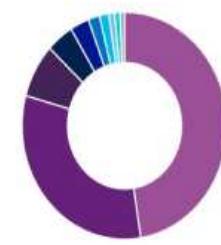
## Cost Management + Billing - Cost analysis

 Search (Ctrl+ /)[Refresh](#) [Tour](#) [Export](#)

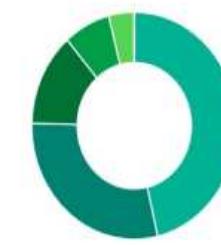
How satisfied are you with cost analysis? [→](#)

Scope : [SAB BVT ...](#)Custom view [▼](#)Feb 2019 [▼](#)Granularity : Daily [▼](#)Group by : Service name [▼](#)[Add filter](#)TOTAL [▼](#)BUDGET: SRIVATSK-MONTHLY... [▼](#)**\$10.6M****\$328.8K** /day (est)Service name [▼](#)

Service	Cost (\$)
hdinsight	\$4.8M
sql database	\$1.4M
storage	\$1.3M
cloud services	\$1.2M
bandwidth	\$0.5M

Location [▼](#)

Location	Cost (\$)
us east	\$5M
us west	\$3.4M
us west 2	\$816.2K
us east 2	\$455.8K
eu north	\$0.5M

Enrollment account name [▼](#)

Enrollment account name	Cost (\$)
aipdept@micr...	\$4.9M
aipdeptq@micr...	\$3.1M
aipdept@micr...	\$1.4M
ai-admin@micr...	\$780.2K
aipdepte@micr...	\$0.5M

## Azure support plans

	<u>BASIC</u> <u>Request support</u>	<u>DEVELOPER</u> <u>Purchase support</u>	<u>STANDARD</u> <u>Purchase support</u>	<u>PROFESSIONAL DIRECT</u> <u>Purchase support</u>	<u>PREMIER</u> <u>Contact Premier</u>
Scope	Available to all Microsoft Azure accounts	Microsoft Azure:	Microsoft Azure:	Microsoft Azure:	All Microsoft Products, including Azure:
		Trial and non-production environments	Production workload environments	Business-critical dependence	Substantial dependence across multiple products
Customer Service, Self-Help and Communities	24x7 access to billing and subscription support, online self-help, documentation, whitepapers and support forums	24x7 access to billing and subscription support, online self-help, documentation, whitepapers and support forums	24x7 access to billing and subscription support, online self-help, documentation, whitepapers and support forums	24x7 access to billing and subscription support, online self-help, documentation, whitepapers and support forums	24x7 access to billing and subscription support, online self-help, documentation, whitepapers and support forums
Best Practices	Access to full set of Azure Advisor recommendations	Access to full set of Azure Advisor recommendations	Access to full set of Azure Advisor recommendations	Access to full set of Azure Advisor recommendations	Access to full set of Azure Advisor recommendations
Health Status and Notifications	Access to personalised Service Health Dashboard and Health API	Access to personalised Service Health Dashboard and Health API	Access to personalised Service Health Dashboard and Health API	Access to personalised Service Health Dashboard and Health API	Access to personalised Service Health Dashboard and Health API
Technical Support	Not available	Business hours access1 to Support Engineers via email	24x7 access to Support Engineers via email and phone	24x7 access to Support Engineers via email and phone	24x7 access to Support Engineers via email and phone
Who Can Open Cases	Not available	Unlimited contacts / unlimited cases			
Third-Party Software Support	Not available	Interoperability and configuration guidance and troubleshooting			
Case Severity/Response Times	Not available	Minimal business impact (Sev C):			
		<8 business hours1	<8 business hours1Moderate business impact (Sev B):	<4 business hours1Moderate business impact (Sev B):	<4 business hours1Moderate business impact (Sev B):
			<4 hoursCritical business impact (Sev A):	<2 hoursCritical business impact (Sev A):	<2 hoursCritical business impact (Sev A):
			<1 hour	<1 hour	<1 hour
					<15 minutes (with Azure Rapid Response or Azure Event Management)
Architecture Support	Not available	General guidance	General guidance	Architectural guidance based on best practice delivered by ProDirect Delivery Manager	Customer specific architectural support such as design reviews, performance tuning, configuration and implementation assistance delivered by Microsoft Azure technical specialists.
Operations Support	Not available	Not available	Not available	Onboarding services, service reviews, Azure Advisor consultations	Technical account manager-led service reviews and reporting
Training	Not available	Not available	Not available	Azure Engineering-led web seminars	Azure Engineering-led web seminars, on-demand training
Proactive Guidance	Not available	Not available	Not available	ProDirect Delivery Manager	Designated Technical Account Manager
Launch Support	Not available	Not available	Not available	Not available	Azure Event Management (available for additional fee)
Pricing	Not available	\$29/mo	\$100/mo	\$1,000/mo	<a href="#">Contact us</a>

# Azure Service Level Agreements (SLAs)

- Uptime is guaranteed (not performance, bandwidth, or feature availability).
- Expressed as a percentage of the total time per month that the service is guaranteed to be up.
- If an incident causes the uptime to fall below the SLA guarantee, you are entitled to a credit towards your monthly service fees.
- Monthly Uptime % =  $(\text{Maximum Available Minutes} - \text{Downtime}) / \text{Maximum Available Minutes} * 100$



Talk about  
Cloud Models  
Azure core infra like Resource Groups, regions  
Networks  
IaaS  
PaaS  
SaaS  
Azure portal  
Creation of Azure Free trial about

## Azure Security Overview

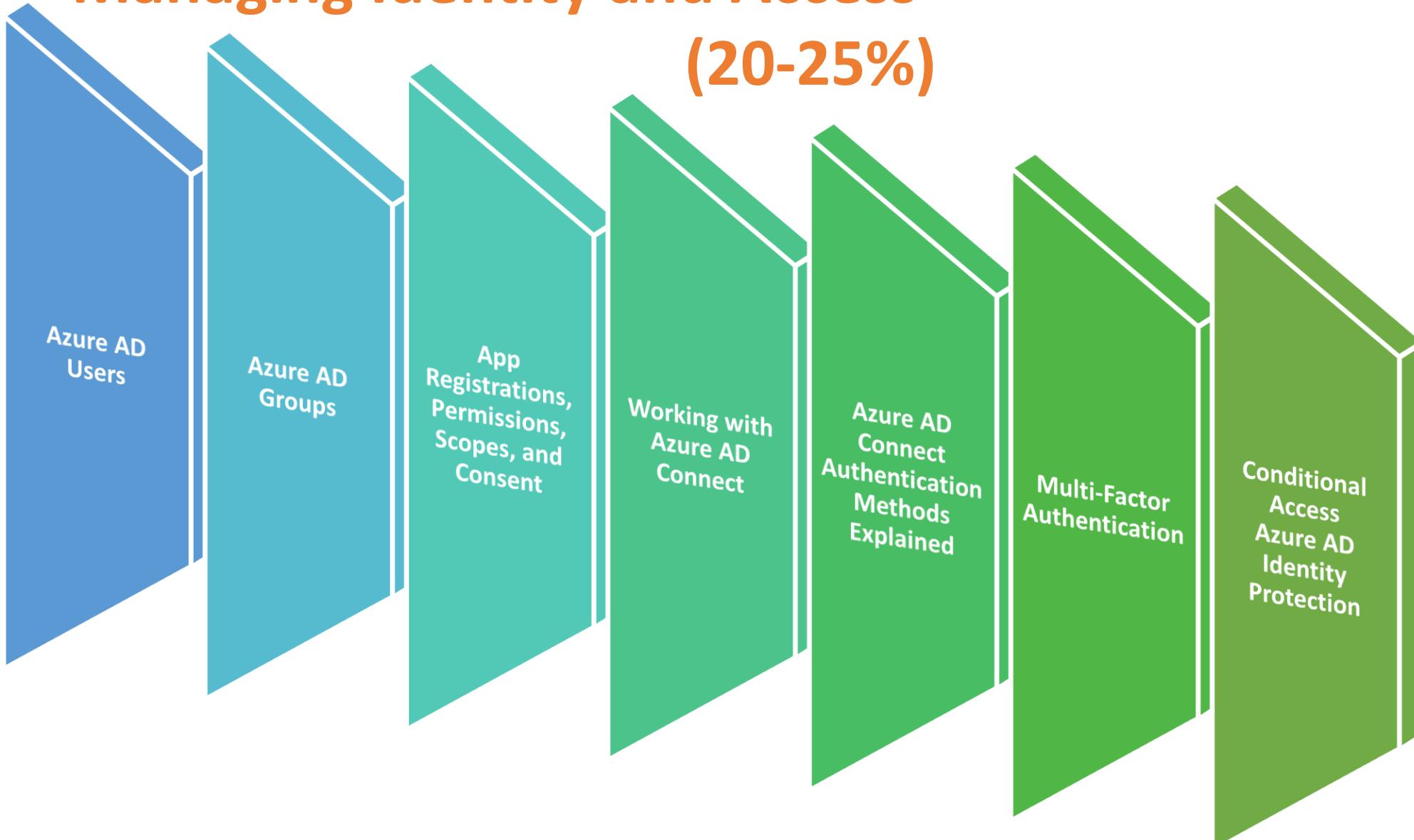
## **Skills measured**

•NOTE: The bullets that appear below each of the skills measured in the document below are intended to illustrate how we are assessing that skill. This list is not definitive or exhaustive.

- Manage identity and access (20-25%)
- Implement platform protection (35-40%)
- Manage security operations (15-20%)
- Secure data and applications (30-35%)

# Managing Identity and Access

(20-25%)



# Azure Active Directory Groups

Security AD Group  
(Static)

Office 365 Group

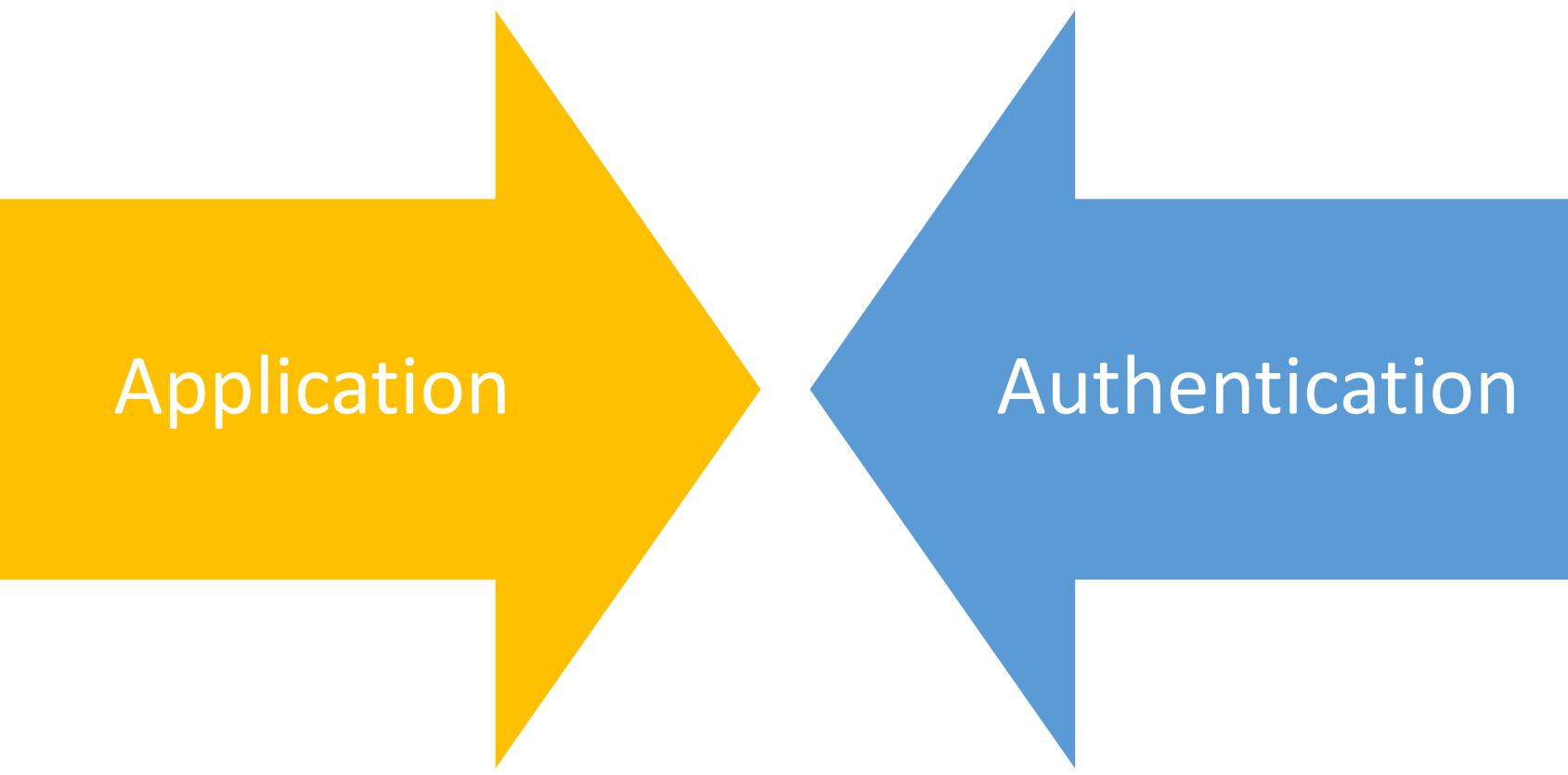
Dynamic Group –  
Based on Attribute  
Query

## Azure Active Directory Groups

- ✓ You also have the ability to add a security group to another security group.
- ✓ This is known as a nested group. There are a few rules that limit the ability to nest groups. If we take a look at those rules, there are just a few that we need to follow. You cannot add groups to a group that's been synchronized with an on premises Active Directory environment by using Azure AD connect, which we'll be discussing in an upcoming lesson.
- ✓ You can't add security groups to 365 groups. You can't add 365 groups to security groups or other 365 groups.
- ✓ You can't assign applications to nested groups.
- ✓ They have to be assigned to each individual group and you can't apply the licenses to nested groups either.
- ✓ So just think about those when you're creating groups and you'll have no problem being able to nest those groups.

## User sign-in with Azure Active Directory Pass-through Authentication





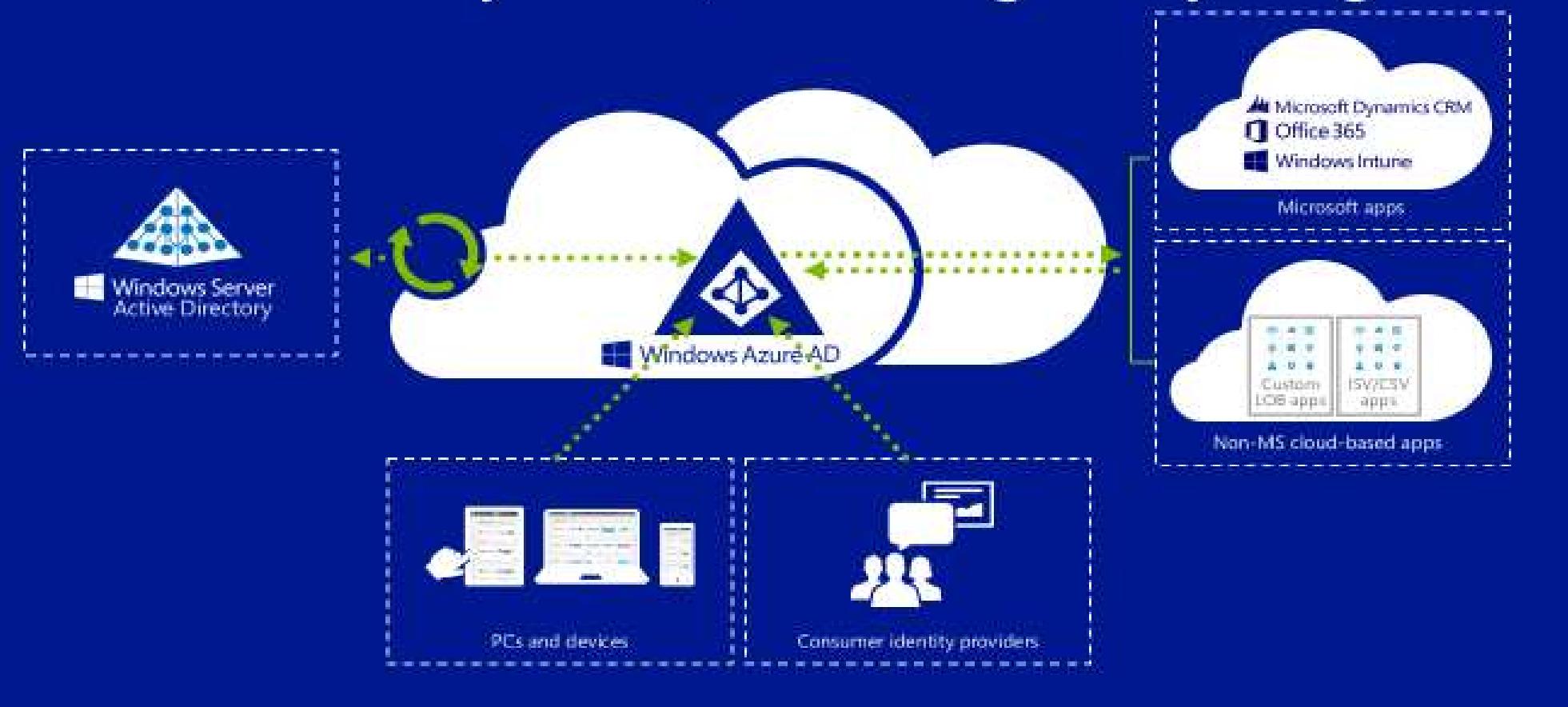
Application

Authentication

# Authentication

# Authentication

Identities everywhere, accessing everything



## Why is this choice important?



It is the first  
important  
decision



It is your  
foundation of  
your infrastructure



It is hard to  
change

## What are your authentication options with Azure AD?

### Cloud authentication

Cloud-only

Password Hash Sync +  
Seamless SSO

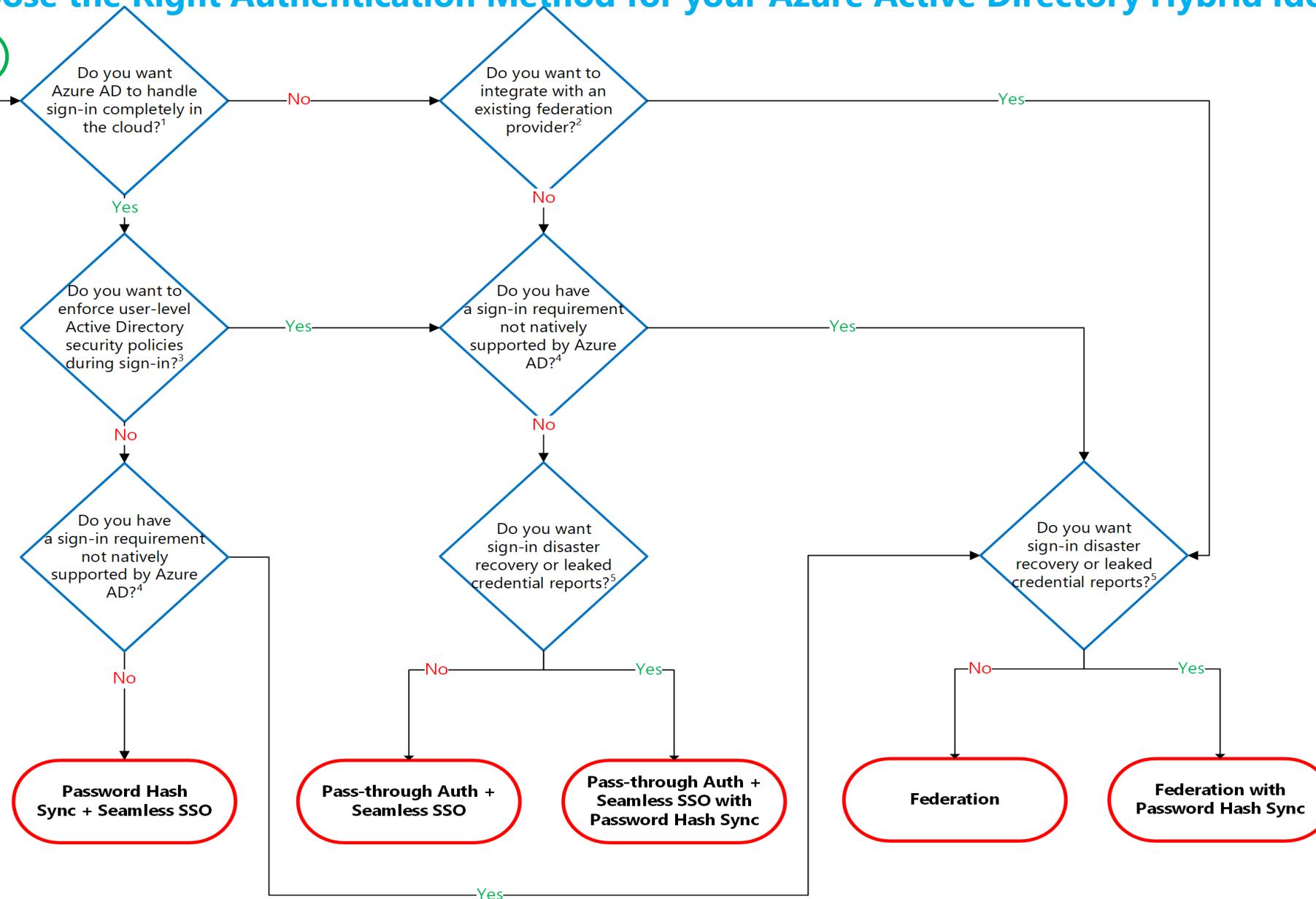
Pass-through authentication +  
Seamless SSO

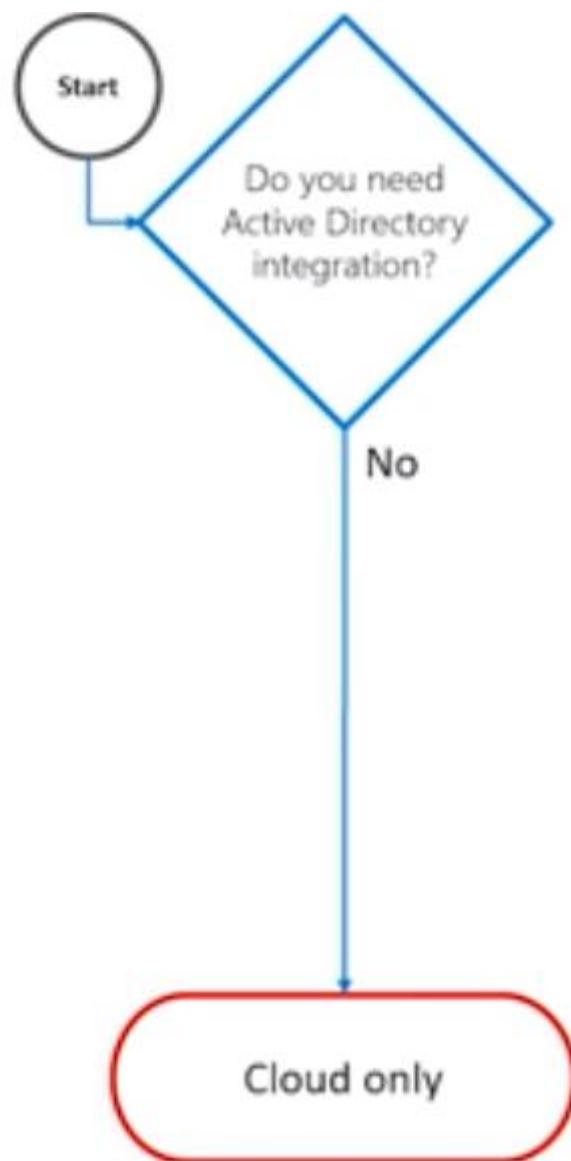
### Federated authentication

AD FS

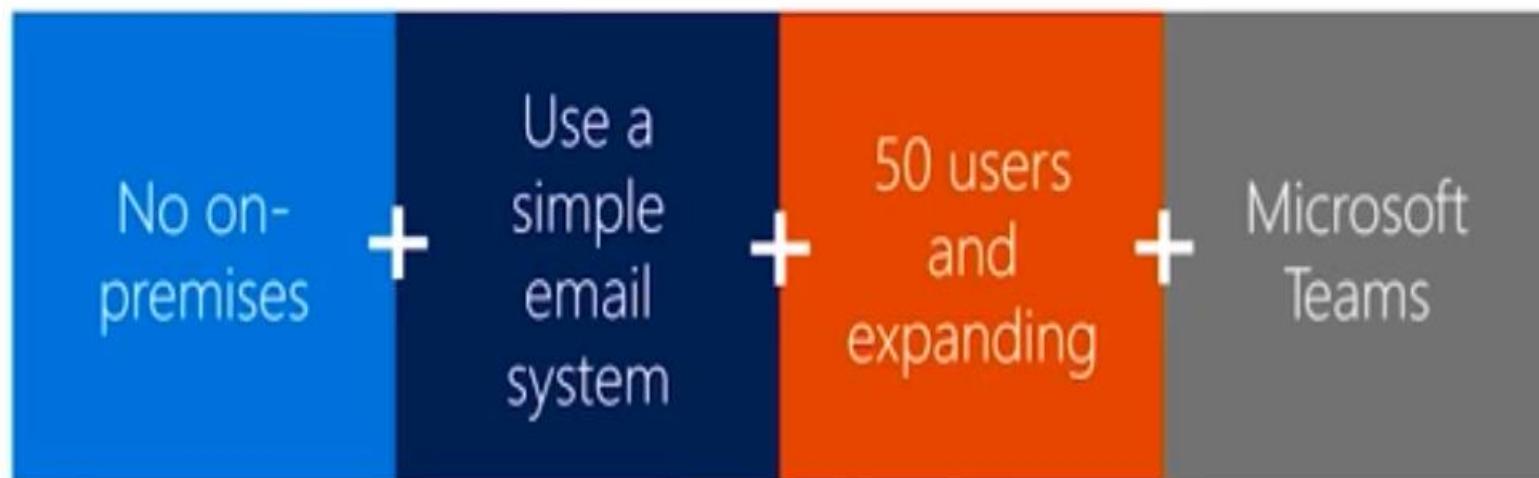
Third party federation providers

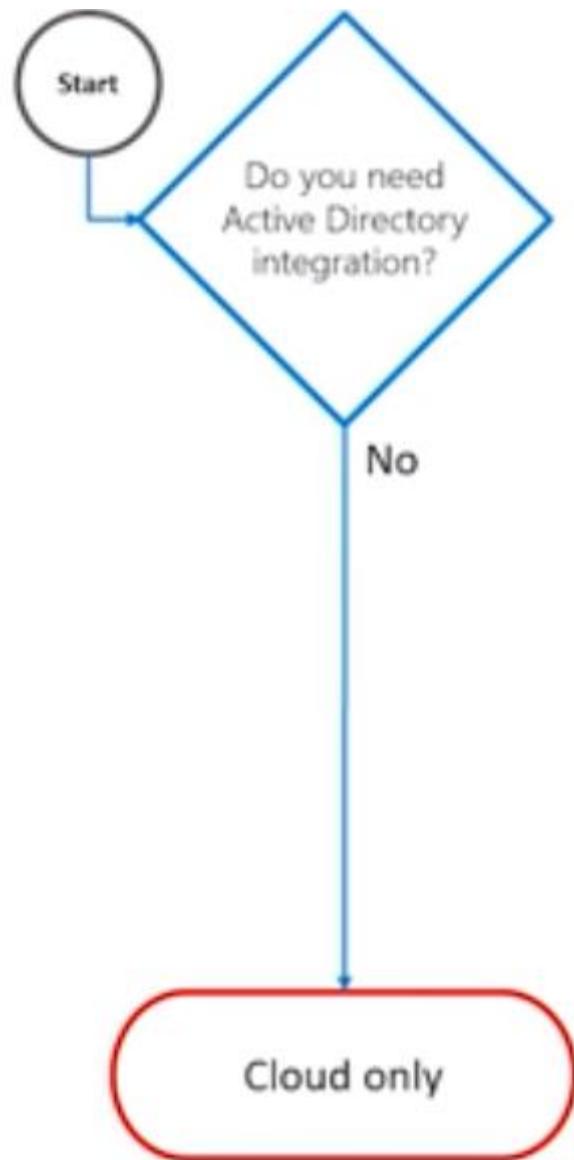
# Choose the Right Authentication Method for your Azure Active Directory Hybrid Identity Solution



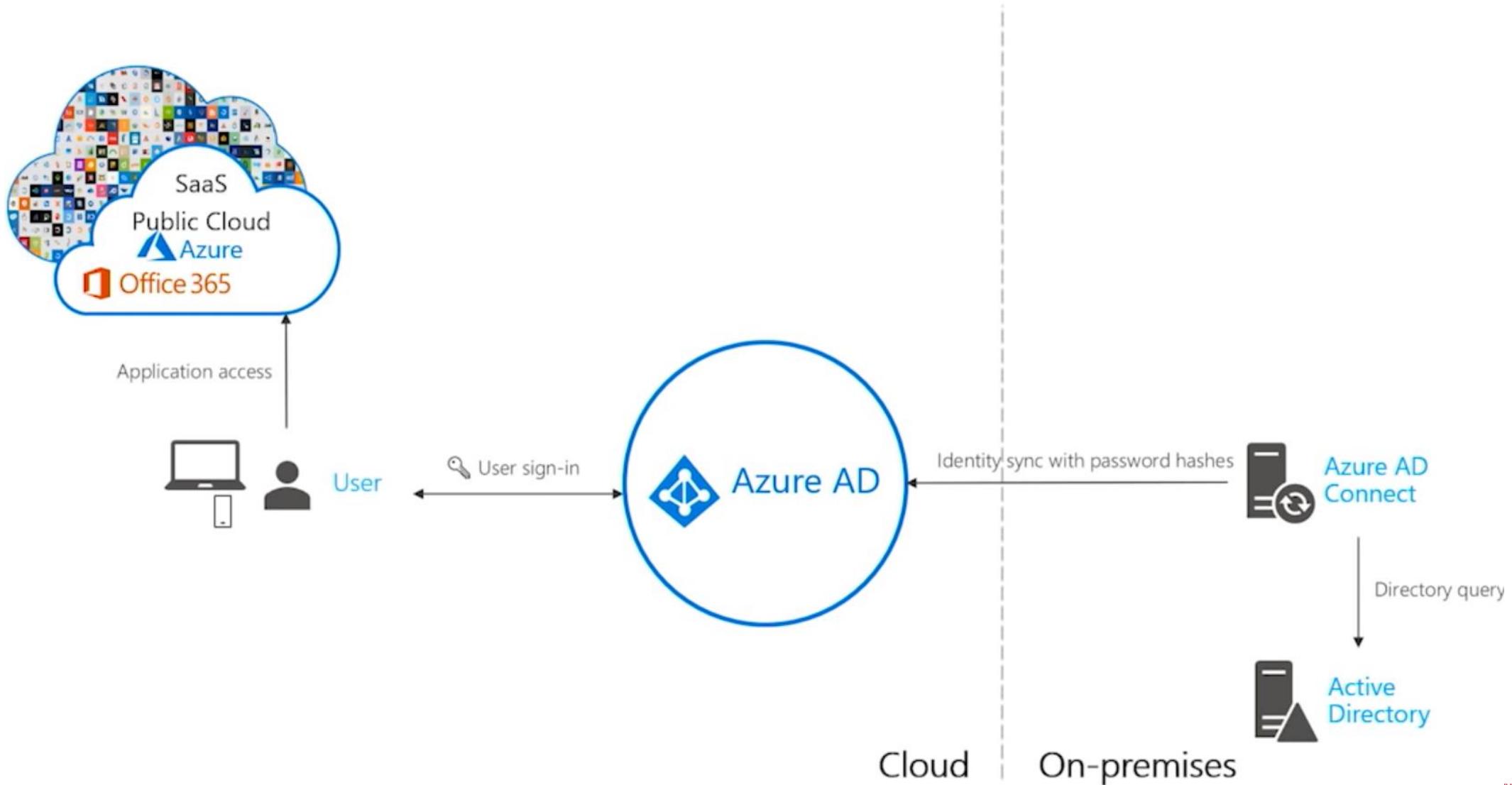


## Wing Tip Toys – Online retailer and toy manufacturer

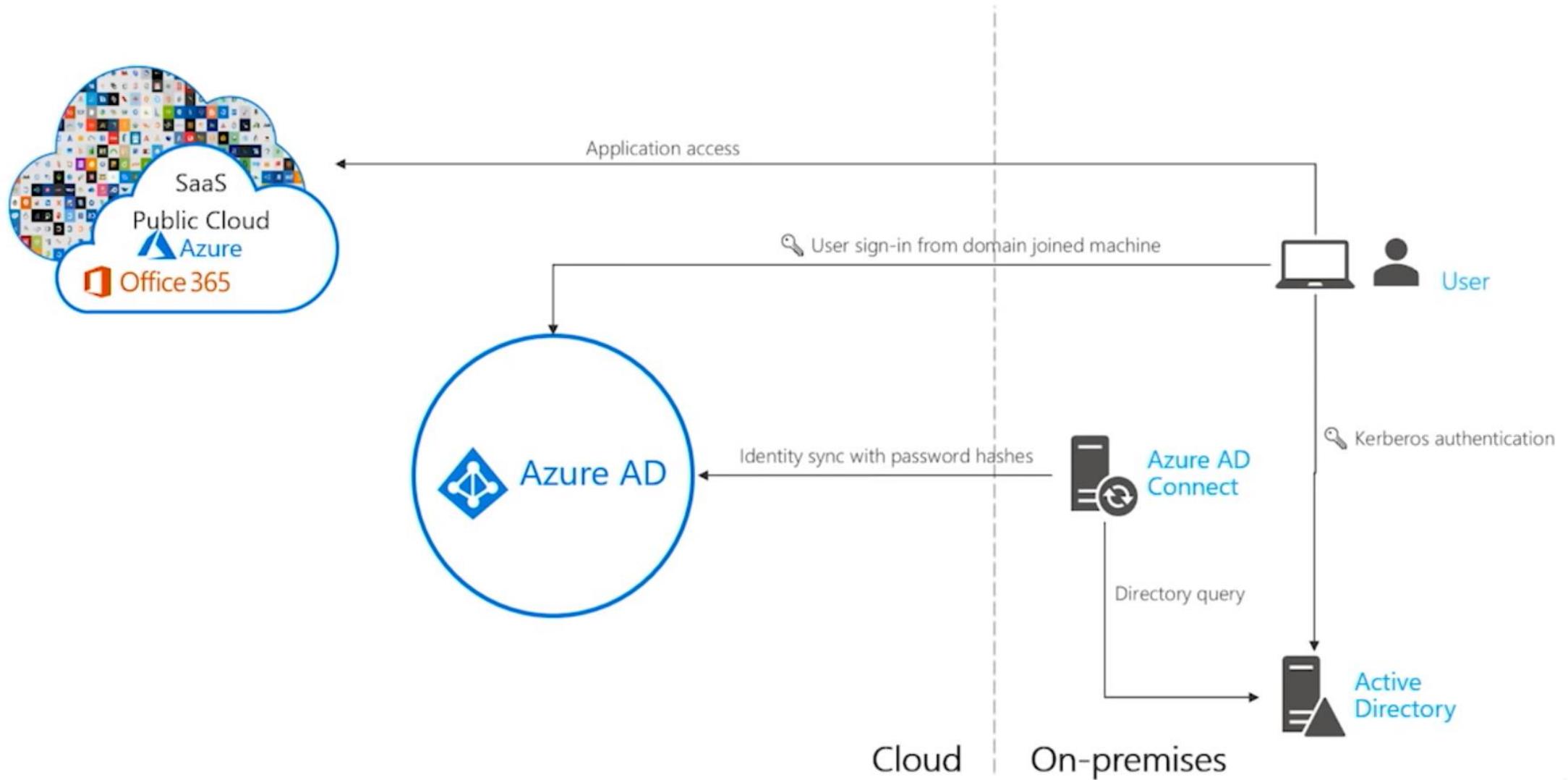




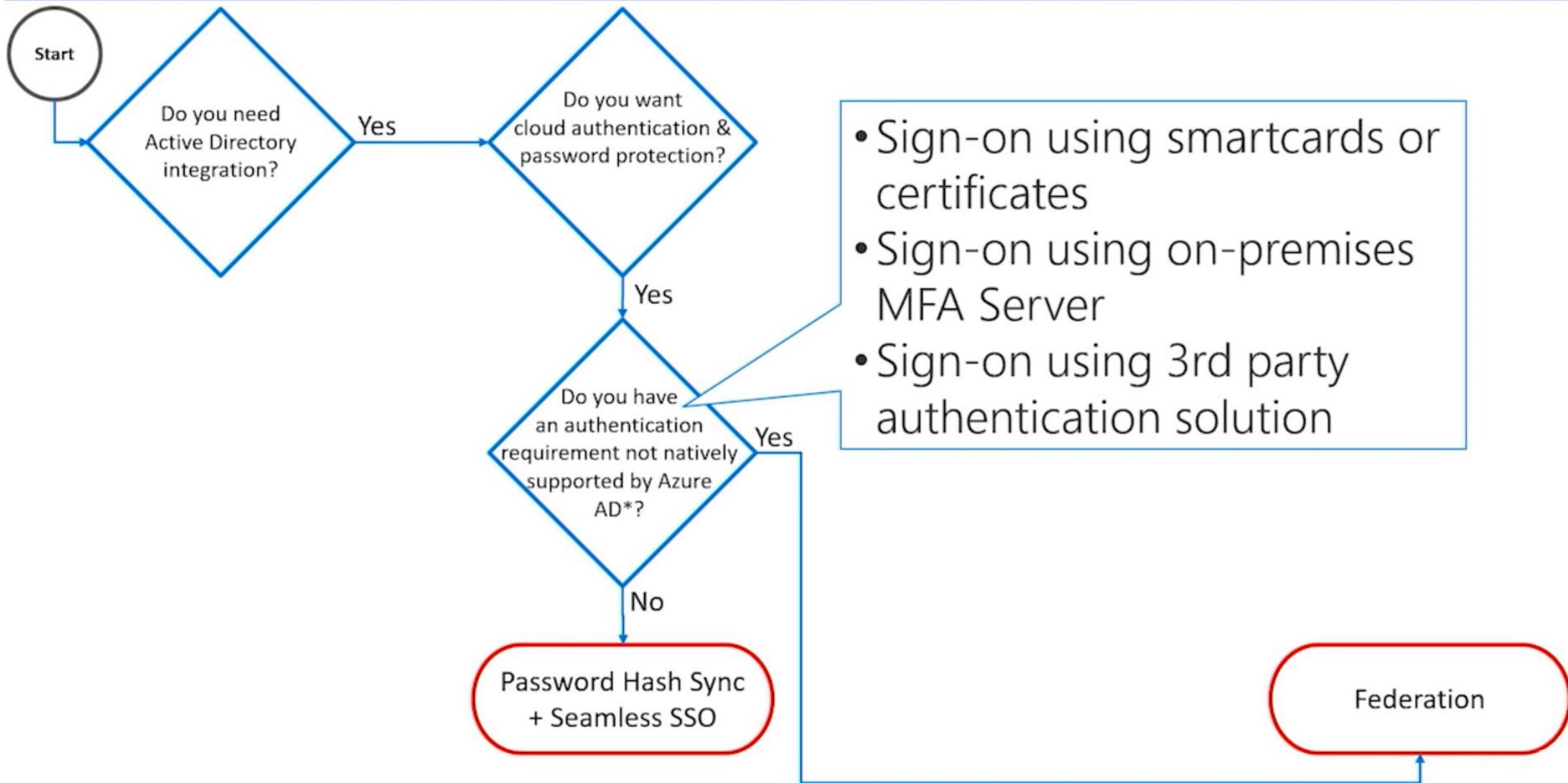
# Password Hash Sync



# Seamless Single Sign On



## Azure AD Authentication decision tree



# Woodgrove Bank – A national financial institution

Strong  
regulatory  
operation



Present in  
almost  
every  
region

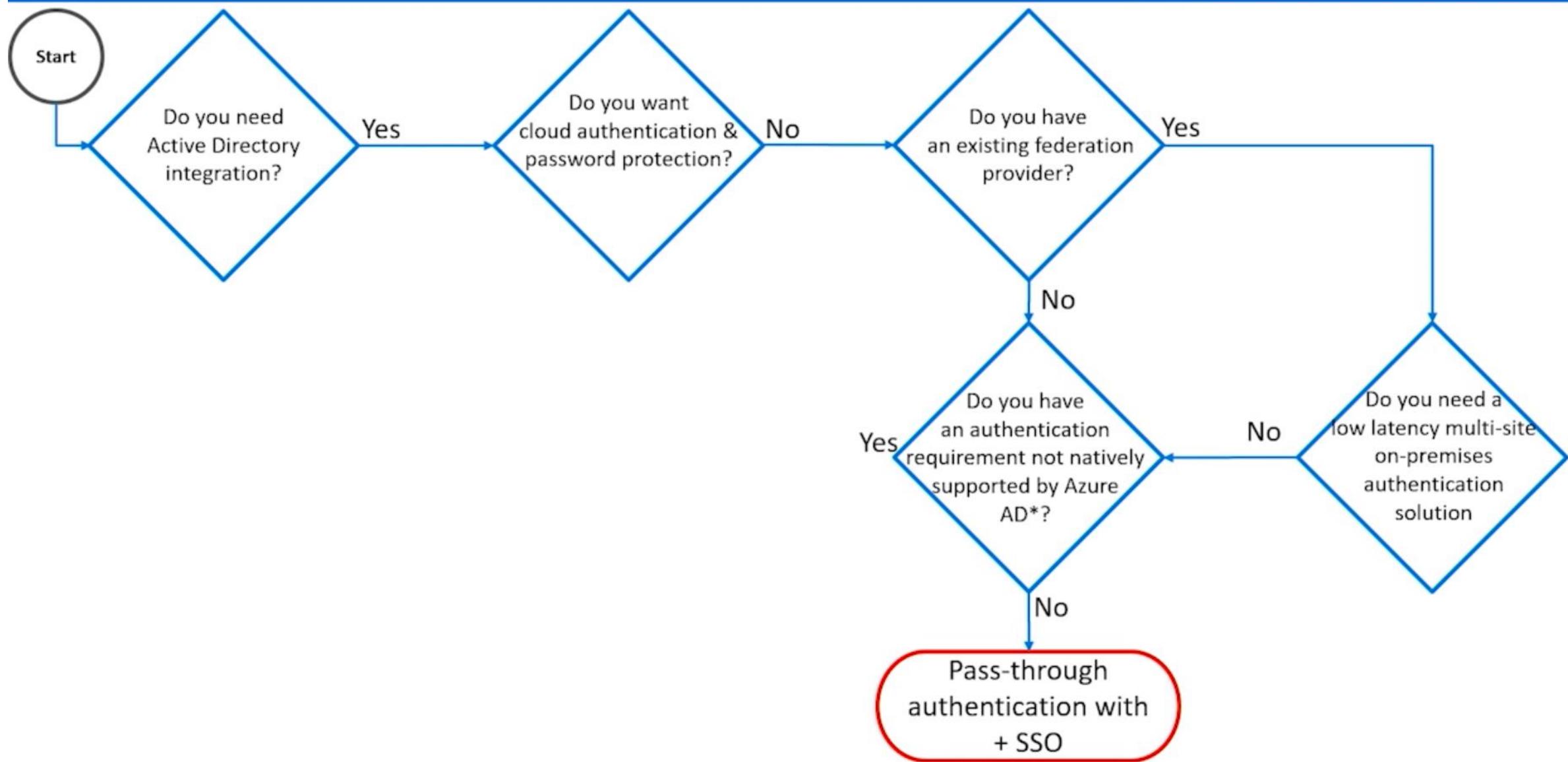


100'000  
employees

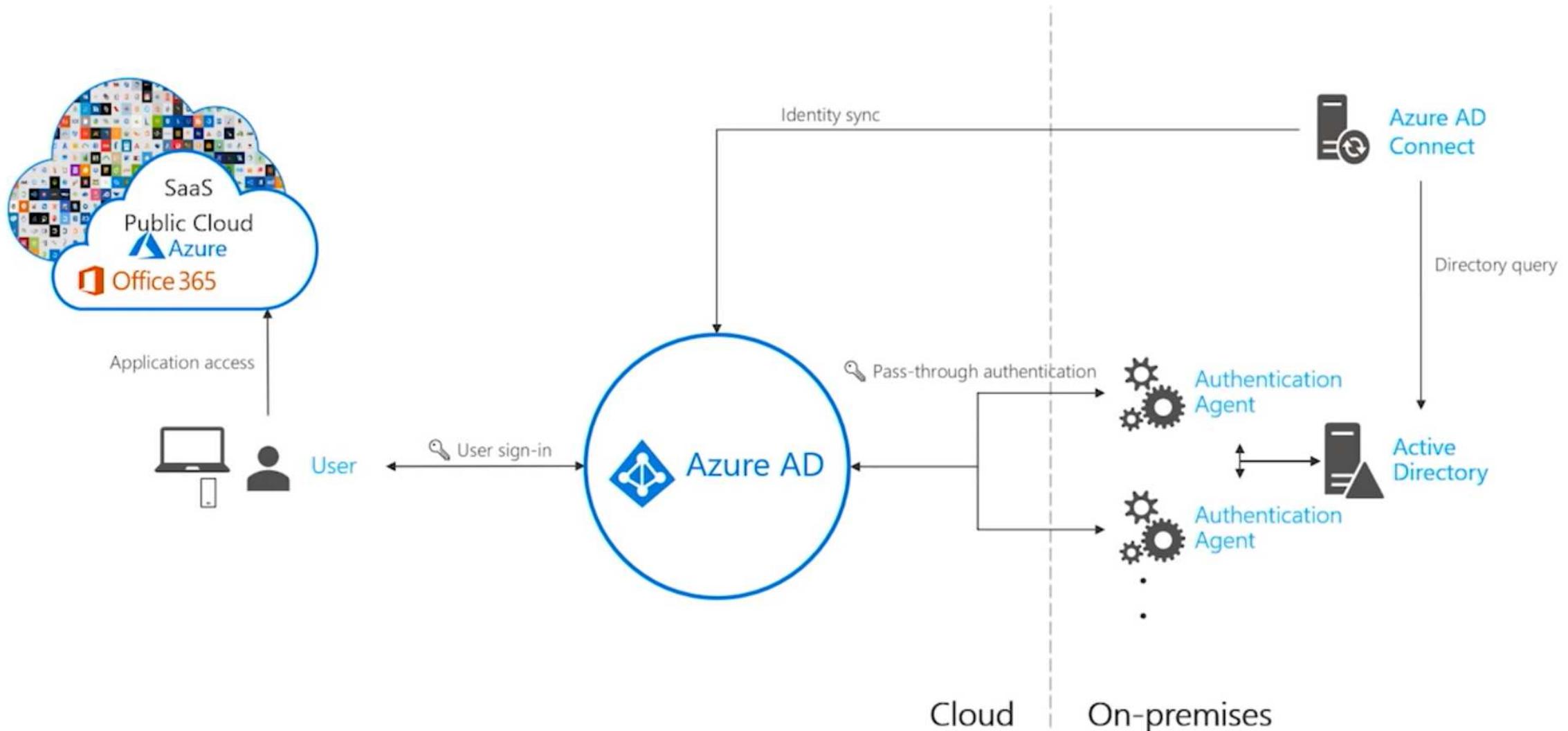


Office 365  
Cloud apps  
LOB apps

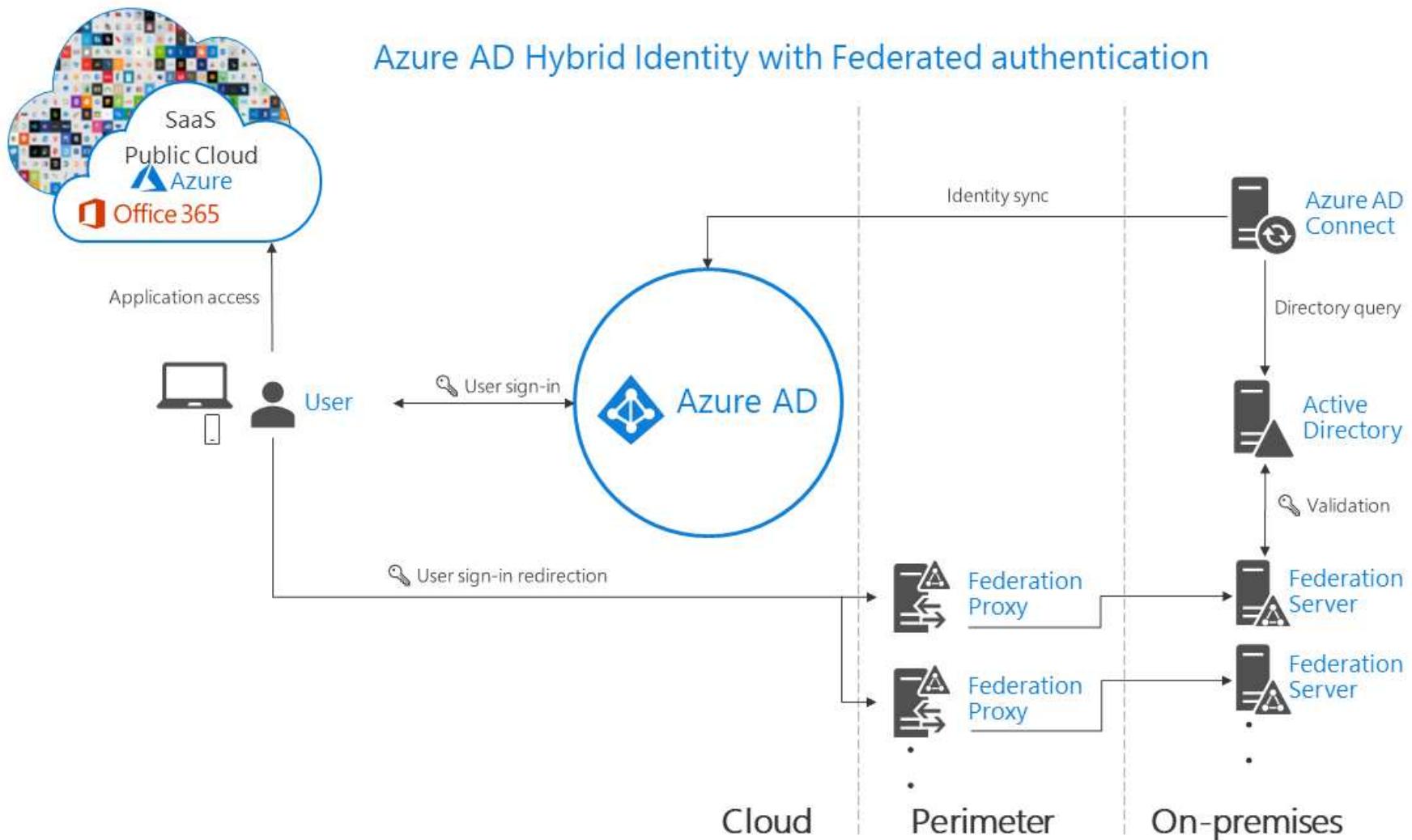
# Azure AD Authentication decision tree



# Pass-through authentication

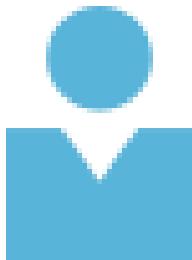


## Azure AD Hybrid Identity with Federated authentication



<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/choose-ad-authn>

Consideration	Password hash synchronization + Seamless SSO	Pass-through Authentication + Seamless SSO	Federation with AD FS
Where does authentication happen?	In the cloud	In the cloud after a secure password verification exchange with the on-premises authentication agent	On-premises
What are the on-premises server requirements beyond the provisioning system: Azure AD Connect?	None	One server for each additional authentication agent	Two or more AD FS servers Two or more WAP servers in the perimeter/DMZ network
What are the requirements for on-premises Internet and networking beyond the provisioning system?	None		Inbound Internet access to WAP servers in the perimeter Inbound network access to AD FS servers from WAP servers in the perimeter Network load balancing
Is there a TLS/SSL certificate requirement?	No	No	Yes
Is there a health monitoring solution?	Not required	Agent status provided by Azure Active Directory admin center	Azure AD Connect Health
Do users get single sign-on to cloud resources from domain-joined devices within the company network?	Yes with Seamless SSO	Yes with Seamless SSO	Yes
What sign-in types are supported?	UserPrincipalName + password	UserPrincipalName + password	UserPrincipalName + password
		Windows-Integrated Authentication by using Seamless SSO	
	Windows-Integrated Authentication by using Seamless SSO	Alternate login ID	sAMAccountName + password
	Alternate login ID		Windows-Integrated Authentication
			Certificate and smart card authentication
			Alternate login ID
Is Windows Hello for Business supported?	Key trust model	Key trust model Requires Windows Server 2016 Domain functional level	Key trust model
What are the multifactor authentication options?	Azure MFA	Azure MFA	Azure MFA
	Custom Controls with Conditional Access	Custom Controls with Conditional Access	Azure MFA server
			Third-party MFA
			Custom Controls with Conditional Access
What user account states are supported?	Disabled accounts (up to 30-minute delay)	Disabled accounts Account locked out Account expired Password expired Sign-in hours	Disabled accounts Account locked out Account expired Password expired Sign-in hours
What are the Conditional Access options?	Azure AD Conditional Access, with Azure AD Premium	Azure AD Conditional Access, with Azure AD Premium	Azure AD Conditional Access, with Azure AD Premium AD FS claim rules
Is blocking legacy protocols supported?	Yes	Yes	Yes
Can you customize the logo, image, and description on the sign-in pages?	Yes, with Azure AD Premium	Yes, with Azure AD Premium	Yes
What advanced scenarios are supported?	Smart password lockout Leaked credentials reports, with Azure AD Premium P2	Smart password lockout	Multisite low-latency authentication system www.PaddyMaddy.com AD FS extranet lockout Integration with third-party identity systems



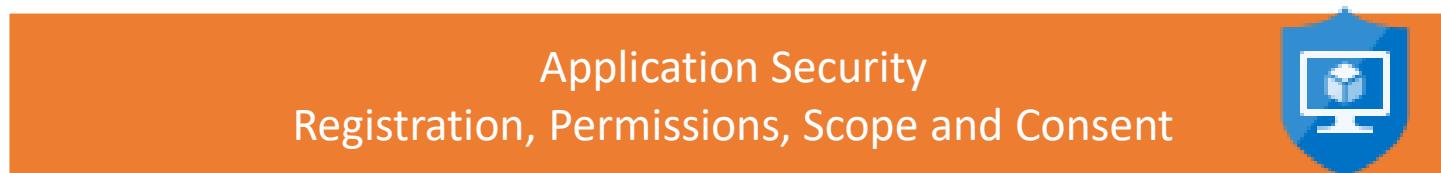
AAD Users



AAD Connect



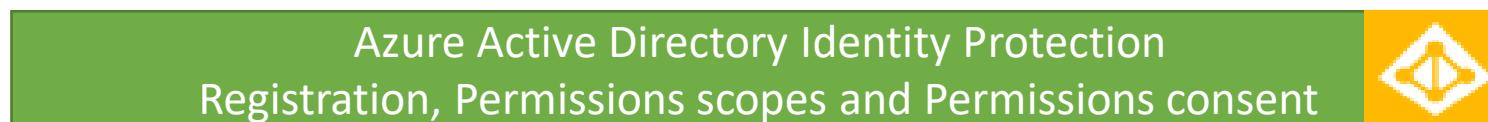
AD Groups

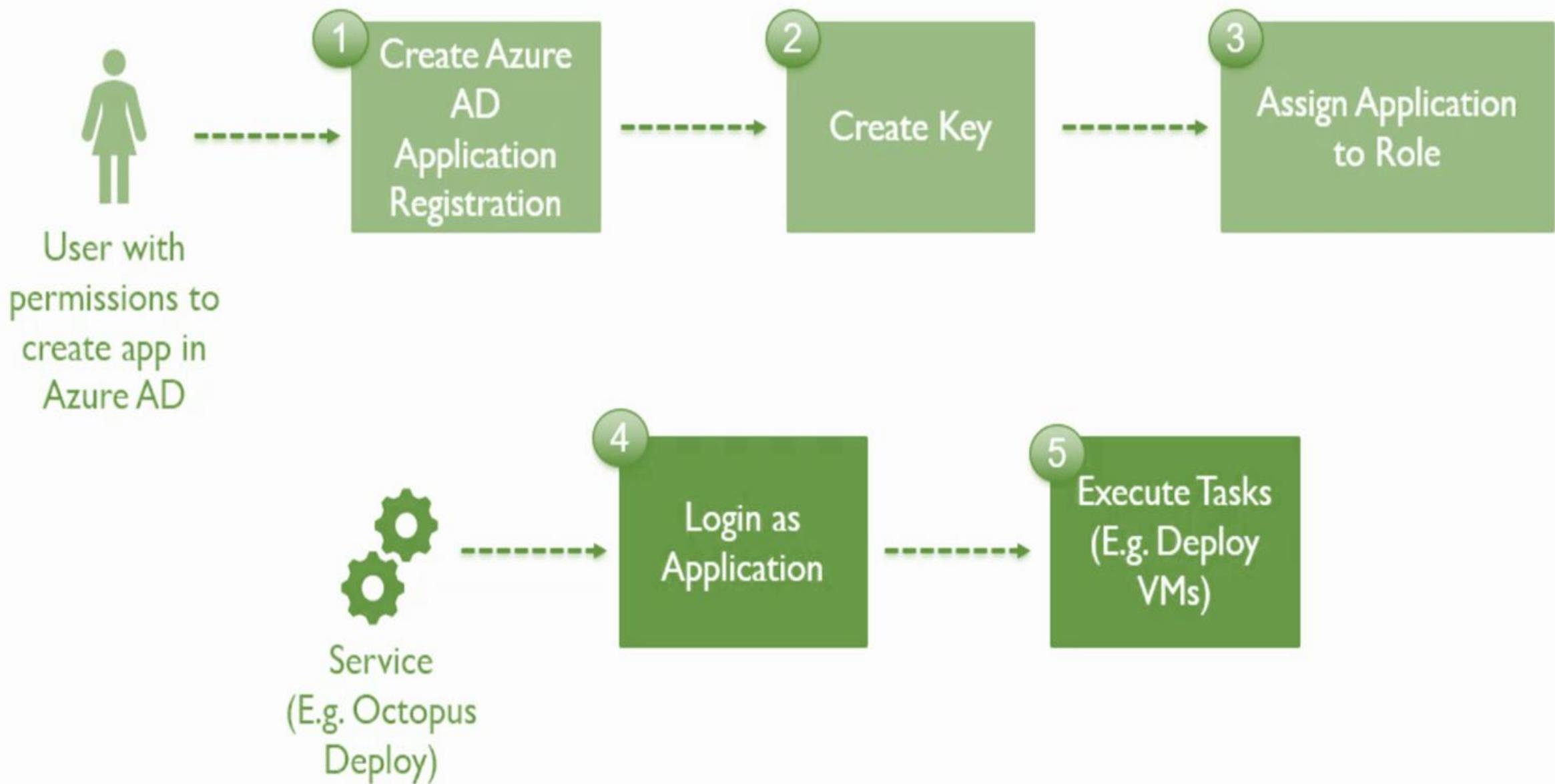


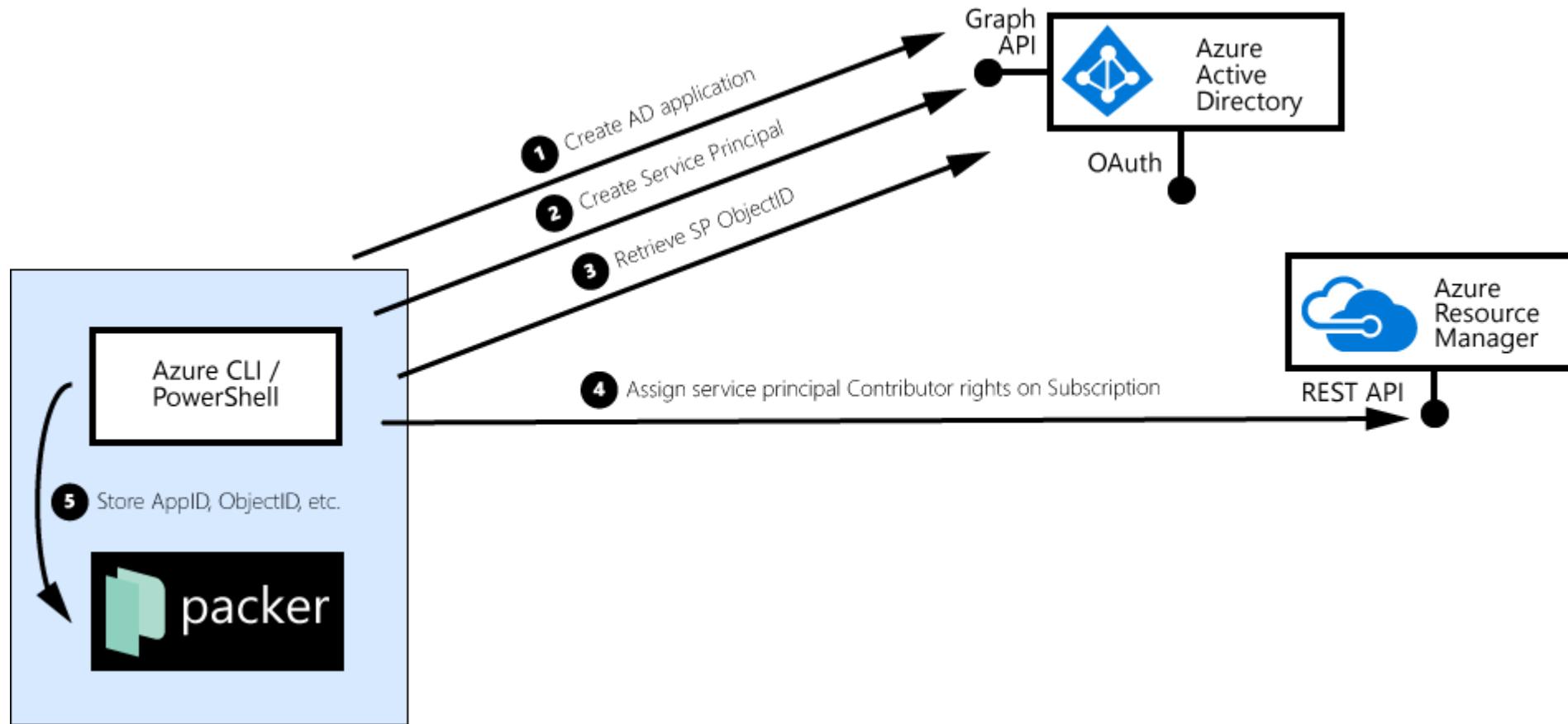
Authentication:  
Password Sync,  
Pass-through  
Authentication



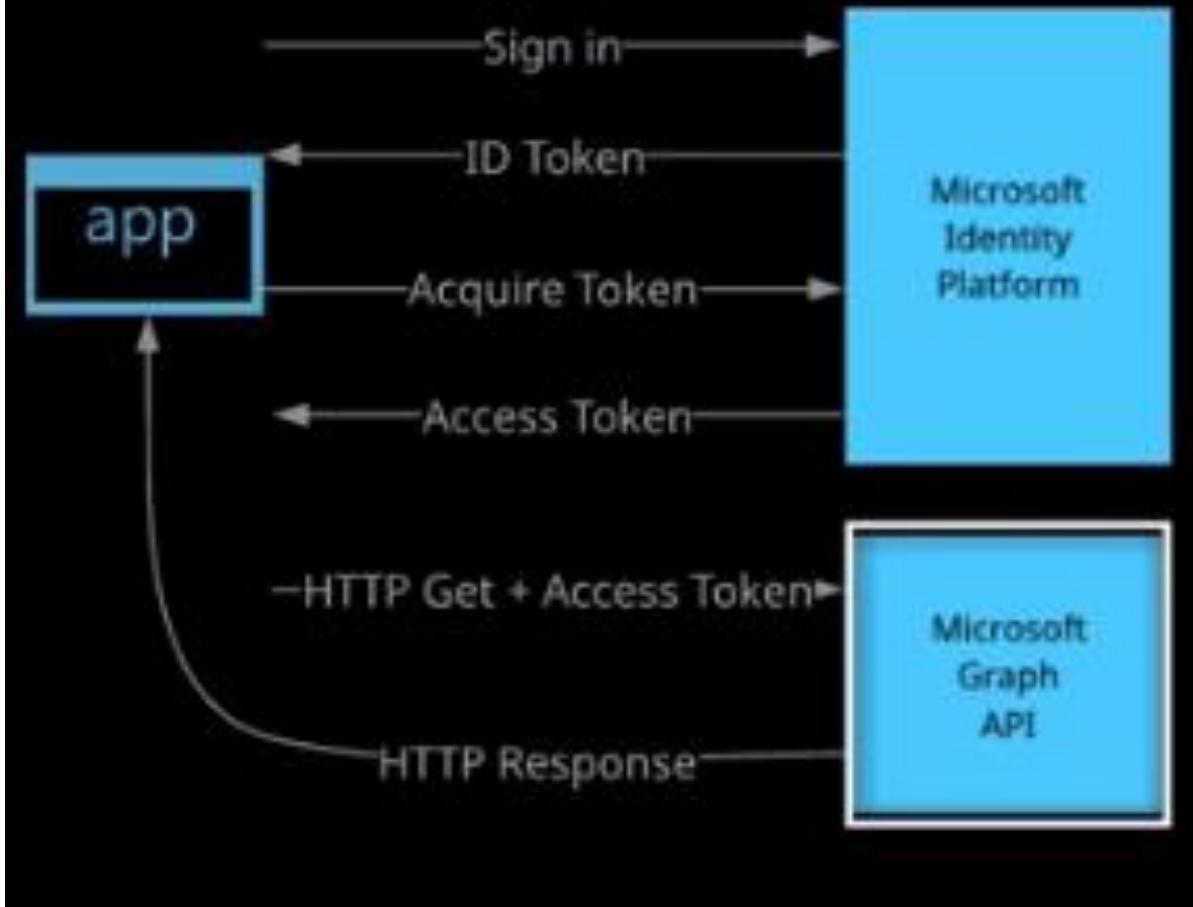
Conditional  
Access





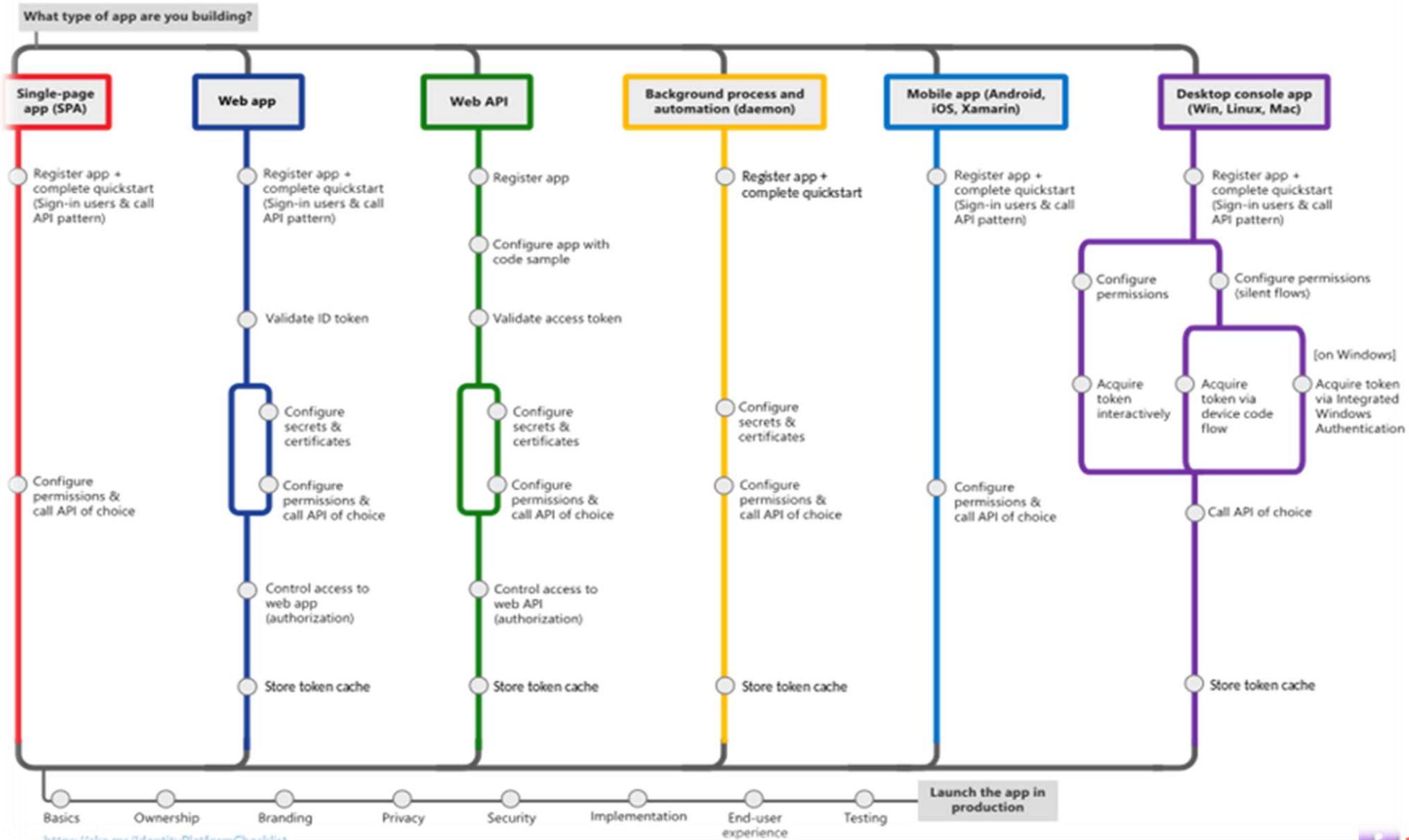


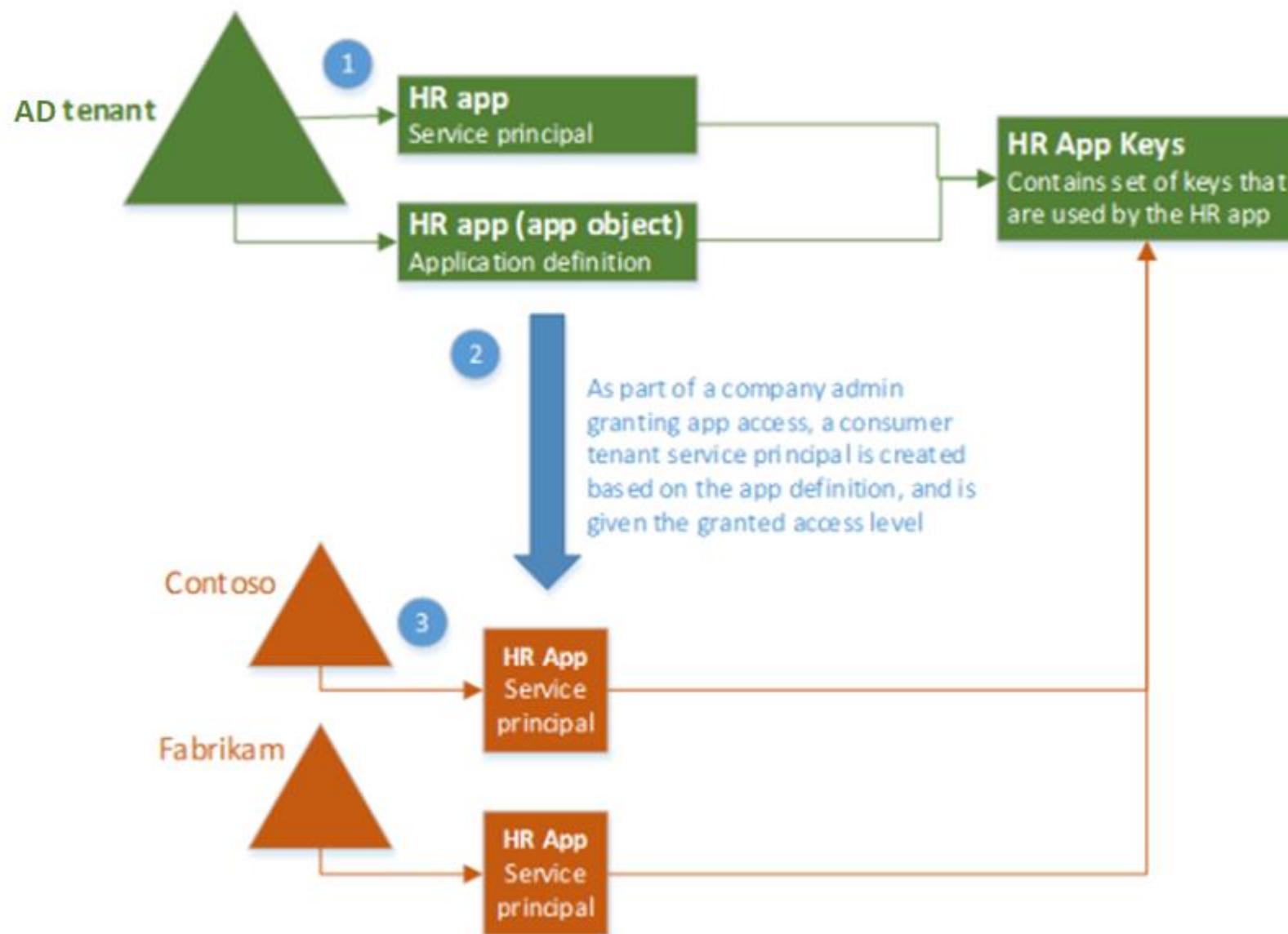
## Securing Applications With Azure Active Directory



# Microsoft identity platform

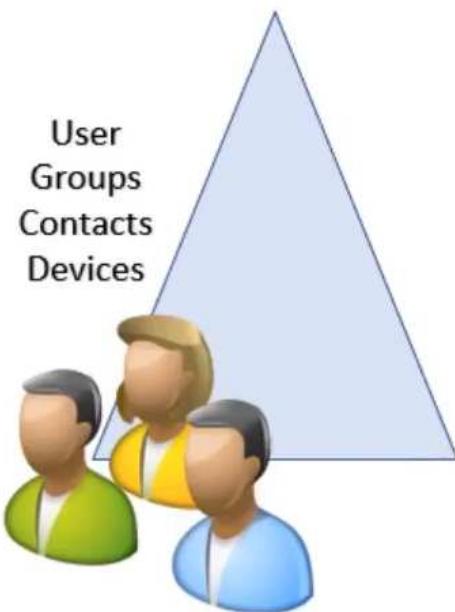
<http://aka.ms/IdentityPlatform>





Azure AD Connect

# Architecture Fundamentals

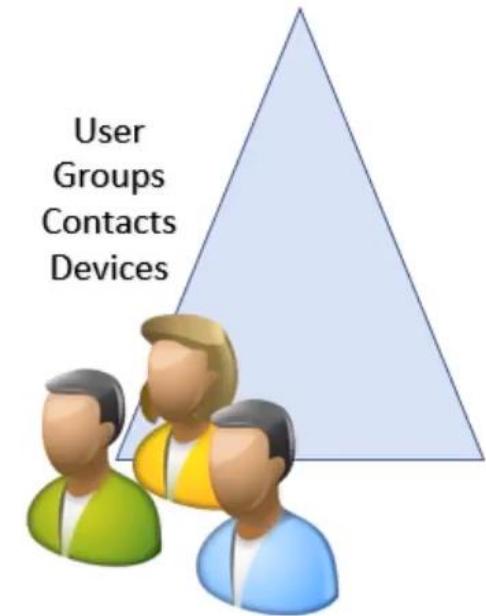


On-Premise Directory

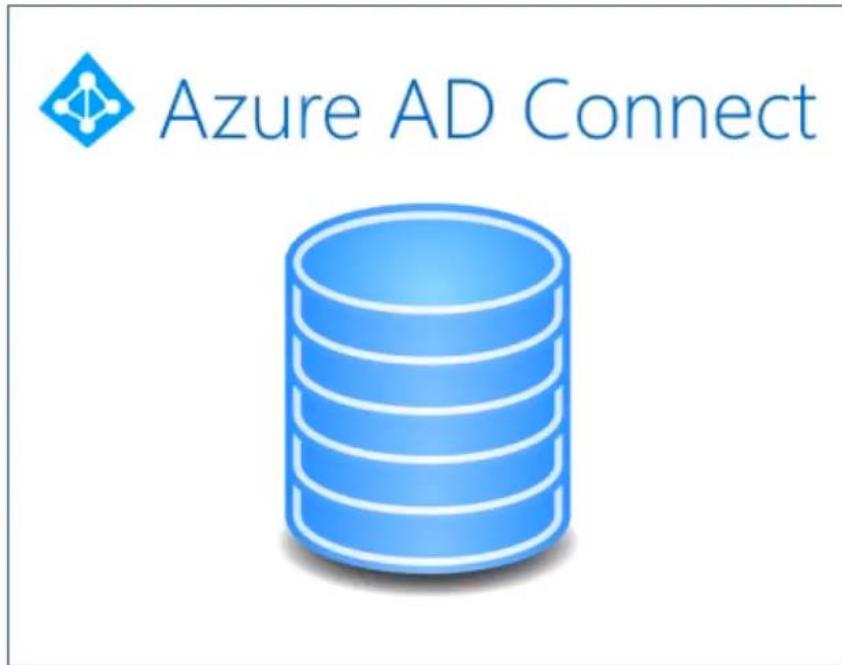


Azure Active Directory

# Azure AD Connect Architecture Fundamentals

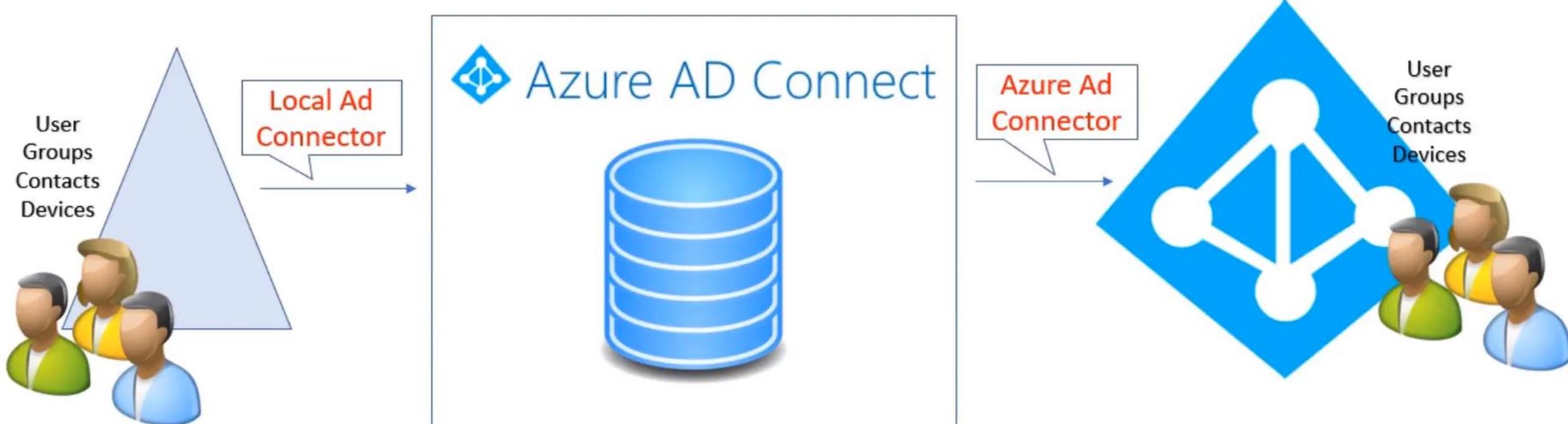


On-Premise Directory



Azure Active Directory

# Azure AD Connect Architecture Fundamentals



On-Premise Directory

Azure Active Directory

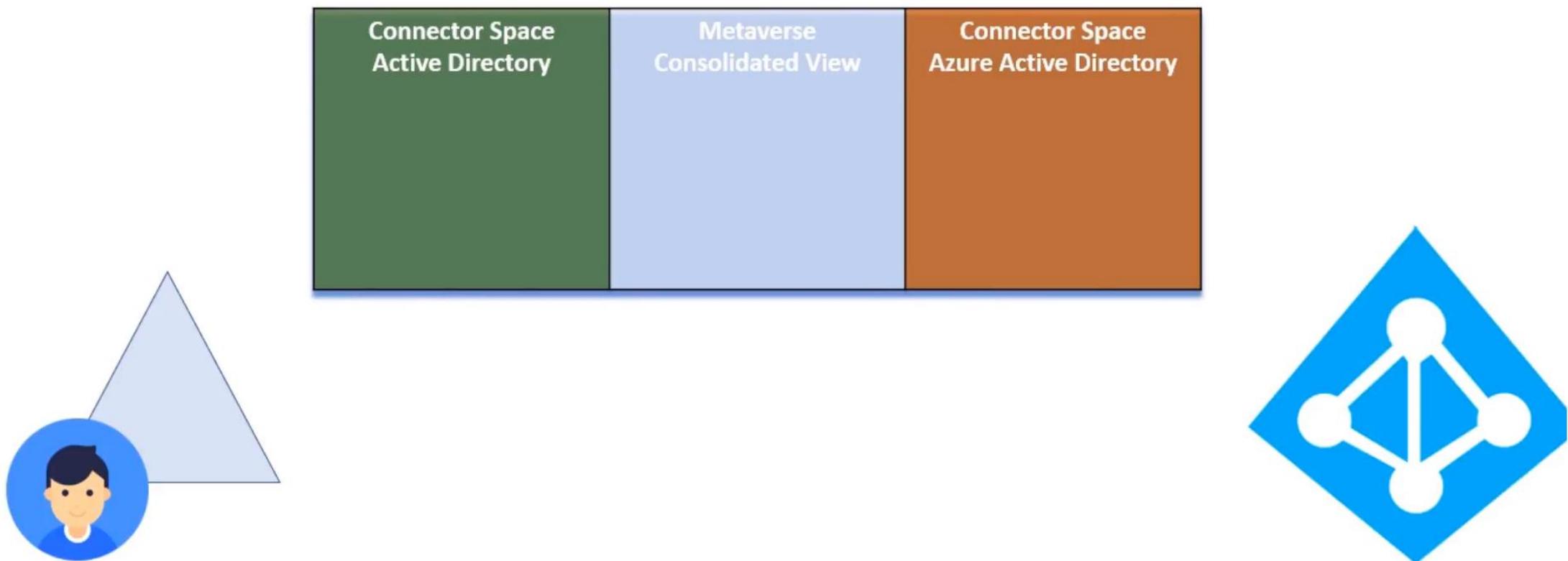
# Azure AD Connect

## Architecture Fundamentals

### Sync Process

### Delta , Full

Import →  
Sync →  
Export ←

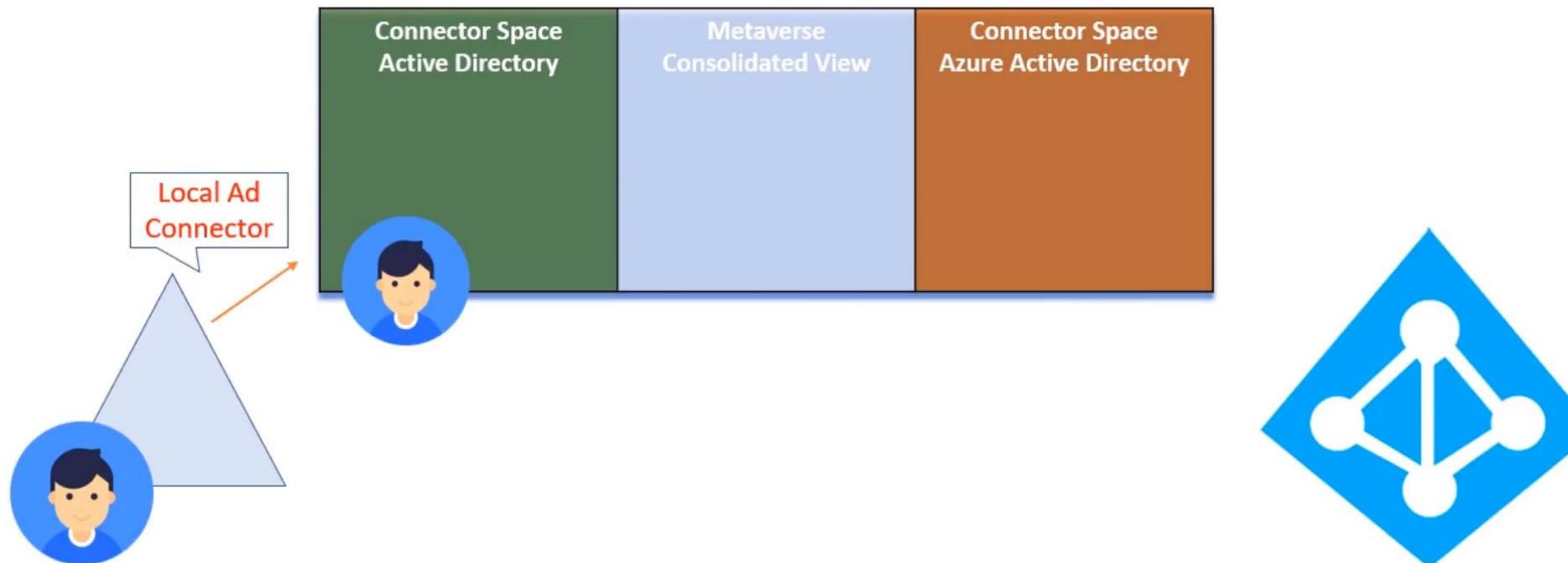


# Azure AD Connect

## Architecture Fundamentals

### Sync Process Delta , Full

Import →  
Sync →  
Export ←



# Azure AD Connect

## Architecture Fundamentals

### Sync Process

#### Delta , Full

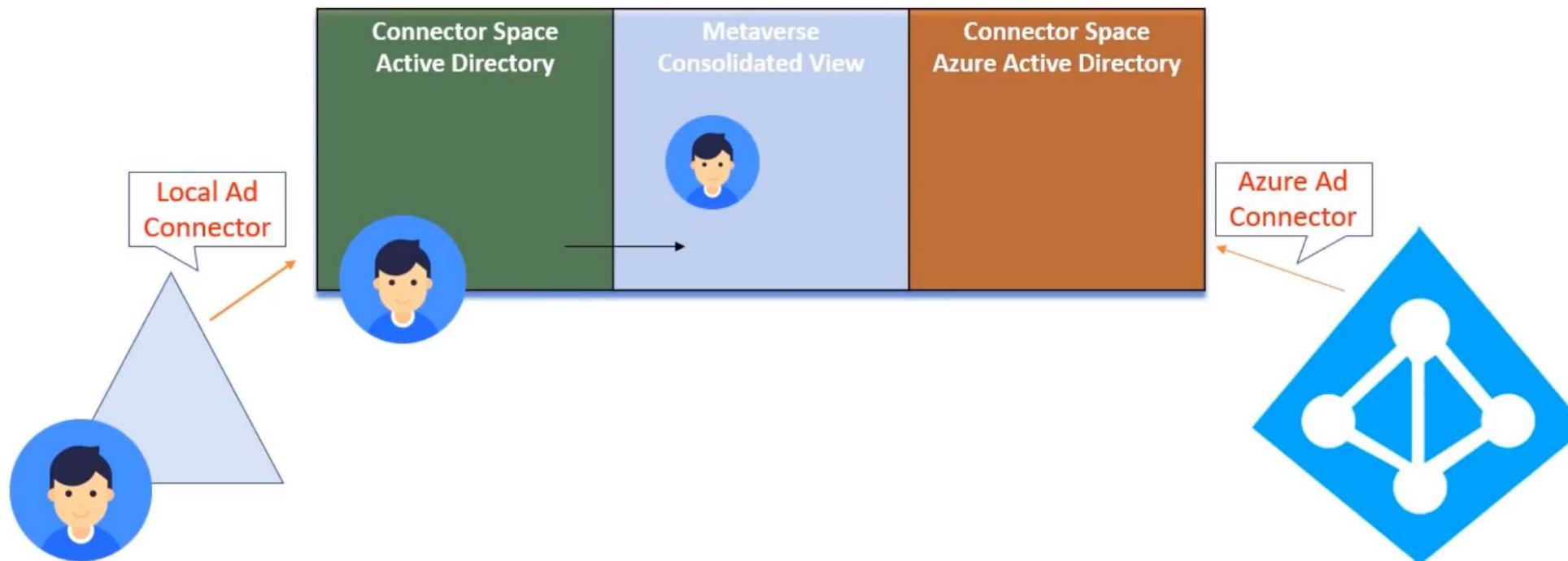
Import →  
Sync →  
Export ←



# Azure AD Connect Architecture Fundamentals

## Sync Process Delta , Full

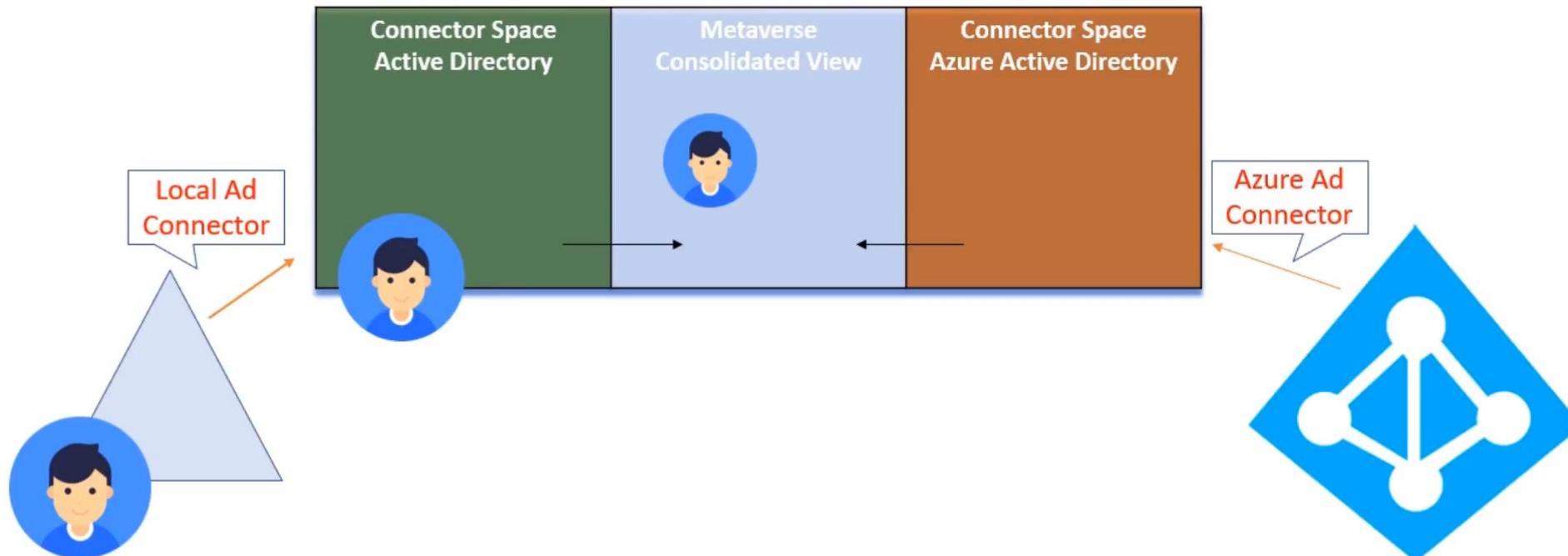
Import   
Sync   
Export 



# Azure AD Connect Architecture Fundamentals

## Sync Process Delta , Full

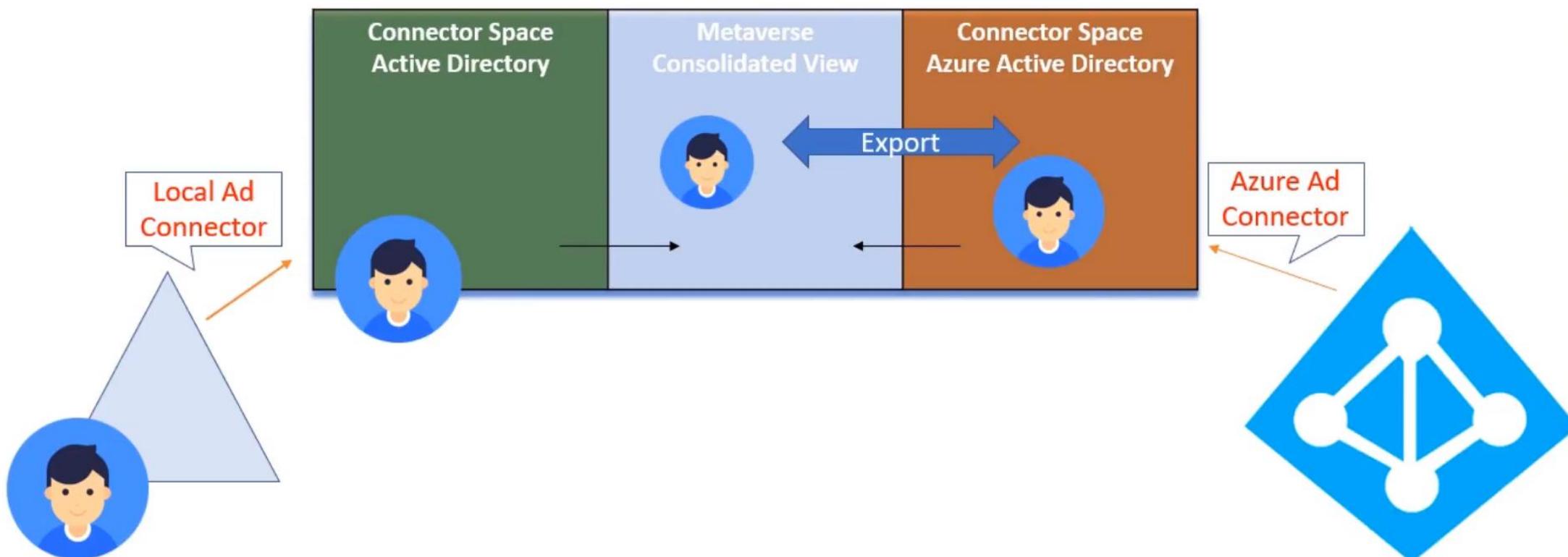
Import  
Sync  
Export



# Azure AD Connect Architecture Fundamentals

## Sync Process Delta , Full

Import →  
Sync →  
Export ←

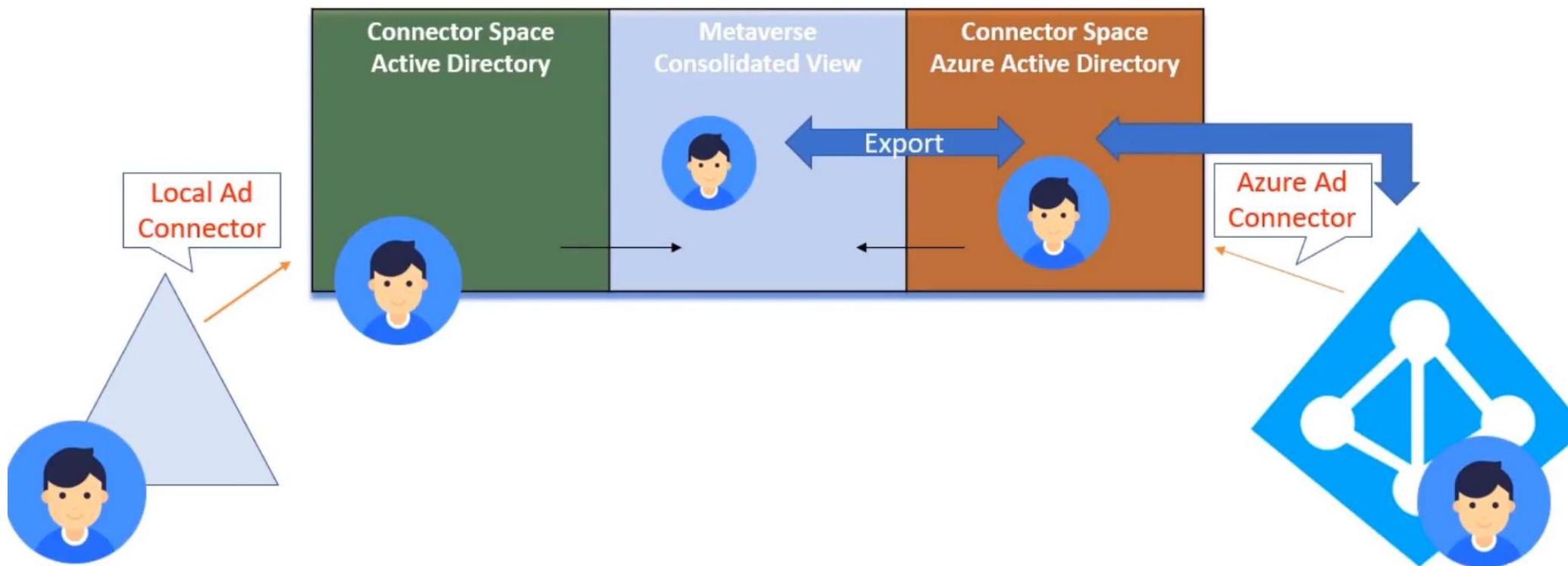


# Azure AD Connect

## Architecture Fundamentals

### Sync Process Delta , Full

Import  
Sync  
Export



# Azure Active Directory

<https://portal.azure.com>

- No Organizational Units
- No Trusts between domains



# Azure Active Directory

Flat Namespace



Users



Groups



Devices

# Pass through Authentication

## How it works ??

HOST/aadg.windows.net.nsatc.net

HOST/autologon.microsoftazuread-sso.com

RestrictedKrbHost/aadg.windows.net.nsatc.net

RestrictedKrbHost/autologon.microsoftazuread-sso.com

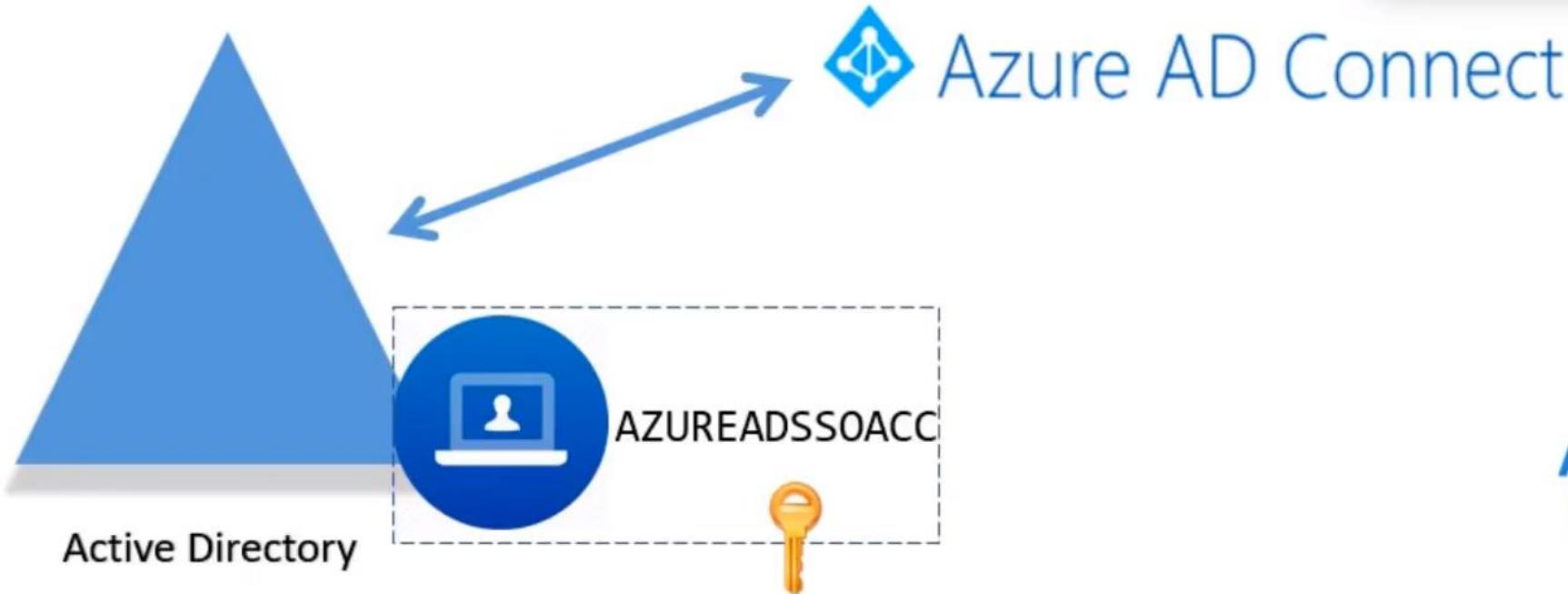
### User sign-in

Select the Sign On method.

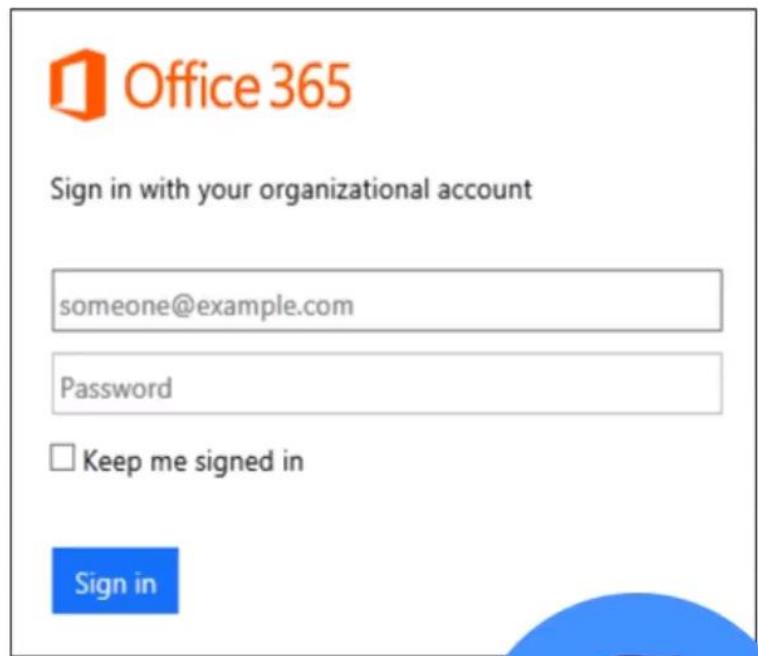
- Password Synchronization [?](#)
- Pass-through authentication [?](#)
- Federation with AD FS [?](#)
- Do not configure [?](#)

Select this option to enable single sign-on for your corporate desktop users:

- Enable single sign-on [?](#)



## User Experience :-



Office 365

Sign in with your organizational account

someone@example.com

Password

Keep me signed in

Sign in

1 – user navigates to  
<https://portal.office.com>



The browser forwards the Kerberos ticket it acquired from Active Directory to Azure AD.  
Azure AD decrypts the Kerberos ticket, which includes the identity of the user signed into the corporate device, using the previously shared key.

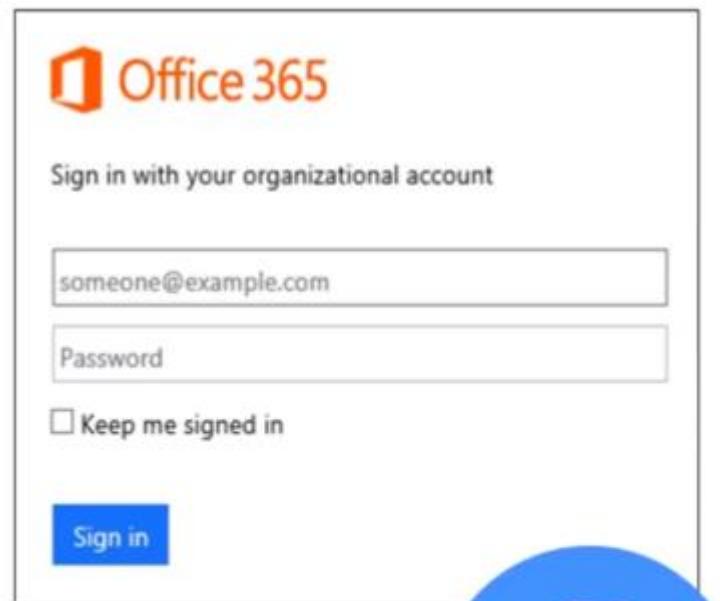
2 - Redirect to  
<https://login.microsoftonline.com>

3- Azure AD returns 401 to the user agent.



The browser, in turn, requests a ticket from Active Directory for the AZUREADSSOACC computer account (which represents Azure AD).

# User Experience



1 – user navigates to  
<https://portal.office.com>

The browser forwards the Kerberos ticket it acquired from Active Directory to Azure AD.  
Azure AD decrypts the Kerberos ticket, which includes the identity of the user signed into the corporate device, using the previously shared key.

2 - Redirect to  
<https://login.microsoftonline.com>



3- Azure AD returns  
401 to the user agent.



Active Directory

The browser, in turn, requests a ticket from Active Directory for the AZUREADSSOACC computer account (which represents Azure AD).

Enter the zone assignments here.

Value name	Value
https://portal.office.com	1
https://login.microsoftonline.com	1
▶ https://autologon.microsoftazuread-sso.com	1
https://secure.aadcdn.microsoftonline-p.com	1
*	

OK Cancel

- 1 = Intranet Zone
- 2 = Trusted Sites Zone
- 3 = Internet Zone
- 4 = Restricted Sites Zone

## Accounts

- There are three accounts which are created when you install AAD Connect.
- First Account – **Msol\_764p69 (AD DS Connector account)**
  - This account is used for read/write operation on Local AD
- Second Account – **Sync\_764... (Azure AD Connector account)**
  - This account is used for read/write operations on Azure AD
- Service Account – **AAD (AD Sync service account)**

Welcome

Express Settings

## Express Settings

If you have a **single** Windows Server Active Directory forest, we will do the following:

- Configure synchronization of identities in the current AD forest of CONCEPTSWORK
- Configure password hash synchronization from on-premises AD to Azure AD
- Start an initial synchronization
- Synchronize all attributes
- Enable Auto Upgrade

[Learn more about express settings](#)

If you would like different settings, click [Customize](#).



Customize

Use express settings



Welcome

Express Settings

Required Components

User Sign-In

## Install required components

No existing synchronization service was found on this computer. The Azure AD Connect synchronization service will be installed. [?](#)

- Specify a custom installation location
- Use an existing SQL Server
- Use an existing service account
- Specify custom sync groups

Previous

Install

Welcome

Express Settings

Required Components

User Sign-In

## Install required components

No existing synchronization service was found on this computer. The Azure AD Connect synchronization service will be installed. 

Specify a custom installation location

INSTALL LOCATION

C:\Program Files\Microsoft Azure AD Sync



 Browse

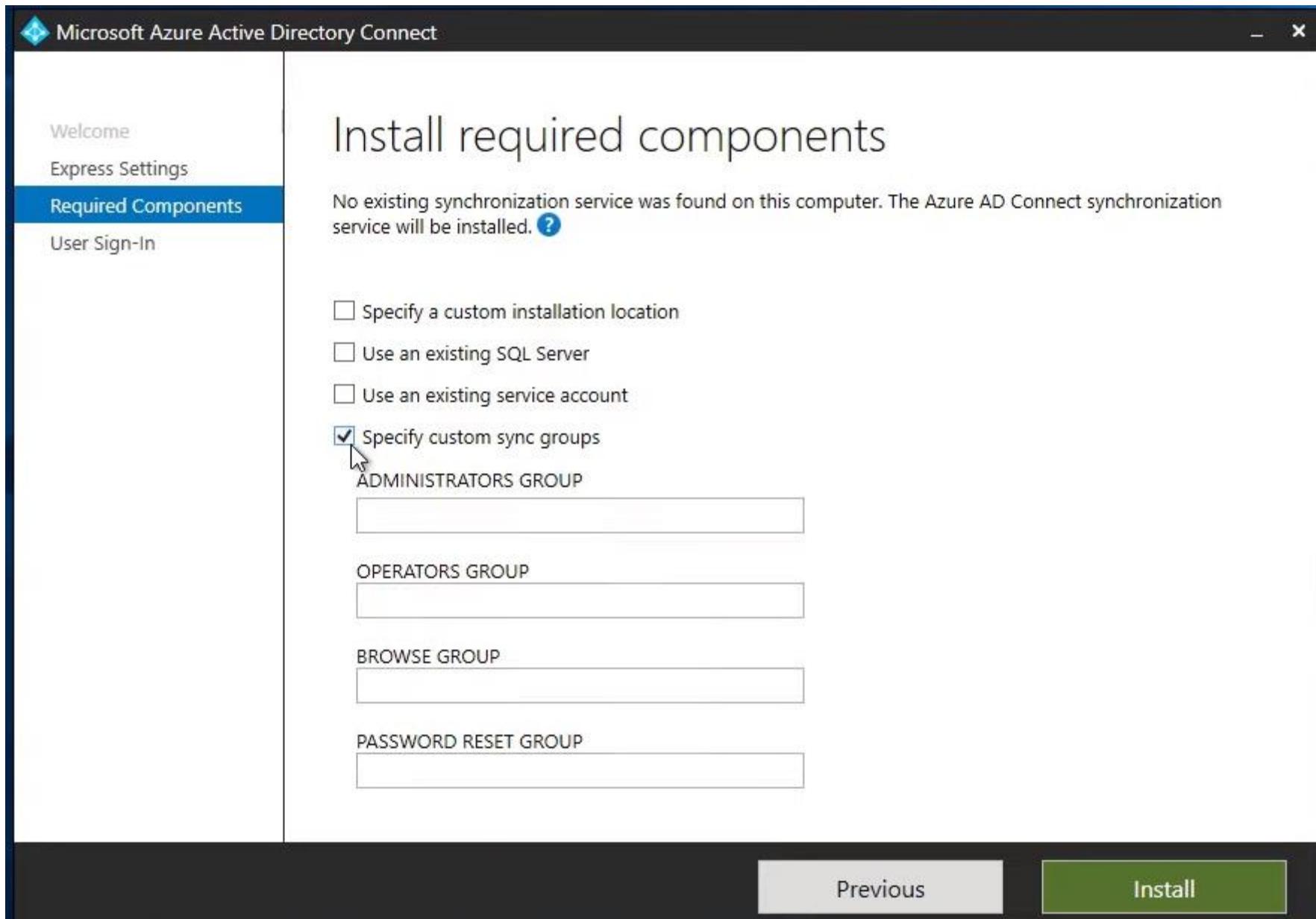
Use an existing SQL Server

Use an existing service account

Specify custom sync groups

Previous

Install



 Microsoft Azure Active Directory Connect

– X

Welcome

Express Settings

Required Components

User Sign-In

Connect to Azure AD

Sync

Connect Directories

Azure AD sign-in

Domain/OU Filtering

Identifying users

Filtering

Optional Features

Configure

## User sign-in

Select the Sign On method. [?](#)

Password Hash Synchronization [?](#)

Pass-through authentication [?](#)

Federation with AD FS [?](#)

Federation with PingFederate [?](#)

Do not configure [?](#)

Select this option to enable single sign-on for your corporate desktop users:

Enable single sign-on [?](#)

Previous

Next

# Azure Active Directory

Flat Namespace



Users



Groups



Devices

# Azure Active Directory

<https://portal.azure.com>

- No Organizational Units
- No Trusts between domains



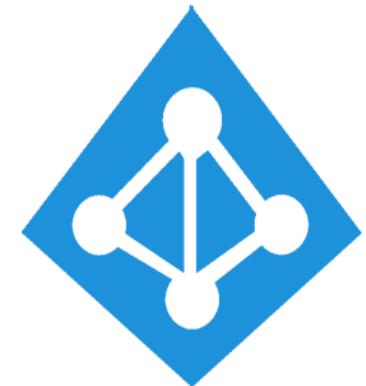
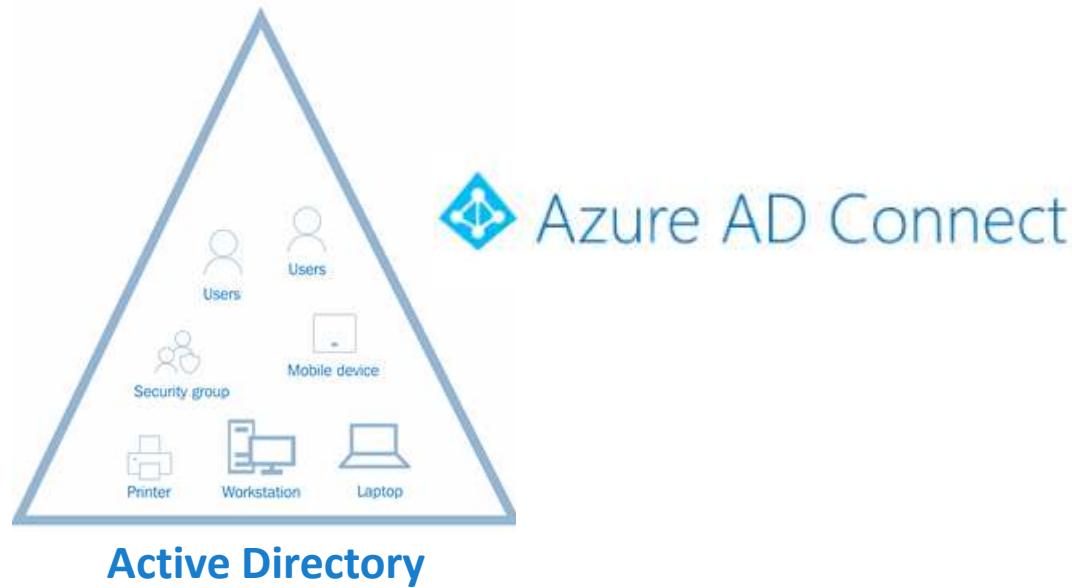
## Identity Models In Azure Active Directory

Cloud only Identities



Azure Active Directory

Synced Identities



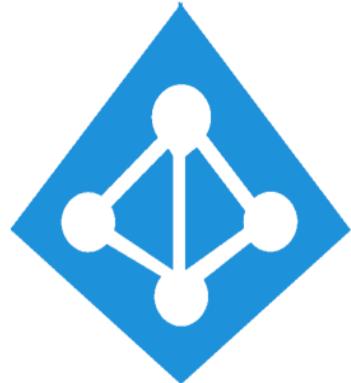
Azure Active Directory

## Azure AD Connect Architecture

Azure AD or Office 365 Subscription – Tenant Name

Tenant Name – Test.Onmicrosoft.com

- Registered with MS Domain
- [User@test.onmicrosoft.com](mailto:User@test.onmicrosoft.com)



Azure Active Directory

OR



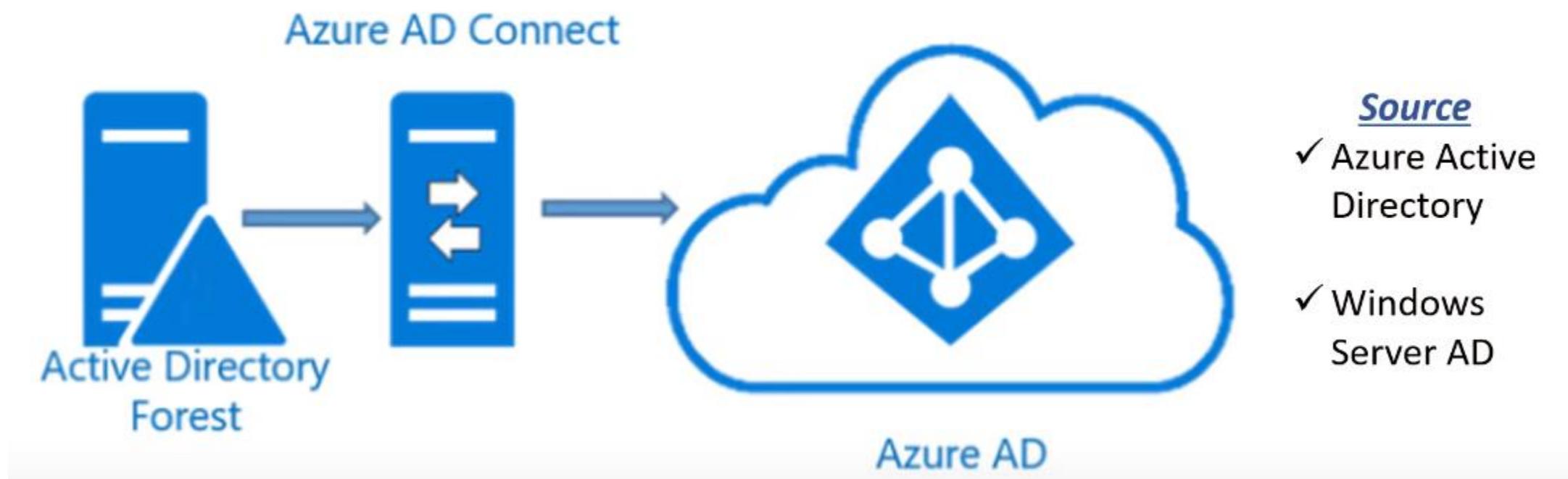
Verify Domain Name →

[User@mycompany.com](mailto:User@mycompany.com)

Verify your Domain Name ex:- mycompany.com

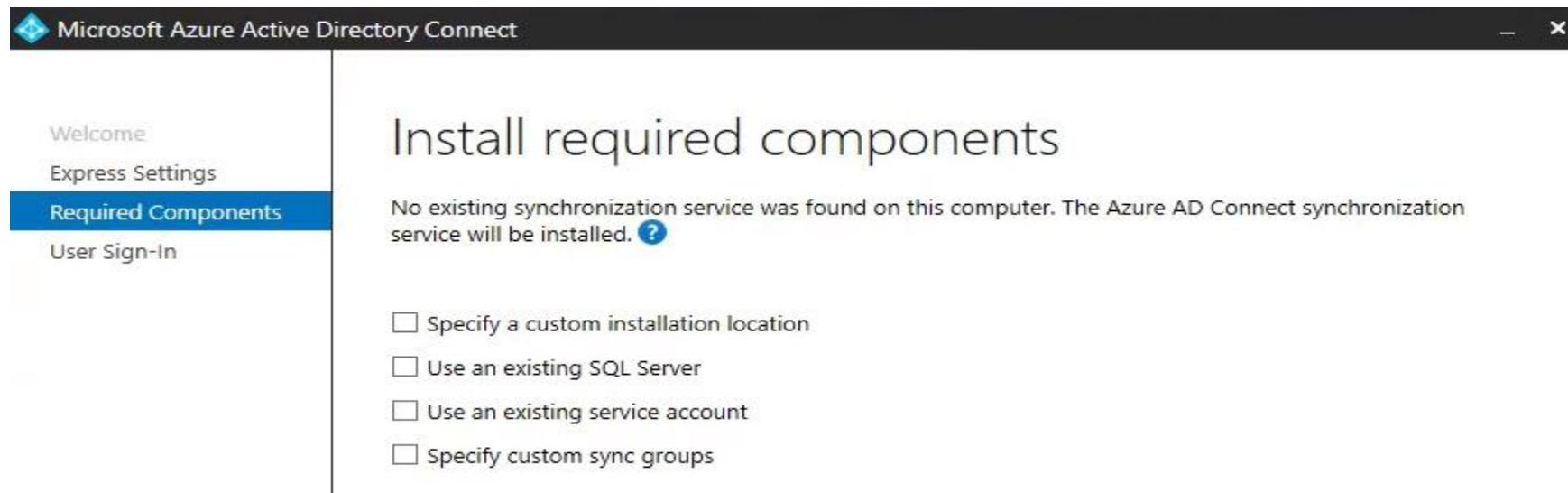
Set as Default UPN for users

ex:- [User@mycompany.com](mailto:User@mycompany.com)



## AAD Connect Installation

- Verify your Domain name
- Domain Joined Windows Server 2008 R2 or Later
- Change mylocaldomainName to UPN name
  - Ex:- mydc.local to **learninmylab.com**
- AAD connect can be installed on Windows 2008 R2 or Later
- Default configuration is for only 50K only (Without Domain), Else its for 300k
- Permissions
  - You need Global Admin Credentials of the Tenant
- SQL express is installed by default which has limitations of 10 GB with can fit for less than 100k Objects
- Use Full SQL if you have more than 100K objects



Microsoft Azure Active Directory Connect

Welcome

Tasks

Connect to Azure AD

**User Sign-In**

Single sign-on

Configure

User sign-in

Select the Sign On method. [?](#)

Password Hash Synchronization [?](#)

Pass-through authentication [?](#)

Federation with AD FS [?](#)

Federation with PingFederate [?](#)

Do not configure [?](#)

Select this option to enable single sign-on for your corporate desktop users:

Enable single sign-on [?](#)



### Password Hash Synchronization:

When you want the authentication to be processed by azure AD and the authentication requests should not be redirected to On-premises

### Pass through Authentication:

When you want the authentication to be processed by azure AD and the authentication request are redirected to On-premises

### Federation with ADFS or Ping Federate:

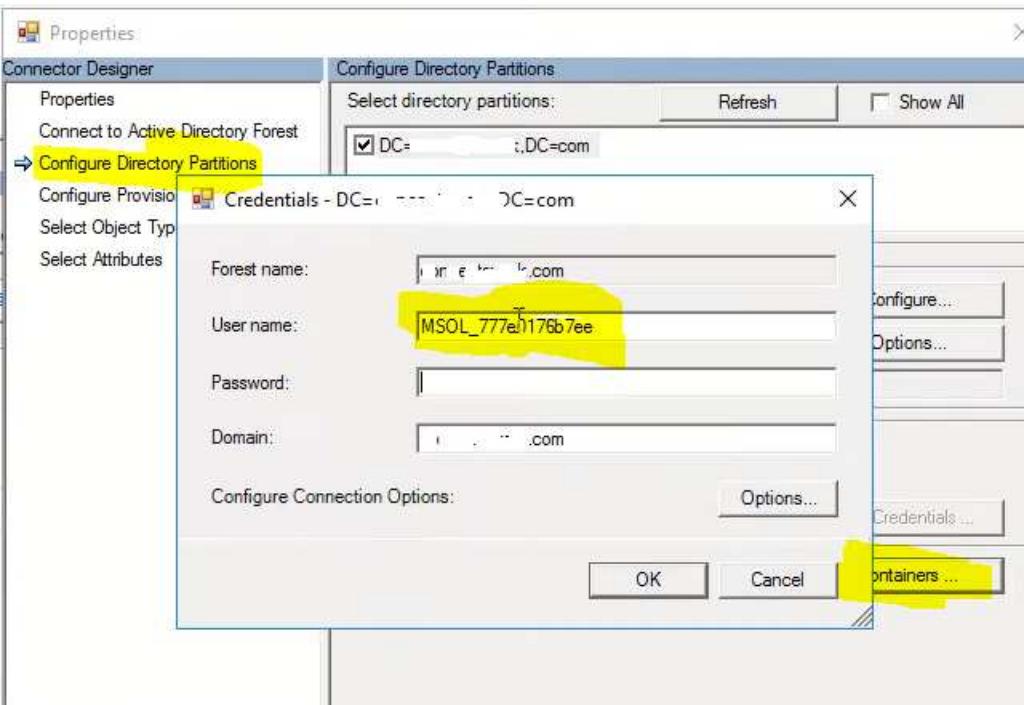
When you want the authentication to be processed by On-prem identity provider and the authentication requests are redirected to On-premises

# Accounts Created by AAD Connect

## Active Directory

1) **Msol\_\*\*\*** Account will be created

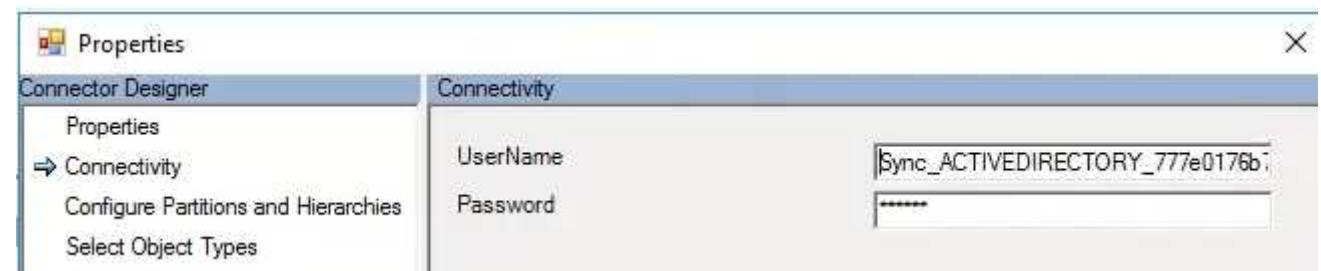
- 1) This account used for read and Write Operations on Local AD
  - ✓ You can find in local AD connector this account info



## Azure Active Directory

2) **Sync\_\*\*\***... Azure Account will be created

- 1) This account used for read and Write Operations on Azure AD



3. Service Account – **AAD (AD Sync Service Account)**

4. If you selected Single Sign-On Computer Account will be created as below



Types of Filtering:-



Group Based.



Domain Based.



OU Based.

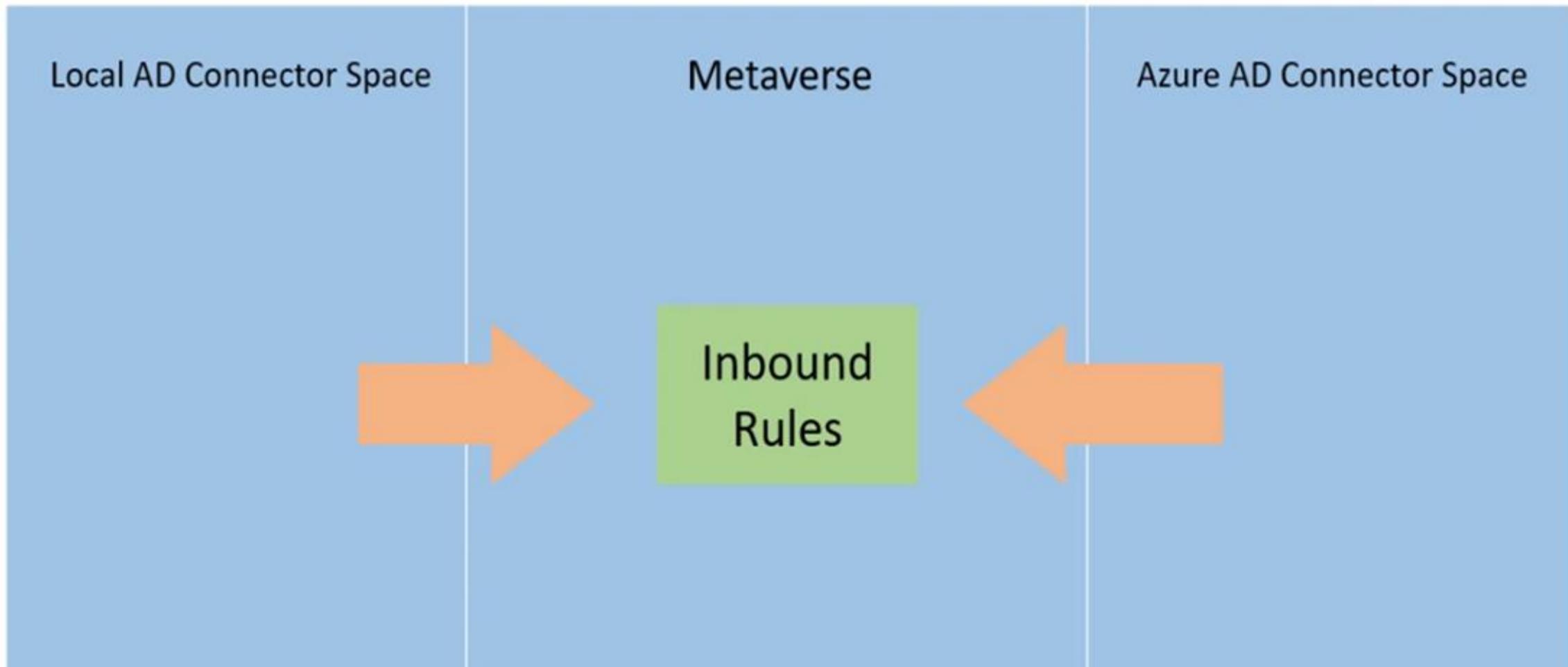


Attribute Level.

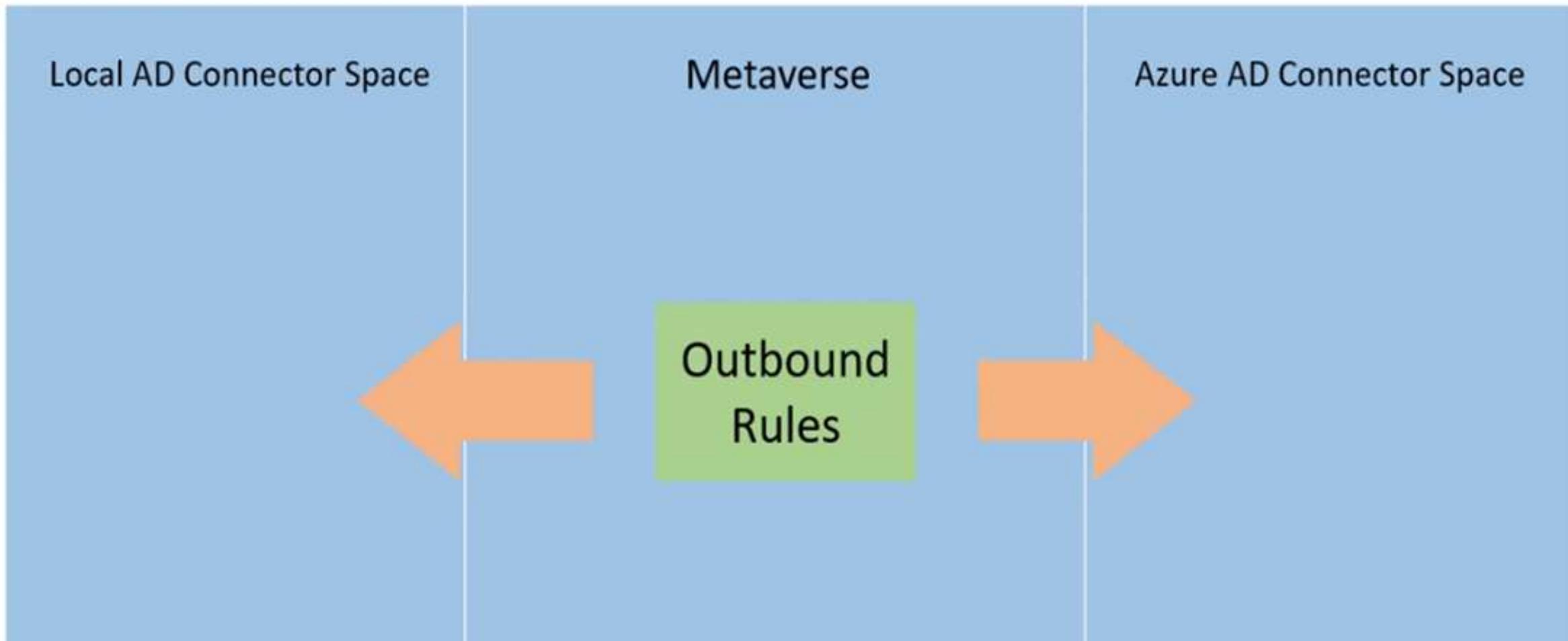
# Synced Identities



# Synchronization Rule Editor



# Synchronization Rule Editor



### Local AD Connector Space



Inbound  
Rules

### Metaverse



Inbound  
Rules

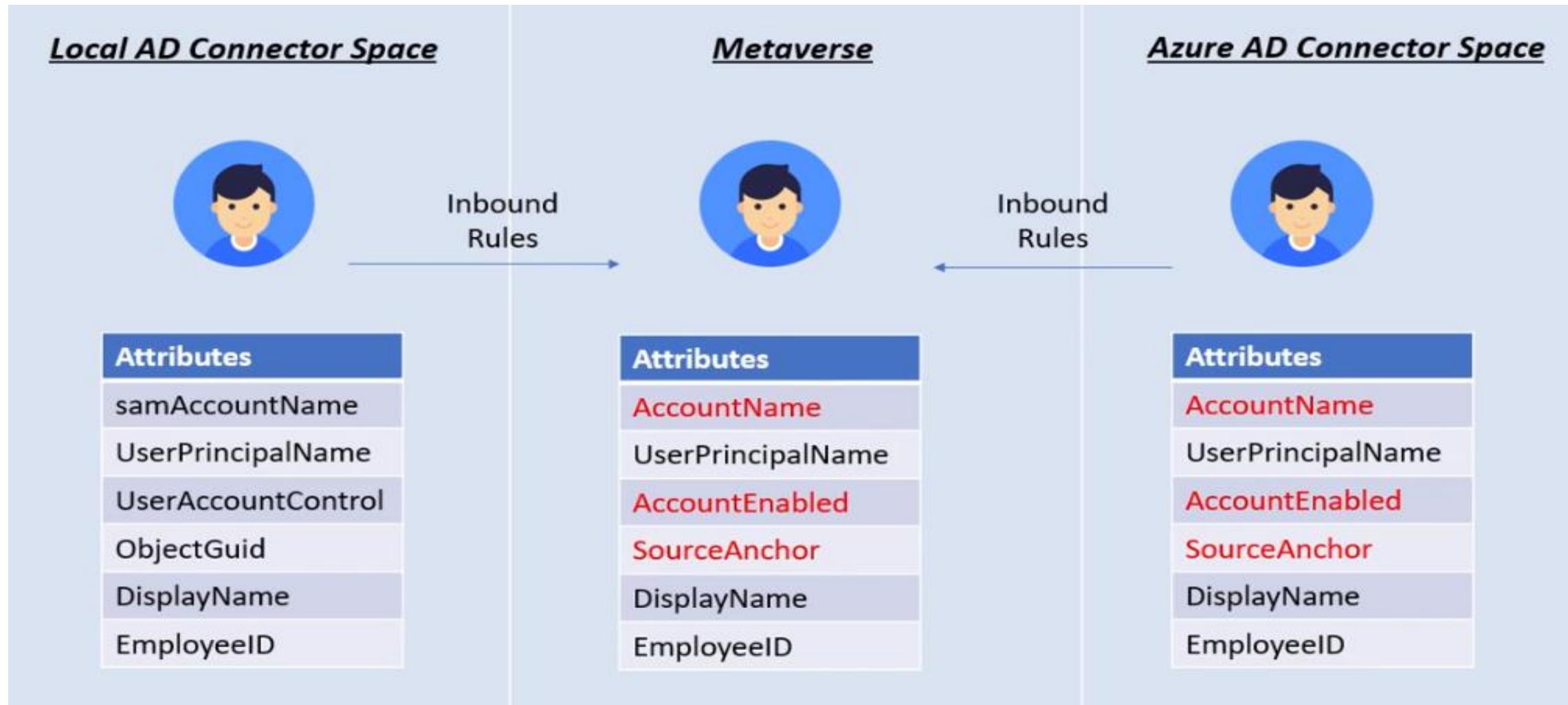
### Azure AD Connector Space



Attributes
samAccountName
UserPrincipalName
UserAccountControl
ObjectGuid
DisplayName
EmployeeID

Attributes
AccountName
UserPrincipalName
AccountEnabled
SourceAnchor
DisplayName
EmployeeID

Attributes
AccountName
UserPrincipalName
AccountEnabled
SourceAnchor
DisplayName
EmployeeID



### Local AD Connector Space



Outbound  
Rules

Attributes
samAccountName
UserPrincipalName
UserAccountControl
ObjectGuid
DisplayName
EmployeeID

### Metaverse



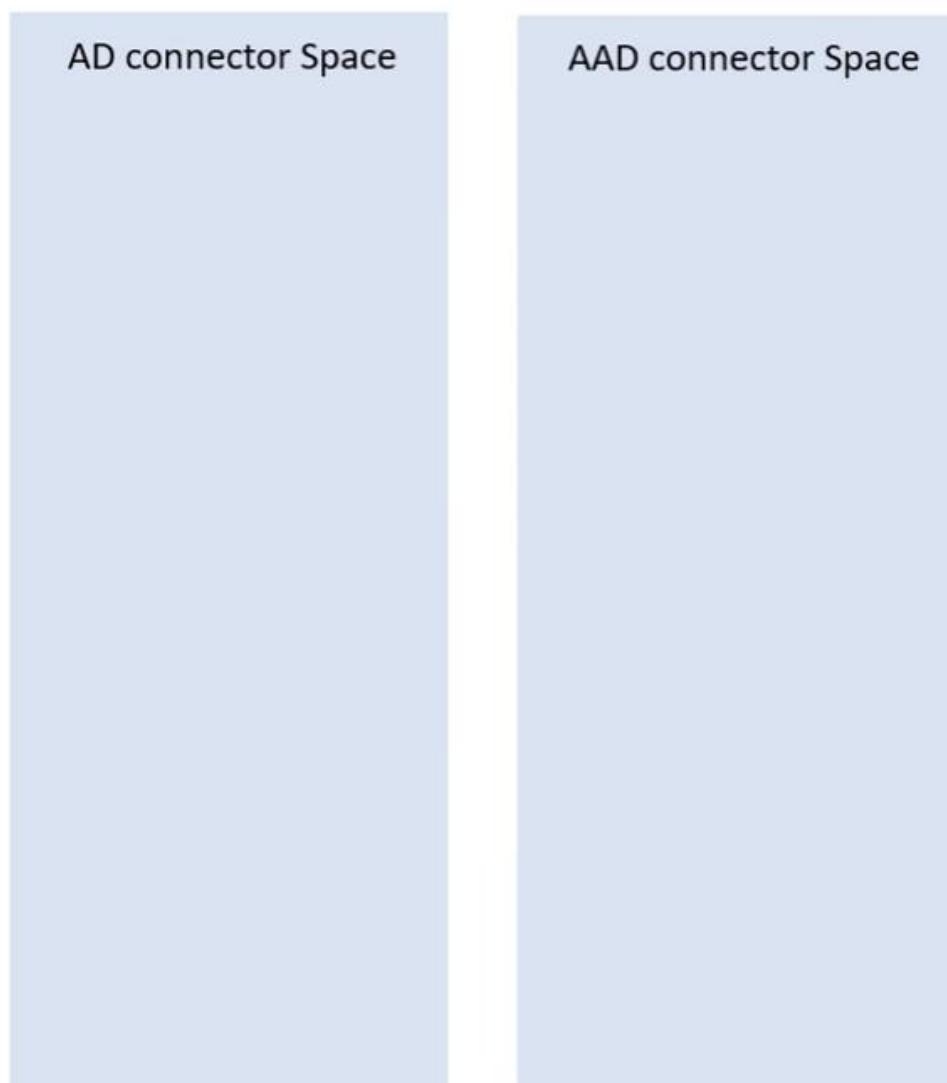
Outbound  
Rules

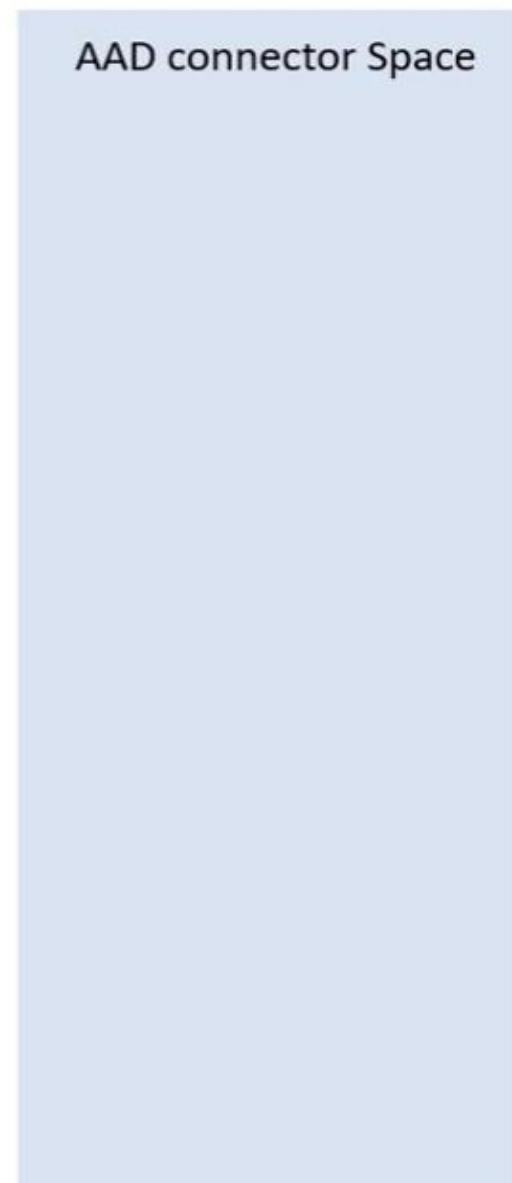
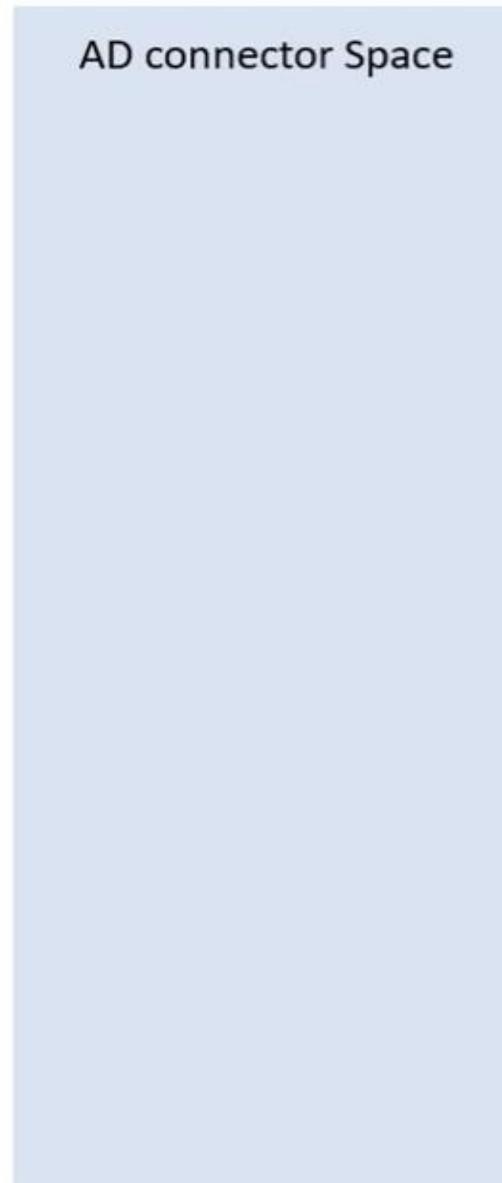
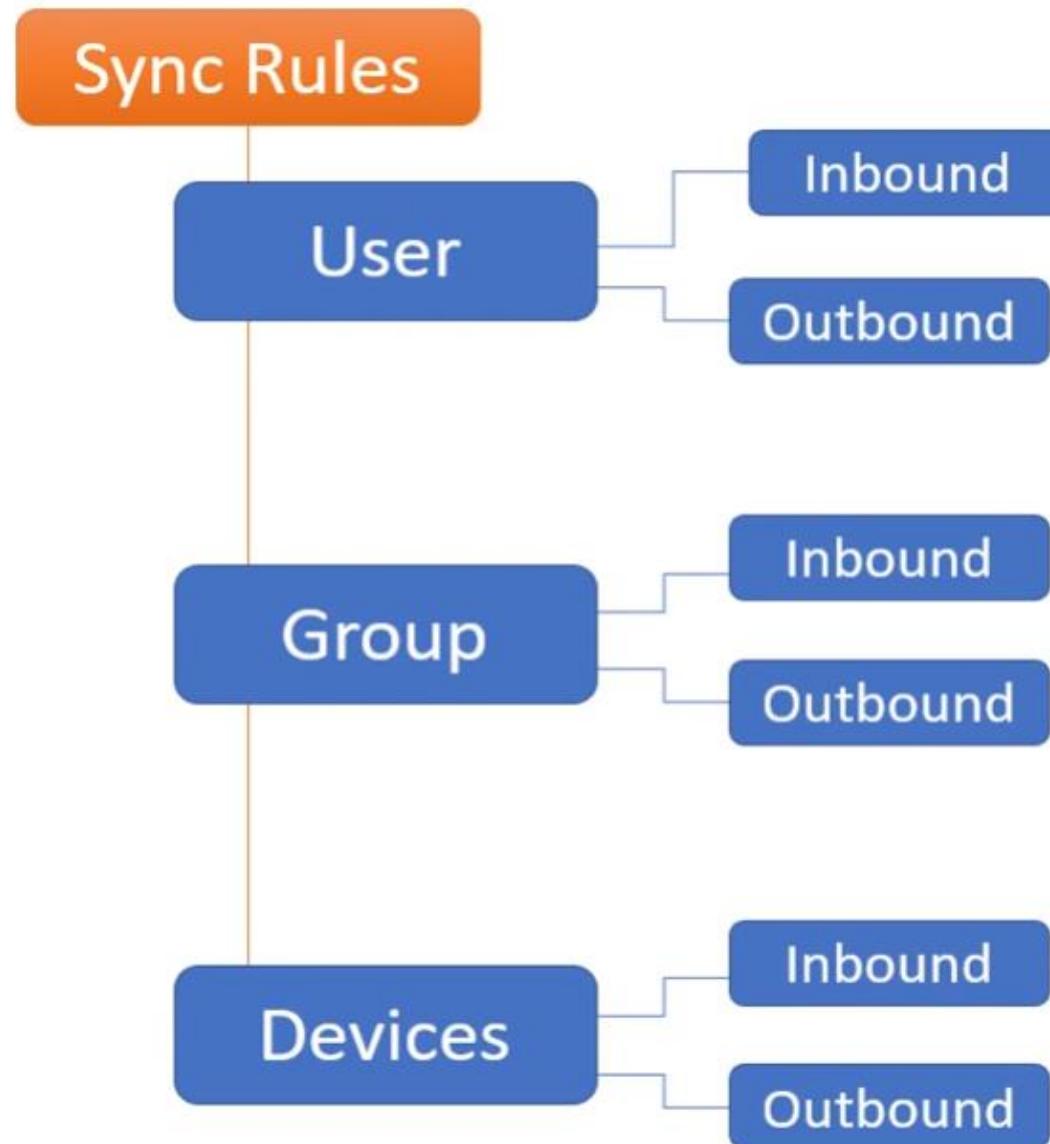
Attributes
AccountName
UserPrincipalName
AccountEnabled
SourceAnchor
DisplayName
EmployeeID

### Azure AD Connector Space

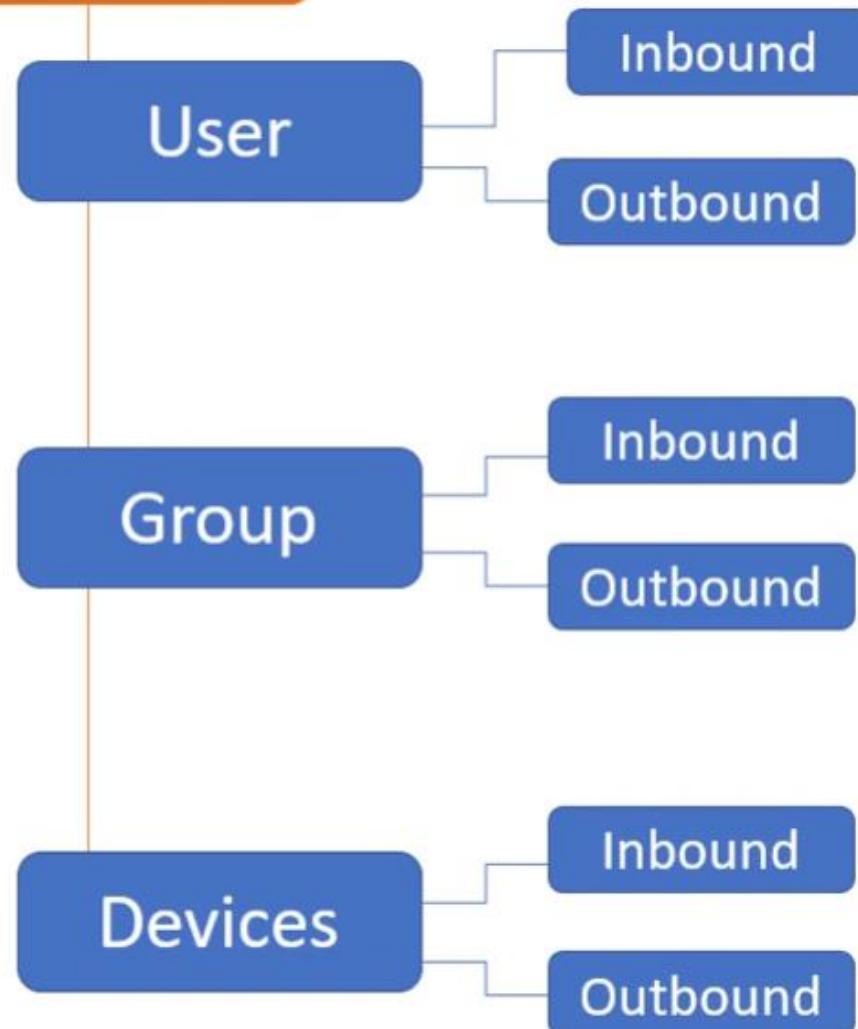


Attributes
AccountName
UserPrincipalName
AccountEnabled
SourceAnchor
DisplayName
EmployeeID





## Sync Rules



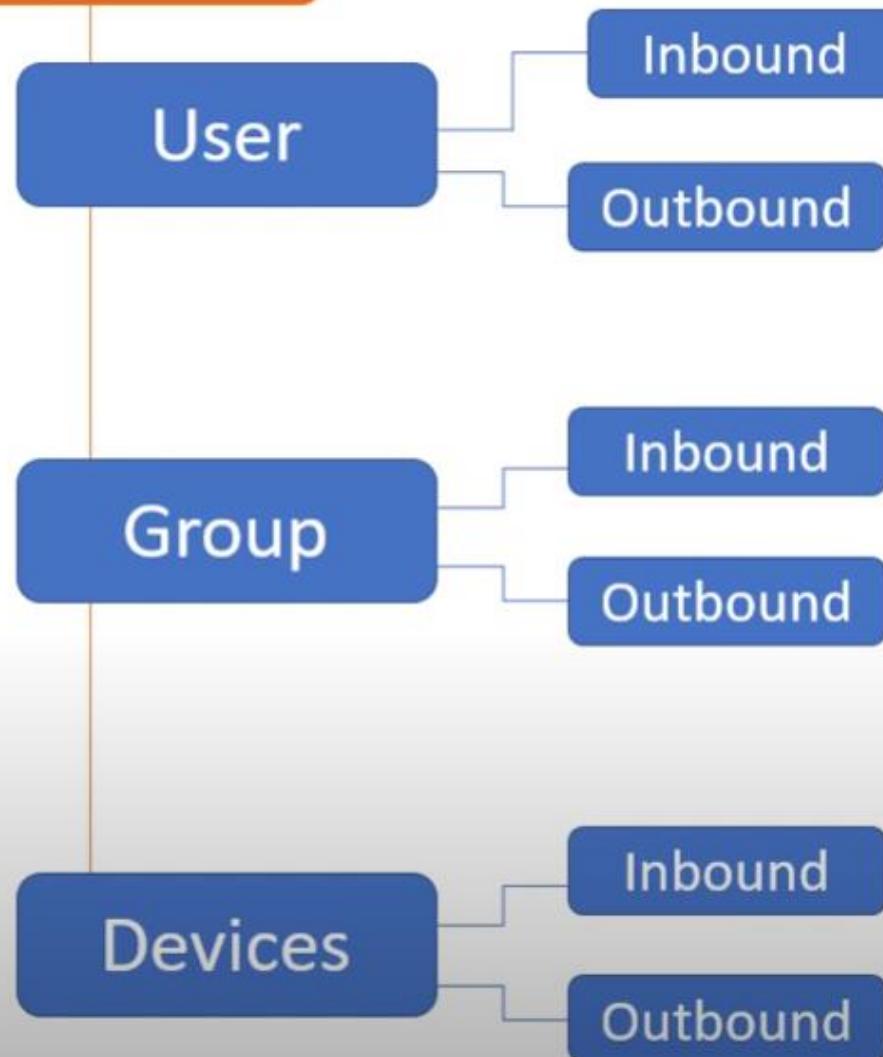
AD connector Space

In from AD - User

AAD connector Space

In from AAD - User

## Sync Rules



AD connector Space

In from AD - User

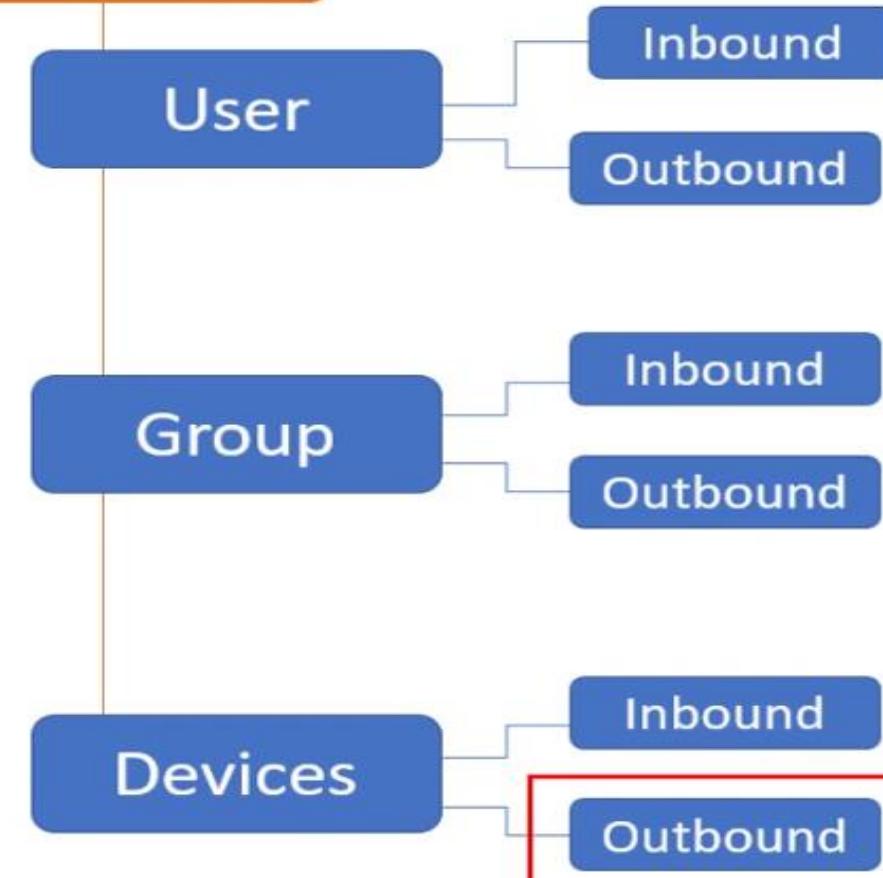
Out to AD - User

AAD connector Space

In from AAD - User

Out to AAD - User

## Sync Rules



### AD connector Space

In from AD - User

Out to AD - User

In from AD - Group

Out to AD - Group

In from AD - Computer

Out to AD - Device

### AAD connector Space

In from AAD - User

Out to AAD - User

In from AAD - Group

Out to AAD - Group

In from AAD - Device

Out to AAD - Device

```
PS C:\Users\Administrator> Get-ADSyncScheduler
```

```
AllowedSyncCycleInterval          : 00:30:00
CurrentlyEffectiveSyncCycleInterval : 00:30:00
CustomizedSyncCycleInterval       :
NextSyncCyclePolicyType          : Delta
NextSyncCycleStartTimeInUTC       : 4/16/2020 1:22:58 PM
PurgeRunHistoryInterval          : 7.00:00:00
SyncCycleEnabled                 : True
MaintenanceEnabled               : True
StagingModeEnabled               : False
SchedulerSuspended               : False
SyncCycleInProgress              : False
```

```
PS C:\Users\Administrator> Start-ADSyncSyncCycle -PolicyType Delta
```

```
Result
```

```
-----
```

```
Success
```

```
PS C:\Users\Administrator> Start-ADSyncSyncCycle -PolicyType Initial.
```

## View and manage your synchronization rules

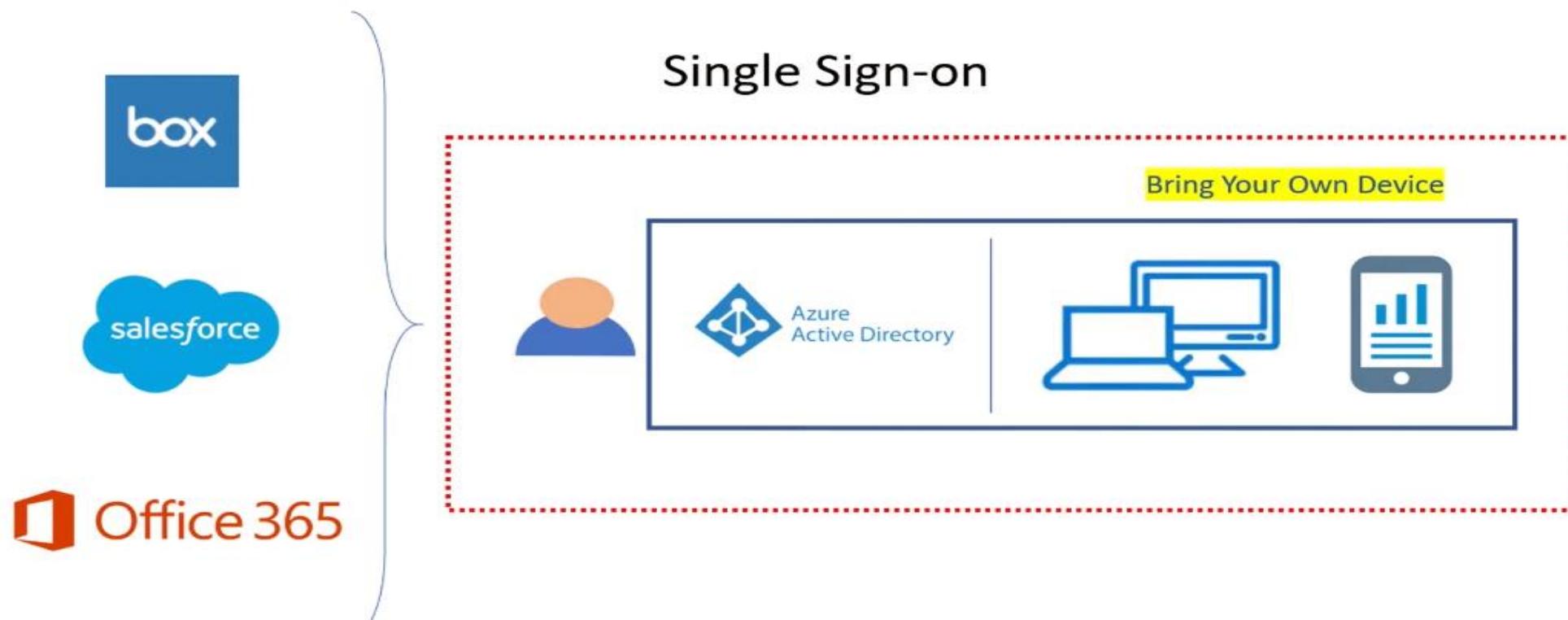
Direction:	MV Object Type:	Connector:	Connector Object Type:	Disabled:	
Outbound				*	<a href="#">Add new rule</a>
Password Sync:	MV attribute:		Connector Attribute:	Rule Type:	
*					
Name	Connector	Precedence	Connector Object Type	Metaverse Object Type	
Out to AAD - User Join	paddylearninmylab.onmicrosoft.com -	115	user	person	
Out to AAD - User Identity	paddylearninmylab.onmicrosoft.com -	116	user	person	
Out to AAD - User ExchangeOnline	paddylearninmylab.onmicrosoft.com -	117	user	person	
Out to AAD - User DynamicsCRM	paddylearninmylab.onmicrosoft.com -	118	user	person	
Out to AAD - User Intune	paddylearninmylab.onmicrosoft.com -	119	user	person	
Out to AAD - User LyncOnline	paddylearninmylab.onmicrosoft.com -	120	user	person	
Out to AAD - User SharePointOnline	paddylearninmylab.onmicrosoft.com -	121	user	person	
Out to AAD - User AzureRMS	paddylearninmylab.onmicrosoft.com -	122	user	person	
Out to AAD - Contact Join	paddylearninmylab.onmicrosoft.com -	123	contact	person	
Out to AAD - Contact Identity	paddylearninmylab.onmicrosoft.com -	124	contact	person	
Out to AAD - Contact ExchangeOnline	paddylearninmylab.onmicrosoft.com -	125	contact	person	
Out to AAD - Contact DynamicsCRM	paddylearninmylab.onmicrosoft.com -	126	contact	person	
Out to AAD - Contact Intune	paddylearninmylab.onmicrosoft.com -	127	contact	person	
Out to AAD - Contact LyncOnline	paddylearninmylab.onmicrosoft.com -	128	contact	person	
Out to AAD - Contact SharePointOnline	paddylearninmylab.onmicrosoft.com -	129	contact	person	
Out to AAD - Contact AzureRMS	paddylearninmylab.onmicrosoft.com -	130	contact	person	

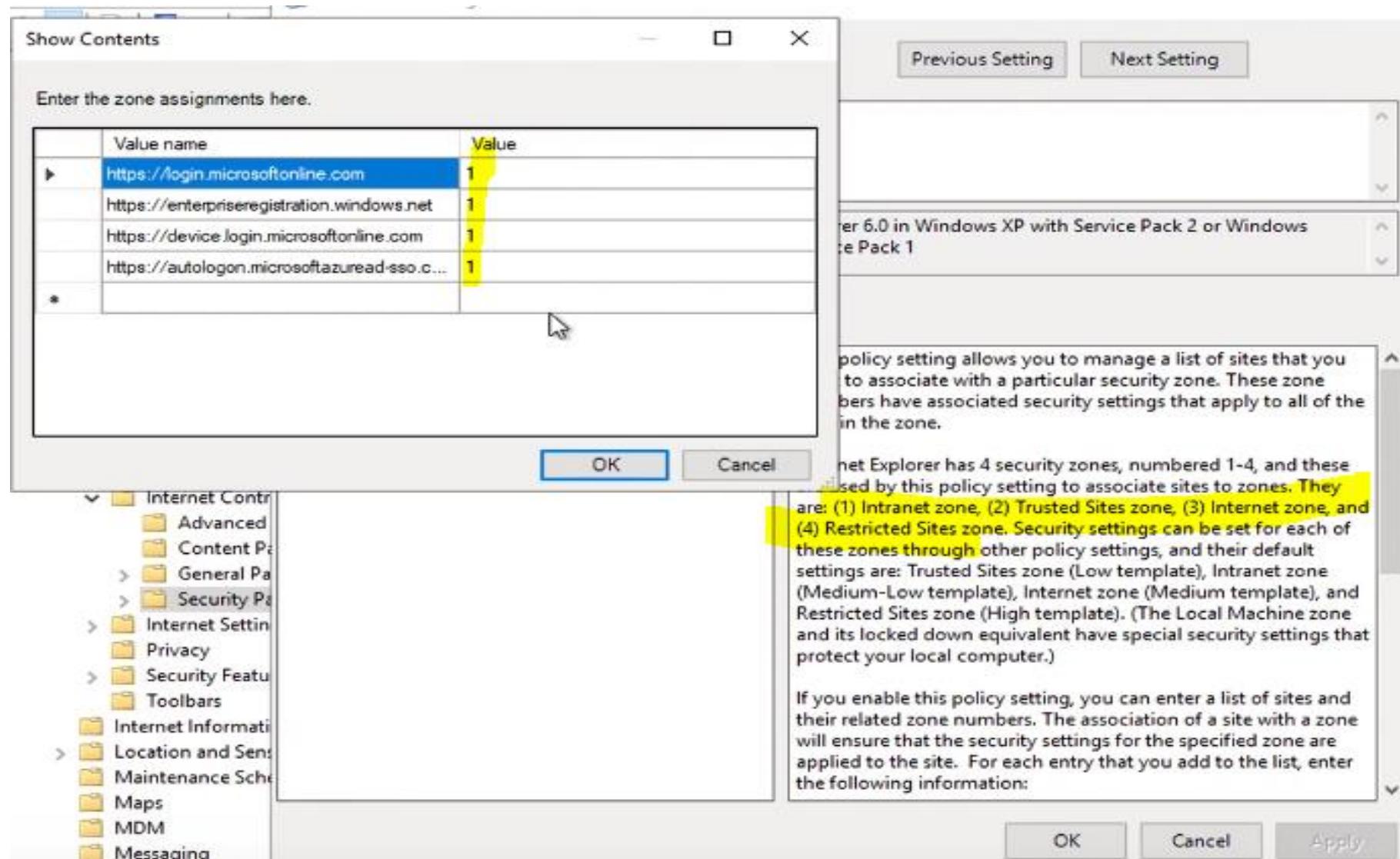
**Out to AAD - User Join**

Type:	Provision	Scoping filters	5
Transformations:	11	Join rules	1
Disabled:	False		

[Disable](#) [View](#) [Edit](#) [Export](#) [Delete](#)

## Personal Device





# Personal Device



Register a Device In Azure Active Directory

OR

Join the device to Azure Active Directory

## Personal Device



### User Experience

**Single Sign on will be enabled on  
Azure AD registered and Azure AD  
Joined Devices**

### Administration

**A Device Identity is created which  
can be manage from Azure Portal**

Managing Devices

Device Identities

Device based Conditional Access

Device  
Management is  
the foundation of  
device based  
conditional Access



## Types of Devices in Azure Active Directory

Azure AD Registered	Azure AD joined	Hybrid Azure AD joined Devices
Personal Email or Local Accounts	Azure AD Accounts	Azure AD accounts - Devices are domain joined as well as Azure AD joined
Windows 10, IOS, Android, MAC OS	This applies only to Windows 10	Windows 7,8 ,10 Windows server 2008 or newer



# Microsoft Azure Multi-Factor Authentication

# What is multi-factor authentication?

Any two or more of the following factors:

Something you know: a password or PIN.

Something you have: a phone, credit card or hardware token.

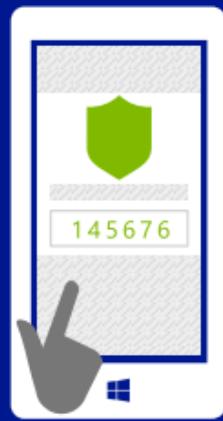
Something you are: a fingerprint, retinal scan or other biometric.

Stronger when using two different channels (out-of-band).



# How It Works

Mobile apps



Phone calls



Text messages



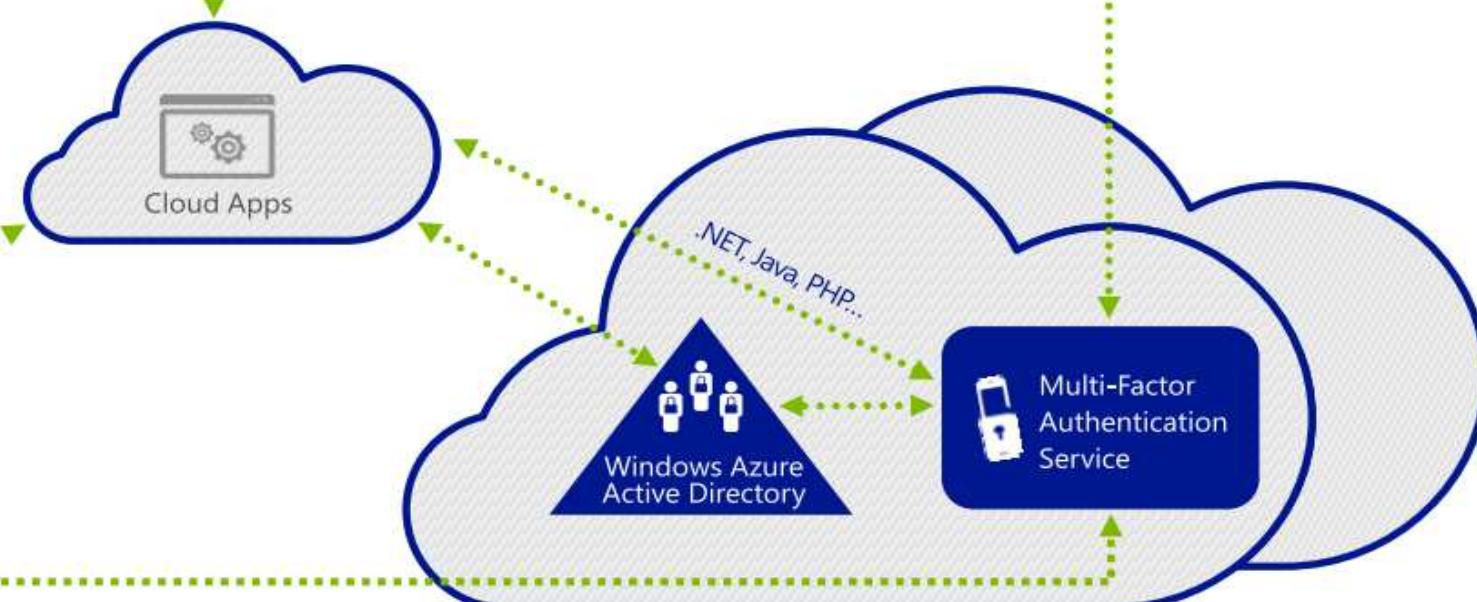
1

Users sign in from any device using their existing username/password.



2

Users must also authenticate using their phone or mobile device before access is granted.



Employees



Convenience



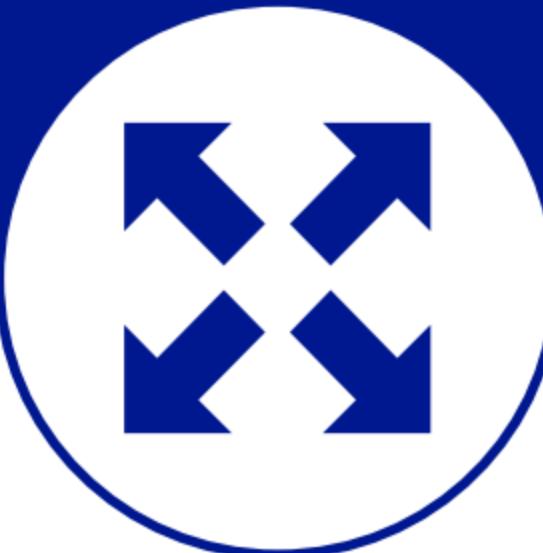
Partners



Customers



Scale



Security



## Convenience



No devices or certificates to purchase, provision, and maintain



No end user training is required



Users replace their own lost or broken phones

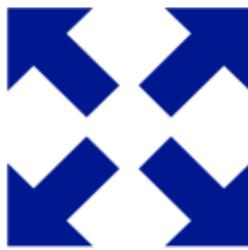


Users manage their own authentication methods and phone numbers



Integrates with existing directory for centralized user management and automated enrollment

# Scale



Works with all leading on-premises applications



Supports ADFS and SAML-based apps for federation to the cloud



Built into Windows Azure Active Directory for use with cloud apps



SDK for integration with custom apps and directories



Reliable, scalable service supports high-volume, mission-critical scenarios

# Security



Strong multi-factor authentication



Real-Time Fraud Alert



PIN option



Reporting and logging for auditing



Enables compliance with NIST 800-63 Level 3, HIPAA, PCI DSS, and other regulatory requirements

# Azure Cloud MFA

# MFA Server

## Conditional Access

Conditional access is automated access control that strengthens user sign-in and access to cloud applications.

Overview

Access Policies

Best practices

Deployment

Who,What,Where  
and How

Dos and Don'ts

# Overview

Not alternative for first-factor authentication  
Passwords are still required.

## Common scenarios

### Sign-in risk

Bad *actor* detection (e.g. leaked credentials)  
When you need more information  
Require MFA  
Block specific applications if unable to obtain proof

### Location

On-premises (named locations) or from Internet  
Countries and regions  
Trusted IPs

### Device Management

What device are you using?

- Corporate owned devices
- BYOD

### Client application

## Conditional Access Policies in Azure AD

**Users and user groups:** to reduce the risk of sensitive data leakage, define which users or groups of users can access applications or resources, paying particular attention to the highly sensitive information sources such as human resources or financial data.

**Connection risk:** Machine Learning algorithms in Azure AD evaluate each connection and give it a low, medium, or high risk score based on the probability that someone other than the legitimate owner of the account is attempting to connect. Anyone with a medium risk must be challenged with multi-factor authentication (MFA) when connecting. If the connection is high risk, access must be blocked. This condition requires Azure AD Identity Protection (see below).

**Location:** a location can be risky if it is a country with limited security policies or if the wireless network is unsecured or simply because it is not a place where the organization usually has activities. You can change the access requirements for connections from locations that are not on a list of safe IP addresses or that are risky for other reasons. Users accessing a service when they are outside the corporate network must be forced to use multi-factor authentication.

**Device platform:** for this condition, you can define a policy for each device platform that blocks access, requires for example compliance with Microsoft Intune, or requires that the device be joined to the domain.

**Device status:** you can use this condition to set policies for devices that are not managed by your organization.

**Client applications:** users can access many applications using different client application types, such as Web applications, mobile applications, or office productivity applications. You can enforce security policies if an access attempt is made by using a client application type that causes known issues, or you can require that only managed devices access certain types of applications.

**Cloud applications:** this condition specifies unique policies for sensitive applications. For example, you can require that HR applications such as Workday be blocked if Azure AD detects a risky connection or if a user tries to access it with an unmanaged device.

# Access Policies

When this Happens

Who are you? Based on

- User/group membership
- What are you accessing?
  - Required: User and Application
  - Others: location, sign-in risk

Do this

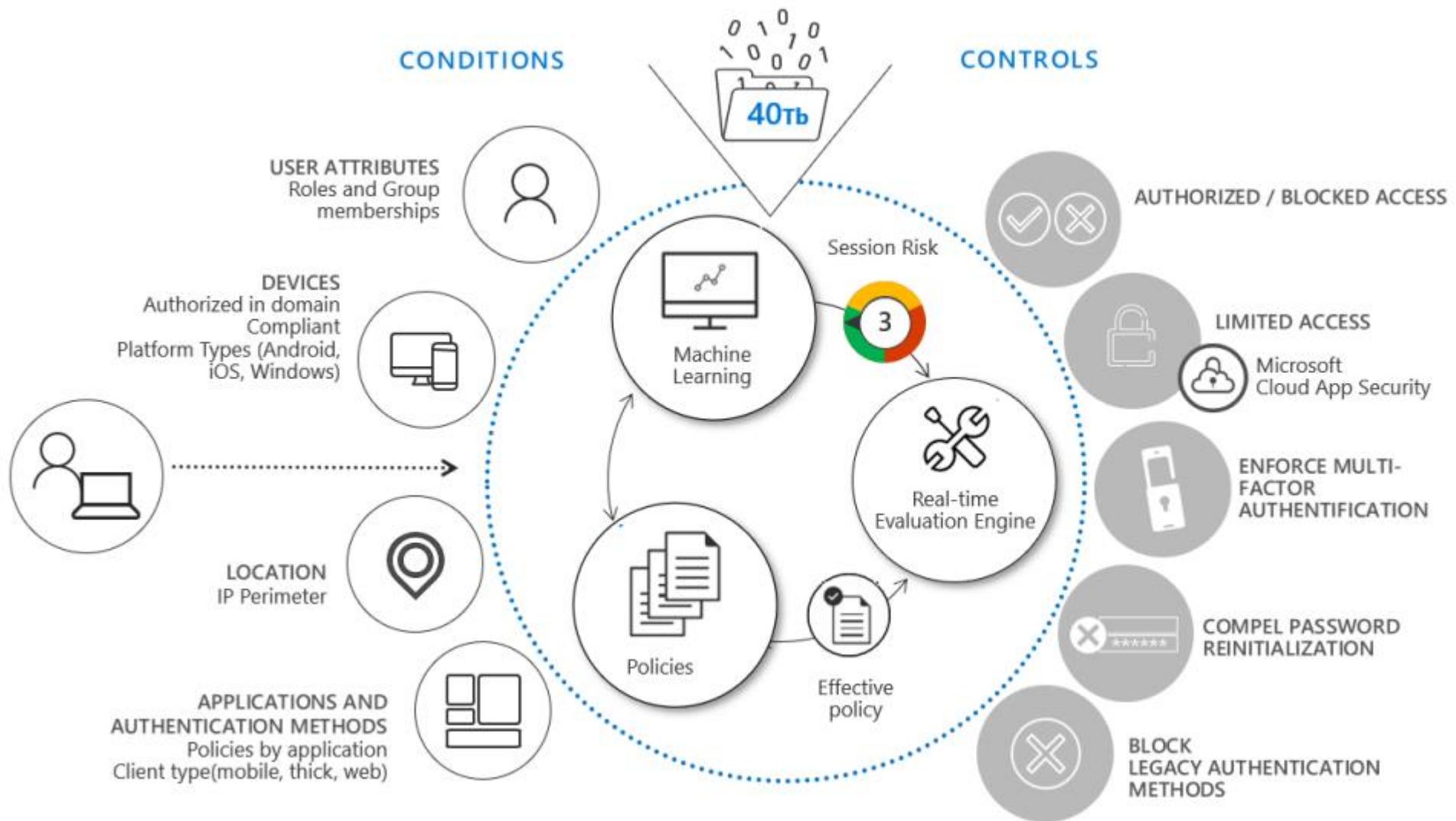
Access control (In order to Gain Access, you must)  
Grant Access

- Use MFA
- Use a compliant device
- Use a hybrid-joined device
- Use an approved client app
  - Outlook App not Gmail App

Session controls

- Limited experience within a cloud app.

# Conditional Access Policies in Azure AD



### Do Not:

Configure For all users or for all cloud applications:

- Block access
- Require compliant device
- Require domain join
- Require app protection policy
- For all users, all cloud apps, and all device platforms
  - Block access
    - This configuration blocks your entire organization, which is definitely not a good idea.

### Do's:

- Use the What-If tool to test policies
- Pilot access using groups
- Don't start with everyone
- Have exclusions for admin personnel
  - Being locked out of Admin Portal is bad

# Conditional Access Policies in Azure AD

New

X

Grant

□

X

 Info

\* Name

Example: 'Device compliance app policy'

## Assignments

Users and groups 

>

Specific users included

Cloud apps 

>

2 apps included

Conditions 

>

1 condition selected

## Access controls

Grant 

>

0 controls selected

Session 

>

0 controls selected

## Enable policy

On

Off

Select

Select the controls to be enforced.

Block access

Grant access

Require multi-factor authentication 

Require device to be marked as compliant 

Require Hybrid Azure AD joined device 

Require approved client app   
[See list of approved client apps](#)

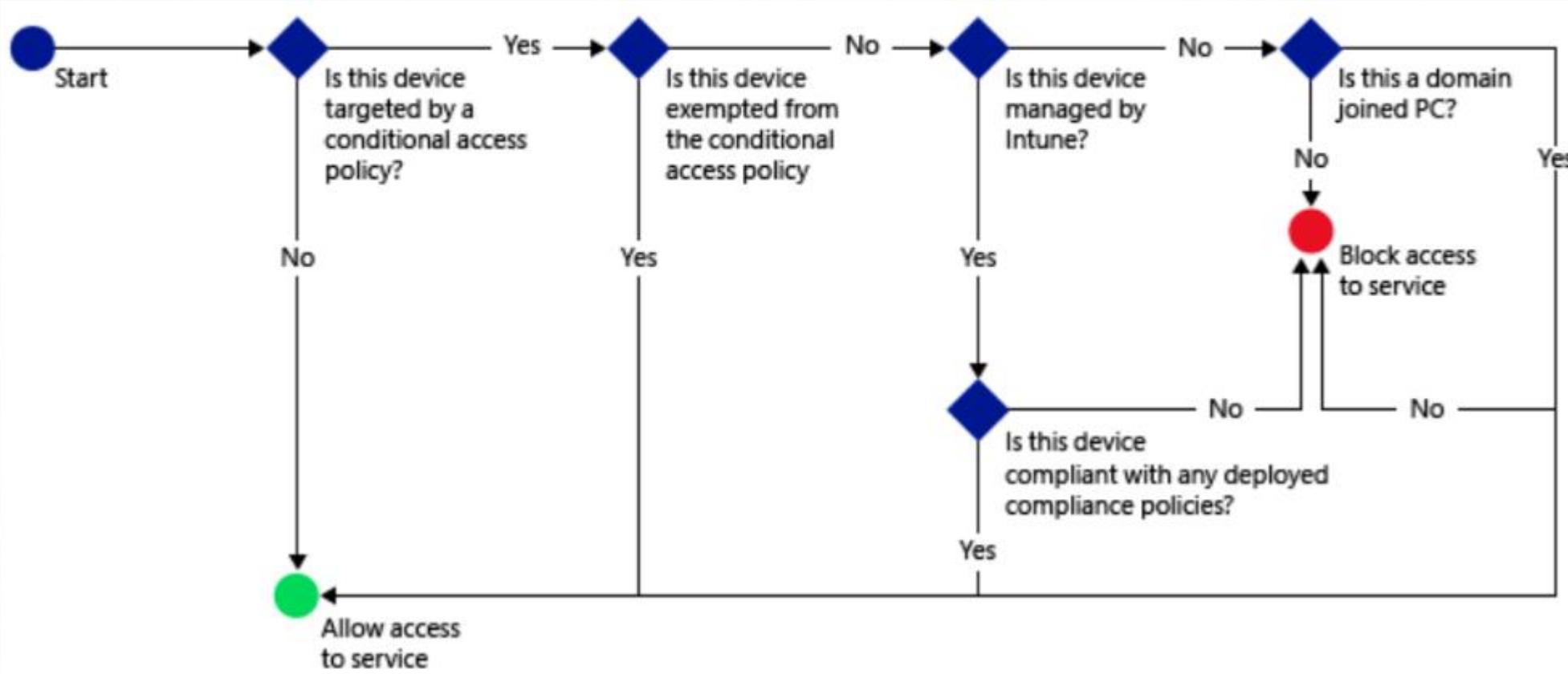
Require app protection policy (preview)   
[See list of policy protected client apps](#)

For multiple controls

Require all the selected controls

Require one of the selected controls

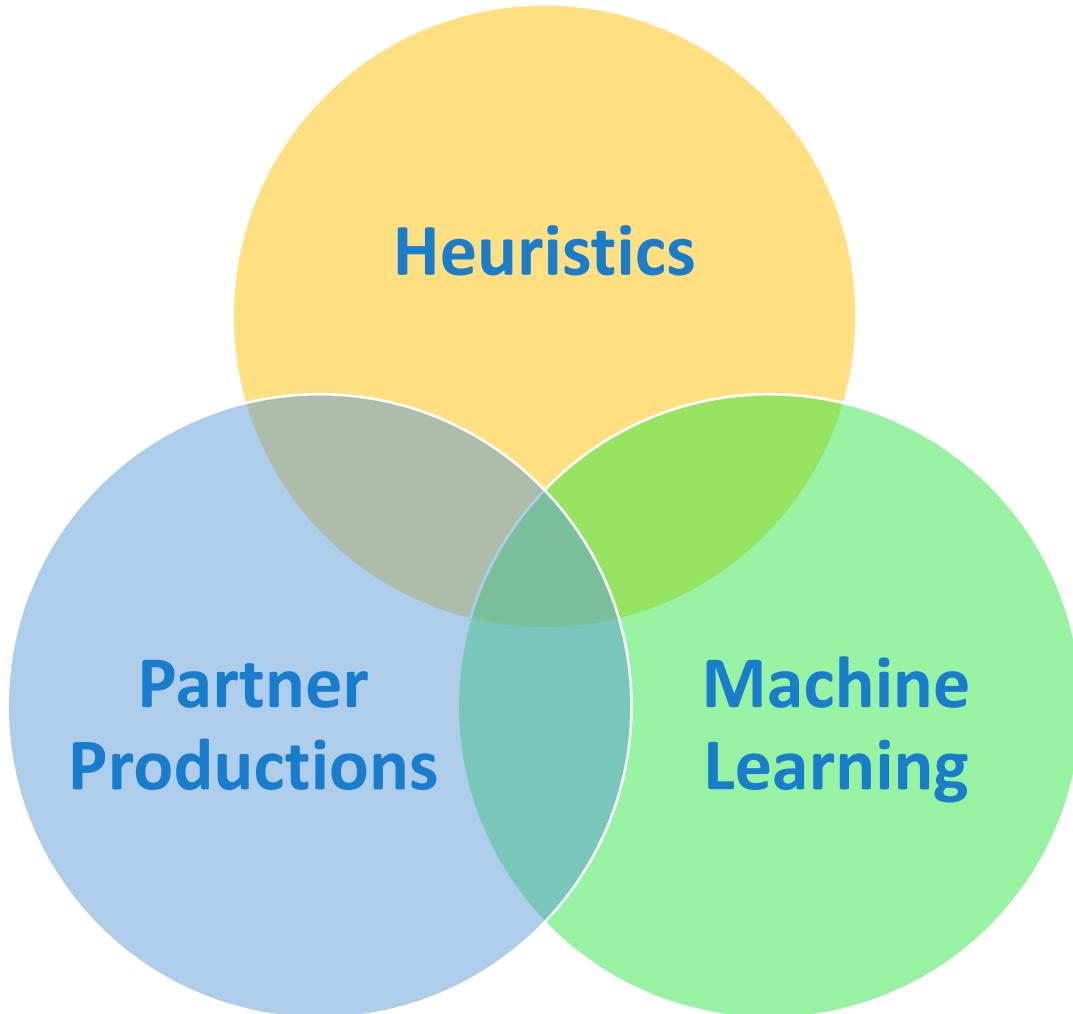
# Conditional access provides access to a service if a device meets specific criteria



# Azure AD Identity Protection – AAD IP



# Azure AD Identity Protection - Detections



## Azure AD Identity Protection – Risk Types

1. User Risk – Probability an identity is compromised
2. Sign-in Risk – Probability a sign-in is compromised
  - Real-time – Based on only real-time detections
  - Aggregate – Based on all detections (Real-time and non real-time)

1. Balance Security and Productivity
2. Reduce time to respond
3. Reduce HelDesk Cost
4. Reduce the volume of Risk data to be dealt Manually

# User Interface

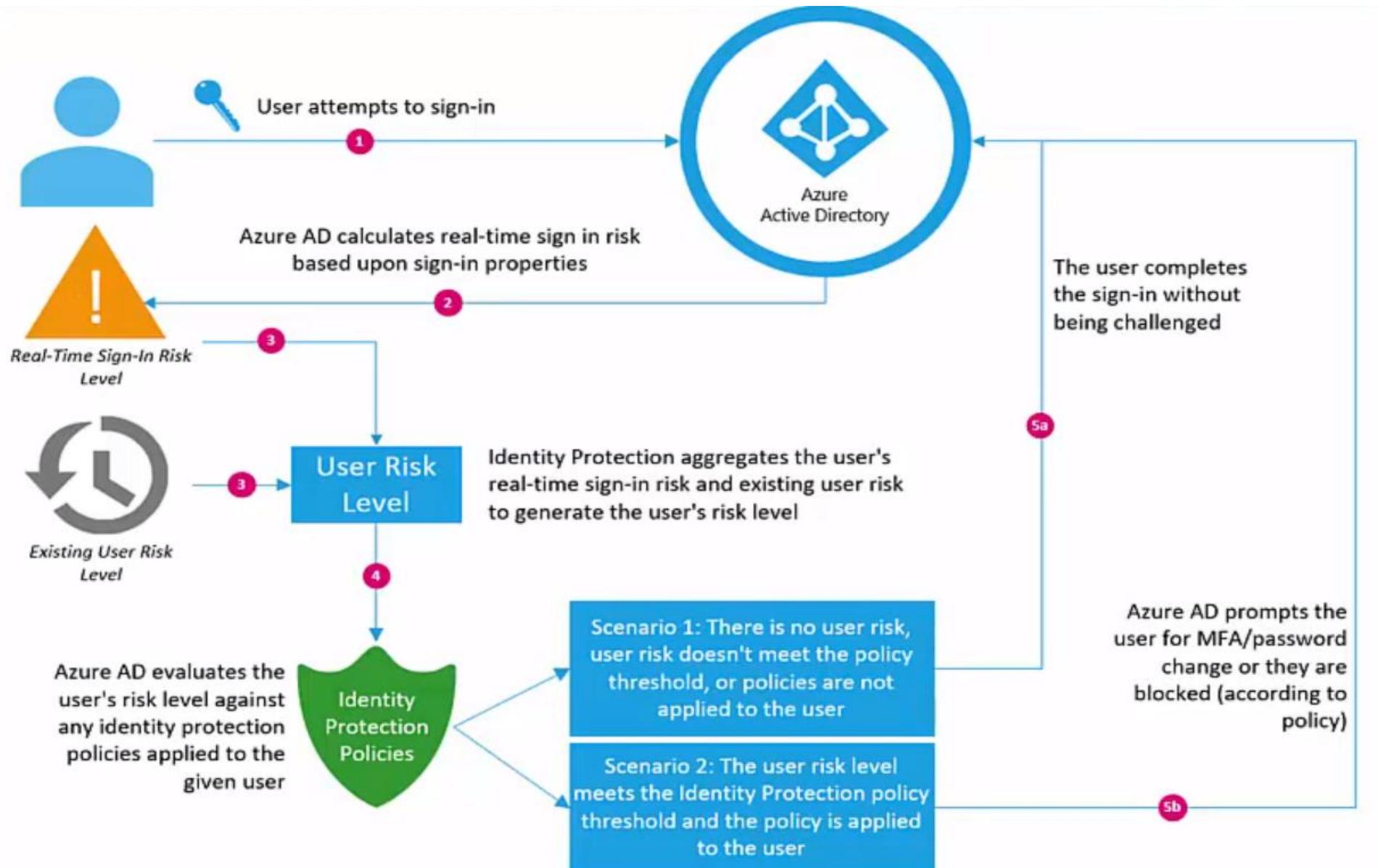
Simplified Risk for  
IT admins

Integration with  
the Sign-in Report

Risk Insights and  
recommendations

Immediate  
protection with risk  
feedback

We can perform  
actions like filter,  
Sorting, Bulk  
Actions



Risky users

User

Sign-ins

Sign-in s1

Sign-in s2

**Detections**

Risk event  
re1

Risk event  
re2

Risk event  
re3

Risk event  
re4

## Azure AD Identity Protection - Product-wide alignment

Entities that matter most	Policies?	Reports?	Public APIs?	Enhanced ML?
Risky users	✓ User risk policy	✓ Risky users report	✓ RiskyUsers API	✓
Risky sign-ins	✓ Sign-in risk policy	✓ Risky sign-ins report	✓ Sign-ins API (with risk info)	✓

## Permissions

Identity Protection requires users be a Security Reader, Security Operator, Security Administrator, Global Reader, or Global Administrator in order to access.

Role	Can do	Can't do
Global administrator	Full access to Identity Protection	
Security administrator	Full access to Identity Protection	Reset password for a user
Security operator	<p>View all Identity Protection reports and Overview blade</p> <p>Dismiss user risk, confirm safe sign-in, confirm compromise</p>	<p>Configure or change policies</p> <p>Reset password for a user</p> <p>Configure alerts</p>
Security reader	<p>View all Identity Protection reports and Overview blade</p>	<p>Configure or change policies</p> <p>Reset password for a user</p> <p>Configure alerts</p> <p>Give feedback on detections</p>

# License requirements

Using this feature requires an Azure AD Premium P2 license. To find the right license for your requirements, see [Comparing generally available features of the Free, Basic, and Premium editions](#).

Capability	Details	Azure AD Premium P2	Azure AD Premium P1	Azure AD Basic/Free
Risk policies	User risk policy (via Identity Protection)	Yes	No	No
Risk policies	Sign-in risk policy (via Identity Protection or Conditional Access)	Yes	No	No
Security reports	Overview	Yes	No	No
Security reports	Risky users	Full access	Limited Information	Limited Information
Security reports	Risky sign-ins	Full access	Limited Information	Limited Information
Security reports	Risk detections	Full access	Limited Information	No
Notifications	Users at risk detected alerts	Yes	No	No
Notifications	Weekly digest	Yes	No	No
	MFA registration policy	Yes	No	No



Azure AD Identity Protection

# Privileged Identity Management (PIM)

Requires an Azure AD Premium P2 license

Azure Active Directory (Azure AD) Privileged Identity Management (PIM) is a service that enables you to manage, control, and monitor access to important resources in your organization. These resources include resources in Azure AD, Azure, and other Microsoft Online Services like Office 365 or Microsoft Intune.

# | Privileged Identity Management (PIM) |



- Exchange Admin
- SharePoint Admin



- Backup Contributor
- Website Contributor



- Global Admin
- Security Admin
- Intune Admin

# Privileged Identity Management (PIM)

- No Need of Granting **Permanent Access** for Resources
- You can make users **Eligible** for privileged access
- JUST-IN-TIME (JIT) ➔ You can define the **time frame** for which the users will get the access
- You will also get notifications as well as you can also monitor all the roles getting assigned in your enterprise

## Reasons to use

# Privileged Identity Management (PIM)



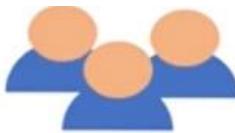
- Exchange Admin
- SharePoint Admin



Users Will always have **PERMANENT** Access to the resources



- Backup Contributor
- Website Contributor



Possibility of **Stale Entries** of Privileged access



- Global Admin
- Security Admin
- Intune Admin



Other admins never **Notified** about the **Changes**

## What does it do?

- Provide **just-in-time** privileged access to Azure AD and Azure resources
- Assign **time-bound** access to resources using start and end dates
- Require **approval** to activate privileged roles
- Enforce **multi-factor authentication** to activate any role
- Use **justification** to understand why users activate
- Get **notifications** when privileged roles are activated
- Conduct **access reviews** to ensure users still need roles
- Download **audit history** for internal or external audit

## Scenarios

### Privileged Role administrator permissions

- Enable approval for specific roles
- Specify approver users or groups to approve requests
- View request and approval history for all privileged roles

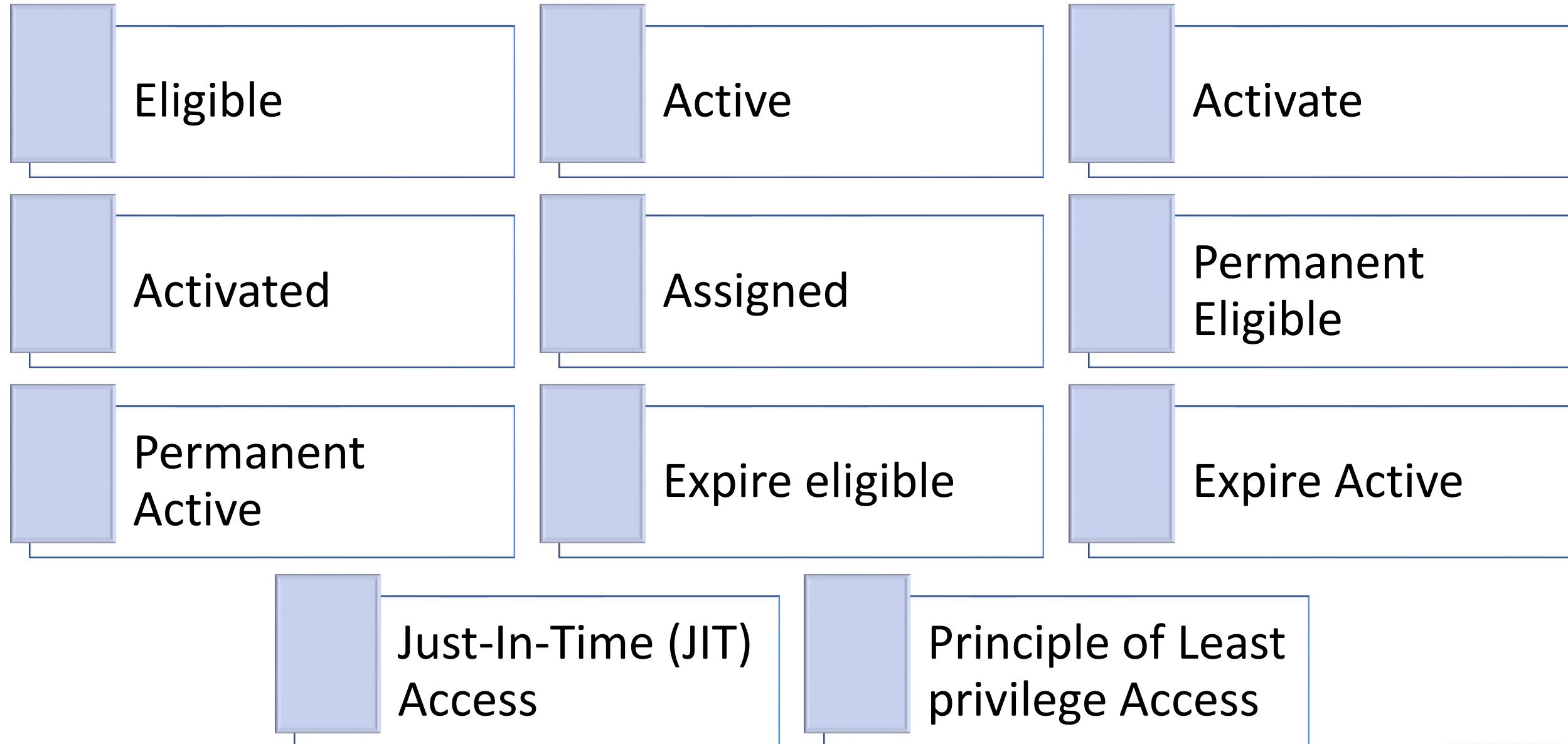
### Approver permissions

- View pending approvals (requests)
- Approve or reject requests for role elevation (single and bulk)
- Provide justification for my approval or rejection

### Eligible role user permissions

- Request activation of a role that requires approval
- View the status of your request to activate
- Complete your task in Azure AD if activation was approved

# Privileged Identity Management (PIM)



Azure AD roles - Quick start

https://portal.azure.com/#blade/Microsoft\_Azure\_PIM/DirectoryRoleManagement

Microsoft Azure

Search resources, services, and docs (G+ /)

Home > Privileged Identity Management - Quick start > Azure AD roles - Quick start

Azure AD roles - Quick start

1/128 Photography

Overview

Quick start

Sign up PIM for Azure AD R...

Tasks

My roles

My requests

Approve requests

Review access

Manage

Roles

Members

Alerts

Access reviews

Wizard

Settings

## Azure AD Privileged Identity Management

Azure AD PIM is a Premium feature that enables you to limit standing admin access to privileged roles and much more. [Learn more](#)

 **Assign**  
Assign users or current admins as eligible admins for specific Azure AD roles, so that they only have access when necessary

 **Activate**  
Activate your eligible admin roles so that you can get limit standing access to the privileged identity

 **Approve**  
View and approve all activation request for specific Azure AD roles that you are configured to approve

Assign eligibility

Activate your role

Approve requests

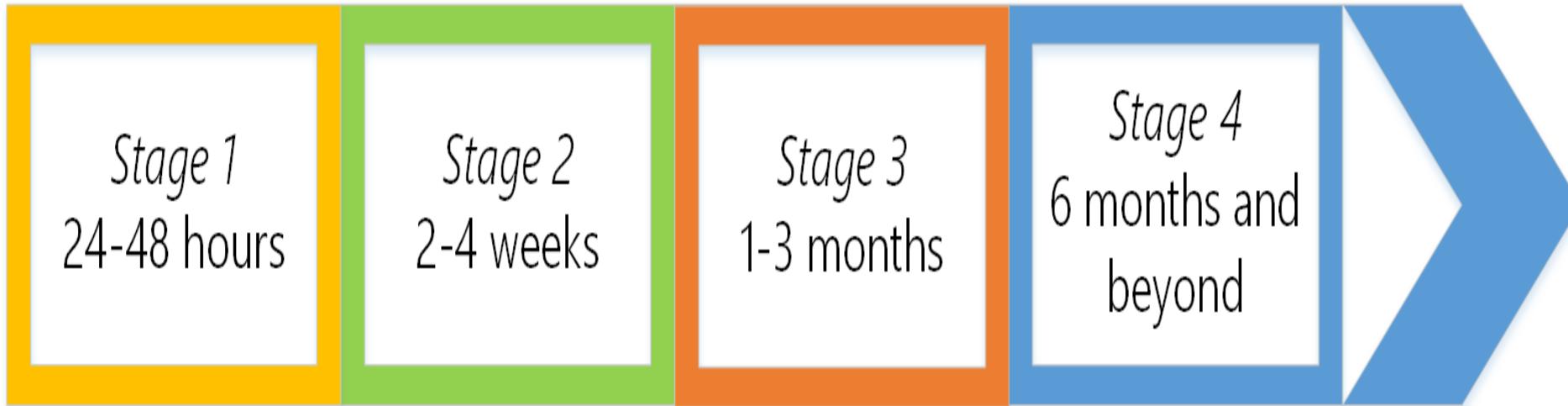


## **Roles you can't manage**

- Account Administrator
- Service Administrator
- Co-Administrator

**These are Classic subscription administrator roles**

## Deployment Path



- Stage 1 (24-48 hours): Critical items that Microsoft recommend you do right away
- Stage 2 (2-4 weeks): Mitigate the most frequently used attack techniques
- Stage 3 (1-3 months): Build visibility and build full control of admin activity
- Stage 4 (six months and beyond): Continue building defenses to further harden your security platform

Demo

End of PIM

# Azure Billing and Subscription Transfer

## Post Transfer tasks

- Key vault - Change Tenant ID on any Key vault
- Re-Enable any Managed Identities
- Re-Register Azure Stack
- All Resources will be online and not impact while transferring

## NETWORK SECURITY MICRO SEGMENTATION

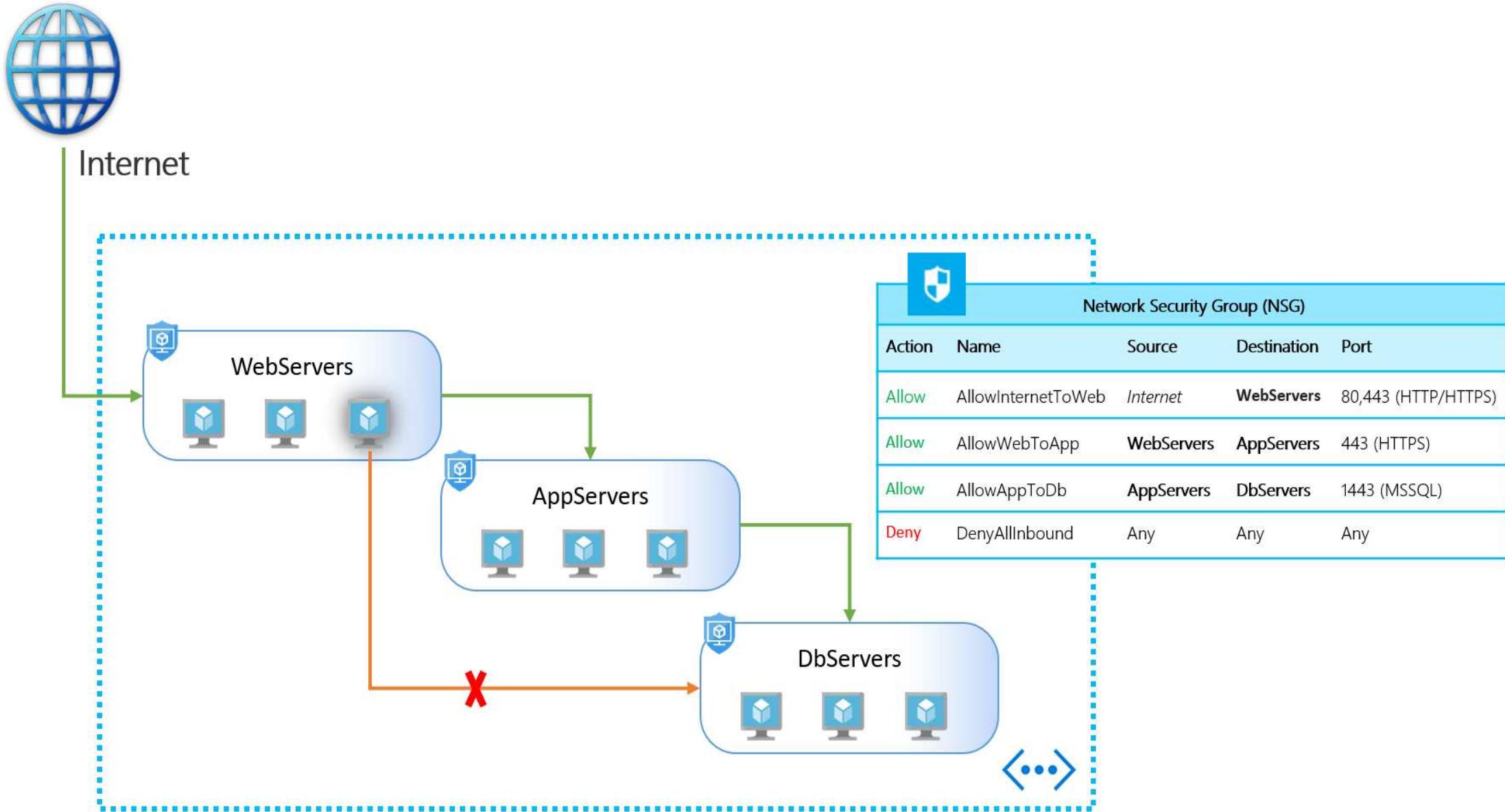
Application security groups enable you to configure network security as a natural extension of an application's structure, allowing you to group virtual machines and define network security policies based on those groups.

The platform handles the complexity of explicit IP addresses and multiple rule sets, allowing you to focus on your business logic.

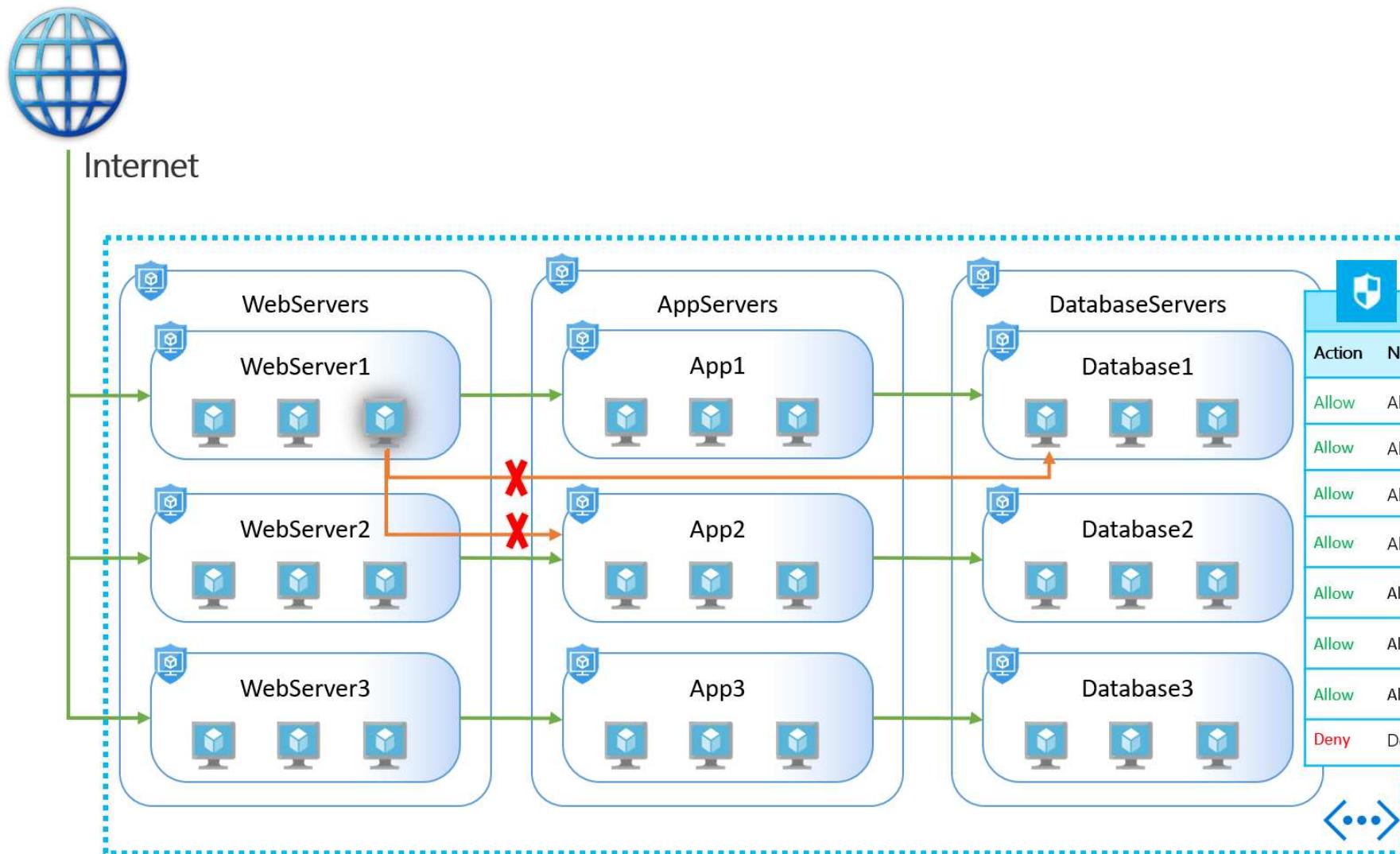
Implementing granular security traffic controls improves isolation of workloads and protects them individually.

If a breach occurs, this technique limits the potential impact of lateral exploration of your networks from hacker

# Application Security Group - ASG



# Application Security Group - ASG

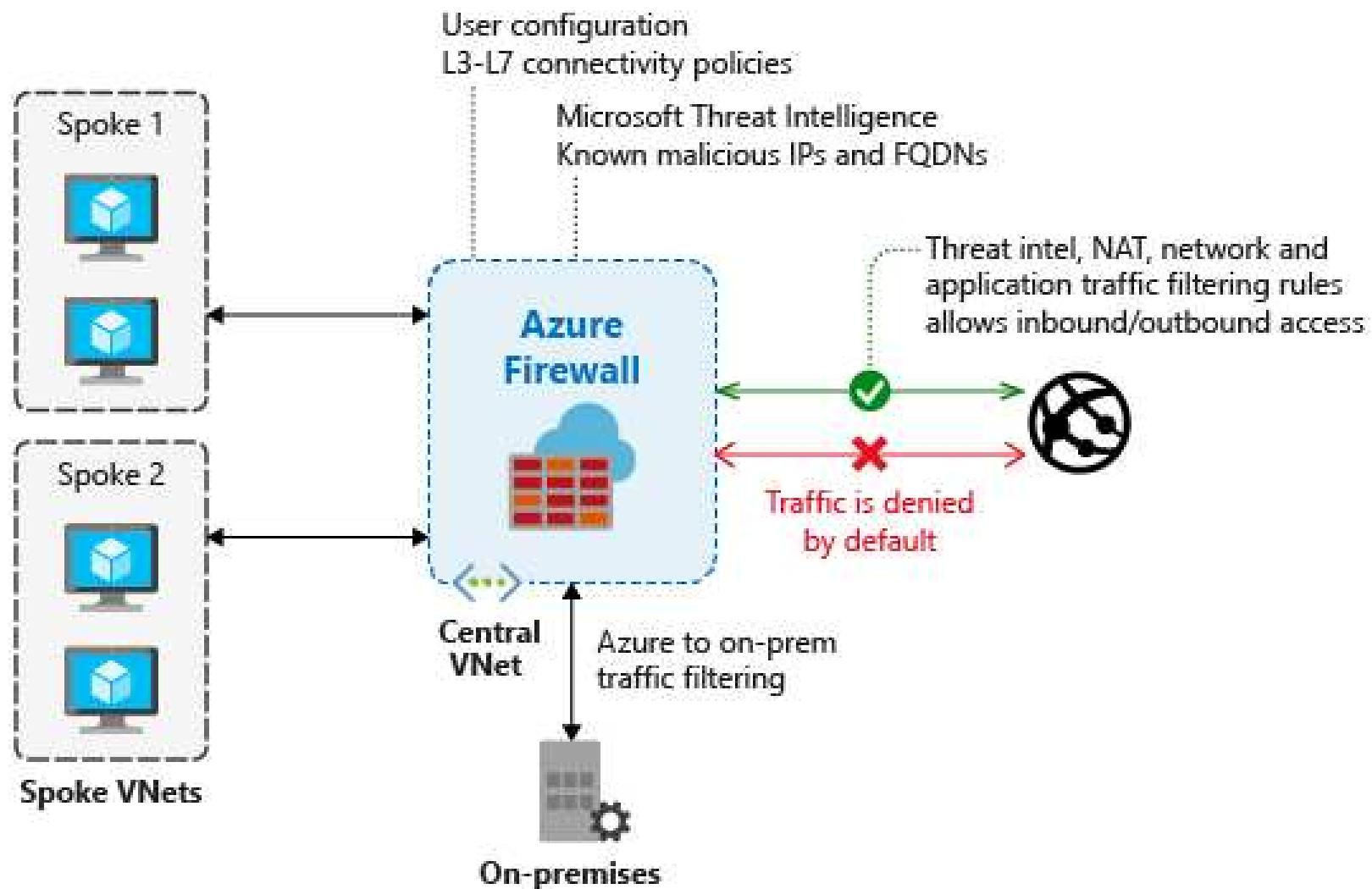


## Application security groups have the following constraints

- ✓ 3,000 per subscription
- ✓ You can specify one application security group as the source and destination in a security rule. You cannot specify multiple application security groups in the source or destination.
- ✓ All network interfaces assigned to an application security group have to exist in the same virtual network that the first network interface assigned to the application security group is in.
  - For example, if the first network interface assigned to an application security group named *AsgWeb* is in the virtual network named *VNet1*, then all subsequent network interfaces assigned to *ASGWeb* must exist in *VNet1*. You cannot add network interfaces from different virtual networks to the same application security group.
- ✓ If you specify an application security group as the source and destination in a security rule, the network interfaces in both application security groups must exist in the same virtual network.
  - For example, if *AsgLogic* contained network interfaces from *VNet1*, and *AsgDb* contained network interfaces from *VNet2*, you could not assign *AsgLogic* as the source and *AsgDb* as the destination in a rule. All network interfaces for both the source and destination application security groups need to exist in the same virtual network.

End of Application security groups

## Azure Firewall



## Azure Firewall

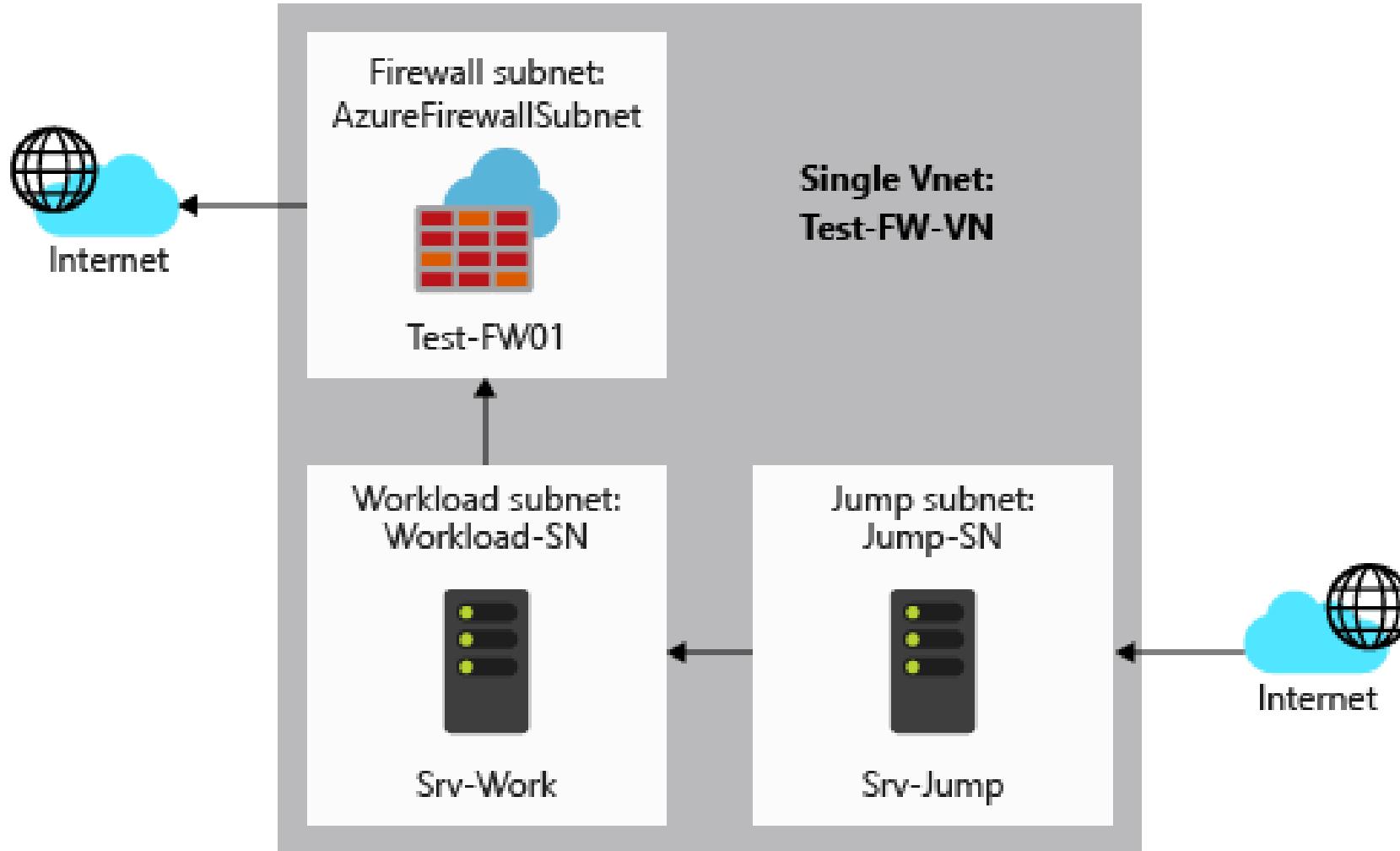
- ✓ *Azure Firewall as a service*
- ✓ Azure Firewall is a managed, cloud-based network security service that protects your Azure Virtual Network resources.
- ✓ It's a fully stateful firewall as a service with built-in high availability and unrestricted cloud scalability.
- ✓ You can centrally create, enforce, and log application and network connectivity policies across subscriptions and virtual networks
- ✓ Azure Firewall uses a static public IP address for your virtual network resources allowing outside firewalls to identify traffic originating from your virtual network.
- ✓ The service is fully integrated with Azure Monitor for logging and analytics.
- ✓ High availability is built in, so no additional load balancers are required and there's nothing you need to configure.
- ✓ Azure Firewall can be configured during deployment to span multiple Availability Zones for increased availability.
  - ✓ With Availability Zones, your availability increases to 99.99% uptime.
  - ✓ There's no additional cost for a firewall deployed in an Availability Zone.
  - ✓ However, there are additional costs for inbound and outbound data transfers associated with Availability Zones.
- ✓ For best performance, deploy one firewall per region.
- ✓ You can centrally create *allow* or *deny* network filtering rules by source and destination IP address, port, and protocol.
- ✓ FQDN tags make it easy for you to allow well-known Azure service network traffic through your firewall
- ✓ Service tags
- ✓ Threat intelligence
- ✓ Outbound SNAT support
- ✓ Inbound DNAT support

## Azure Firewall Limitations & known Issues

- Network filtering rules for non-TCP/UDP protocols (such as ICMP) don't work for Internet-bound traffic.
- You cannot move Azure Firewall to a different resource group or subscription.
- Limited port range
- No custom DNS Support. Only Azure DNS supported
- No SNAT/DNAT for private IP destinations

Know issues ➔ <https://docs.microsoft.com/en-us/azure/firewall/overview#known-issues>

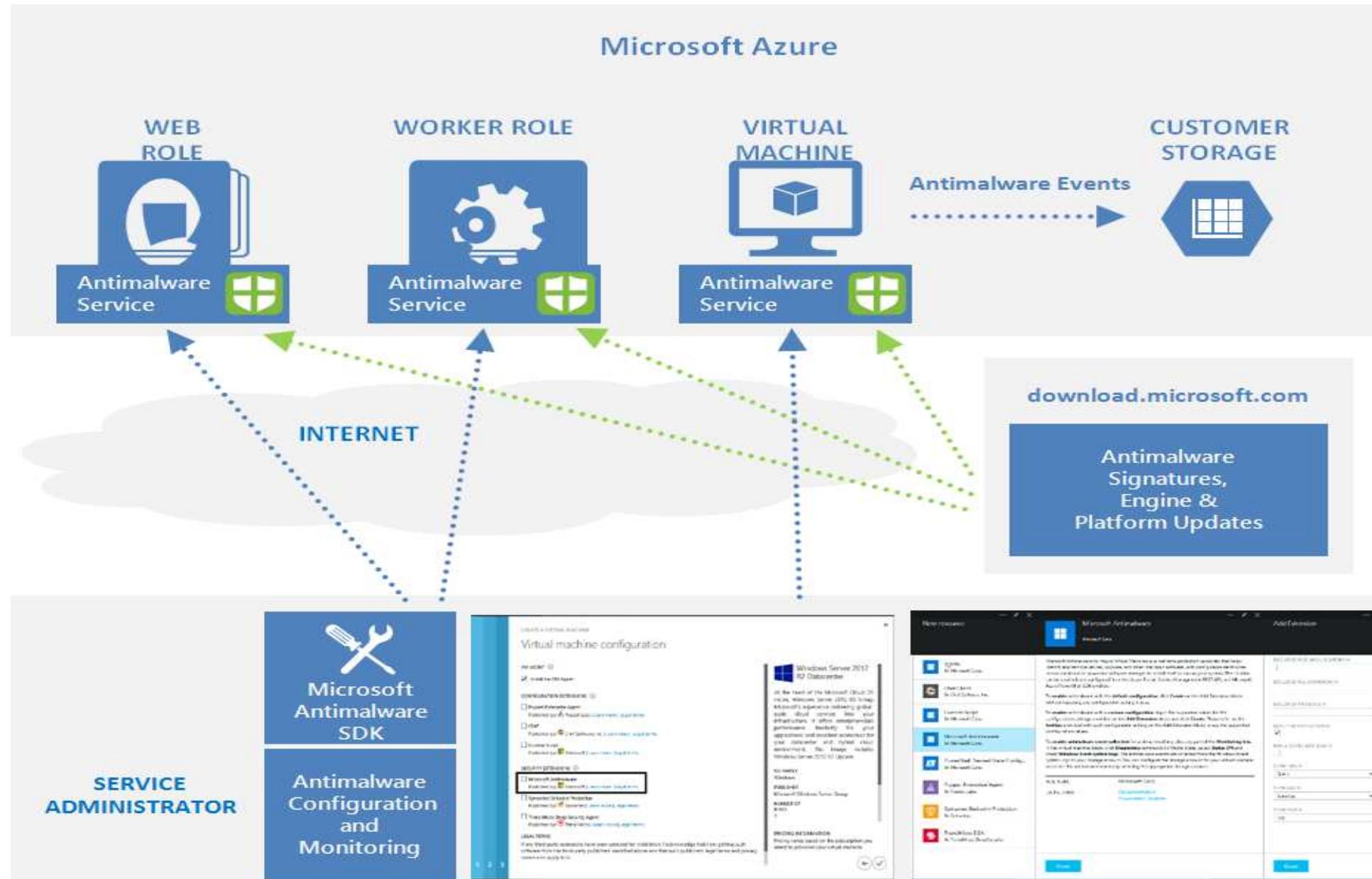
## Azure Firewall



## Microsoft Antimalware for Azure Cloud Services and Virtual Machines

- ✓ **Real-time protection** - monitors activity in Cloud Services and on Virtual Machines to detect and block malware execution.
- ✓ **Scheduled scanning** - Scans periodically to detect malware, including actively running programs.
- ✓ **Malware remediation** - automatically takes action on detected malware, such as deleting or quarantining malicious files and cleaning up malicious registry entries.
- ✓ **Signature updates** - automatically installs the latest protection signatures (virus definitions) to ensure protection is up-to-date on a pre-determined frequency.
- ✓ **Antimalware Engine updates** – automatically updates the Microsoft Antimalware engine.
- ✓ **Antimalware Platform updates** – automatically updates the Microsoft Antimalware platform.
- ✓ **Active protection** - reports telemetry metadata about detected threats and suspicious resources to Microsoft Azure to ensure rapid response to the evolving threat landscape, as well as enabling real-time synchronous signature delivery through the Microsoft Active Protection System (MAPS).
- ✓ **Samples reporting** - provides and reports samples to the Microsoft Antimalware service to help refine the service and enable troubleshooting.
- ✓ **Exclusions** – allows application and service administrators to configure exclusions for files, processes, and drives.
- ✓ **Antimalware event collection** - records the antimalware service health, suspicious activities, and remediation actions taken in the operating system event log and collects them into the customer's Azure Storage account.

# Microsoft Antimalware for Azure Cloud Services and Virtual Machines



Setting	Options	Default	Description
<b>Enable Antimalware</b>	true (lower case sensitive)	None	true - Enables the Antimalware service false – not supported <b>Note</b> – This is a required configuration setting to enable the Antimalware service
<b>Exclusions Extensions</b>	extension1, extension2, ... ...	None	List of file extensions to exclude from scanning. Example: gif, log, txt excludes files with the .gif, .log, or .txt extension from being scanned. Each excluded file extension should be added as a separate row element value in your antimalware XML configuration or semicolon separated in antimalware JSON configuration
<b>Exclusions Paths</b>	Path1, Path2 ... ...	None	List of paths to files or folders to exclude from scanning. Example: e:\approot\worker.dll, e:\approot\temp excludes the file worker.dll in the e:\approot folder and anything under the folder e:\approot\temp from being scanned. <b>Note:</b> For antimalware JSON configuration for virtual machines, use two backslashes (\\\) instead of one to escape properly. For example: e:\\approot\\worker.dll Each excluded path should be added as a separate row element value in your antimalware XML configuration or semicolon separated in antimalware JSON configuration
<b>Exclusions Processes</b>	process1, process2, ... ...	None	List of process exclusions. Any file opened by an excluded process will not be scanned (the process itself will still be scanned – to exclude the process itself, use the ExcludedPaths option). Example: C:\Program Files\MyApp.exe excludes any files opened by MyApp.exe from being scanned. Each excluded process should be added as a separate row element value in your antimalware XML configuration or semicolon separated in antimalware JSON configuration
<b>RealtimeProtectionEnabled</b>	true false (lower case sensitive)	true	true – Enables real-time protection false – Disables real-time protection Default = true when AntimalwareEnabled = true
<b>ScheduledScanSettings isEnabled</b>	true false (lower case sensitive)	false	Enables or disables a periodic scan for active malware on the system Default = false
<b>ScheduledScanSettings Day</b>	0 – 8	7	0 – scan daily, 1 – Sunday, 2 – Monday, 3 – Tuesday..., 7 – Saturday, 8 – disabled Default = 7 if only ScheduledScanSettings isEnabled = true
<b>ScheduledScanSettings Time</b>	0 – 1440	120	Hour at which to begin the scheduled scan. Measured in 60 minute increments from midnight 60 mins = 1:00 AM 120 mins = 2:00 AM ... 1380 mins = 11:00 PM Default = 120 mins if ScheduledScanSettings isEnabled = true
<b>ScheduledScanSettings Scan Type</b>	Quick/Full	Quick	Default = Quick if ScheduledScanSettings isEnabled = true
<b>Monitoring</b>	ON OFF	OFF	ON - Enable Antimalware event collection to user subscription storage using Azure Diagnostics extension OFF – Disable Antimalware event collection to user subscription storage by removing antimalware monitoring configuration in Azure Diagnostics extension if it was previously turned ON
<b>StorageAccountName</b>	Storage Account Name	None	Storage account name for your Azure store table to collect antimalware events in storage <b>Note</b> - Storage account name is required if monitoring is specified as ON

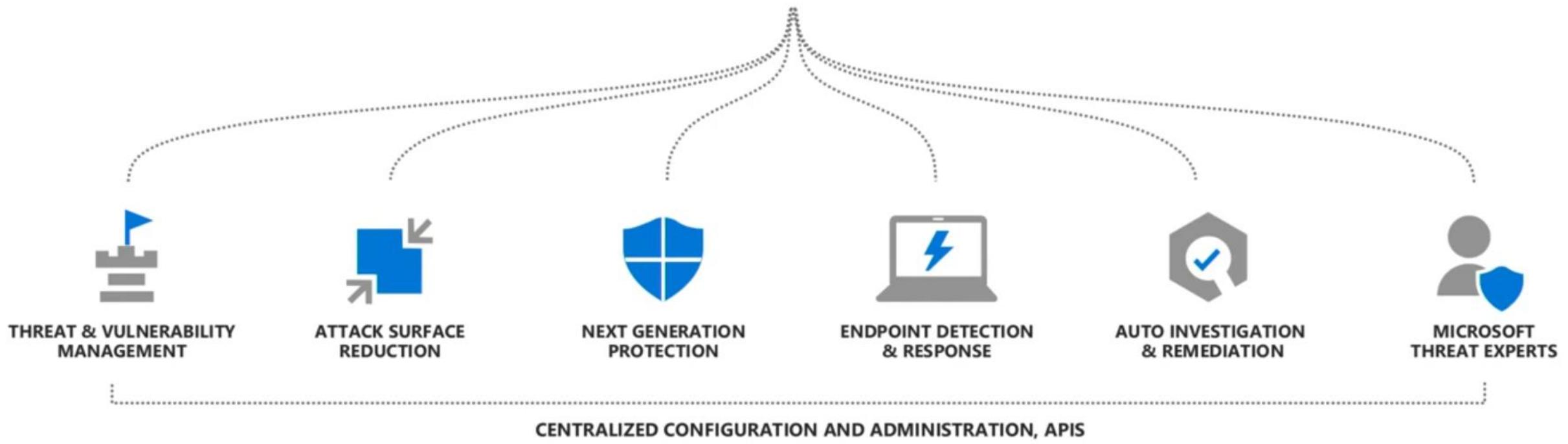
Setting	Options	Default	Description	Setting	Options	Default	Description
<b>Enable Antimalware</b>	true (lower case sensitive)	None	true - Enables the Antimalware service  false – not supported  <b>Note</b> – This is a required configuration setting to enable the Antimalware service	<b>Exclusions Processes</b>	process1, process2, ... ...	None	List of process exclusions. Any file opened by an excluded process will not be scanned (the process itself will still be scanned – to exclude the process itself, use the ExcludedPaths option).  Example:  C:\Program Files\MyApp.exe excludes any files opened by MyApp.exe from being scanned.  Each excluded process should be added as a separate row element value in your antimalware XML configuration or semicolon separated in antimalware JSON configuration
<b>Exclusions Extensions</b>	extension1, extension2, ... ...	None	List of file extensions to exclude from scanning. Example: gif, log, txt excludes files with the .gif, .log, or .txt extension from being scanned.  Each excluded file extension should be added as a separate row element value in your antimalware XML configuration or semicolon separated in antimalware JSON configuration	<b>RealtimeProtectionEnabled</b>	true false (lower case sensitive)	true	true – Enables real-time protection false – Disables real-time protection Default = true when AntimalwareEnabled = true
<b>Exclusions Paths</b>	path1, path2 ... ...	None	List of paths to files or folders to exclude from scanning. Example: e:\approot\worker.dll, e:\approot\temp excludes the file worker.dll in the e:\approot folder and anything under the folder e:\approot\temp from being scanned.  <b>Note:</b> For antimalware JSON configuration for virtual machines, use two backslashes (\\) instead of one to escape properly. For example: e:\\approot\\worker.dll  Each excluded path should be added as a separate row element value in your antimalware XML configuration or semicolon separated in antimalware JSON configuration	<b>ScheduledScanSettings isEnabled</b>	true false (lower case sensitive)	false	Enables or disables a periodic scan for active malware on the system  Default = false
				<b>ScheduledScanSettings Day</b>	0 – 8	7	0 – scan daily, 1 – Sunday, 2 – Monday, 3 – Tuesday..., 7 – Saturday, 8 – disabled  Default = 7 if only ScheduledScanSettings isEnabled = true
				<b>ScheduledScanSettings Time</b>	0 – 1440	120	Hour at which to begin the scheduled scan. Measured in 60 minute increments from midnight  60 mins = 1:00 AM 120 mins = 2:00 AM ... 1380 mins = 11:00 PM  Default = 120 mins if ScheduledScanSettings isEnabled = true
				<b>ScheduledScanSettings Scan Type</b>	Quick/Full	Quick	Default = Quick if ScheduledScanSettings isEnabled = true
				<b>Monitoring</b>	ON OFF	OFF	ON – Enable Antimalware event collection to user subscription storage using Azure Diagnostics extension  OFF – Disable Antimalware event collection to user subscription storage by removing antimalware monitoring configuration in Azure Diagnostics extension if it was previously turned ON
				<b>StorageAccountName</b>	Storage Account Name	None	Storage account name for your Azure store table to collect antimalware events in storage <b>Note</b> – Storage account name is required if monitoring is specified as ON



# Microsoft Defender

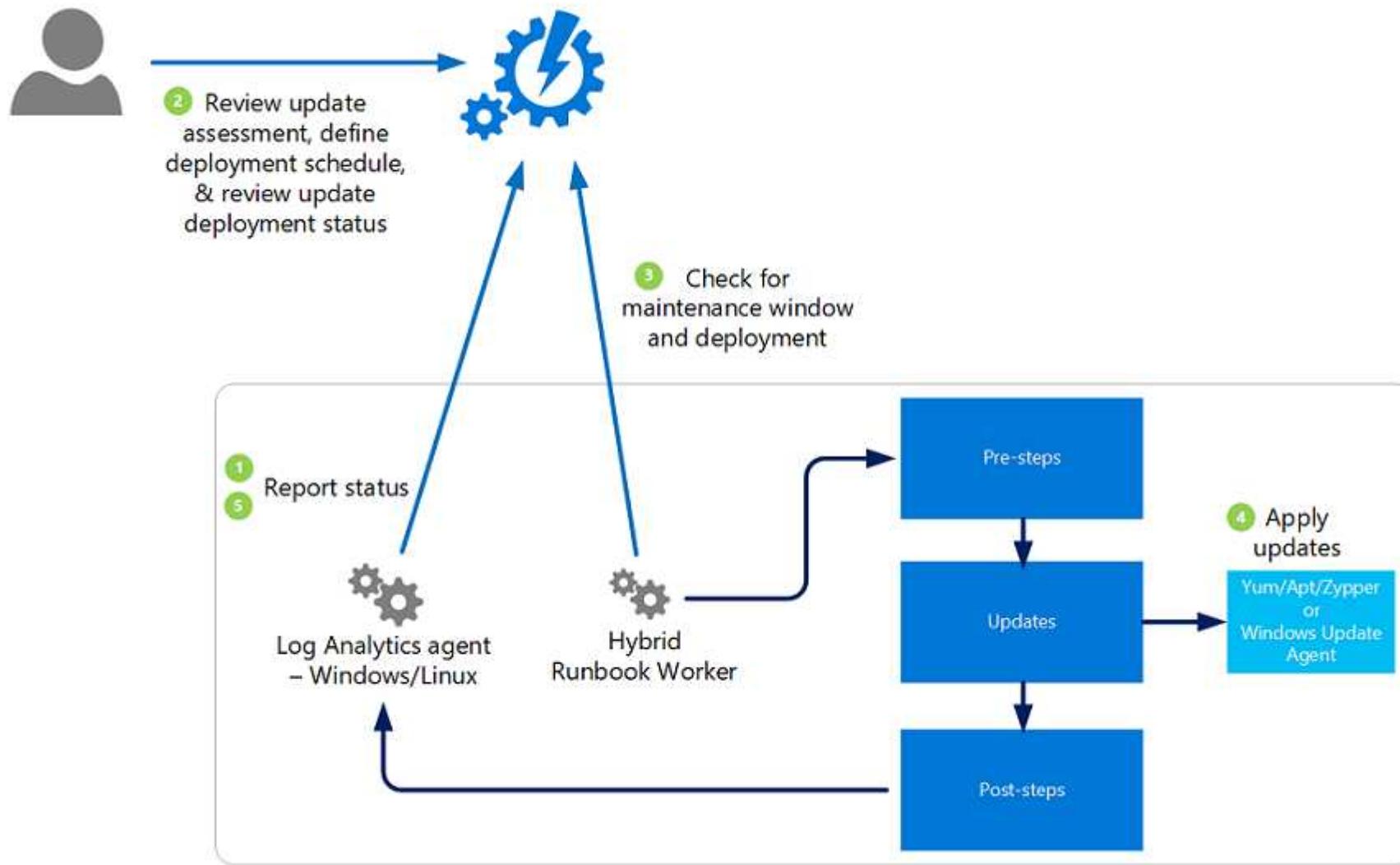
## Advanced Threat Protection

Built-in. Cloud-powered.



- You can use Update Management in Azure Automation to manage operating system updates for your Windows and Linux machines in Azure, in on-premises environments, and in other cloud environments.
- You can quickly assess the status of available updates on all agent machines and manage the process of installing required updates for servers.
- To Enable Update Management
  - From your Azure Automation account for one or more Azure machines.
  - Manually for non-Azure machines.
  - For a single Azure VM from the Virtual machine page in the Azure portal. This scenario is available for Linux and Windows VMs.
  - For multiple Azure VMs by selecting them from the Virtual machines page in the Azure portal.

# Update Management



### Supported client types

Windows Server 2019

Windows Server 2016

Windows Server 2012 R2

Windows Server 2012 / 2008 R2

CentOS 6 (x86/x64) and 7 (x64)

Red Hat Enterprise 6 (x86/x64) and 7 (x64)

SUSE Linux Enterprise Server 11 (x86/x64) and 12 (x64)

Ubuntu 14.04 LTS, 16.04 LTS, and 18.04 (x86/x64)

### Unsupported client types

Windows client

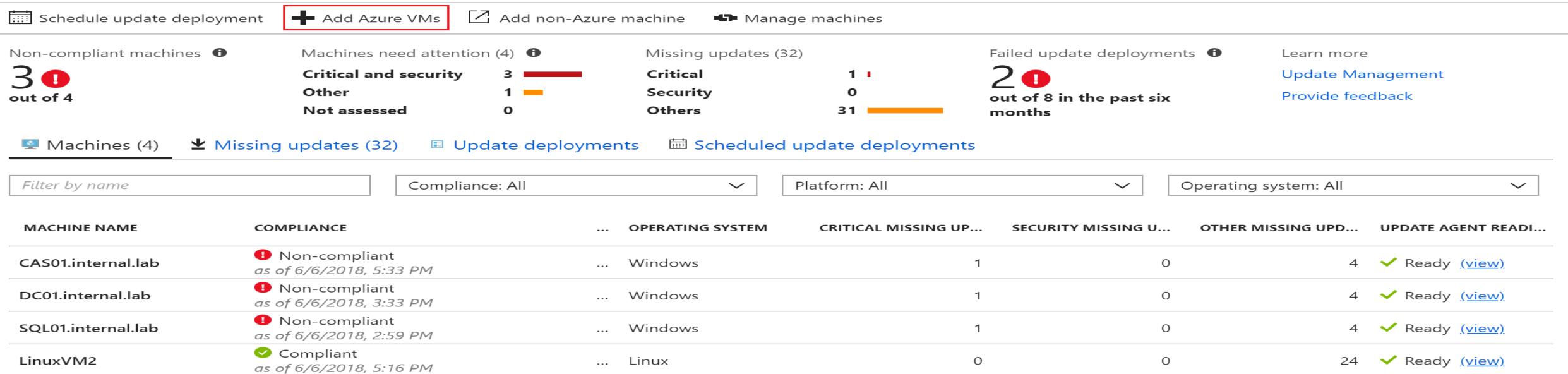
Windows Server 2016 Nano Server

Azure Kubernetes Service Nodes

## Manage updates for Multiple Azure Virtual Machines

Azure Automation Update Management to manage updates and patches for your Windows and Linux virtual machines

- ✓ Onboard virtual machines.
- ✓ Assess the status of available updates.
- ✓ Schedule installation of required updates.
- ✓ Review deployment results to verify that updates were applied successfully to all virtual machines for which Update Management is enabled.



The screenshot shows the Azure Update Management dashboard. At the top, there are four summary cards: 'Non-compliant machines' (3 out of 4), 'Machines need attention' (4), 'Missing updates' (32), and 'Failed update deployments' (2 out of 8 in the past six months). Below these are four navigation links: 'Schedule update deployment', 'Add Azure VMs' (highlighted with a red box), 'Add non-Azure machine', and 'Manage machines'. The main content area has tabs for 'Machines (4)', 'Missing updates (32)', 'Update deployments', and 'Scheduled update deployments'. The 'Missing updates (32)' tab is selected. Below this are four filter dropdowns: 'Filter by name', 'Compliance: All', 'Platform: All', and 'Operating system: All'. The main table lists four machines: CAS01.internal.lab, DC01.internal.lab, SQL01.internal.lab, and LinuxVM2. The table columns include: MACHINE NAME, COMPLIANCE, OPERATING SYSTEM, CRITICAL MISSING UPD..., SECURITY MISSING U..., OTHER MISSING UPD..., and UPDATE AGENT READI... . The LinuxVM2 row shows 'Compliant' status, while the other three are 'Non-compliant'.

MACHINE NAME	COMPLIANCE	OPERATING SYSTEM	CRITICAL MISSING UPD...	SECURITY MISSING U...	OTHER MISSING UPD...	UPDATE AGENT READI...
CAS01.internal.lab	Non-compliant as of 6/6/2018, 5:33 PM	Windows	1	0	4	✓ Ready <a href="#">(view)</a>
DC01.internal.lab	Non-compliant as of 6/6/2018, 3:33 PM	Windows	1	0	4	✓ Ready <a href="#">(view)</a>
SQL01.internal.lab	Non-compliant as of 6/6/2018, 2:59 PM	Windows	1	0	4	✓ Ready <a href="#">(view)</a>
LinuxVM2	Compliant as of 6/6/2018, 5:16 PM	Linux	0	0	24	✓ Ready <a href="#">(view)</a>

- ✓ For Linux computers, the expected timeframe is the last hour.
- ✓ For Windows computers, the expected timeframe is the last 12 hours

## Manage updates for Multiple Azure Virtual Machines

- ✓ For Linux computers, the expected timeframe is the last hour.
- ✓ For Windows computers, the expected timeframe is the last 12 hours
- ✓ In addition to the scan schedule, the scan for update compliance is initiated within 15 minutes of the MMA being restarted, before update installation, and after update installation.
- ✓ For a Linux computer, the compliance scan is performed every hour by default. If the MMA agent is restarted, a compliance scan is initiated within 15 minutes.
- ✓ It can take between 30 minutes and 6 hours for the dashboard to display updated data from managed computers.

## Update classification

- ✓ Critical updates
- ✓ Security updates
- ✓ Update rollups
- ✓ Feature packs
- ✓ Service packs
- ✓ Definition updates
- ✓ Tools
- ✓ Updates
- ✓ Updates to include/exclude
- ✓ Schedule settings
- ✓ Recurrence & Once
- ✓ Pre-scripts + Post-scripts
- ✓ Maintenance window (minutes)
- ✓ Reboot control
- ✓ Reboot if required
- ✓ Always reboot
- ✓ Never reboot
- ✓ Only reboot - will not install updates



thank you!



- Overview Azure Role-based Access Control
- Understand How Azure RBAC Works
- Multiple role assignments
- Deny assignments
- How Azure RBAC determines
- License requirements

## AZURE ROLE-BASED ACCESS CONTROL

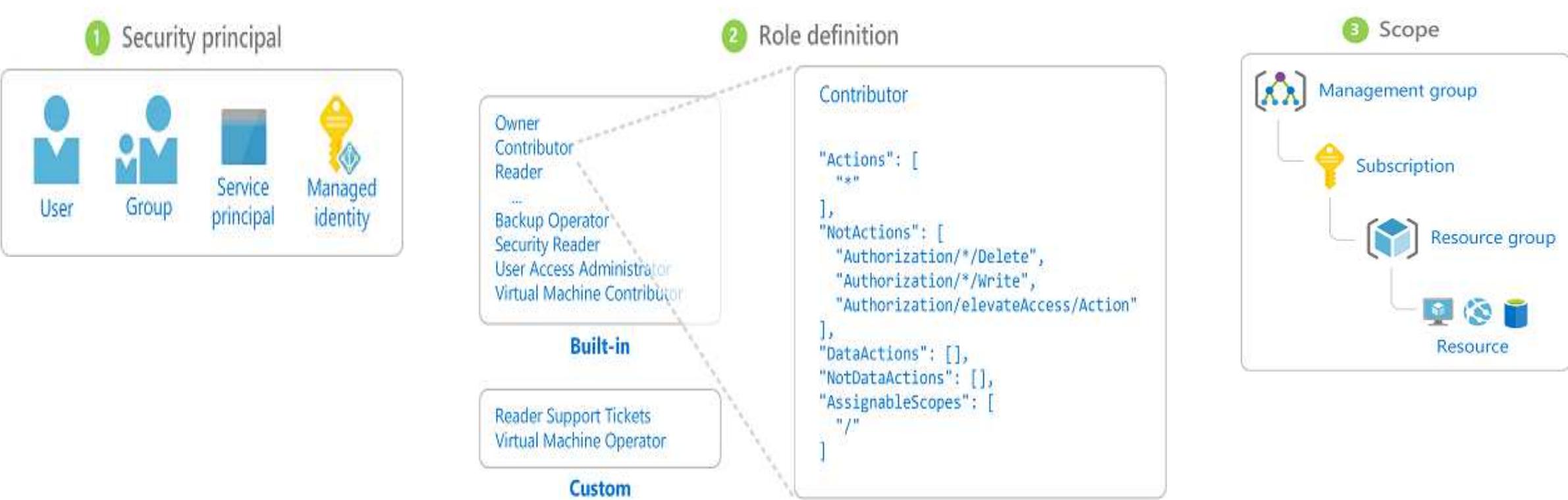
Access management for cloud resources is a critical function for any organization that is using the cloud. Azure role-based access control (Azure RBAC) helps you manage who has access to Azure resources, what they can do with those resources, and what areas they have access to.

### Examples

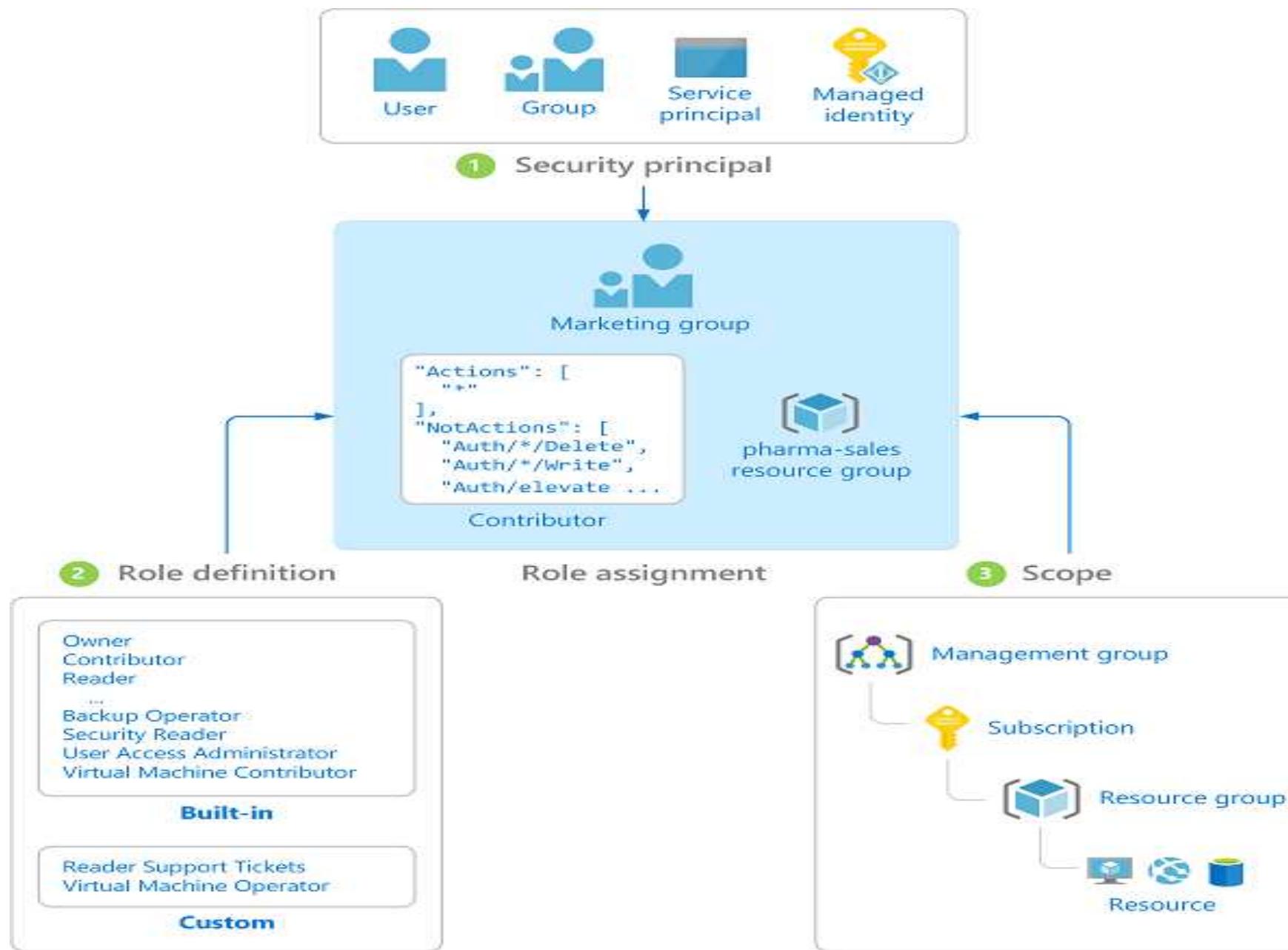
- ❑ Allow one user to manage virtual machines in a subscription and another user to manage virtual networks
- ❑ Allow a DBA group to manage SQL databases in a subscription
- ❑ Allow a user to manage all resources in a resource group, such as virtual machines, websites, and subnets
- ❑ Allow an application to access all resources in a resource group

# How Azure RBAC Works

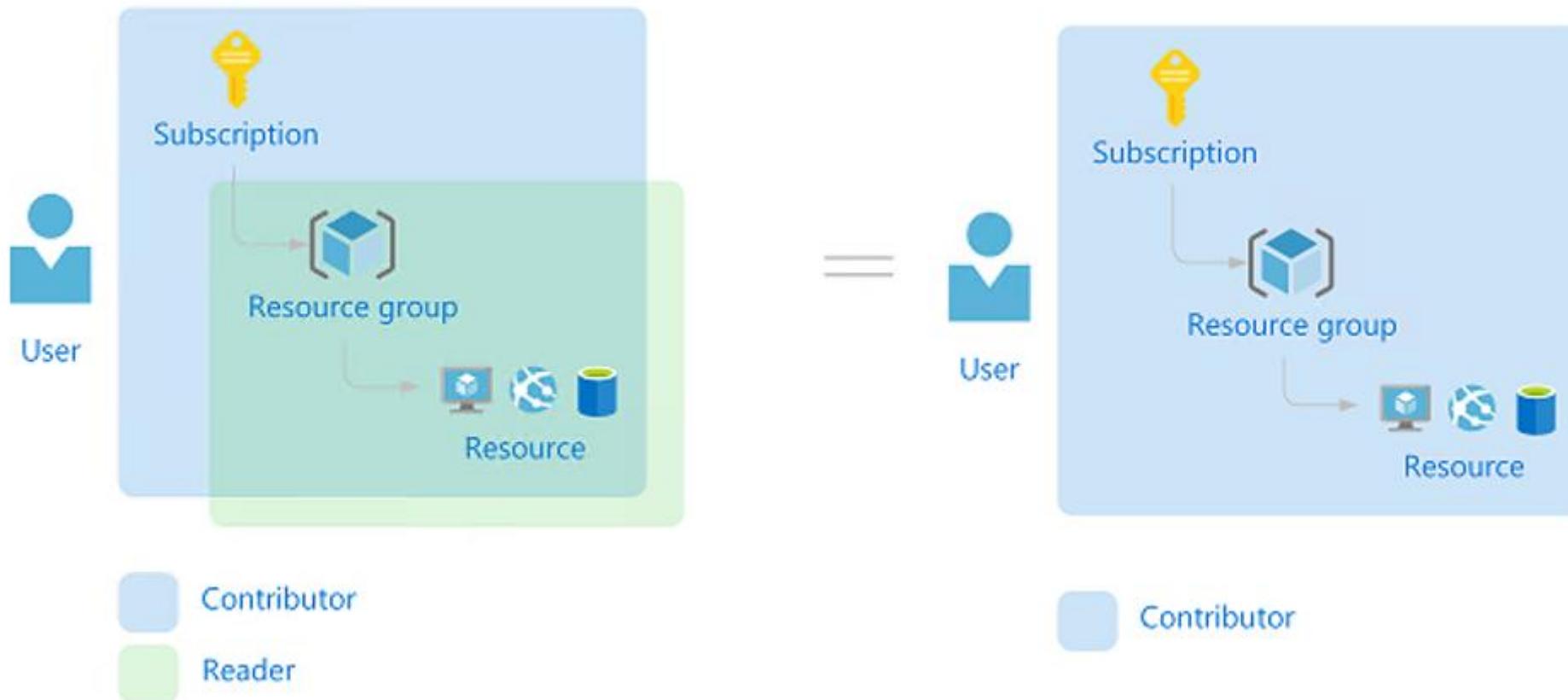
- The way you control access to resources using Azure RBAC is to create role assignments.
- This is a key concept to understand – it's how permissions are enforced.
- A role assignment consists of three elements: security principal, role definition, and scope.



# How Azure RBAC Works



## MULTIPLE ROLE ASSIGNMENTS



- ❑ Deny assignments block users from performing specified actions even if a role assignment grants them access.
- ❑ Deny assignments take precedence over role assignments.

## HOW AZURE RBAC Determines

1. A user (or service principal) acquires a token for Azure Resource Manager.
  - The token includes the user's group memberships (including transitive group memberships).
2. The user makes a REST API call to Azure Resource Manager with the token attached.
3. Azure Resource Manager retrieves all the role assignments and deny assignments that apply to the resource upon which the action is being taken.
4. Azure Resource Manager narrows the role assignments that apply to this user or their group and determines what roles the user has for this resource.
5. Azure Resource Manager determines if the action in the API call is included in the roles the user has for this resource.
6. If the user doesn't have a role with the action at the requested scope, access is not granted. Otherwise, Azure Resource Manager checks if a deny assignment applies.
7. If a deny assignment applies, access is blocked. Otherwise access is granted.

- Overview Azure Role-based Access Control
- Understand How Azure RBAC Works
- Multiple role assignments
- Deny assignments
- How Azure RBAC determines
- License requirements



thank you!



## MANAGED IDENTITIES

Managed identities for Azure resources is the new name for the service formerly known as Managed Service Identity (MSI)

A common challenge when building cloud applications is how to manage the credentials in your code for authenticating to cloud services

The managed identities for Azure resources feature is free with Azure AD for Azure subscriptions. There's no additional cost.

### Terminology

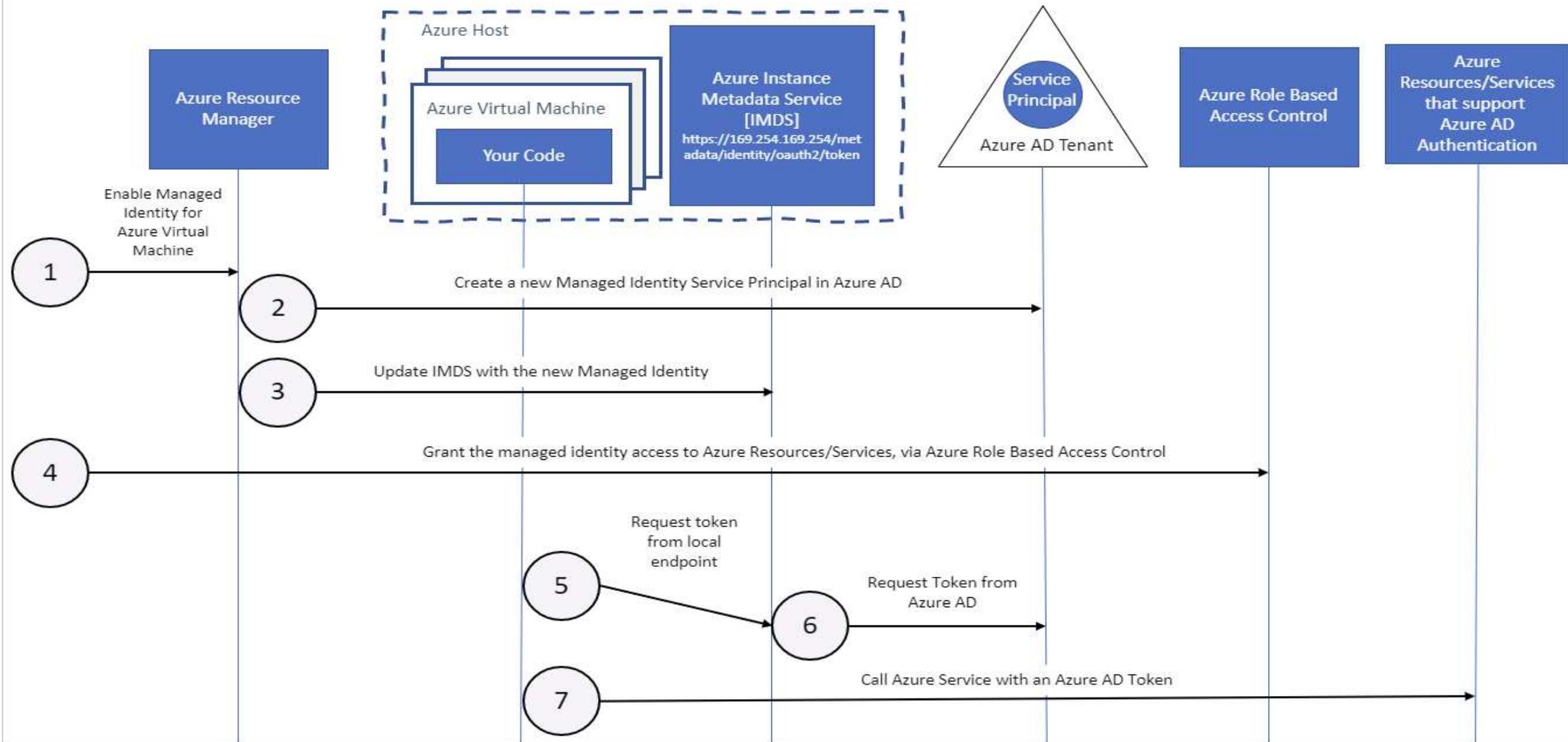
- ✓ **Client ID** - a unique identifier generated by Azure AD that is tied to an application and service principal during its initial provisioning.
- ✓ **Principal ID** - the object ID of the service principal object for your managed identity that is used to grant role-based access to an Azure resource.
- ✓ **Azure Instance Metadata Service (IMDS)** - a REST endpoint accessible to all IaaS VMs created via the Azure Resource Manager. The endpoint is available at a well-known non-routable IP address (169.254.169.254) that can be accessed only from within the VM.

### There are two types of managed identities:

- ✓ A **system-assigned managed identity** is enabled directly on an Azure service instance. When the identity is enabled, Azure creates an identity for the instance in the Azure AD tenant that's trusted by the subscription of the instance. After the identity is created, the credentials are provisioned onto the instance. The lifecycle of a system-assigned identity is directly tied to the Azure service instance that it's enabled on. If the instance is deleted, Azure automatically cleans up the credentials and the identity in Azure AD.
- ✓ A **user-assigned managed identity** is created as a standalone Azure resource. Through a create process, Azure creates an identity in the Azure AD tenant that's trusted by the subscription in use. After the identity is created, the identity can be assigned to one or more Azure service instances. The lifecycle of a user-assigned identity is managed separately from the lifecycle of the Azure service instances to which it's assigned.

Managed identities are service principals of a special type, which are locked to only be used with Azure resources. When the managed identity is deleted, the corresponding service principal is automatically removed.

# MANAGED IDENTITIES



## MANAGED IDENTITIES

Property	System-assigned managed identity	User-assigned managed identity
Creation	Created as part of an Azure resource (for example, an Azure virtual machine or Azure App Service)	Created as a stand-alone Azure resource
Lifecycle	Shared lifecycle with the Azure resource that the managed identity is created with. When the parent resource is deleted, the managed identity is deleted as well.	Independent life-cycle. Must be explicitly deleted.
Sharing across Azure resources	Cannot be shared. It can only be associated with a single Azure resource.	Can be shared The same user-assigned managed identity can be associated with more than one Azure resource.
Common use cases	Workloads that are contained within a single Azure resource Workloads for which you need independent identities. For example, an application that runs on a single virtual machine	Workloads that run on multiple resources and which can share a single identity. Workloads that need pre-authorization to a secure resource as part of a provisioning flow. Workloads where resources are recycled frequently, but permissions should stay consistent. For example, a workload where multiple virtual machines need to access the same resource

## How a system-assigned managed identity works with an Azure VM

1. Azure Resource Manager receives a request to enable the system-assigned managed identity on a VM.
2. Azure Resource Manager creates a service principal in Azure AD for the identity of the VM. The service principal is created in the Azure AD tenant that's trusted by the subscription.
3. Azure Resource Manager configures the identity on the VM by updating the Azure Instance Metadata Service identity endpoint with the service principal client ID and certificate.
4. After the VM has an identity, use the service principal information to grant the VM access to Azure resources. To call Azure Resource Manager, use role-based access control (RBAC) in Azure AD to assign the appropriate role to the VM service principal. To call Key Vault, grant your code access to the specific secret or key in Key Vault.
5. Your code that's running on the VM can request a token from the Azure Instance Metadata service endpoint, accessible only from within the VM: <http://169.254.169.254/metadata/identity/oauth2/token>
  - The resource parameter specifies the service to which the token is sent. To authenticate to Azure Resource Manager, use `resource=https://management.azure.com/`.
  - API version parameter specifies the IMDS version, use `api-version=2018-02-01` or greater.
6. A call is made to Azure AD to request an access token (as specified in step 5) by using the client ID and certificate configured in step 3. Azure AD returns a JSON Web Token (JWT) access token.
7. Your code sends the access token on a call to a service that supports Azure AD authentication.

## How a user-assigned managed identity works with an Azure VM

1. Azure Resource Manager receives a request to create a user-assigned managed identity.
2. Azure Resource Manager creates a service principal in Azure AD for the user-assigned managed identity. The service principal is created in the Azure AD tenant that's trusted by the subscription.
3. Azure Resource Manager receives a request to configure the user-assigned managed identity on a VM and updates the Azure Instance Metadata Service identity endpoint with the user-assigned managed identity service principal client ID and certificate.
4. After the user-assigned managed identity is created, use the service principal information to grant the identity access to Azure resources. To call Azure Resource Manager, use RBAC in Azure AD to assign the appropriate role to the service principal of the user-assigned identity. To call Key Vault, grant your code access to the specific secret or key in Key Vault.
5. Your code that's running on the VM can request a token from the Azure Instance Metadata Service identity endpoint, accessible only from within the VM: <http://169.254.169.254/metadata/identity/oauth2/token>
  - The resource parameter specifies the service to which the token is sent. To authenticate to Azure Resource Manager, use `resource=https://management.azure.com/`.
  - The client ID parameter specifies the identity for which the token is requested. This value is required for disambiguation when more than one user-assigned identity is on a single VM.
  - The API version parameter specifies the Azure Instance Metadata Service version. Use `api-version=2018-02-01` or higher.
6. A call is made to Azure AD to request an access token (as specified in step 5) by using the client ID and certificate configured in step 3. Azure AD returns a JSON Web Token (JWT) access token.
7. Your code sends the access token on a call to a service that supports Azure AD authentication.

# Managed Identities for Azure Resources can be used to Authenticate to Services that support Azure AD Authentication

### Windows VM

- Access Azure Data Lake Store
- Access Azure Resource Manager
- Access Azure SQL
- Access Azure Storage by using an access key
- Access Azure Storage by using shared access signatures
- Access a non-Azure AD resource with Azure Key Vault

### Linux VM

- Access Azure Container Registry
- Access Azure Data Lake Store
- Access Azure Resource Manager
- Access Azure Storage by using an access key
- Access Azure Storage by using shared access signatures
- Access a non-Azure AD resource with Azure Key Vault

### Other Azure services

- Azure App Service
- Azure API Management
- Azure Container Instances
- Azure Container Registry Tasks
- Azure Event Hubs
- Azure Functions
- Azure Kubernetes Service
- Azure Logic Apps
- Azure Service Bus
- Azure Data Factory



# DEMO with LAB



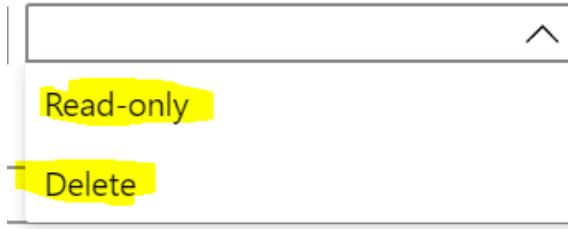


thank you!



## Azure Resource Locks

Lock type



- **CanNotDelete** means authorized users can still read and modify a resource, but they can't delete the resource.
- **ReadOnly** means authorized users can read a resource, but they can't delete or update the resource. Applying this lock is similar to restricting all authorized users to the permissions granted by the **Reader** role.

`New-AzResourceLock -LockName LockGroup -LockLevel CanNotDelete -ResourceGroupName exampleresourcegroup`

`az lock create --name LockSite --lock-type CanNotDelete --resource-group exampleresourcegroup --resource-name examplesite --resource-type Microsoft.Web/sites`

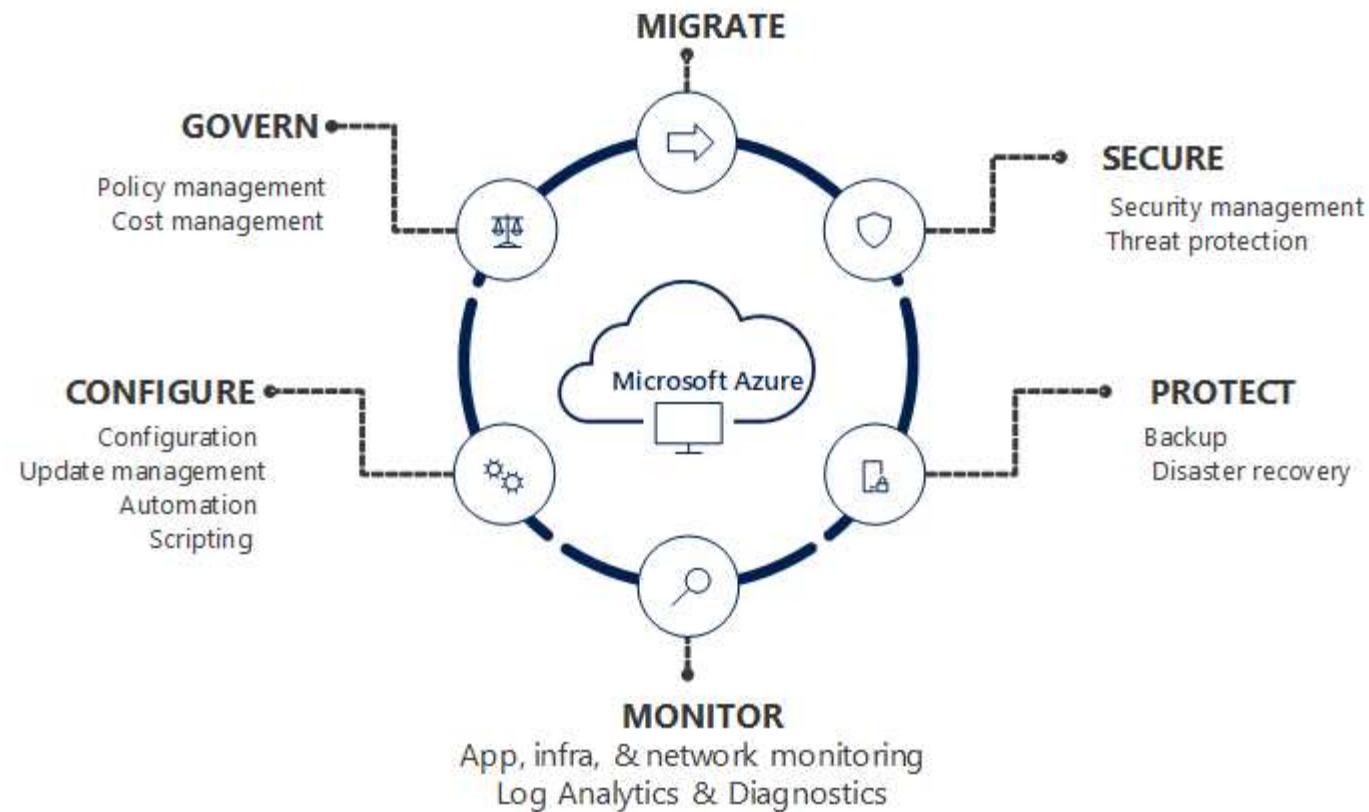
- Unlike RBAC Resources locks apply a restriction across all the Users and Roles
- We must have access to `Microsoft.Authorization/*` or `Microsoft.Authorization/locks/*` actions to create or delete Management Locks
- Owner and User Access Administrator are the only built-in roles granted those actions



thank you!

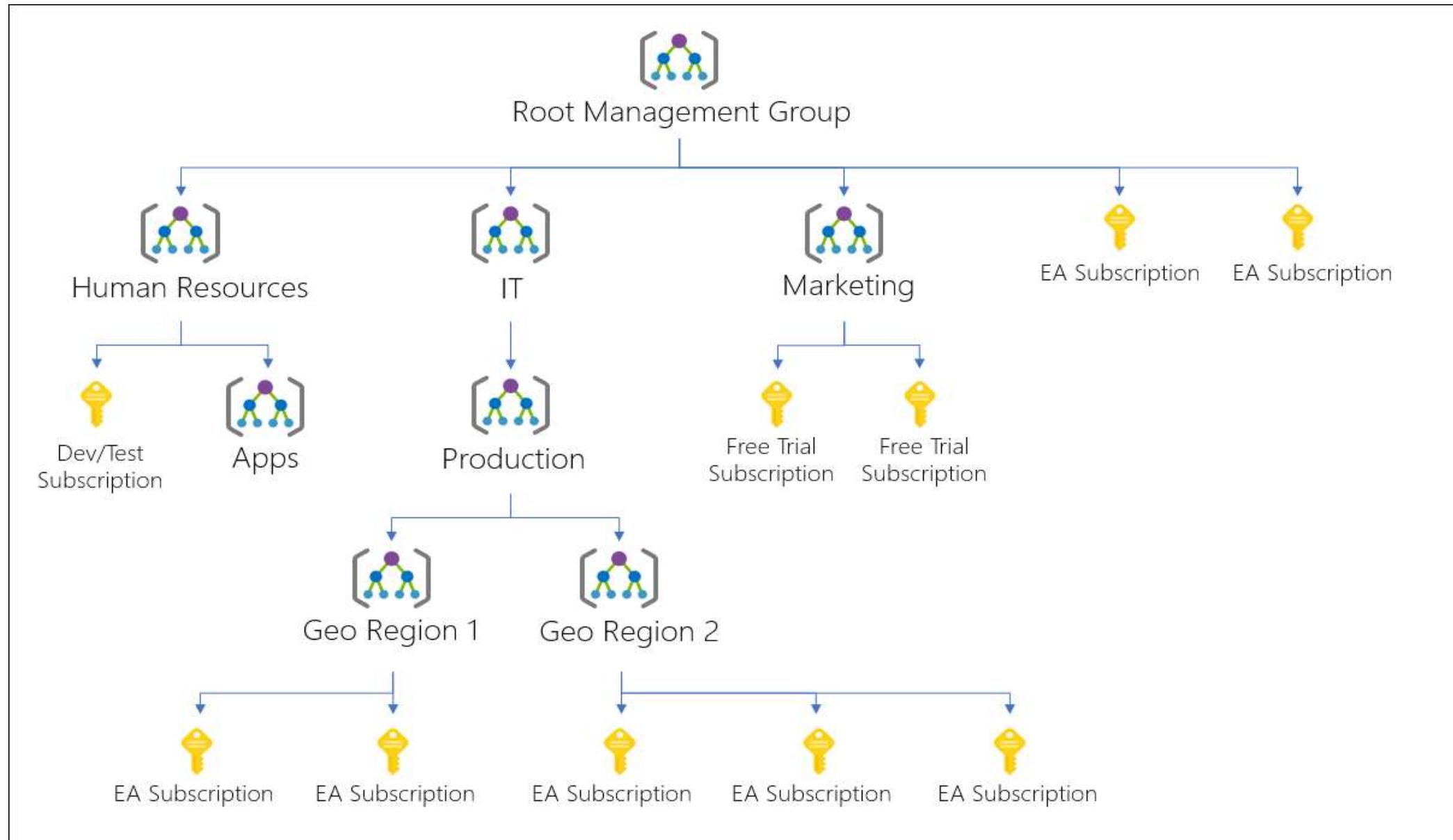


# Azure Management



- If your organization has many subscriptions, you may need a way to efficiently manage access, policies, and compliance for those subscriptions.
- Azure management groups provide a level of scope above subscriptions. You organize subscriptions into containers called "management groups" and apply your governance conditions to the management groups.
- All subscriptions within a management group automatically inherit the conditions applied to the management group.
- Management groups give you enterprise-grade management at a large scale no matter what type of subscriptions you might have.
- All subscriptions within a single management group must trust the same Azure Active Directory tenant
- For example, you can apply policies to a management group that limits the regions available for virtual machine (VM) creation.
- This policy would be applied to all management groups, subscriptions, and resources under that management group by only allowing VMs to be created in that region.
- Each directory is given a single top-level management group called the "Root" management group.
  - ✓ This root management group is built into the hierarchy to have all management groups and subscriptions fold up to it.
  - ✓ This root management group allows for global policies and RBAC assignments to be applied at the directory level.

## Management Groups



## **Important facts about management groups**

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

## Azure Policy

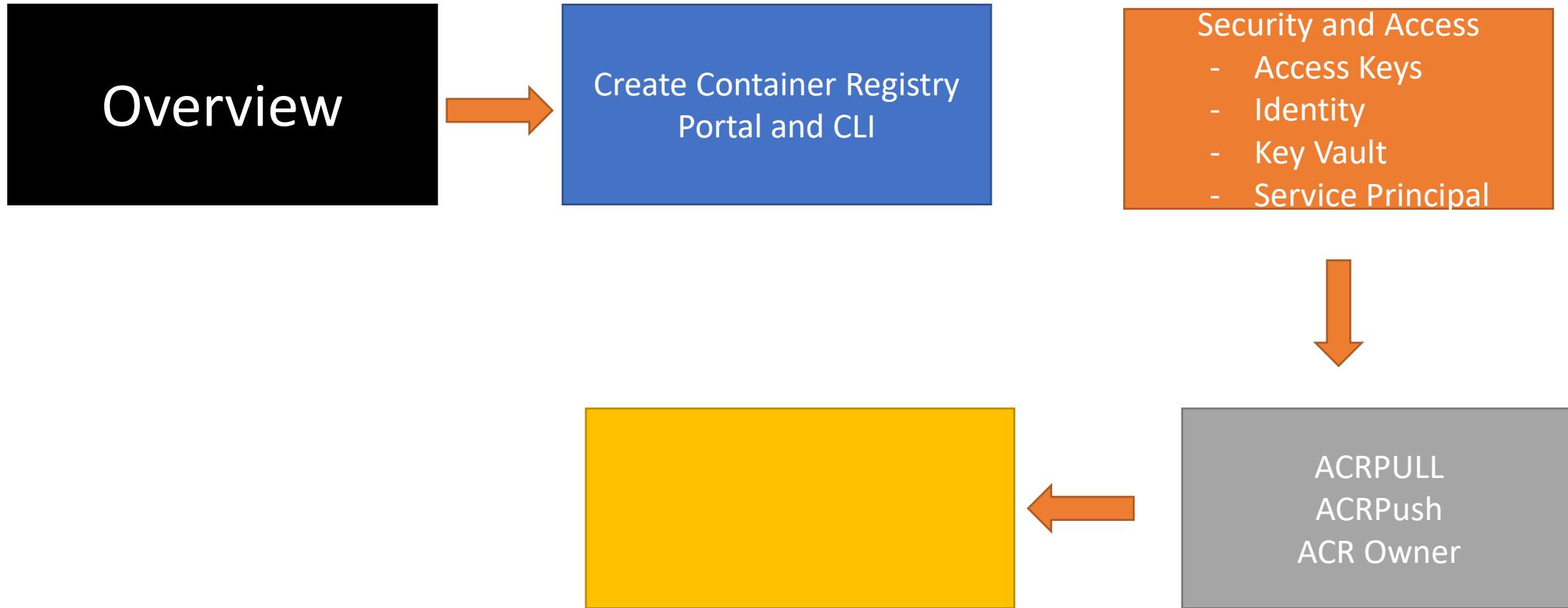
- Azure Policy helps to enforce organizational standards and to assess compliance at-scale.
- Through its compliance dashboard, it provides an aggregated view to evaluate the overall state of the environment, with the ability to drill-down to the per-resource, per-policy granularity.
- It also helps to bring your resources to compliance through bulk remediation for existing resources and automatic remediation for new resources.
- Common use cases for Azure Policy include implementing governance for resource consistency, regulatory compliance, security, cost, and management.
- Policy definitions for these common use cases are already available in your Azure environment as built-ins to help you get started.





thank you!



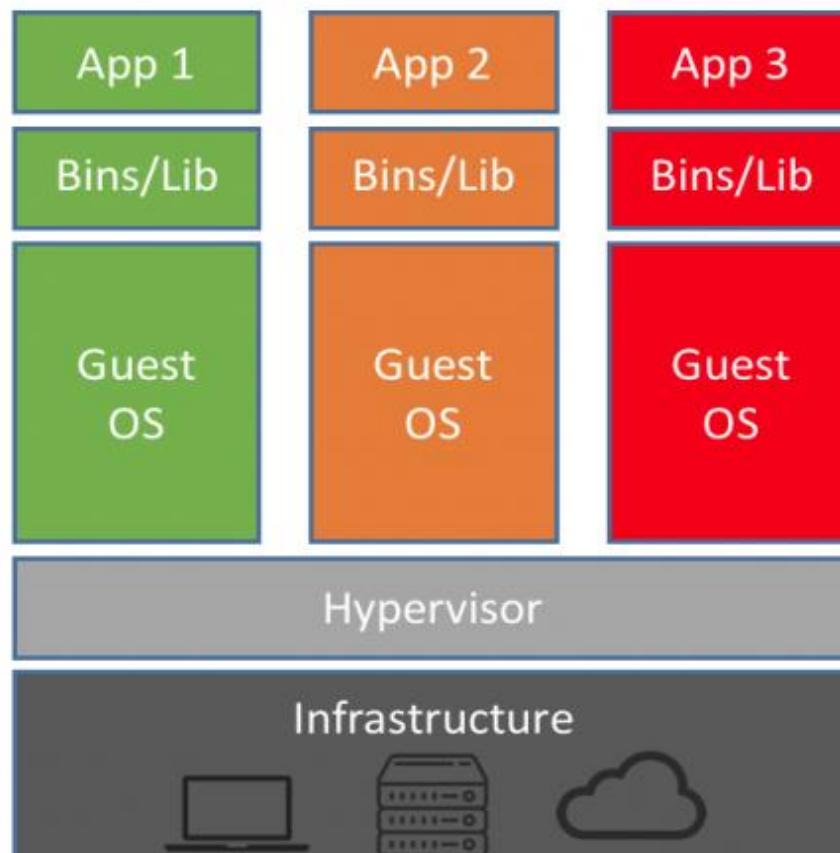


### Why Containers

- It works on any machines
- Every environment looks the same
- Increased velocity
- Run anywhere
  - Linux
  - Windows
  - Cloud
  - Drones, Raspberry PI, IoT

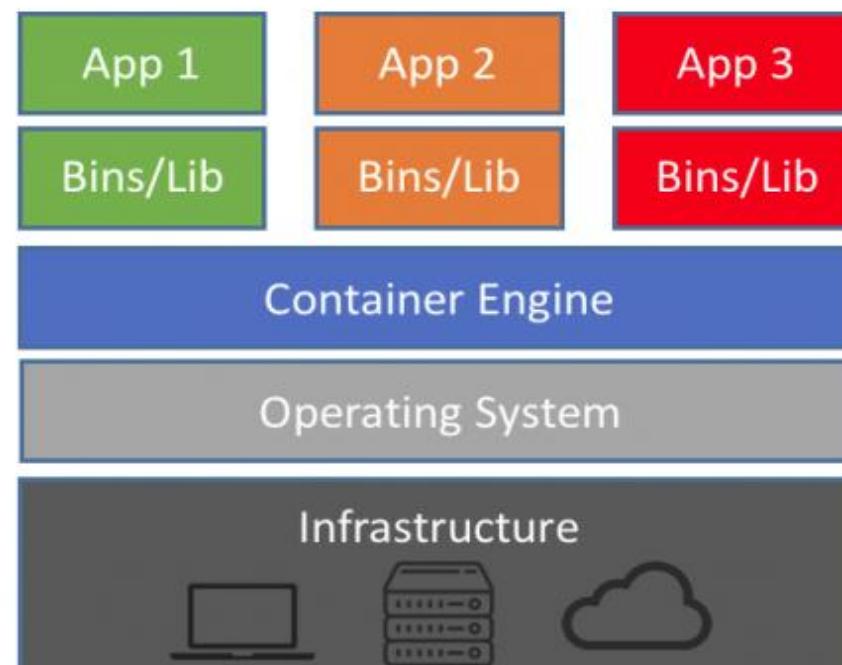
## Virtual Machines vs Containers

Separate OS per instance  
Large footprint  
Slower start-up



Machine Virtualization

Shared Host OS Kernel  
Portability  
Faster scalability



Containers

## Azure Container Services

- Azure container instances – ACI
- Azure Container Registry - ACR

### What can you build with Azure Container Instances?



→ Data processing jobs



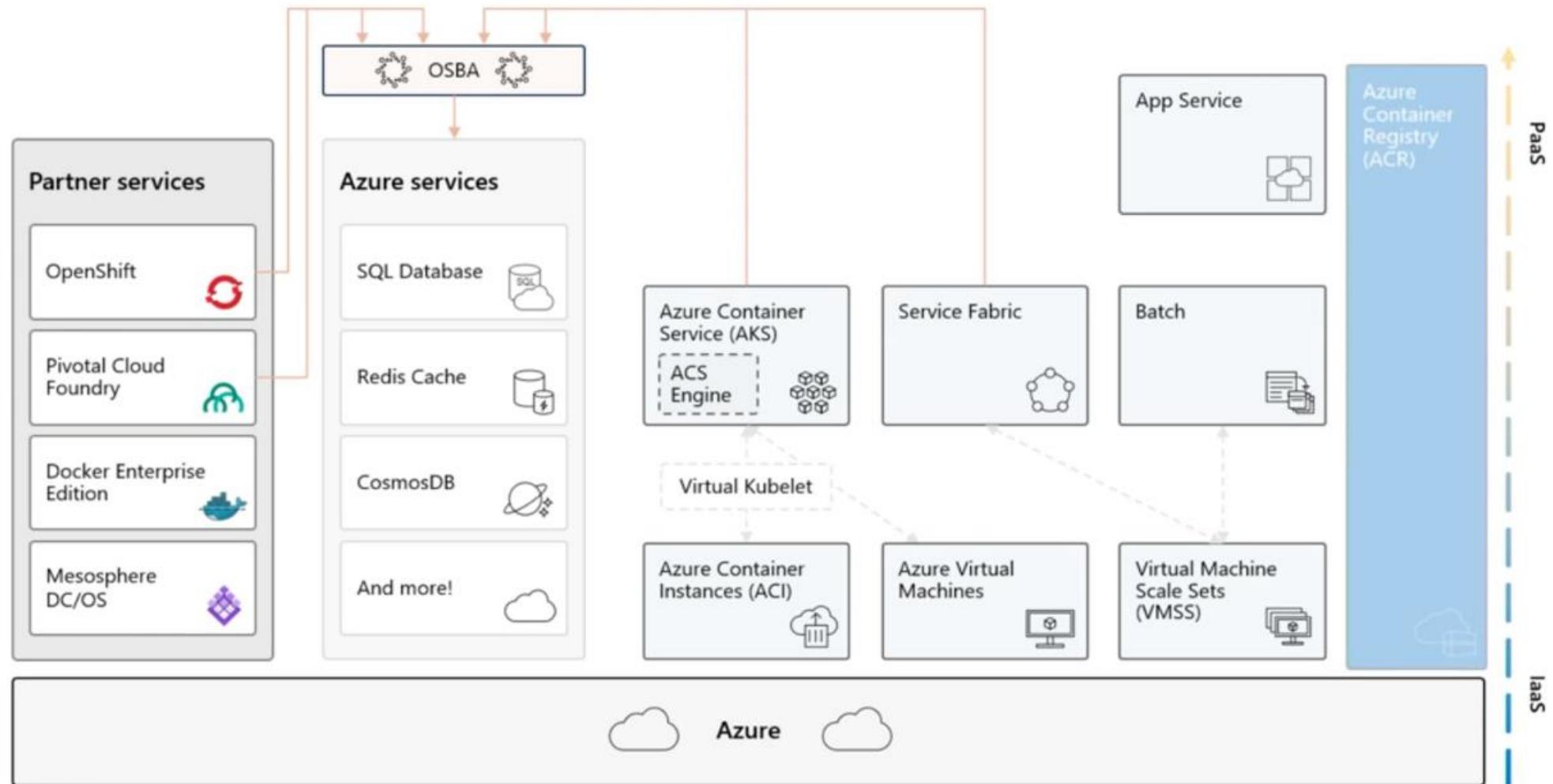
→ Event-driven applications with Azure Logic Apps



→ Virtual nodes, elasticity for Kubernetes on AKS

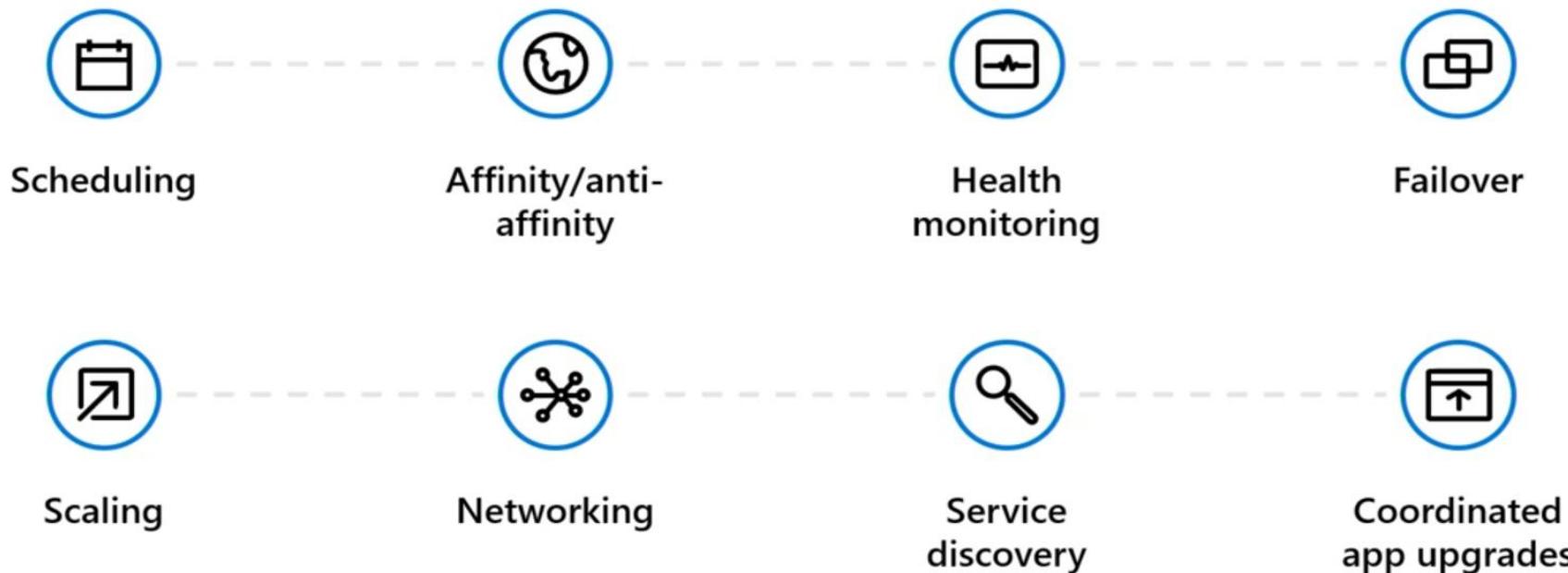
- ❑ A repository for storing container images
  - ❑ Public registries Ex:- Docker Hub – Free & readymade
  - ❑ You can secure with Private Registries & secure Storage of Images
  - ❑ Your Team can store not Just docker Images Mesosphere Kubernetes - MKE, docker swarm or Kubernetes
  - ❑ This helps your DevOPS team to seamless integration and they can use Azure CLI commands to work on them.
  - ❑ Azure Container Registry can be configure Geo-Replication
- 
- ❑ **ACR Commands**
    - Az ACR login
    - Docker Pull
    - Docker Push
    - Docker RMI

# Azure Container Registry



# Azure Kubernetes Service (AKS)

## The elements of orchestration



All services

 Search Containers

Overview

Categories

All

General

Compute

Networking

Storage

Web

Mobile

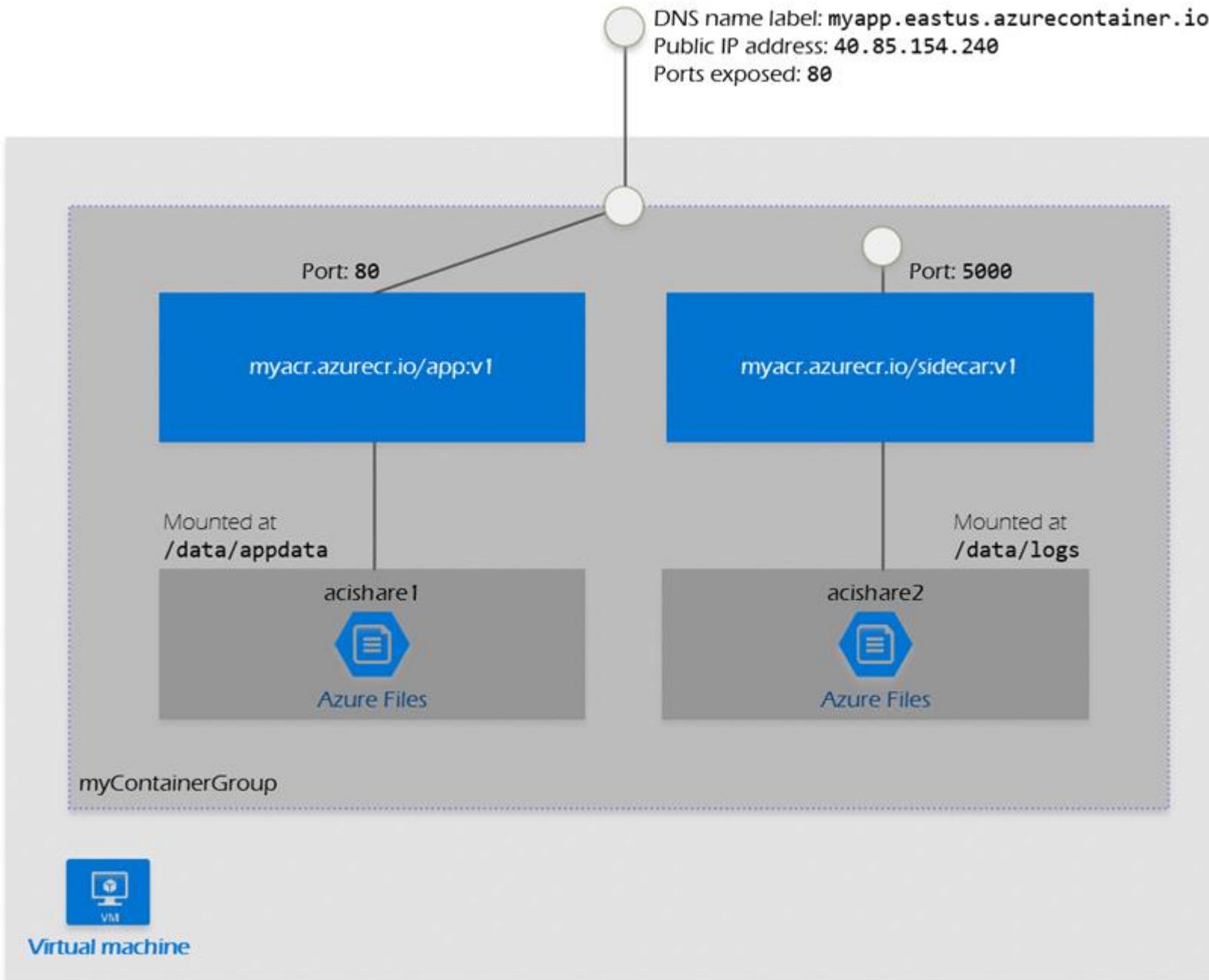
Containers

CONTAINERS (7)

 Container services (deprecated) Kubernetes services Batch accounts App Services Container instances Container registries Service Fabric clusters

Demo From Portal on Containers and conclude

## Container Group



## 1. Container Registry

- Use a private registry
- Monitor and scan container images
- Twistlock and Aqua Security
- Protect credentials
  - Encryption
  - Role Based Access Control
  - Azure Key Vault
- Scan for vulnerabilities
- Enforce network segmentation on running containers
- Monitor container activity and user access
- Monitor container resource activity
- Log all container administrative user access for auditing

## 2. Container Instances

- Network security
- Azure Firewall
  - IDS/IPS
  - Threat Intelligence
- Azure Web Application Firewall
- Record network packets and flow logs
- Azure Application Gateway
- Central Logging and monitoring
  - Enable Audit logging for Azure resources
  - Application, System, Security, Storage logs
  - Monitor and review Logs
  - Centralize anti-malware logging
  - Enable DNS query logging
  - Enable command-line audit logging
- Identity and access control
  - Use single sign-on (SSO) with Azure Active Directory
  - Use multi-factor authentication
  - Use dedicated machines (Privileged Access Workstations)

## 2. Container Instances

- Manage Azure resources from only approved location
- Alert on account login behavior deviation
- Data protection
- Maintain an inventory of sensitive Information
- Isolate systems storing or processing sensitive information
- Monitor and block unauthorized transfer of sensitive information
- Encrypt all sensitive information in transit
- Use an active discovery tool to identify sensitive data
- Use Azure RBAC to control access to resources
- Encrypt sensitive information at rest
- Run automated vulnerability scanning tools
- Deploy automated operating system patch management solution
- Deploy automated third-party software patch management solution
- Compare back-to-back vulnerability scans
- Physically or logically segregate high risk applications
- Penetration tests and red team exercises

Azure container  
Registry Tasks

Azure container  
Registry Security

Container  
Instances

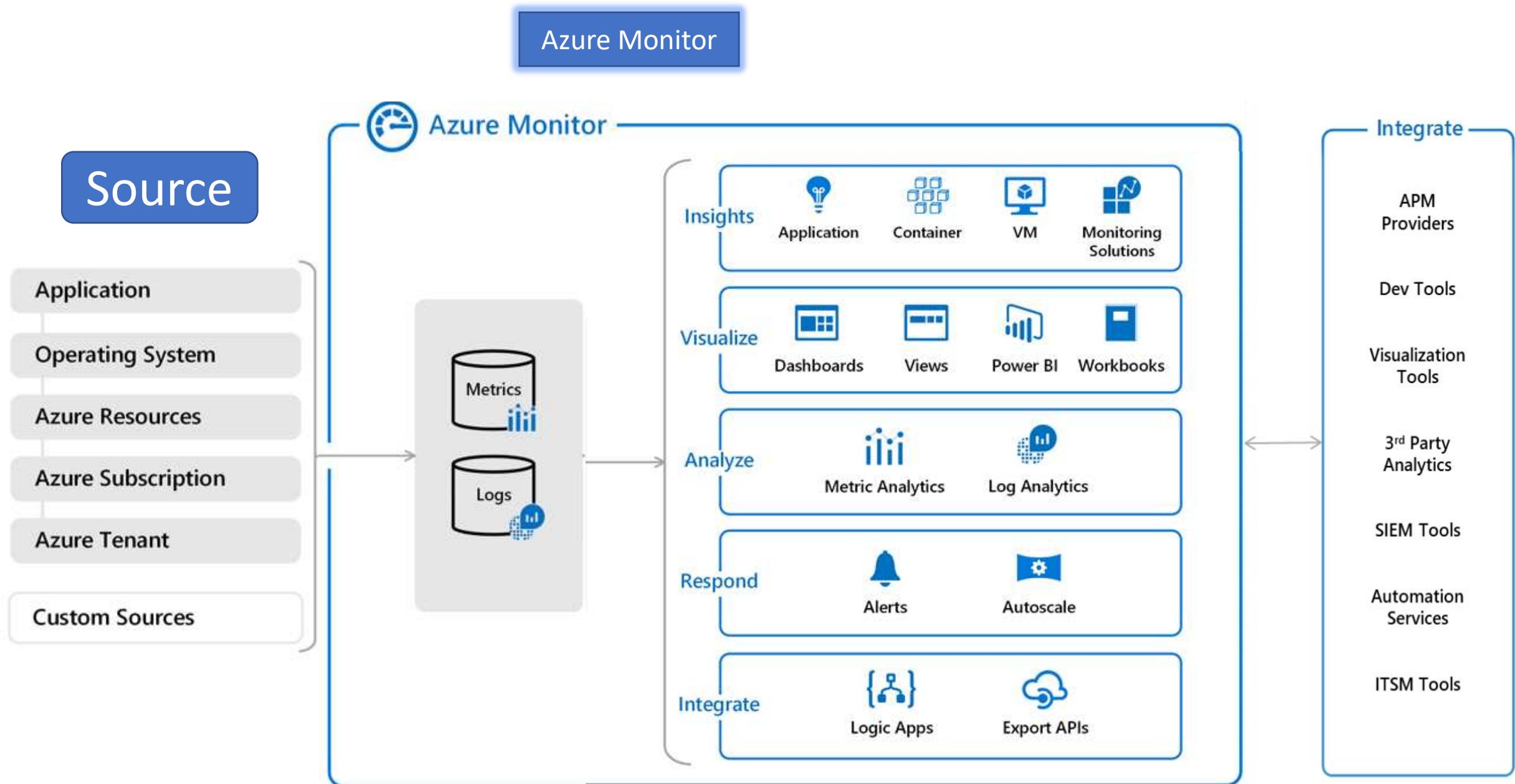
Content Trust



thank you!

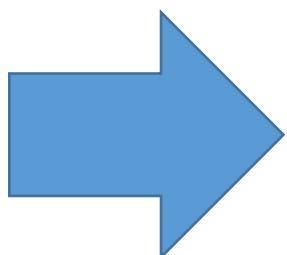


- Detect and diagnose issues across applications and dependencies with **Application Insights**.
- Correlate infrastructure issues with **Azure Monitor for VMs** and **Azure Monitor for Containers**.
- Drill into your monitoring data with **Log Analytics** for troubleshooting and deep diagnostics.
- Support operations at scale with **smart alerts** and **automated actions**.
- Create visualizations with Azure **dashboards** and **workbooks**.



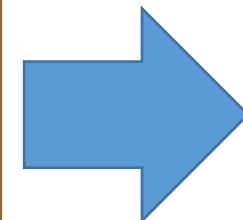
## Data Source

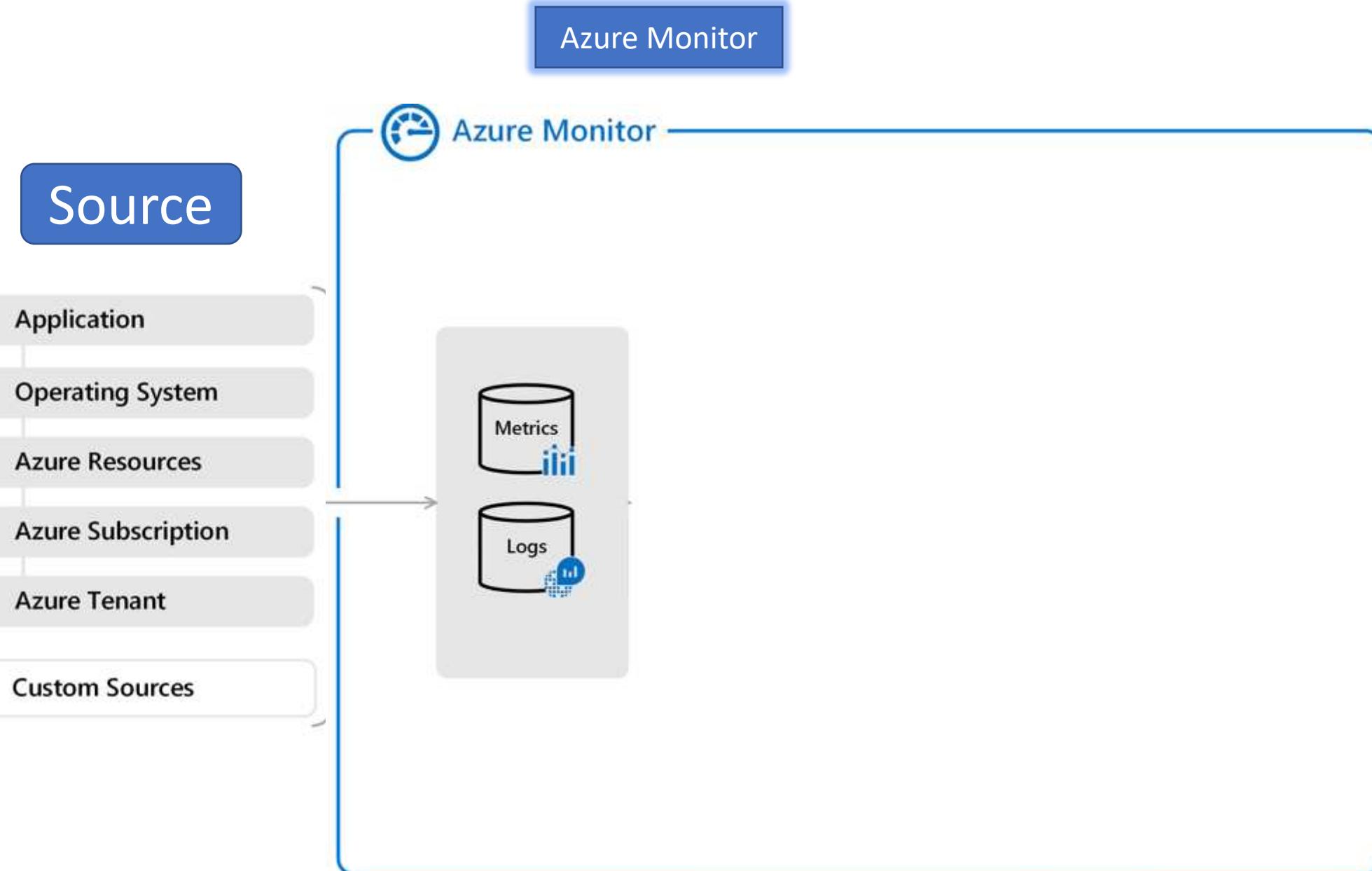
- Tenant
  - Audit Logs
- Subscription
  - Service Health
  - Activity Log
- Resources
  - Metrics
  - Diagnostic Logs
  - Monitoring Solutions
- Guest OS
  - Diagnostics Extension
  - Log analytics Agent
  - Dependency Agent
- Application
  - Application insights



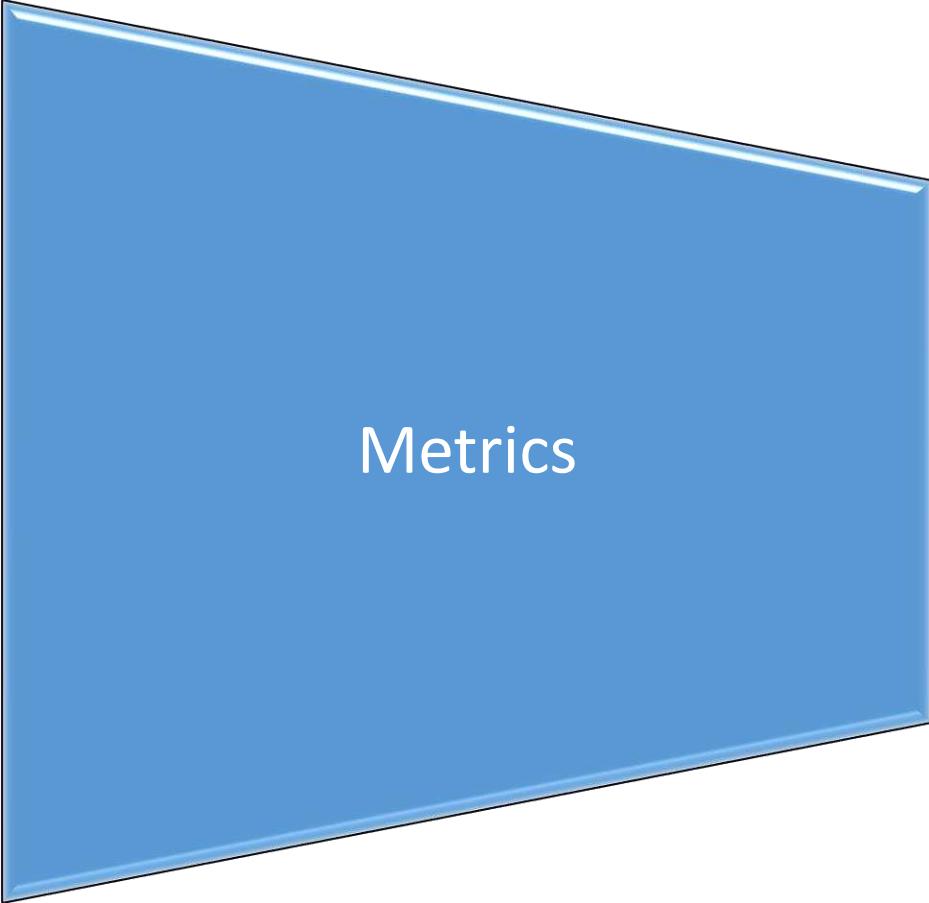
## Monitoring Data Type

- Metrics
- Logs

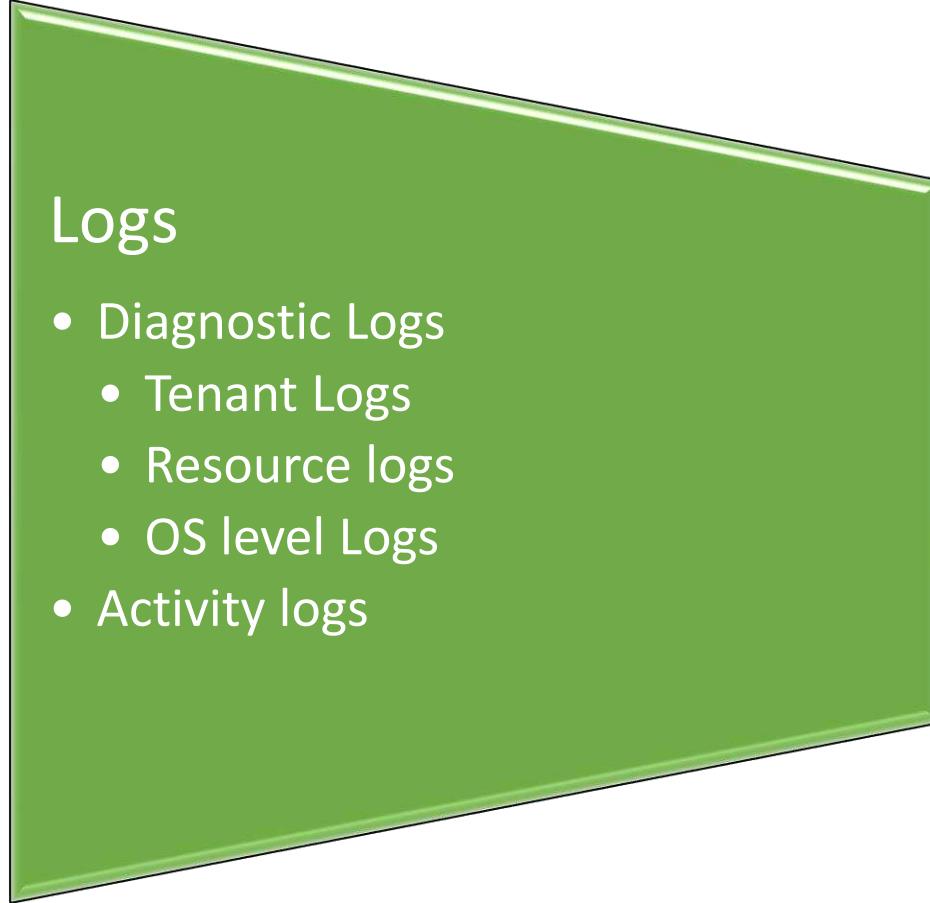




# Monitoring Data Type



Metrics



## Logs

- Diagnostic Logs
  - Tenant Logs
  - Resource logs
  - OS level Logs
  - Activity logs

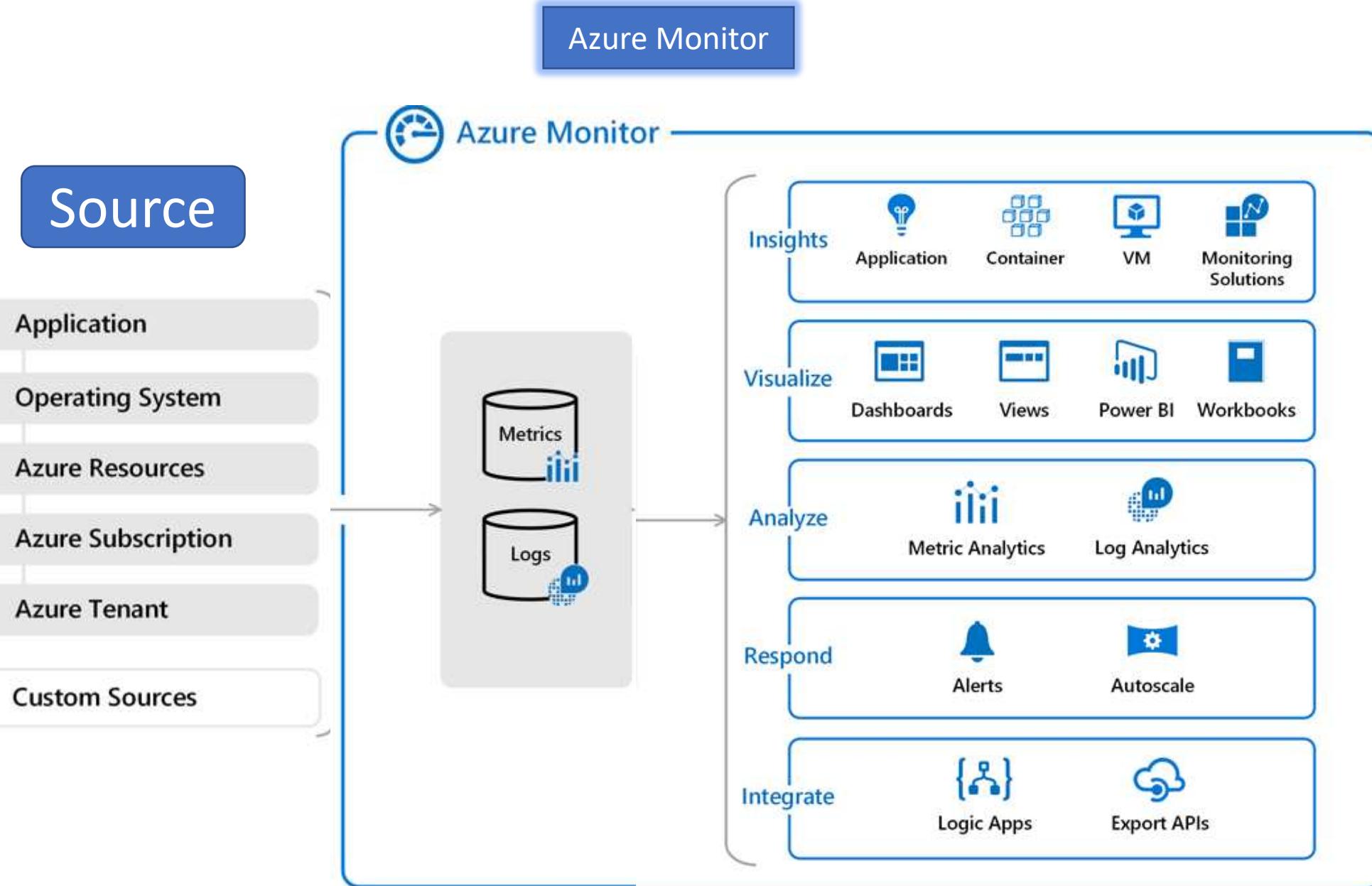
# Monitoring Data Type

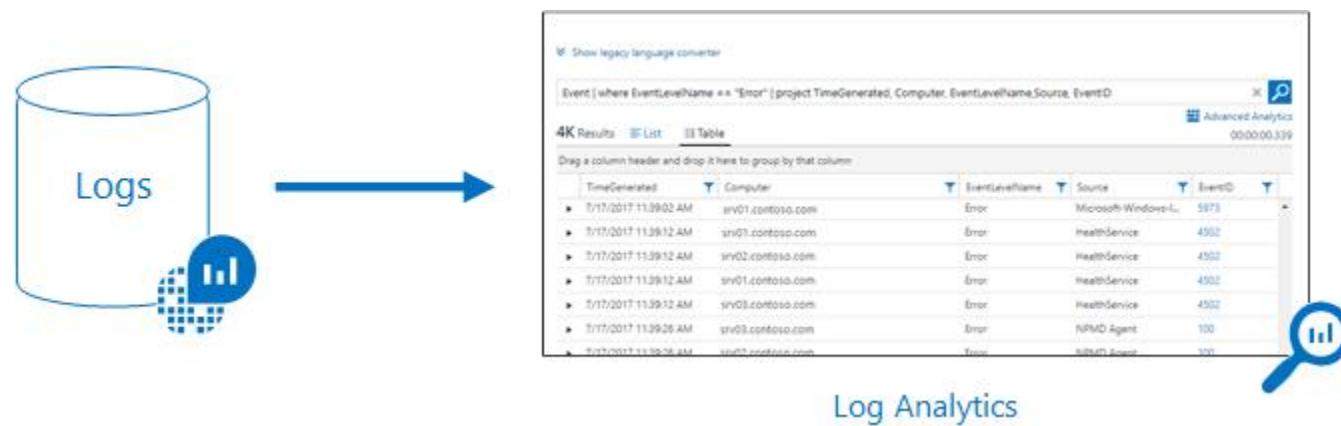


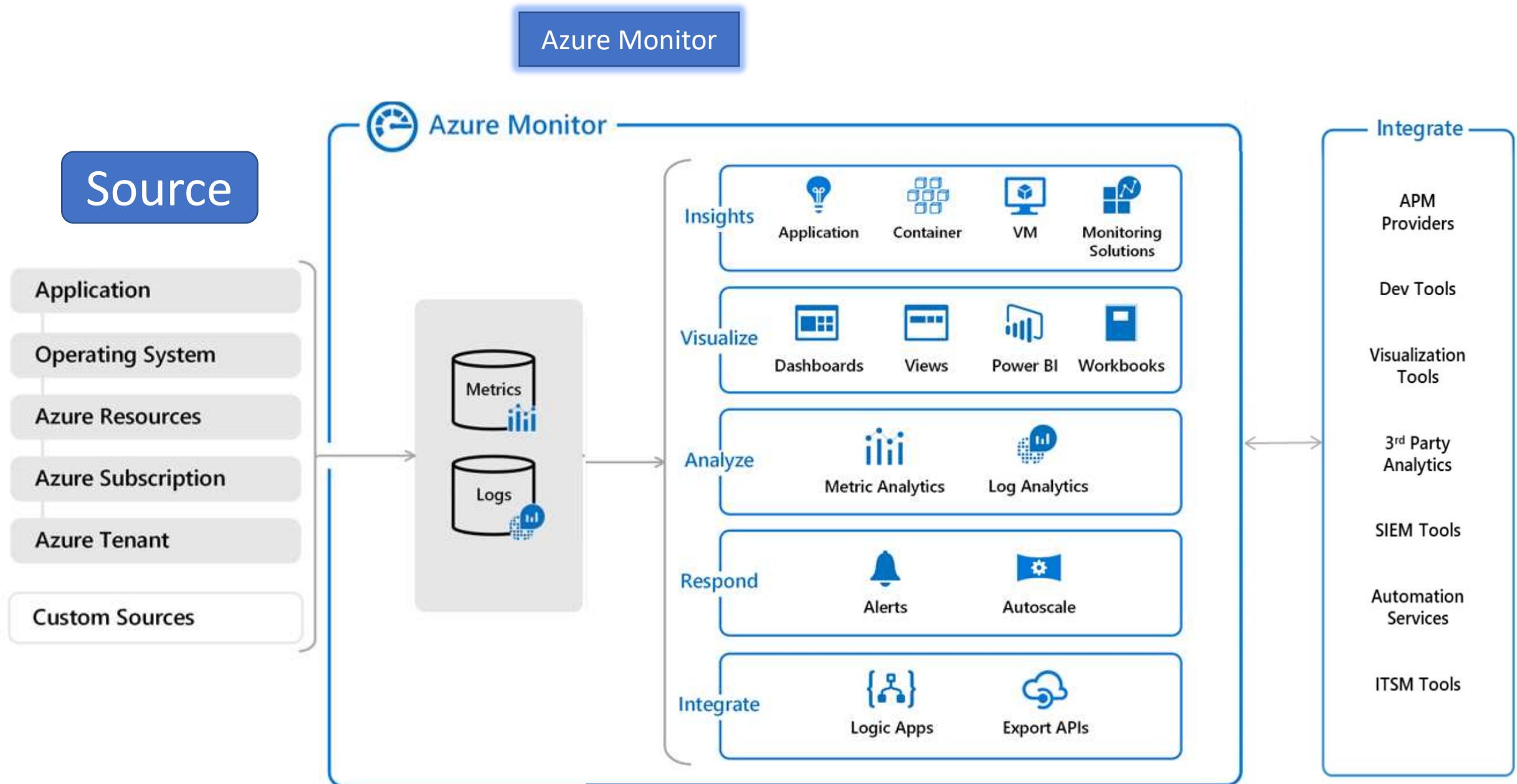
Metrics

## Logs

- Diagnostic Logs
  - Tenant Logs
  - Resource logs
  - OS level Logs
- Activity logs
  - Put, Post and Delete
    - Administrative
    - Service Health
    - Resource Health
  - Alert
  - Auto scale
  - Security
  - Policy



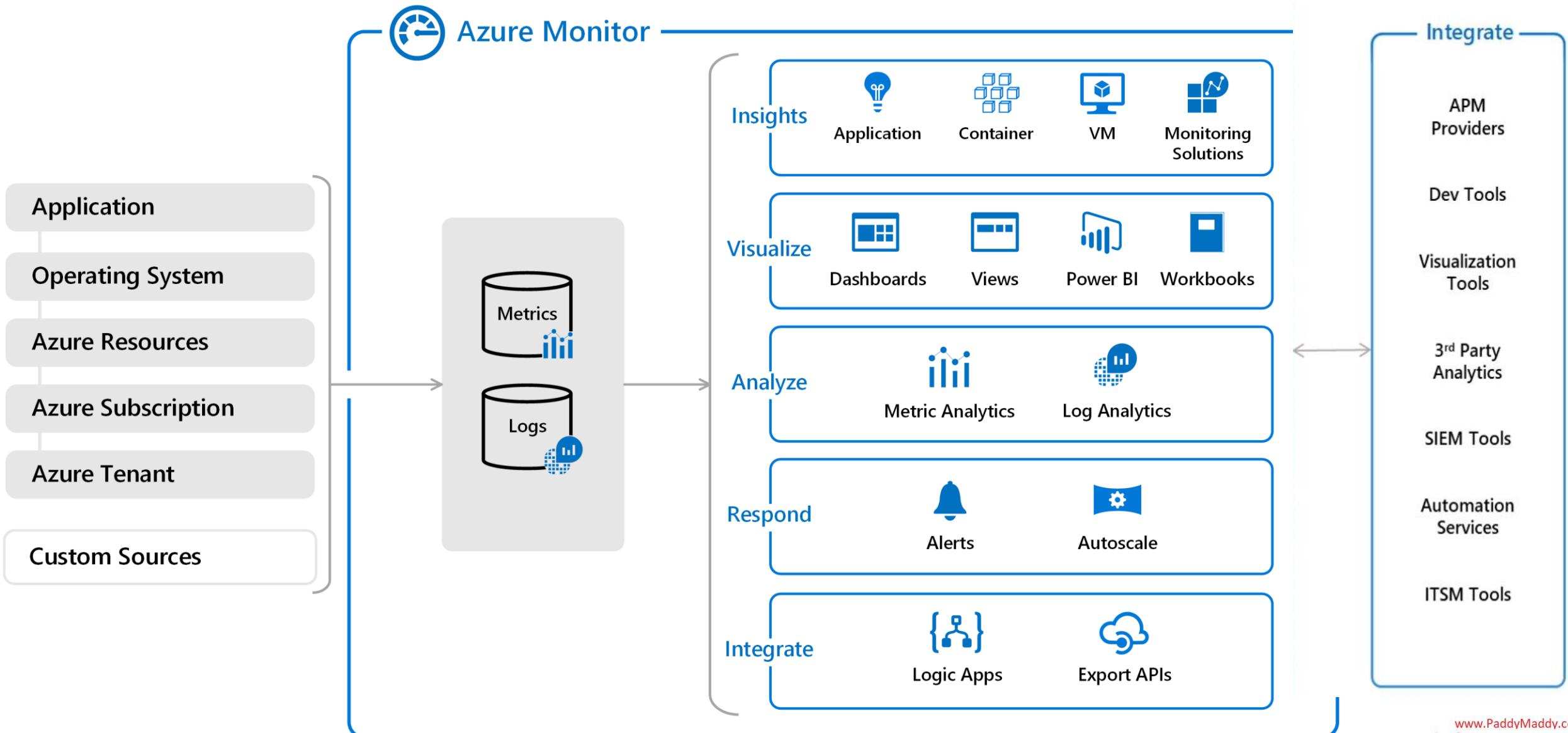




## What data does Azure Monitor collect?

- Azure Monitor can collect data from a variety of sources. You can think of monitoring data for your applications in tiers ranging from your application, any operating system and services it relies on, down to the platform itself. Azure Monitor collects data from each of the following tiers:
- **Application monitoring data:** Data about the performance and functionality of the code you have written, regardless of its platform.
- **Guest OS monitoring data:** Data about the operating system on which your application is running. This could be running in Azure, another cloud, or on-premises.
- **Azure resource monitoring data:** Data about the operation of an Azure resource.
- **Azure subscription monitoring data:** Data about the operation and management of an Azure subscription, as well as data about the health and operation of Azure itself.
- **Azure tenant monitoring data:** Data about the operation of tenant-level Azure services, such as Azure Active Directory.

# Azure Monitor



## What is Log Analytics?

Log Analytics is the primary tool in the Azure portal for writing log queries and interactively analyzing their results. Even if a log query is used elsewhere in Azure Monitor, you'll typically write and test the query first using Log Analytics.

Azure Monitor Logs is based on [Azure Data Explorer](#), and log queries are written using the same **Kusto query language (KQL)**. This is a rich language designed to be easy to read and author, and you should be able to start using it with minimal guidance.

- ❑ **Alert rules:** Alert rules proactively identify issues from data in your workspace. Each alert rule is based on a log search that is automatically run at regular intervals. The results are inspected to determine if an alert should be created.
- ❑ **Dashboards:** You can pin the results of any query into an Azure dashboard which allow you to visualize log and metric data together and optionally share with other Azure users.
- ❑ **Views:** You can create visualizations of data to be included in user dashboards with View Designer. Log queries provide the data used by tiles and visualization parts in each view.
- ❑ **Export:** When you import log data from Azure Monitor into Excel or Power BI, you create a log query to define the data to export.
- ❑ **PowerShell:** You can run a PowerShell script from a command line or an Azure Automation runbook that uses **Get-AzOperationalInsightsSearchResults** to retrieve log data from Azure Monitor. This cmdlet requires a query to determine the data to retrieve.
- ❑ **Azure Monitor Logs API:** The Azure Monitor Logs API allows any REST API client to retrieve log data from the workspace. The API request include

## Azure Monitor Log Analytics

### What does a log query look like?

SecurityEvent

```
| where TimeGenerated > ago(7d)  
| where EventID == 4625  
| summarize count() by Computer, bin(TimeGenerated, 1h)  
| render timechart
```

```
app("ContosoRetailWeb").requests  
| summarize count() by bin(timestamp,1hr)  
| join kind= inner (Perf  
| summarize avg(CounterValue)  
by bin(TimeGenerated,1hr))  
on $left.timestamp == $right.TimeGenerated
```

The screenshot shows the Azure Log Analytics query editor interface. The top navigation bar includes 'New Query 1\*', a '+' button, the workspace name 'contosoretail-it', a 'Schema' tab, a 'Filter' tab, and a search bar. The main area has a 'RUN' button and a 'Time range: Last 24 hours' selector. Below these are 'Save', 'Copy link', 'Export', 'New alert rule', and 'Pin' buttons. The query editor displays the following log query:

```
Event  
| where EventLevelName == "Error"  
| project TimeGenerated, Computer, EventLevelName, Source, EventID
```

The results pane shows a table of log entries from the last 24 hours. The table has columns: TimeGenerated [Local Time], Computer, EventLevelName, Source, and EventID. The data is as follows:

TimeGenerated [Local Time]	Computer	EventLevelName	Source	EventID
2018-08-15T08:28:34.953	ContosoAzADDS1.ContosoRetail.com	Error	Microsoft-Windows-COMRuntime	10,031
2018-08-15T08:28:44.000	sqlserver-1.contoso.com	Error	MSSQLSERVER	9,642
2018-08-15T08:09:32.093	ContosoAzADDS1.ContosoRetail.com	Error	Microsoft-Windows-COMRuntime	10,031
2018-08-15T08:10:10.703	mycon	Error	Microsoft-Windows-Perflib	1,023
2018-08-15T07:50:09.190	ContosoWeb1.ContosoRetail.com	Error	Microsoft-Windows-CAPI2	513
2018-08-15T07:50:15.447	ContosoWeb1.ContosoRetail.com	Error	Microsoft-Windows-CAPI2	513
2018-08-15T08:02:32.517	On-Premise-16S	Error	Microsoft-Windows-Perflib	1,008
2018-08-15T07:39:30.017	ContosoMABSVM1.ContosoRetail.com	Error	Microsoft-Windows-COMRuntime	10,031

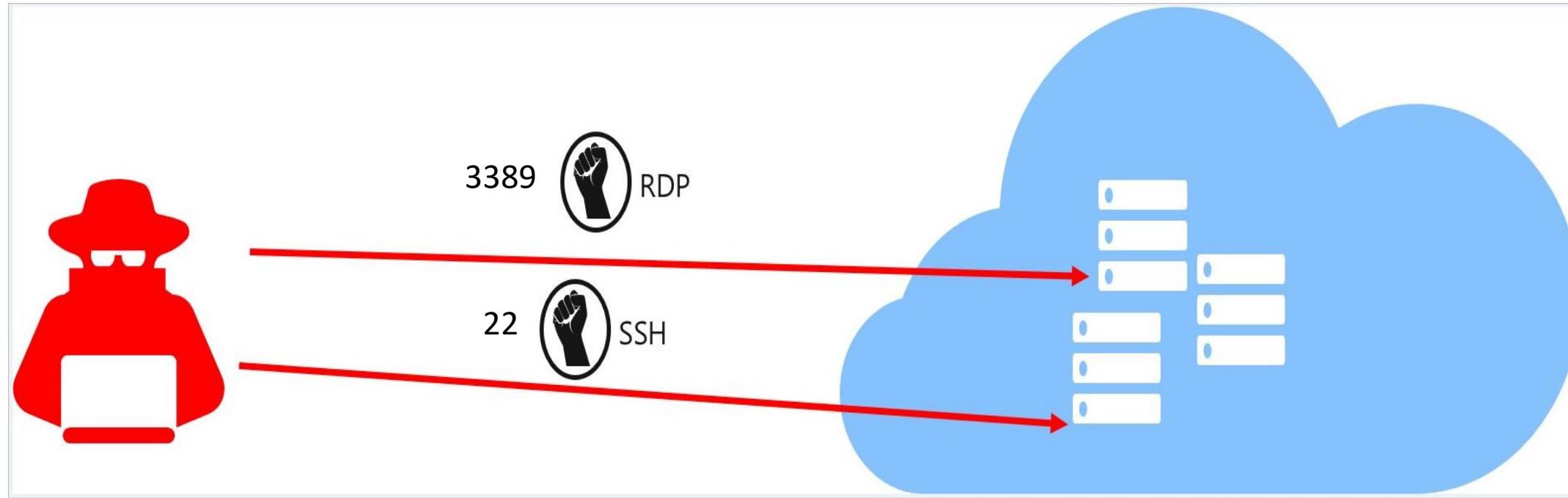
Details for the results table include: contosoretail-it, 00:00:01.072, 411 records, Display time (UTC-07:00).



thank you!



## Secure your Management Ports with Just-in-time (JIT) Access



A photograph of a swimming pool with multiple lanes. The water is a clear blue. In the foreground, a hand is holding a silver stopwatch. The background shows the lane lines and the edge of the pool. A white rectangular box with the text "thank you!" is overlaid on the image.

thank you!



- ❑ **Security Operations Section** - Azure PlayBook and how we can use those to proactively notify us or perform an action based on a triggered alert in Azure security center.
- ❑ A PlayBook is simply a collection of procedures, and the procedures are executed when the PlayBook is triggered.
- ❑ Now we can trigger a PlayBook against security alerts that are generated in Microsoft Azure Security Center.



thank you!



## Storage Analytics Data Retention Policies

### mydemoappstorageac | Diagnostic settings (classic)

Storage account

Search (Ctrl+ /) < Save Discard Refresh

Status: **On**

**Blob properties** (highlighted)

File properties Table properties Queue properties

Hour metrics

Enable

Include API metrics

Delete data after 7 days

7

Minute metrics

Enable

Logging

Logging version: 1.0

Read

Write

Delete

Firewalls and virtual networks

Advanced security

Properties

Locks

Export template

**Blob service**

Containers

Custom domain

Data protection

Azure CDN

Add Azure Search

**File service**

File shares

Soft delete



A photograph of a swimming pool with multiple lanes. The water is a vibrant blue. In the foreground, a hand is holding a silver stopwatch. The background shows the pool's edge with red and white lane markers.

thank you!

- ❑ An unique corporate or governmental standard, and that's called data sovereignty.
- ❑ Data sovereignty simply means that your data has to reside within a certain country, usually within the country where your corporation resides.



thank you!



- **Secrets Management** - Azure Key Vault can be used to Securely store and tightly control access to tokens, passwords, certificates, API keys, and other secrets
- **Key Management** - Azure Key Vault can also be used as a Key Management solution. Azure Key Vault makes it easy to create and control the encryption keys used to encrypt your data.
- **Certificate Management** - Azure Key Vault is also a service that lets you easily provision, manage, and deploy public and private Transport Layer Security/Secure Sockets Layer (TLS/SSL) certificates for use with Azure and your internal connected resources.
- **Store secrets backed by Hardware Security Modules** - The secrets and keys can be protected either by software or FIPS 140-2 Level 2 validated HSMs

## Why use Azure Key Vault

**Centralize application secrets**

**Securely store secrets and keys**

**Monitor access and use**

**Simplified administration of application secrets**

**Integrate with other Azure services**

## Azure Key Vault Demo Overview

- ❑ Create a Key vault
- ❑ We will create a secret in Key Vault for Password – **vmAdminPassword**
- ❑ Create a ARM Template for Azure VM creation
- ❑ Modify ARM template parameter file with Azure Key vault ID and use Secret
- ❑ Use ARM VM template and deploy a VM with Azure CLI
  - ✓ This will not prompt us for enter Password instead it will get the password from Azure key vault resource ID

A photograph of a swimming pool with multiple lanes. The water is a bright blue. Lane lines are visible, and red and white flags are hanging across the pool. In the bottom right corner, a person's hand is holding a silver stopwatch. The stopwatch has a white face with red and black markings. The text "thank you!" is overlaid on the image in a white box.

thank you!

## Azure Databases

### Databases



#### Azure API for FHIR

Easily create and deploy a FHIR service for health data solutions and interoperability



#### Azure Cache for Redis

Power applications with high-throughput, low-latency data access



#### Azure Cosmos DB

Globally distributed, multi-model database for any scale



#### Azure Database for MariaDB

Managed MariaDB database service for app developers



#### Azure Database for MySQL

Managed MySQL database service for app developers



#### Azure Database for PostgreSQL

Managed PostgreSQL database service for app developers



#### Azure Database Migration Service

Simplify on-premises database migration to the cloud



#### Azure SQL

Modern SQL family for migration and app modernization



#### Azure SQL Database

Managed, intelligent SQL in the cloud



#### Azure SQL Edge (Preview)

Small-footprint, edge-optimized data engine with built-in AI



#### Azure SQL Managed Instance

Managed, always up-to-date SQL instance in the cloud



#### SQL Server on Azure Virtual Machines

Host enterprise SQL Server apps in the cloud



#### Table Storage

NoSQL key-value store using semi-structured datasets

### Managed Database's

## Azure Databases

### Databases

#### Azure API for FHIR

Easily create and deploy a FHIR service for health data solutions and interoperability

#### Azure SQL Database

Managed, intelligent SQL in the cloud

#### Azure Cache for Redis

Power applications with high-throughput, low-latency data access

#### Azure Database for PostgreSQL

Managed PostgreSQL database service for app developers

#### Azure Database for MySQL

Managed MySQL database service for app developers

#### Azure SQL Edge PREVIEW

Small-footprint, edge-optimised data engine with built-in AI

#### SQL Managed Instance

Managed, always up-to-date SQL instance in the cloud

#### SQL Server on Virtual Machines

Host enterprise SQL Server apps in the cloud

#### Azure Cosmos DB

Globally distributed, multi-model database for any scale

#### Table Storage

NoSQL key-value store using semi-structured datasets

#### Azure Database for MariaDB

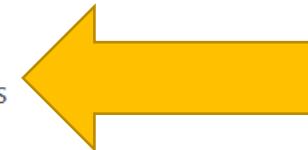
Managed MariaDB database service for app developers

#### Azure Database Migration Service

Simplify on-premises database migration to the cloud

#### Azure SQL

Modern SQL family for migration and app modernisation



Marketplace 

My Saved List

X

Pricing : All

Operating System : All

Publisher : All

Recently created

Service Providers

Categories

Get Started

AI + Machine Learning

Analytics

Blockchain

Compute

Containers

Databases

Developer Tools

DevOps

Identity

Integration

Internet of Things

IT &amp; Management Tools

Media

Mixed Reality

Networking

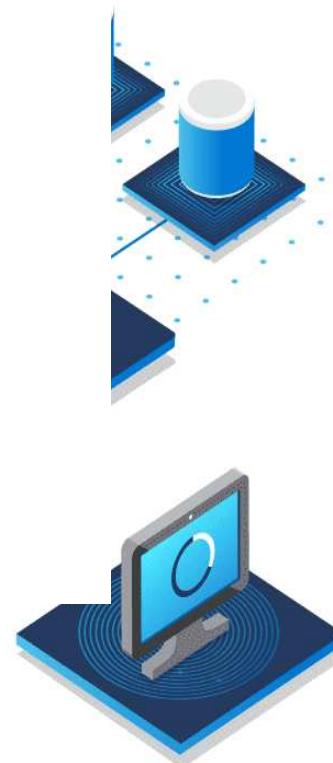
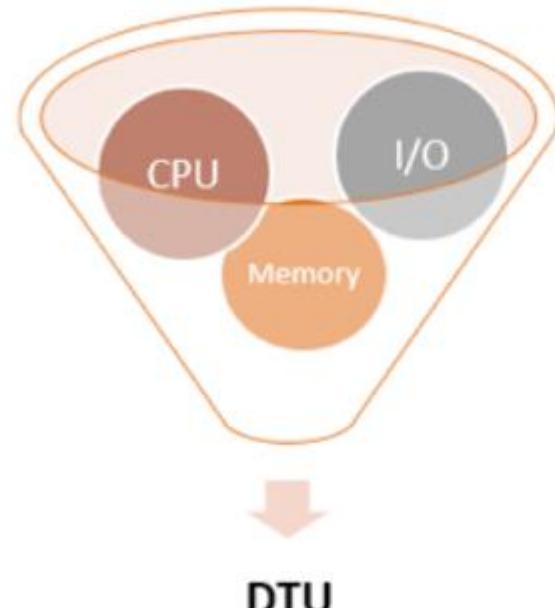
Security

Software as a Service (SaaS)

Storage

Web

Name	Publisher	Category
 Database Performance Analyzer	SolarWinds	Analytics
 Heimdall Database Proxy <span data-bbox="550 429 627 453">Free trial</span>	Heimdall Data	Analytics
 EXASOL Analytics Database (BYOL)	EXASOL	Analytics
 Exasol Analytics Database (EnterpriseSupport,PAYG)	EXASOL	Analytics
 Azure Database for MySQL	Microsoft	Databases
 Postgres Pro Standard Database 10 (VM)	Postgres Professional	Databases
 Tidal Migrations -Premium Insights for Database <span data-bbox="550 717 627 741">Free trial</span>	tidalmigrations.com	
 Moodle with Azure Database for MySQL	Bitnami	Web
 TIBCO Graph Database	TIBCO Software Inc.	Analytics
 SQL Database	Microsoft	Databases
 Azure Database for MariaDB	Microsoft	Databases
 Azure Database for PostgreSQL	Microsoft	Databases
 Oracle Database 19.3.0.0	Oracle	Databases
 DataSunrise Data & Database Security for Azure	DataSunrise, Inc.	Analytics
 Postgres Pro Enterprise Database 10 (VM) <span data-bbox="550 1177 627 1202">Free trial</span>	Postgres Professional	Databases
 Striim for Real-Time Integration to SQL Database	Striim, Inc.	Analytics
 Postgres Pro Enterprise Database 9.6 (VM) <span data-bbox="550 1293 627 1317">Free trial</span>	Postgres Professional	Databases
 Postgres Pro Standard Database 11 (VM)	Postgres Professional	Databases
 Postgres Pro Standard Database 9.6 (VM)	Postgres Professional	Databases
Postgres Pro Standard Database 12 (VM)	Postgres Professional	Databases
Postgres Pro Enterprise Database 12 (VM) <span data-bbox="550 1523 627 1440">Free trial</span>	Postgres Professional	Databases



- We store data in tables with rows and columns.
- SQL server features like stored procedures, user defined functions and all of the T-SQL language
- Relational Database-as-a-Service
- Uses latest stable version of Microsoft SQL
- You can migrate the database from on-premises to Azure SQL Database with Microsoft Data migration Assistant
- Performance with DTU's /**Elastic pool eDTU**

Microsoft provides a number of different deployment options for its Azure SQL Database offerings

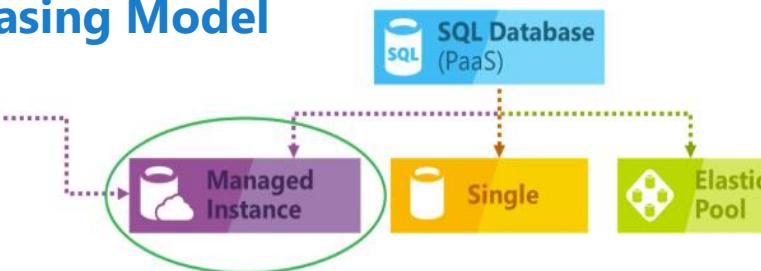
# Azure SQL Database Managed Instance

- ❑ Part of the Azure SQL product family, Azure SQL Managed Instance is the intelligent, scalable cloud database service that combines the broadest SQL Server database engine compatibility with all the benefits of a fully managed and evergreen platform as a service.
- ❑ SQL Managed Instance has near 100% compatibility with the latest SQL Server (Enterprise Edition) database engine, providing a native [virtual network \(VNet\)](#) implementation that addresses common security concerns, and a [business model](#) favorable for existing SQL Server customers.
- ❑ SQL Managed Instance allows existing SQL Server customers to lift and shift their on-premises applications to the cloud with minimal application and database changes.
- ❑ At the same time, SQL Managed Instance preserves all PaaS capabilities (automatic patching and version updates, [automated backups, high availability](#)) that drastically reduce management overhead and TCO.

## What is SQL Database Managed Instance?

### vCore-based Purchasing Model

New deployment option that enables [frictionless migration](#) for SQL apps and [modernization](#) in a fully managed service



#### Easy lift and shift

- Fully-fledged SQL instance with nearly 100% compat with on-prem

#### Fully managed PaaS

- Built on the same PaaS service infrastructure
- All PaaS features

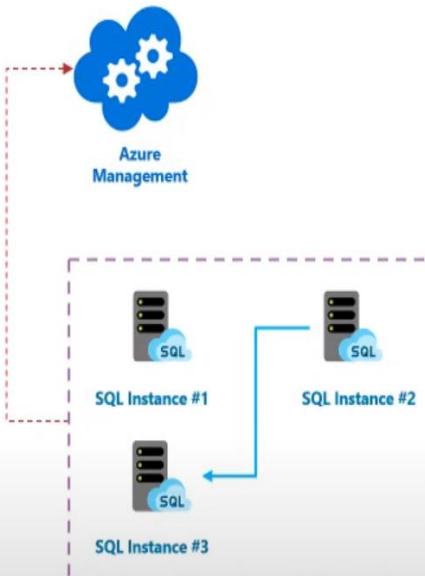
#### Full isolation and security

- Native VNET implementation
- Private IP addresses

#### New business model

- Competitive
- Transparent
- Frictionless

## Azure SQL Managed Instance



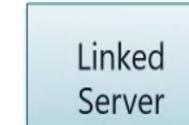
CLR



SQL Agent



Cross Database Queries



Linked Server



SQL Profiler



Native Restore



Log Shipping



Trans. Replication



Service Broker

# Azure Synapse Analytics

formerly

## know as Azure SQL Data Warehouse

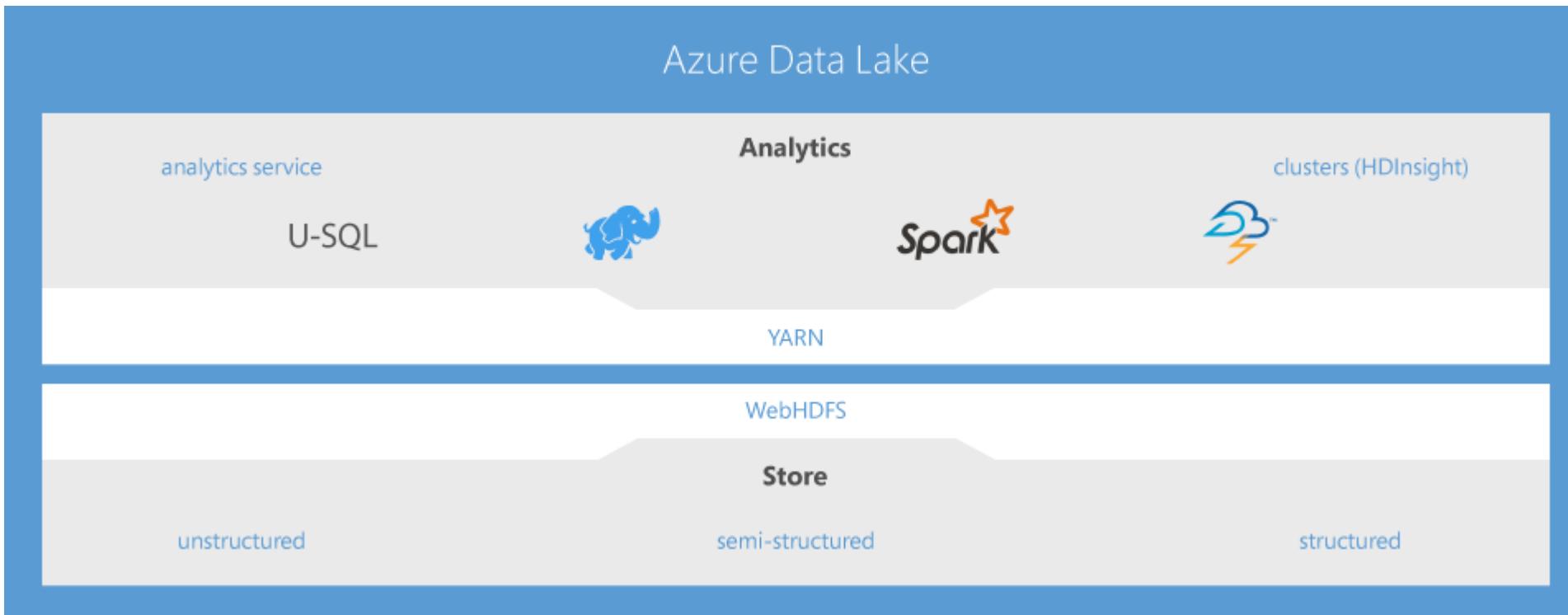
- ❑ Azure Synapse is an analytics service that brings together enterprise data warehousing and Big Data analytics.
- ❑ It gives you the freedom to query data on your terms, using either serverless on-demand or provisioned resources—at scale.
- ❑ Azure Synapse brings these two worlds together with a unified experience to ingest, prepare, manage, and serve data for immediate BI and machine learning needs.

### Key component of a big data solution



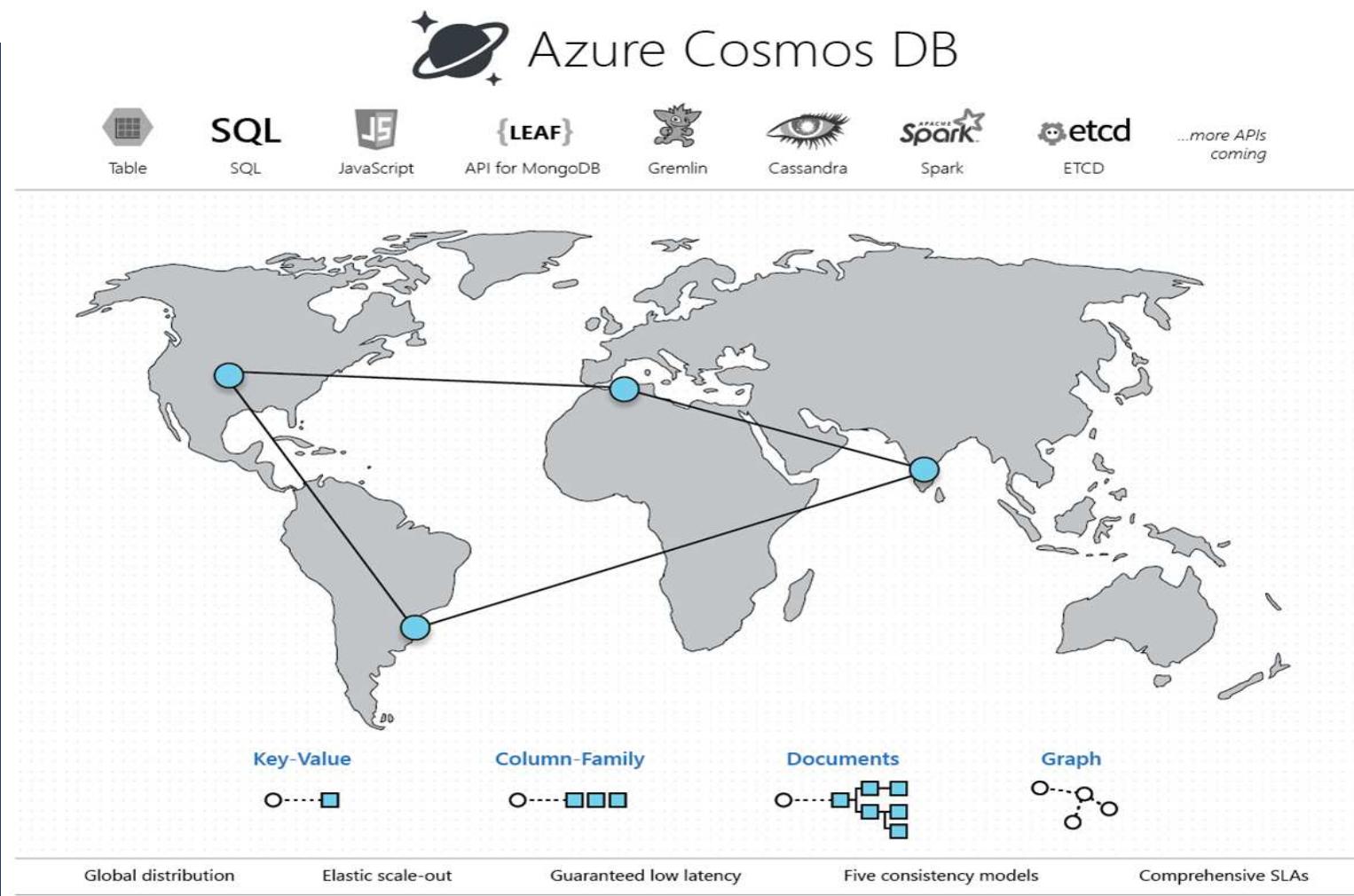
## Azure Data Lake Storage.

- ❑ Azure Data Lake includes all the capabilities required to make it easy for developers, data scientists and analysts to store data of any size, shape and speed, and do all types of processing and analytics across platforms and languages.
- ❑ It removes the complexities of ingesting and storing all of your data while making it faster to get up and running with batch, streaming and interactive analytics.
- ❑ Azure Data Lake works with existing IT investments for identity, management and security for simplified data management and governance.
- ❑ It also integrates seamlessly with operational stores and data warehouses so you can extend current data applications



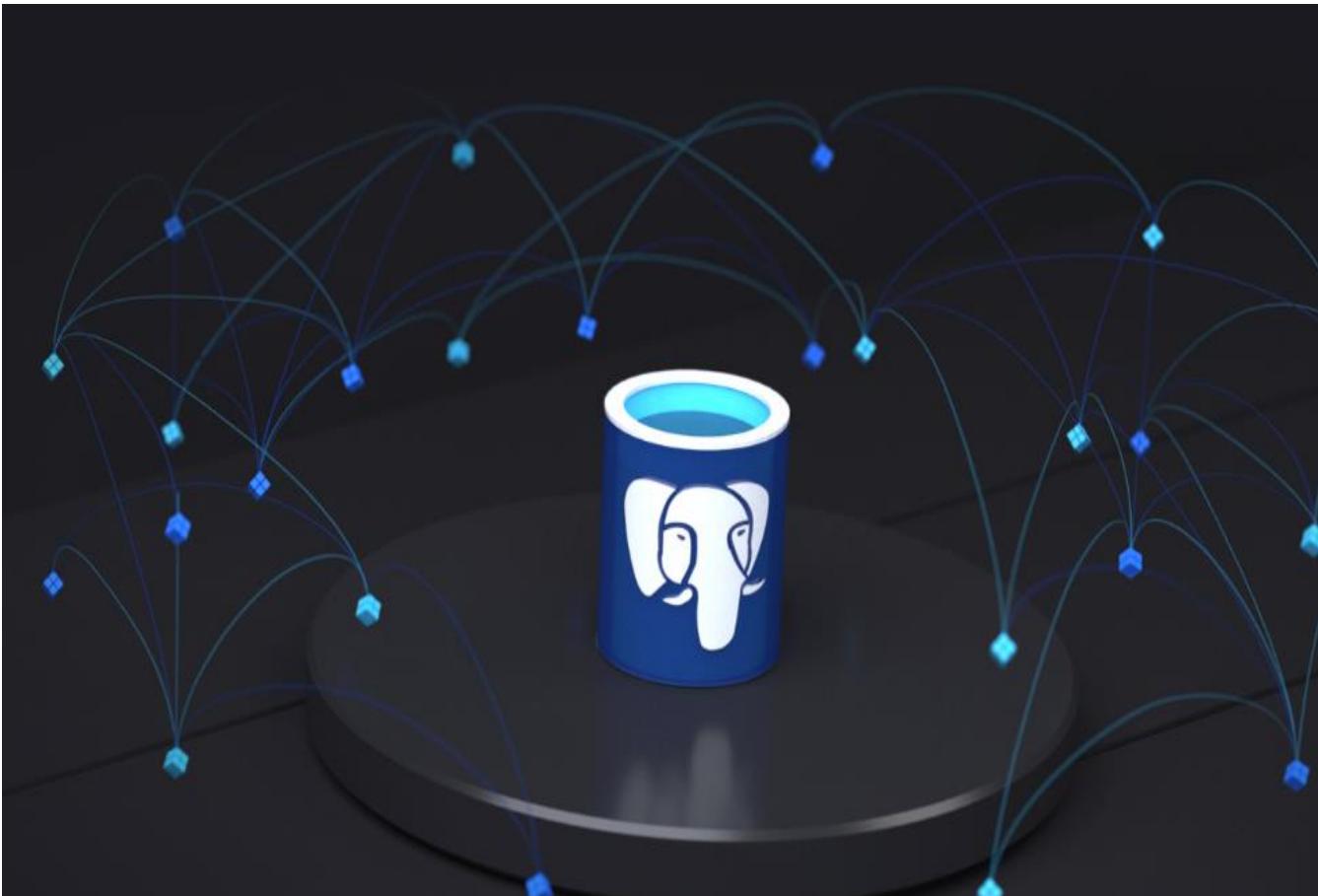
## Cosmos DB

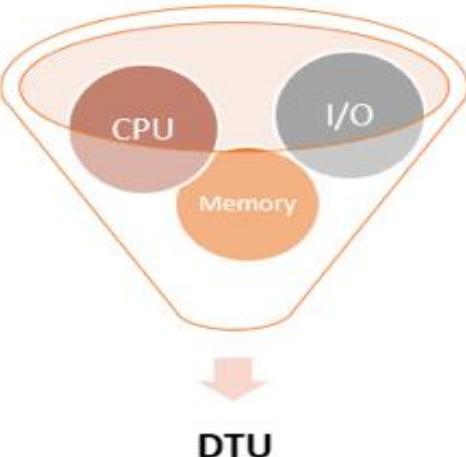
Azure Cosmos DB is Microsoft's globally distributed, multi-model database service. With a click of a button, Cosmos DB enables you to elastically and independently scale throughput and storage across any number of Azure regions worldwide. You can elastically scale throughput and storage, and take advantage of fast, single-digit-millisecond data access using your favorite API including: SQL, MongoDB, Cassandra, Tables, or Gremlin.



## Azure Database for PostgreSQL

- ❑ Azure Database for PostgreSQL is fully –Managed, community PostgreSQL in the azure cloud.
- ❑ Focus on application innovation, not database management, with fully managed and intelligent Azure Database for PostgreSQL. Scale your workload quickly with ease and confidence.
- ❑ Azure Database for PostgreSQL Hyperscale is now Azure Arc–enabled. You can run this service on premises on infrastructure of your choice with cloud benefits like automation, hyperscale, unified management, and a cloud billing model with reserved capacity pricing now available.



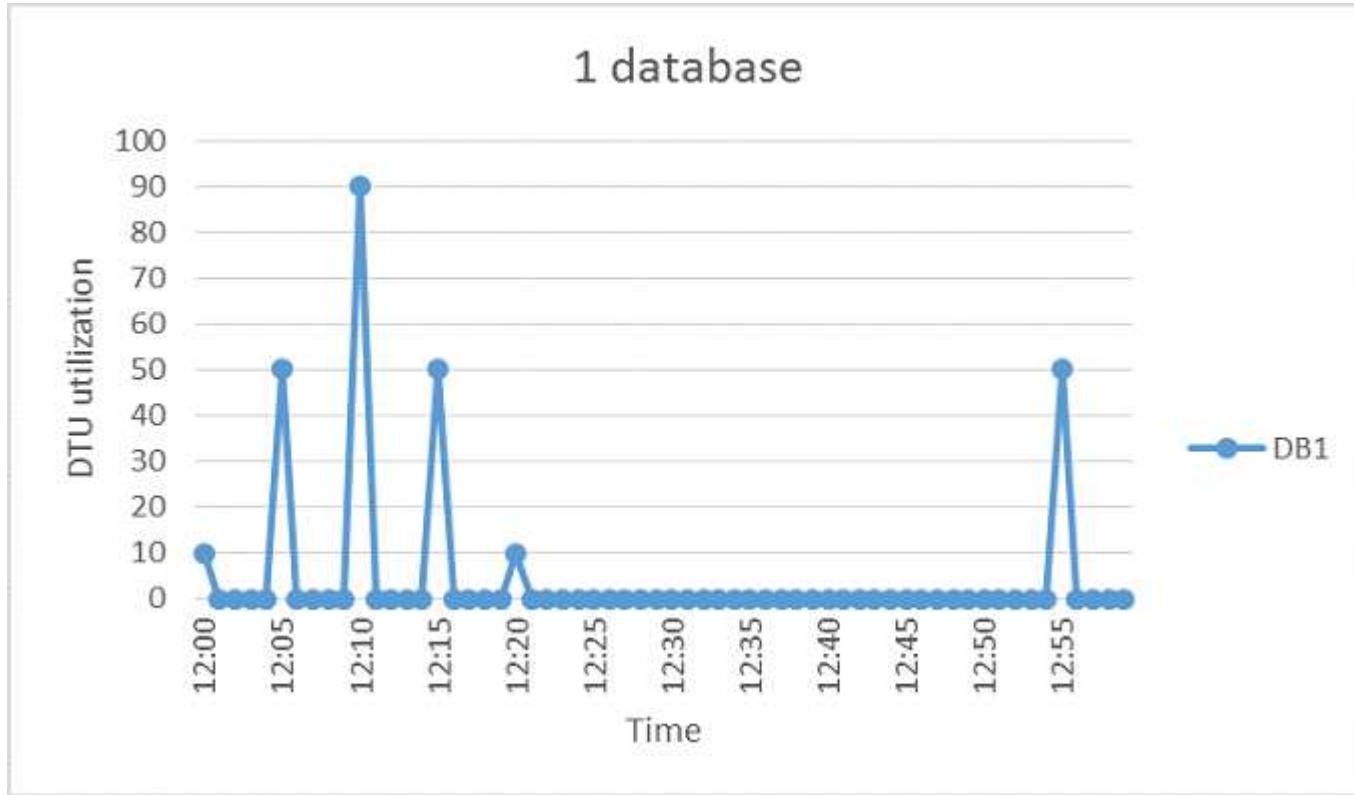


	<b>Basic</b>	<b>Standard</b>	<b>Premium</b>
<b>Target workload</b>	Development and production	Development and production	Development and production
<b>Uptime SLA</b>	99.99%	99.99%	99.99%
<b>Maximum backup retention</b>	7 days	35 days	35 days
<b>CPU</b>	Low	Low, Medium, High	Medium, High
<b>IO throughput (approximate)</b>	1-5 IOPS per DTU	1-5 IOPS per DTU	25 IOPS per DTU
<b>IO latency (approximate)</b>	5 ms (read), 10 ms (write)	5 ms (read), 10 ms (write)	2 ms (read/write)
<b>Columnstore indexing</b>	N/A	S3 and above	Supported
<b>In-memory OLTP</b>	N/A	N/A	Supported
<b>Maximum DTU</b>	5	3000 (S12)	4000 (P15)
<b>Maximum Storage Size</b>	2 GB	250 GB	1 TB

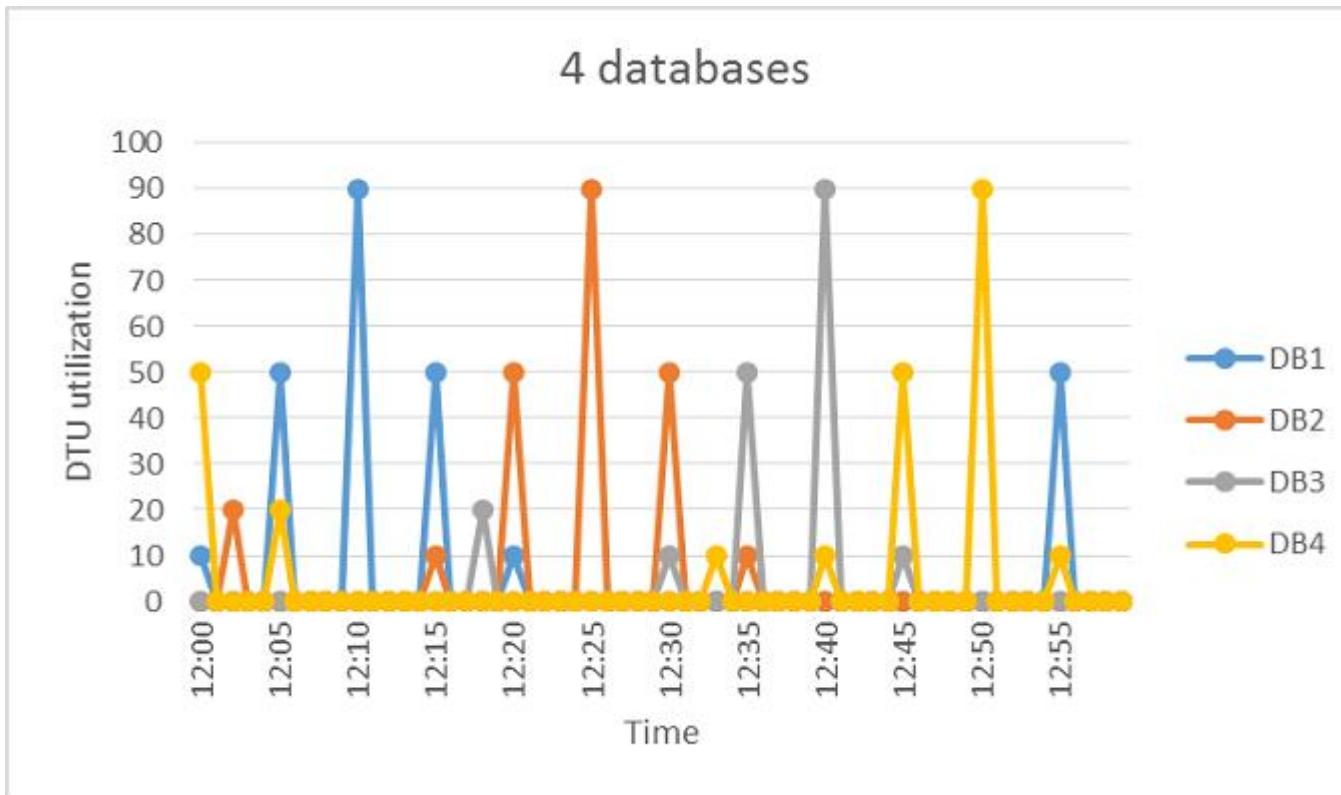
## Mapping DTUs to Traditional Hardware

Number Cores	IOPS	DTUs	Service Tier	Comparable Azure VM Size
1 core, 5% utilization	10	5	Basic	Standard_A0, barely used
<1 core	150	100	Standard S0-S3	Standard_A0, not fully utilized
1 core	up to 4000	500	Premium – P4	Standard_DS1_v2
2-3 cores	up to 12000	1000	Premium – P6	Standard_DS3_v2
4-5 cores	up to 20000	1750	Premium – P11	Standard_DS4_v2
6-13	up to 48000	4000	Premium – P15	Standard_DS5_v2

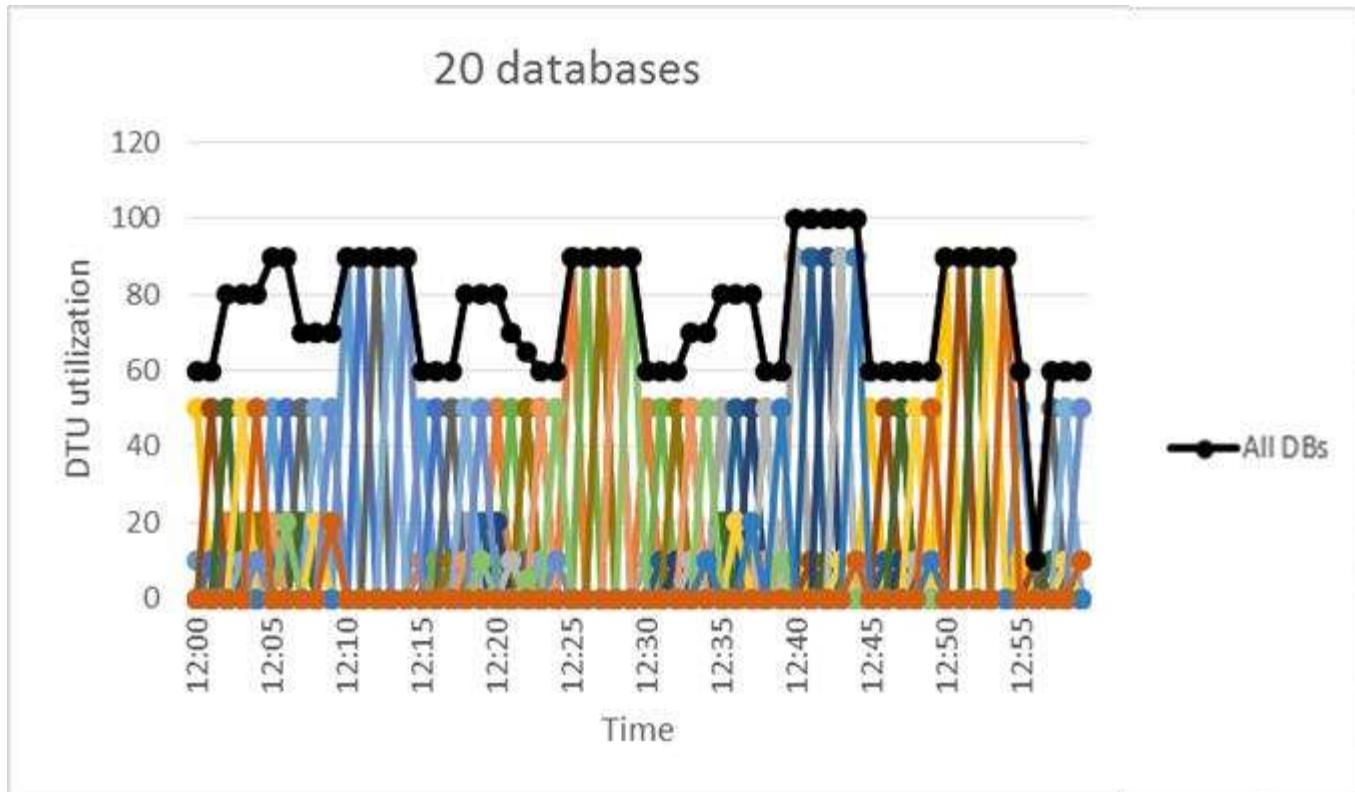
## Assessing database utilization patterns



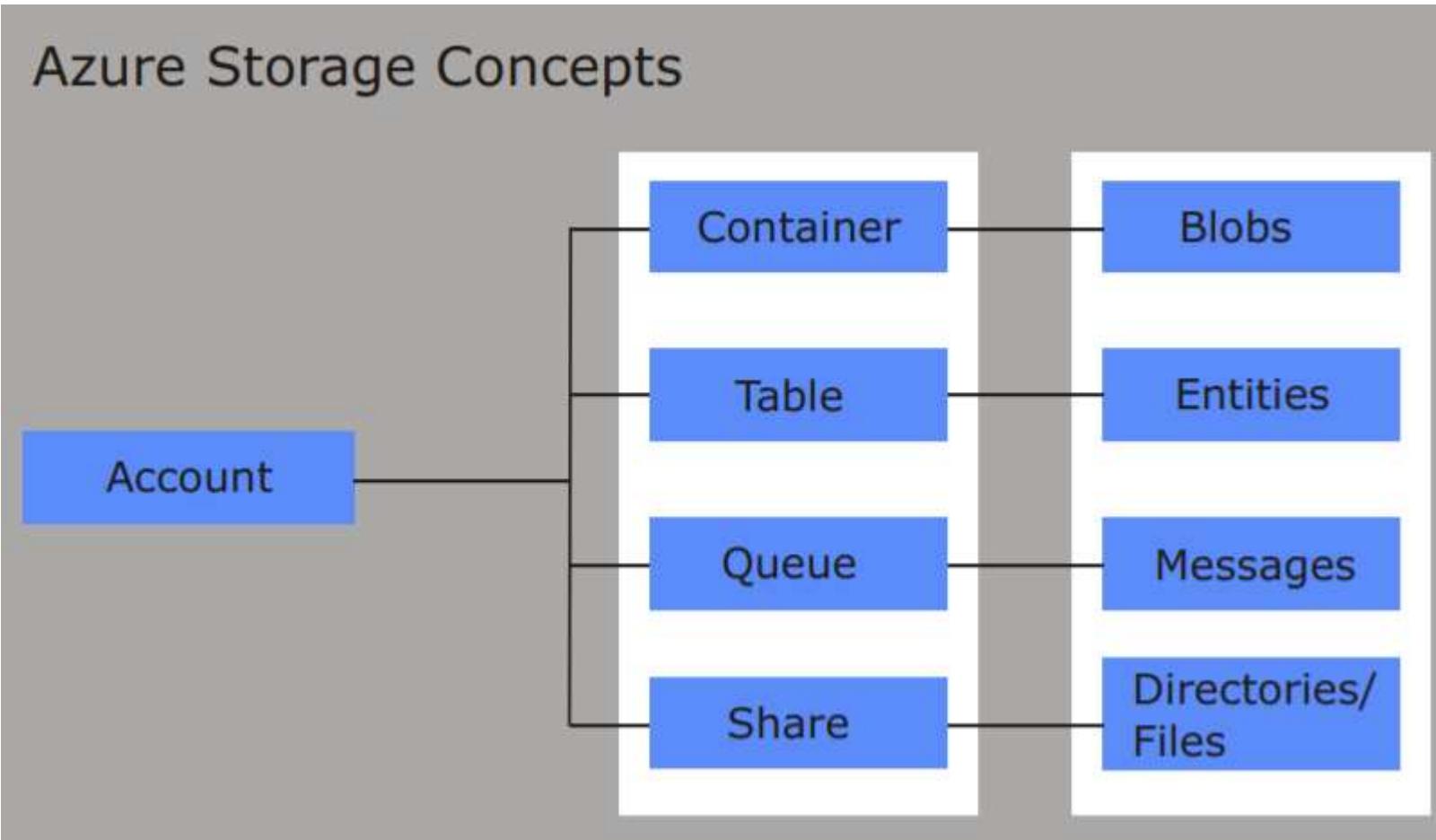
## Assessing database utilization patterns



## Assessing database utilization patterns



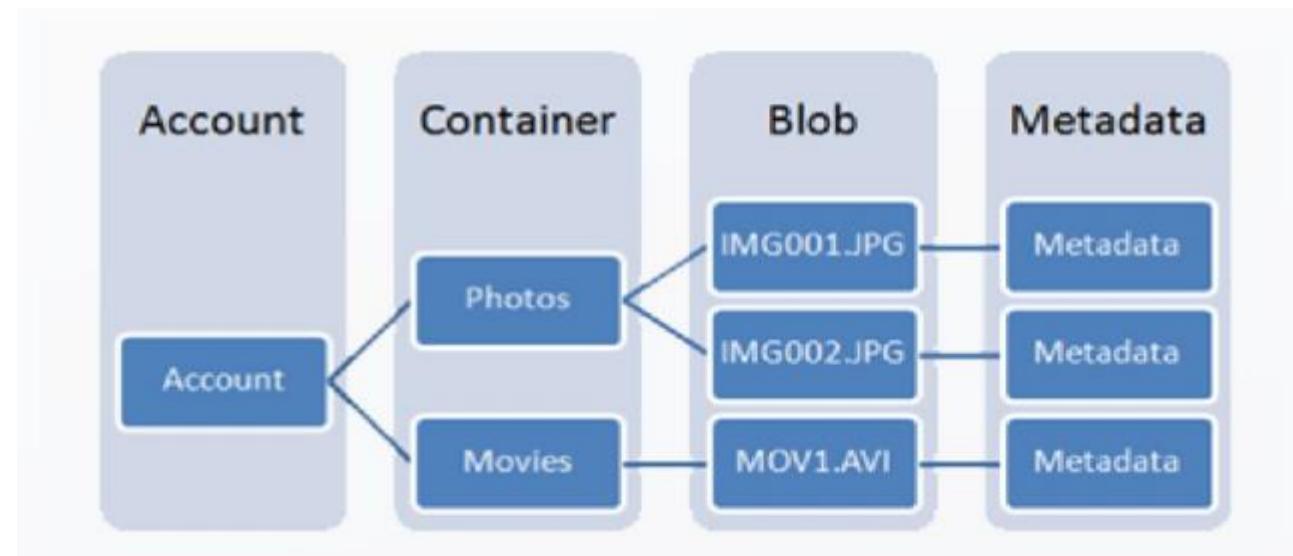
# Azure Storage Account



**Blob Storage:** For users with large amounts of unstructured data to store in the cloud, Blob storage offers a cost-effective and scalable solution. You can use Blob storage to store content such as:

- Data sharing- Documents, photos, videos, music, blogs etc
- Simple REST Interface for putting, getting or deleting blobs.
- Backups of files, computers, databases, and devices.
- Configuration data for cloud applications.
- Big data, such as logs and other large datasets.

Every blob is organized into a container. Containers also provide a useful way to assign security policies to groups of objects. A storage account can contain any number of containers, and a container can contain any number of blobs, up to the 500 TB capacity limit of the storage account.



## SECURING OUR STORAGE ACCOUNTS

### Access Keys

- 1. Key1
- 2. Key2

### SAS

- 1. Account SAS
- 2. Services SAS

## MEDIUM SEVERITY

Someone has accessed your Storage account 'mystorageaccount' from an unusual location.

## Activity details

**Subscription ID** 00000000-0000-0000-0000-000000000000

**Storage account** mystorageaccount

**Storage type** Blob

**Container** mycontainer

**Application** myTestApplication

**IP address** 192.168.1.100

**Location** Washington, United States

**Data center** scus

**Date** May 17, 2018 7:50 UTC

**Potential causes** Unauthorized access that exploits an opening in the firewall. Legitimate access from a new location

**Investigation steps** For a full investigation, configure diagnostics logs for read, write, and delete

**Remediation steps** Be sure to follow the principle of "least privilege" and limit access to your data

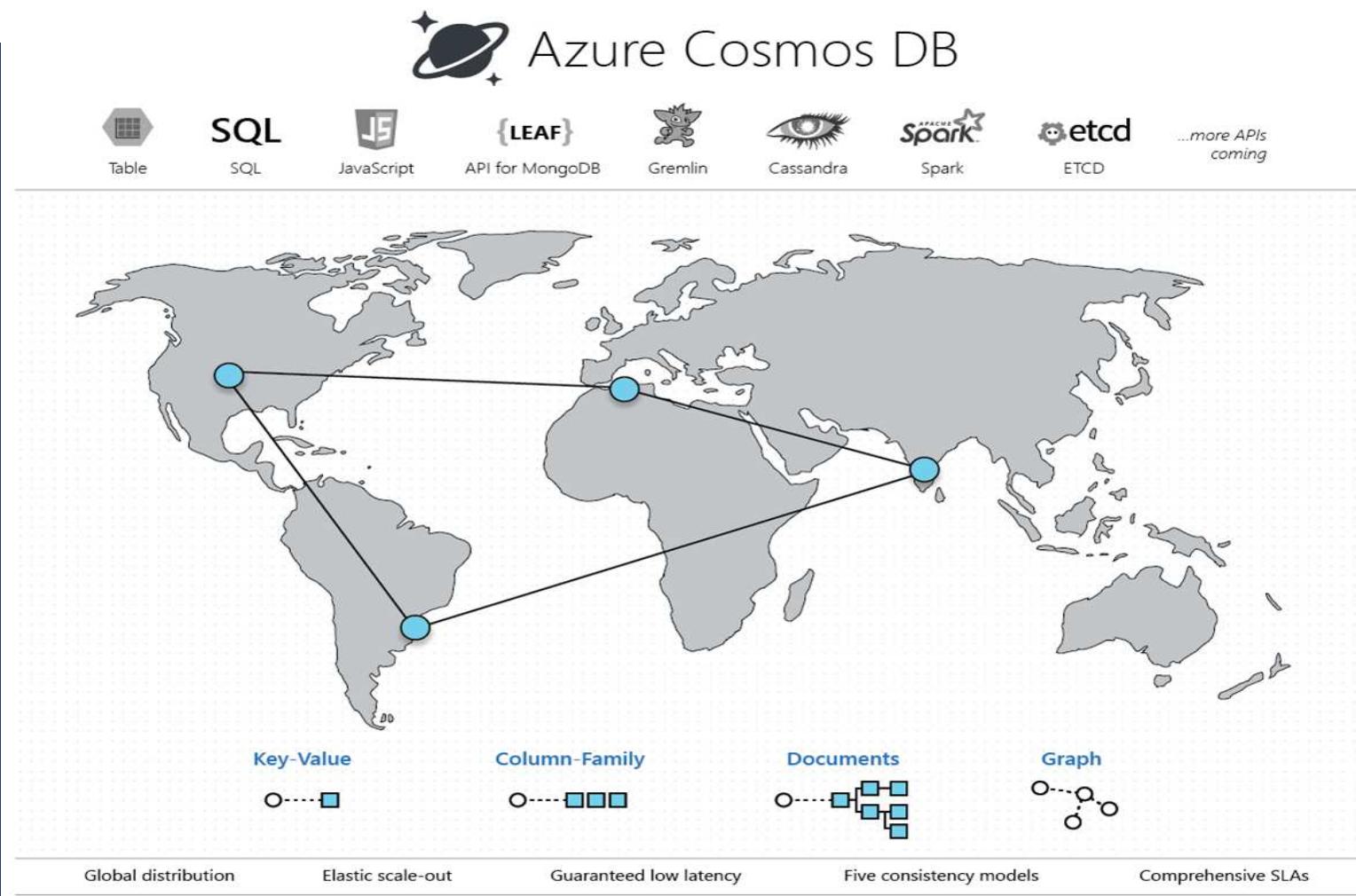


thank you!

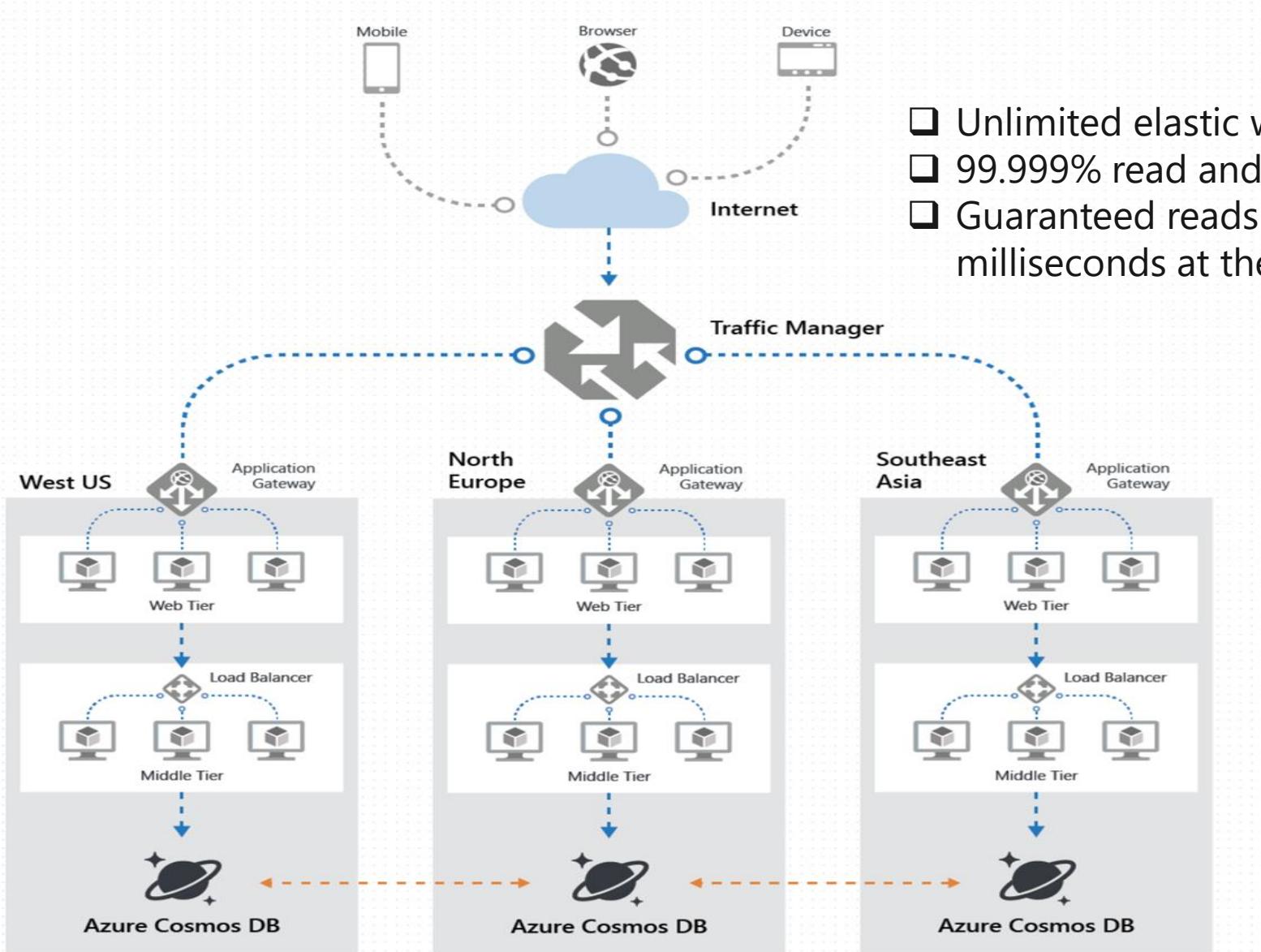


## Cosmos DB

Azure Cosmos DB is Microsoft's globally distributed, multi-model database service. With a click of a button, Cosmos DB enables you to elastically and independently scale throughput and storage across any number of Azure regions worldwide. You can elastically scale throughput and storage, and take advantage of fast, single-digit-millisecond data access using your favorite API including: SQL, MongoDB, Cassandra, Tables, or Gremlin.



## Global Data Distribution with Azure Cosmos DB

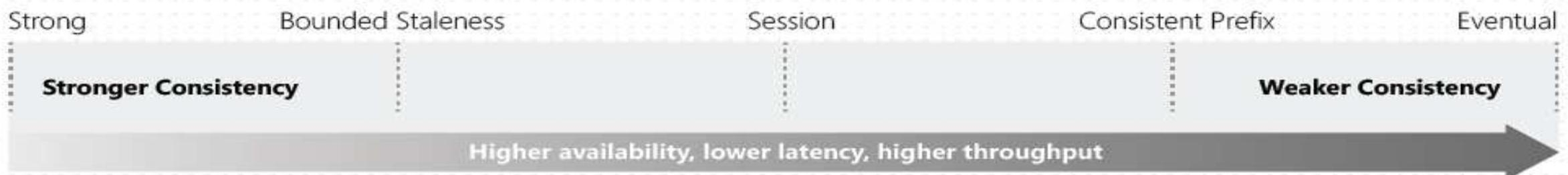


- ❑ Unlimited elastic write and read scalability.
- ❑ 99.999% read and write availability all around the world.
- ❑ Guaranteed reads and writes served in less than 10 milliseconds at the 99th percentile.

### API's Examples

- ❑ Document DB (SQL) API
- ❑ MongoDB API
- ❑ Graph / Gremlin API
- ❑ Tables / Key/Value API

## Consistency levels in Azure Cosmos DB



- Ensures Documents in Replicates do not lag behind the primary
- Recommended for applications that require all replicas to exactly match the primary at any point in time
- Negative affect on the write operations

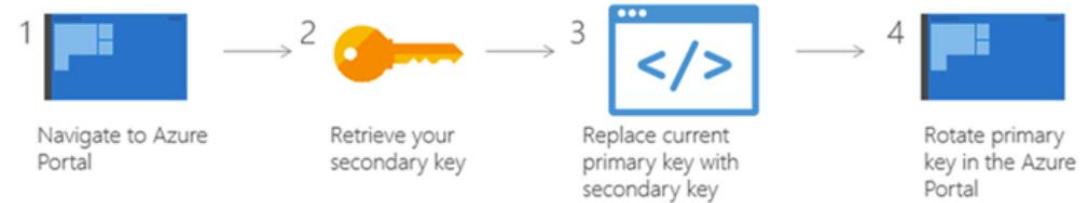
- Ensures database operates at peak efficiency
- Recommended for al apps that requited high performance
- Read operations against a replica can return stale data

## Secure access to data in Azure Cosmos DB

Azure Cosmos DB uses two types of keys to authenticate users and provide access to its data and resources.

1. Master keys
2. Resource tokens

### 1. Master keys



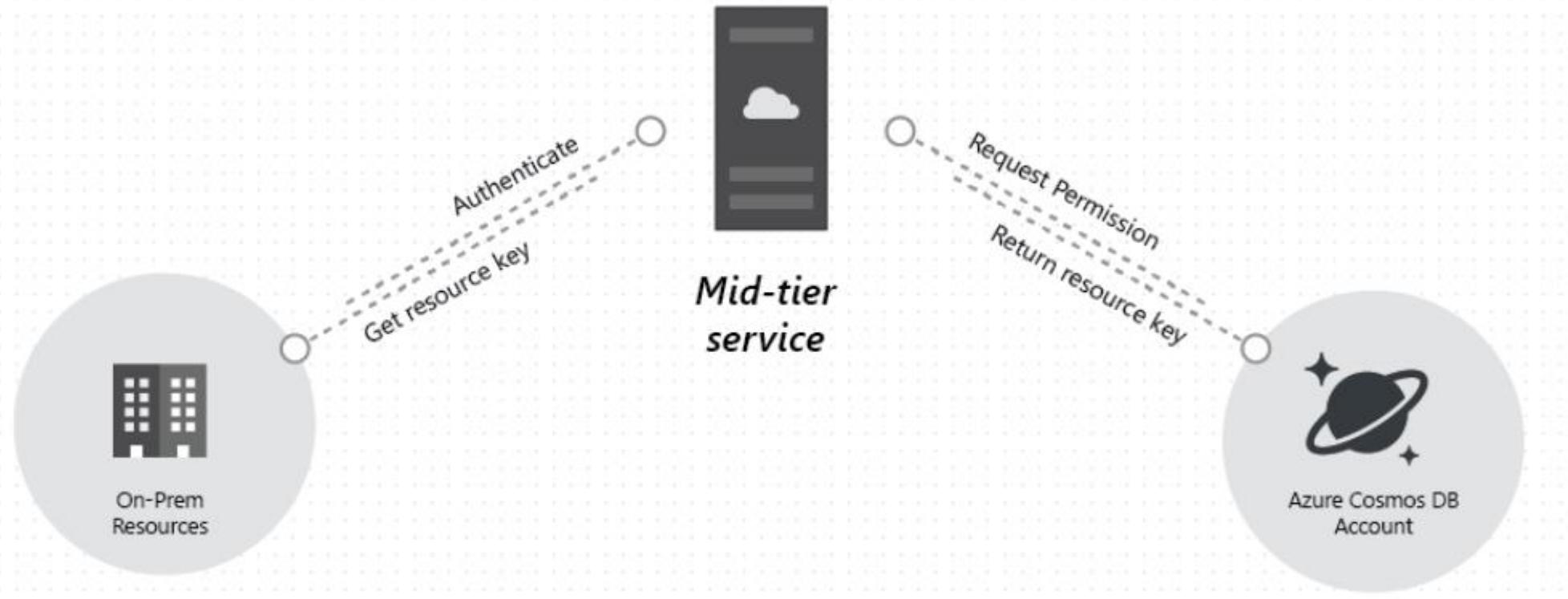
Master keys provide access to all the administrative resources for the database account. Master keys:

- Provide access to accounts, databases, users, and permissions.
- Cannot be used to provide granular access to containers and documents.
- Are created during the creation of an account.
- Can be regenerated at any time.

### 2. Resource tokens

- Provide access to specific containers, partition keys, documents, attachments, stored procedures, triggers, and UDFs.
- Are created when a user is granted permissions to a specific resource.
- Are recreated when a permission resource is acted upon on by POST, GET, or PUT call.
- Use a hash resource token specifically constructed for the user, resource, and permission.
- Are time bound with a customizable validity period. The default valid time span is one hour. Token lifetime, however, may be explicitly specified, up to a maximum of five hours.
- Provide a safe alternative to giving out the master key.
- Enable clients to read, write, and delete resources in the Cosmos DB account according to the permissions they've been granted. [www.PaddyMaddy.com](http://www.PaddyMaddy.com)

## Secure access to data in Azure Cosmos DB



## Encrypting Data at Rest and in Motion

### Encrypting Data at Rest

Rest would be obviously anything that is not moving

### Motion

Any piece of data that's moving between service's or outside of azure to a client or between different computers

Azure DataBase

Azure Cosmos DB

Azure Data Lake Encryption

## Encrypting Data at Rest and in Motion

### Encrypting Data at Rest

Rest would be obviously anything that is not moving

### Motion

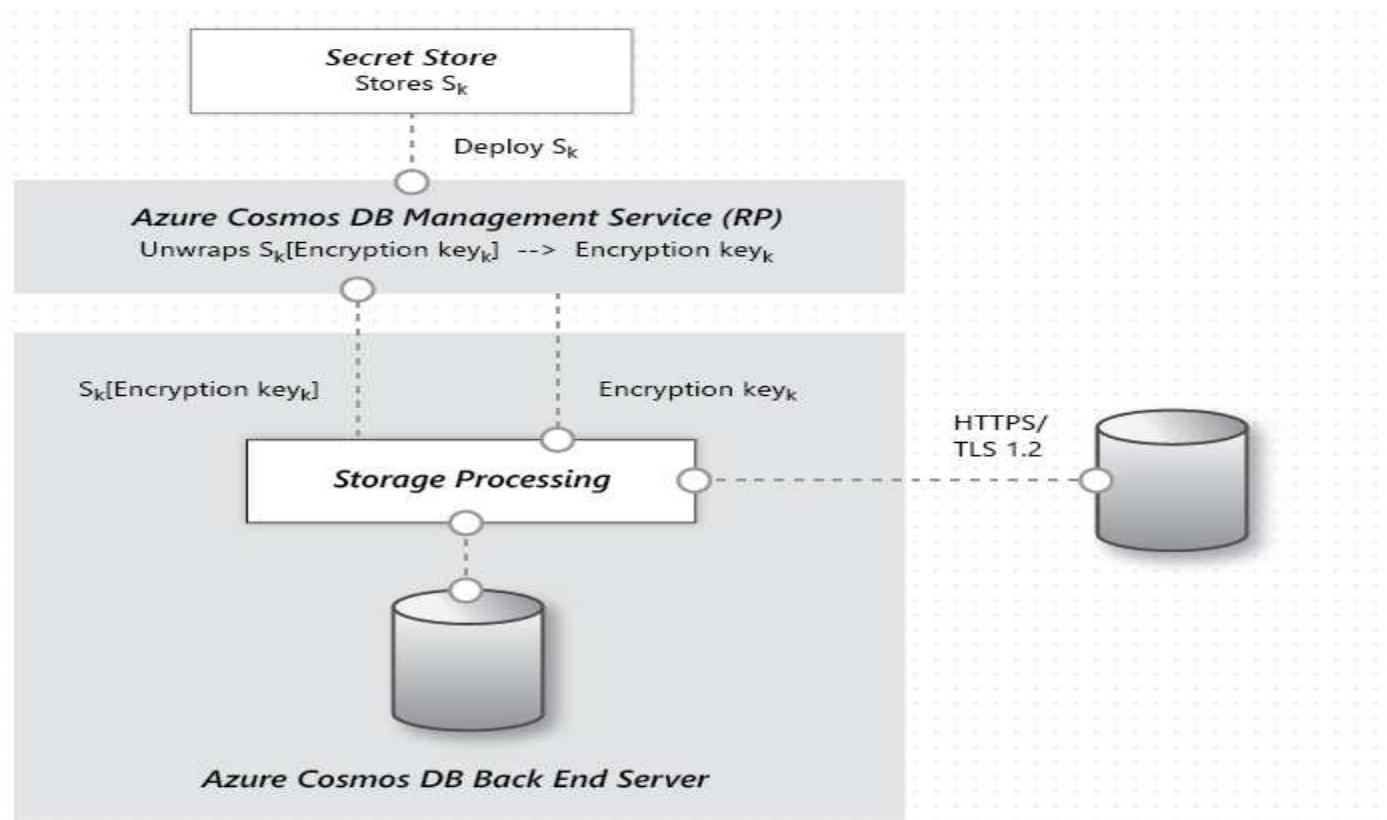
Any piece of data that's moving between service's or outside of azure to a client or between different computers

### Transparent Data Encryption

- SQL Server
- Azure SQL Database
- Azure SQL Data warehouse
- Data Lake
- AES and triple Data encryption standard
- Database encryption key

## Data Encryption in Azure Cosmos DB

As a PaaS service, Azure Cosmos DB is very easy to use. Because all user data stored in Azure Cosmos DB is encrypted at rest and in transport, you don't have to take any action. Another way to put this is that encryption at rest is "on" by default. There are no controls to turn it off or on. Azure Cosmos DB uses AES-256 encryption on all regions where the account is running.



## Encrypting Data in Motion

### **TLS/ SSL**

- Transport layer Security
  - Between cloud and customer
- Storing Authentication
- Message Privacy
- Integrity
- Perfect Forward Secrecy – PFS
  - Protects data between customers client systems and cloud
- Shared Access signatures**
  - Delegate access to Azure Storage Objects
- Data Lake**
  - Data in transit is always encrypted in Data Lake Store
  - Https is the only Protocol available for REST Interface

# Azure Disk Encryption

**VIRTUAL MACHINES RECOMMENDATIONS**

**TOTAL**

Missing disk encryption	2 of 2 VMs	<div style="width: 100%; background-color: red;"></div>
-------------------------	------------	---------------------------------------------------------

Virtual machines

NAME	ONBOARDING	SYSTEM UPDATES	ANTIMALWARE	BASELINE	DISK ENCRYPTION
ASC-VM1	✓	✓	✓	✓	!
ASC-VM2	✓	✓	✓	✓	!

## Supported operating systems

- Windows client: Windows 8 and later.
- Windows Server: Windows Server 2008 R2 and later.

## Best Practices

- ❑ Adopt a Policy of Identity as the Primary Security Perimeter
- ❑ Secure your keys and Credentials to Secure your PasS
- ❑ Manage our PasS Resources directly whenever possible
- ❑ Use strong authentication and authorization
- ❑ Use a web application firewall
- ❑ Monitor app performance
- ❑ Perform penetration testing

## SSL / TLS Certificates – Secure Data and Applications

## Application Insights Synthetic Security Transactions

Application insights monitors your app service by running recurring tests to monitor availability and responsiveness.

Types of availability tests - There are three types of availability tests:

- ❑ URL ping test: a simple test that you can create in the Azure portal.
- ❑ Multi-step web test: A recording of a sequence of web requests, which can be played back to test more complex scenarios.  
Multi-step web tests are created in Visual Studio Enterprise and uploaded to the portal for execution.
- ❑ Custom Track Availability Tests: If you decide to create a custom application to run availability tests, the `TrackAvailability()` method can be used to send the results to Application Insights.