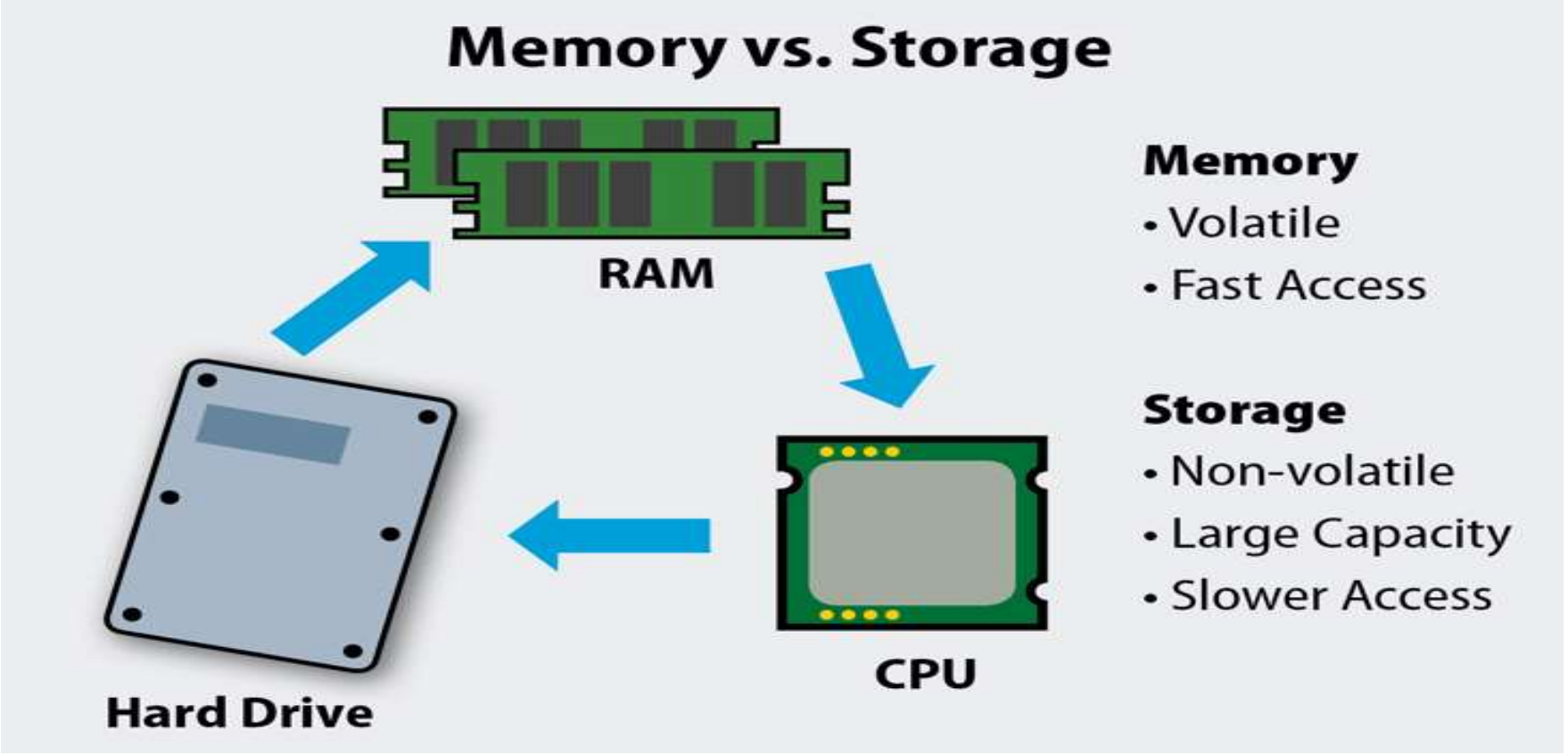
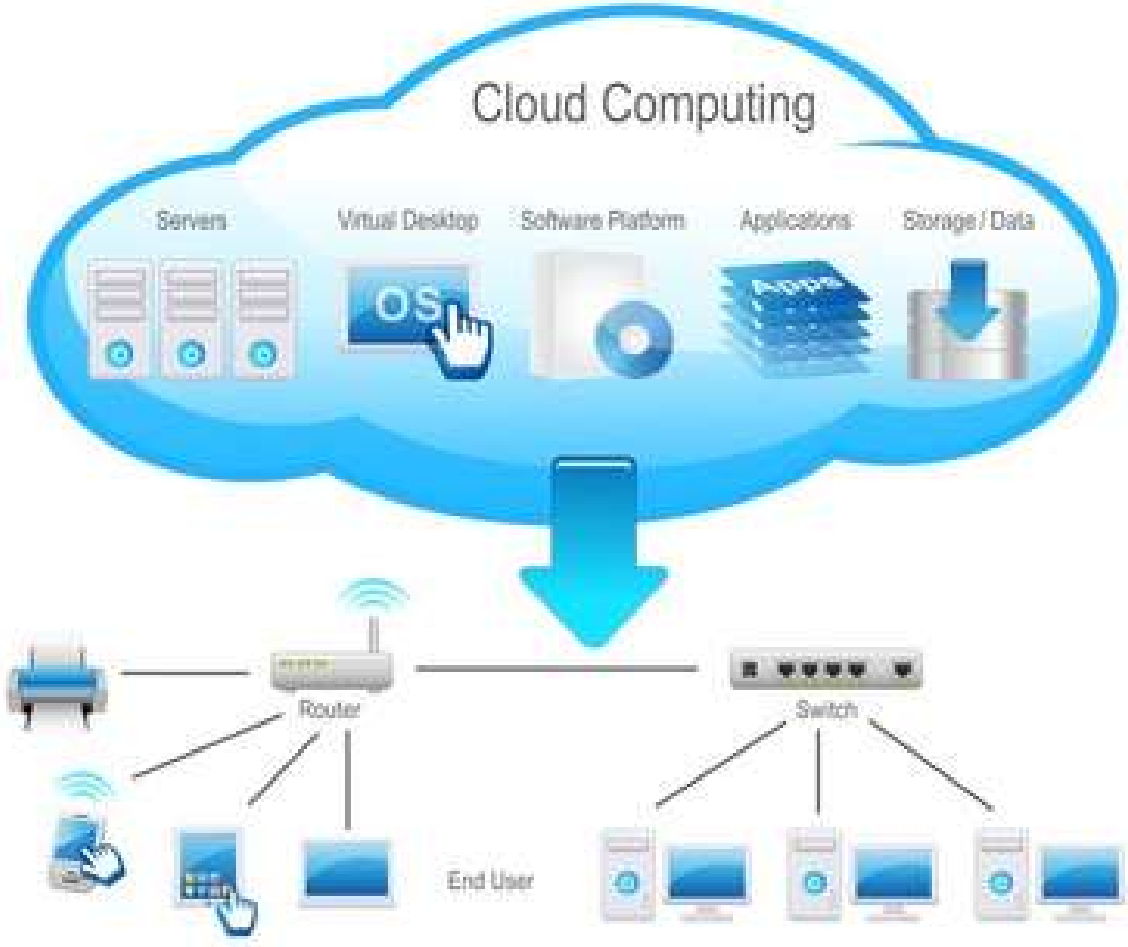
Cloud Computing



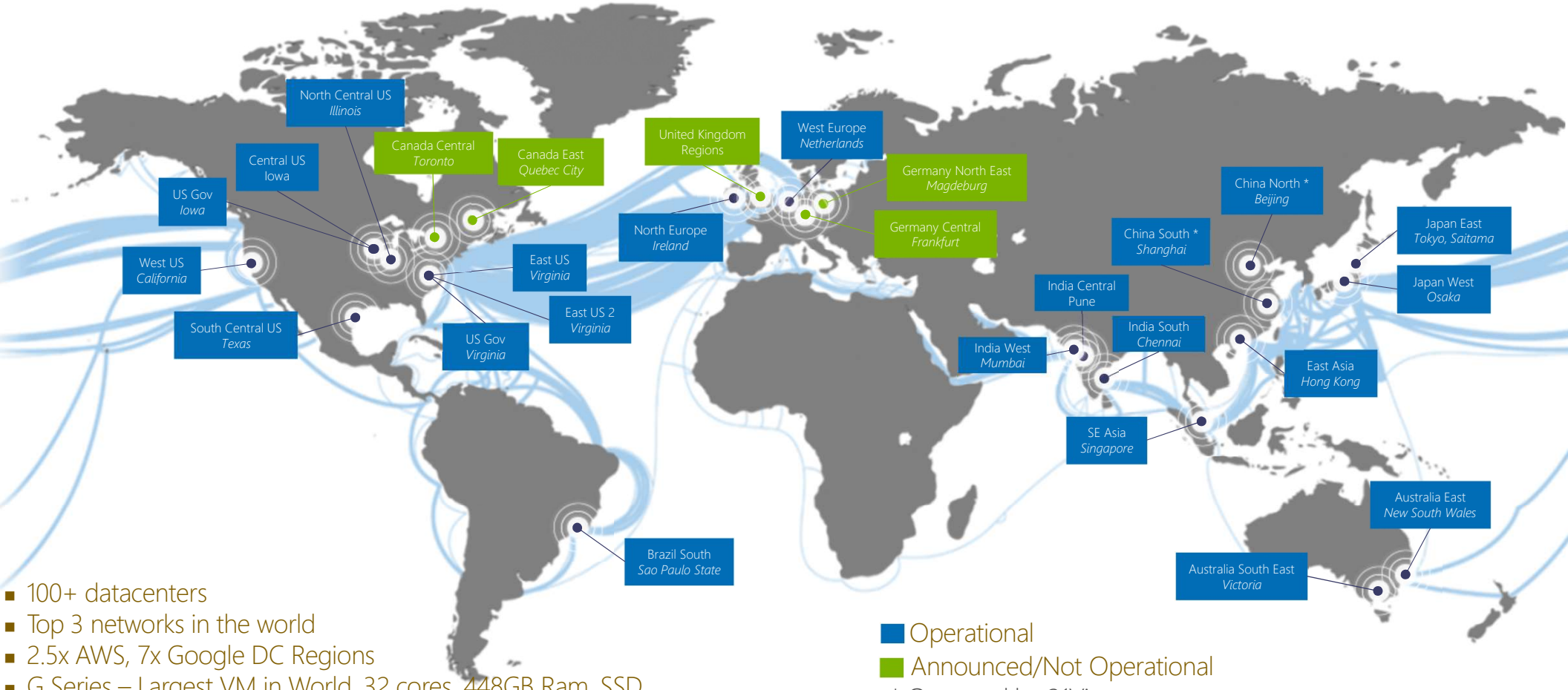
Cloud Computing

Cloud Computing



Hyper scale Infrastructure is the enabler

27 Regions Worldwide, 22 ONLINE…huge capacity around the world…growing every year



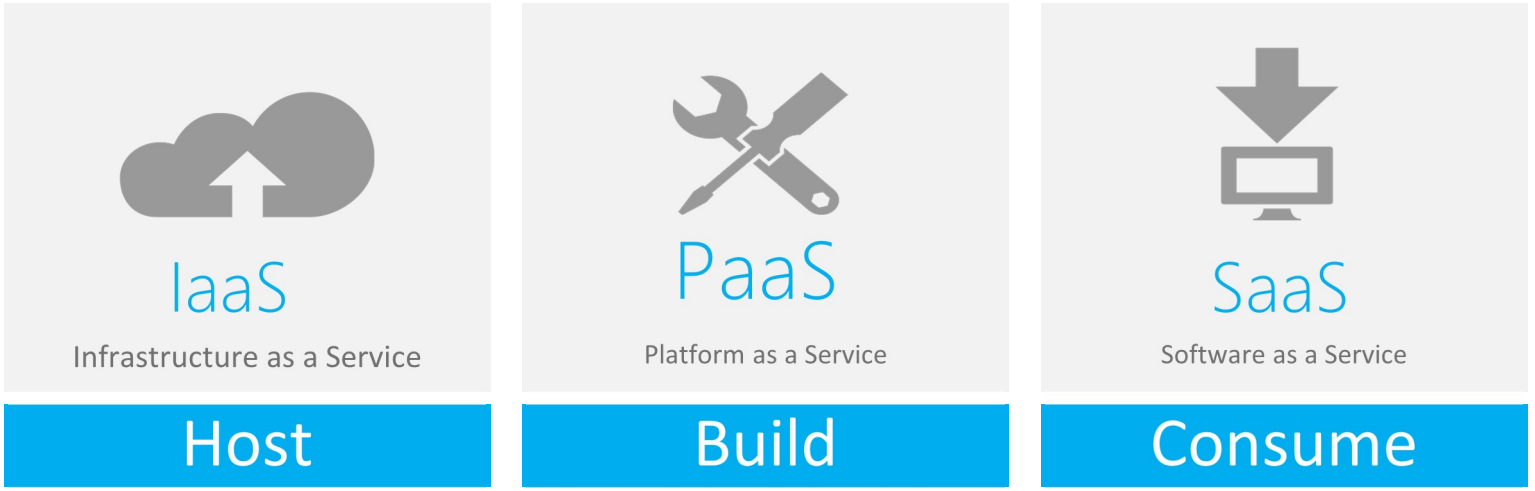
- 100+ datacenters
- Top 3 networks in the world
- 2.5x AWS, 7x Google DC Regions
- G Series – Largest VM in World, 32 cores, 448GB Ram, SSD…

Operational

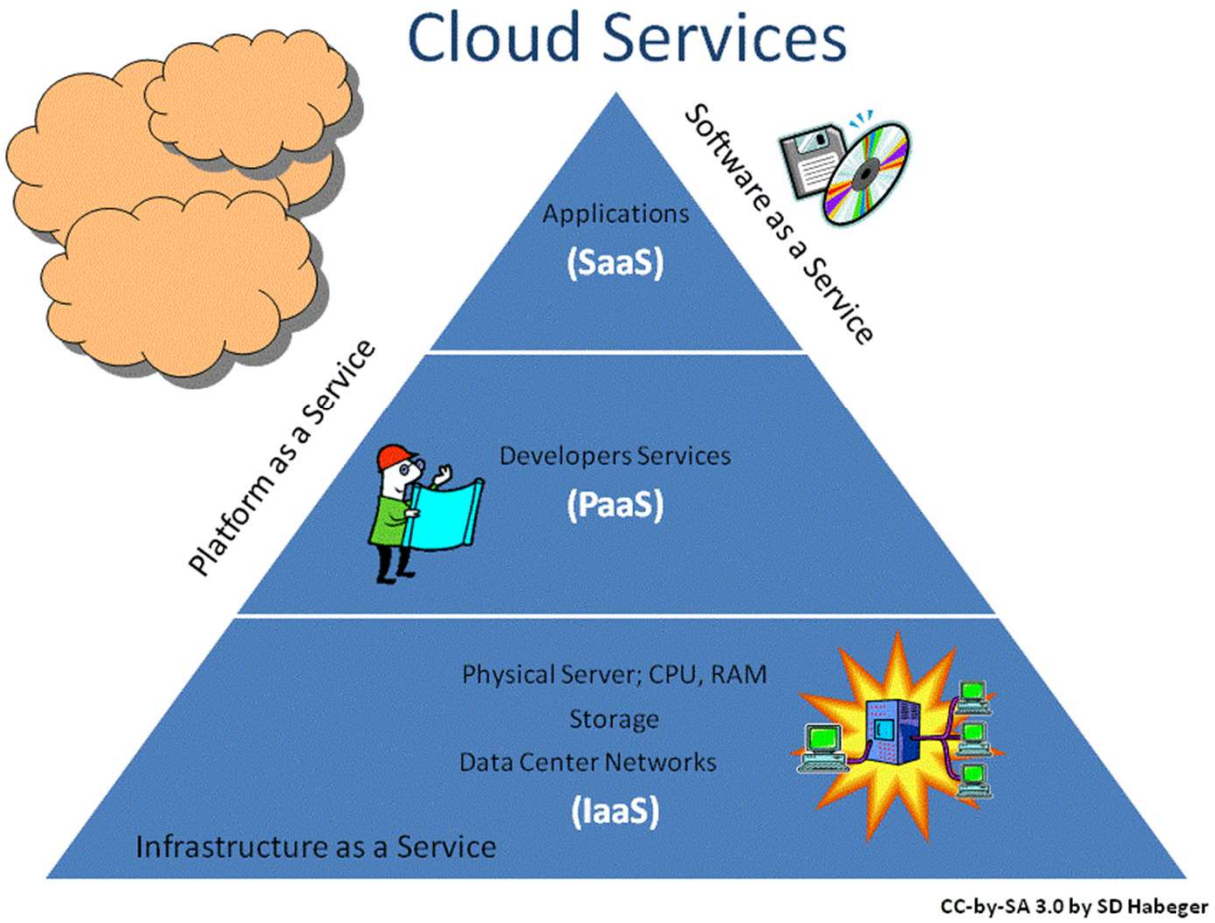
Announced/Not Operational

* Operated by 21Vianet

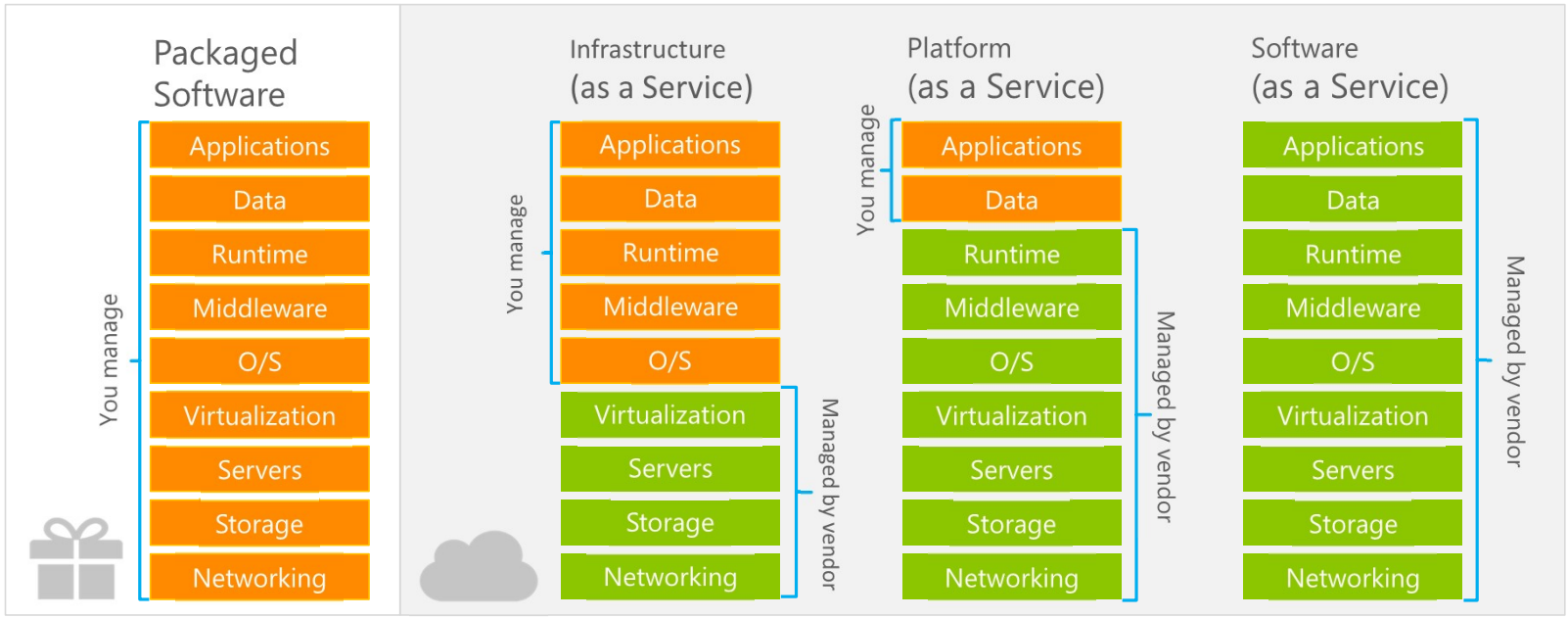
Cloud Computing Service Types



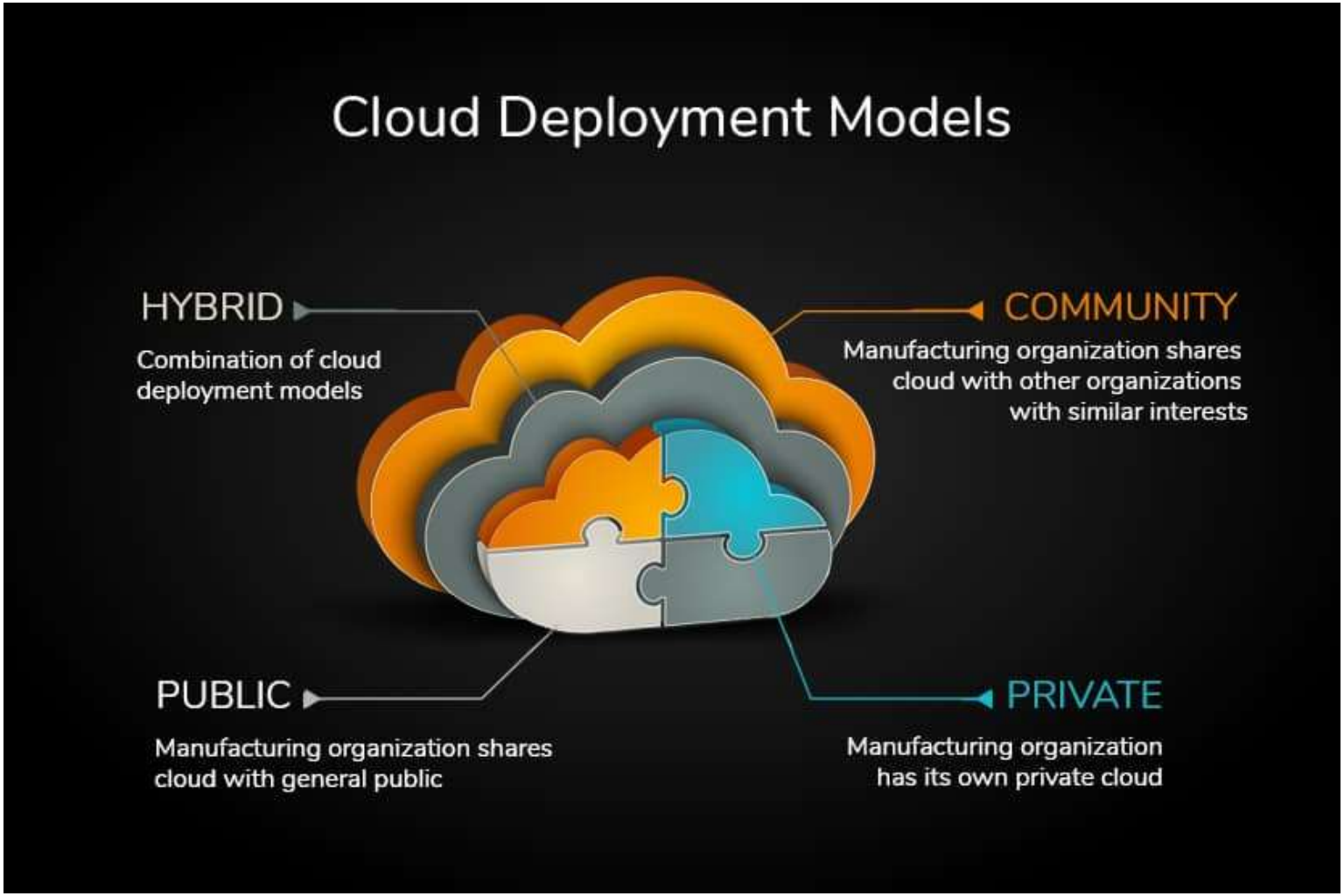
Cloud Computing



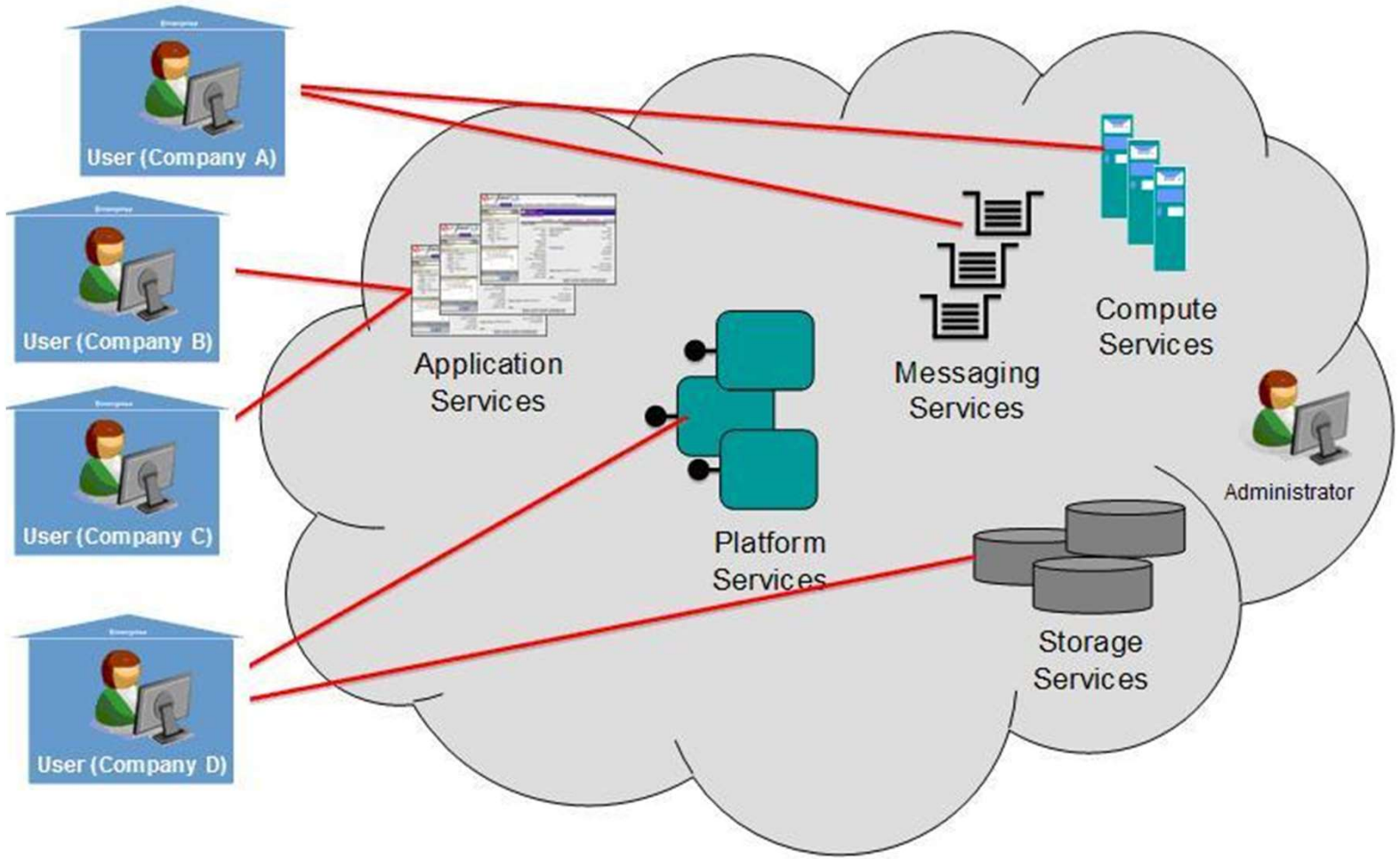
Cloud Computing (continued)



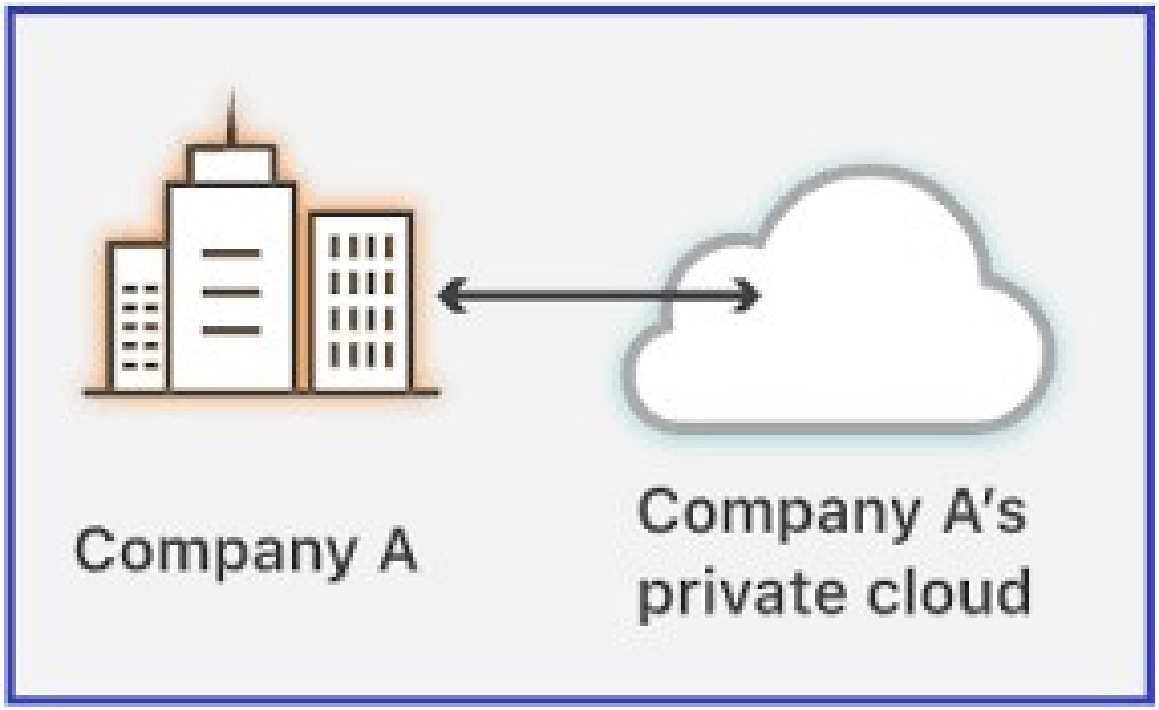
Cloud Computing Models



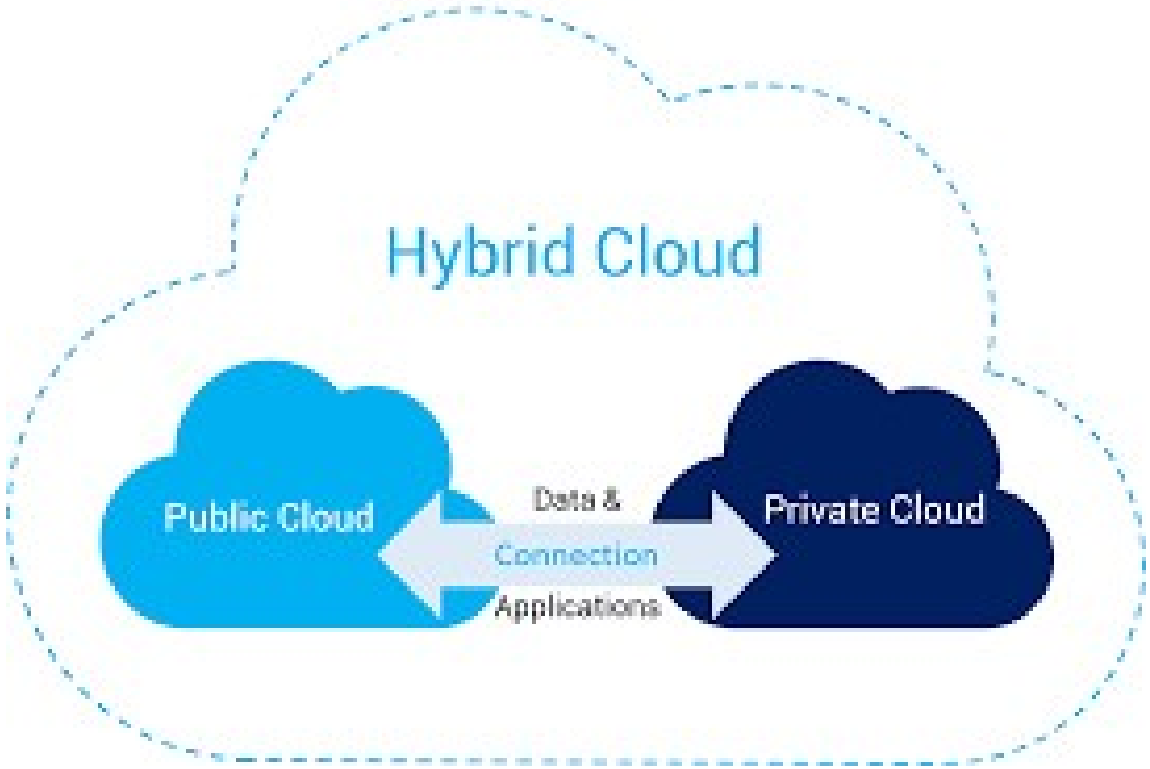
Public Cloud Computing



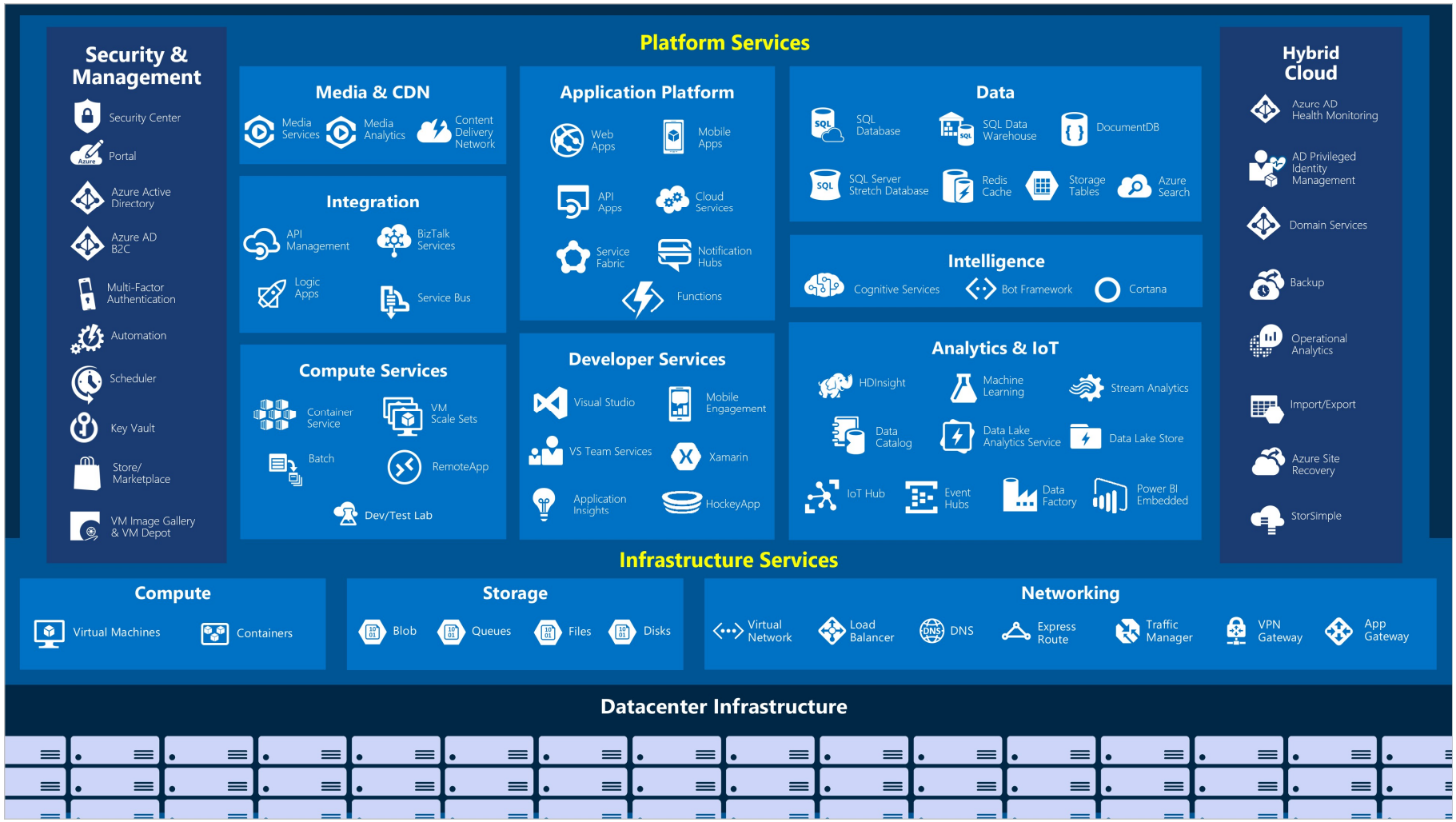
Private Cloud Computing



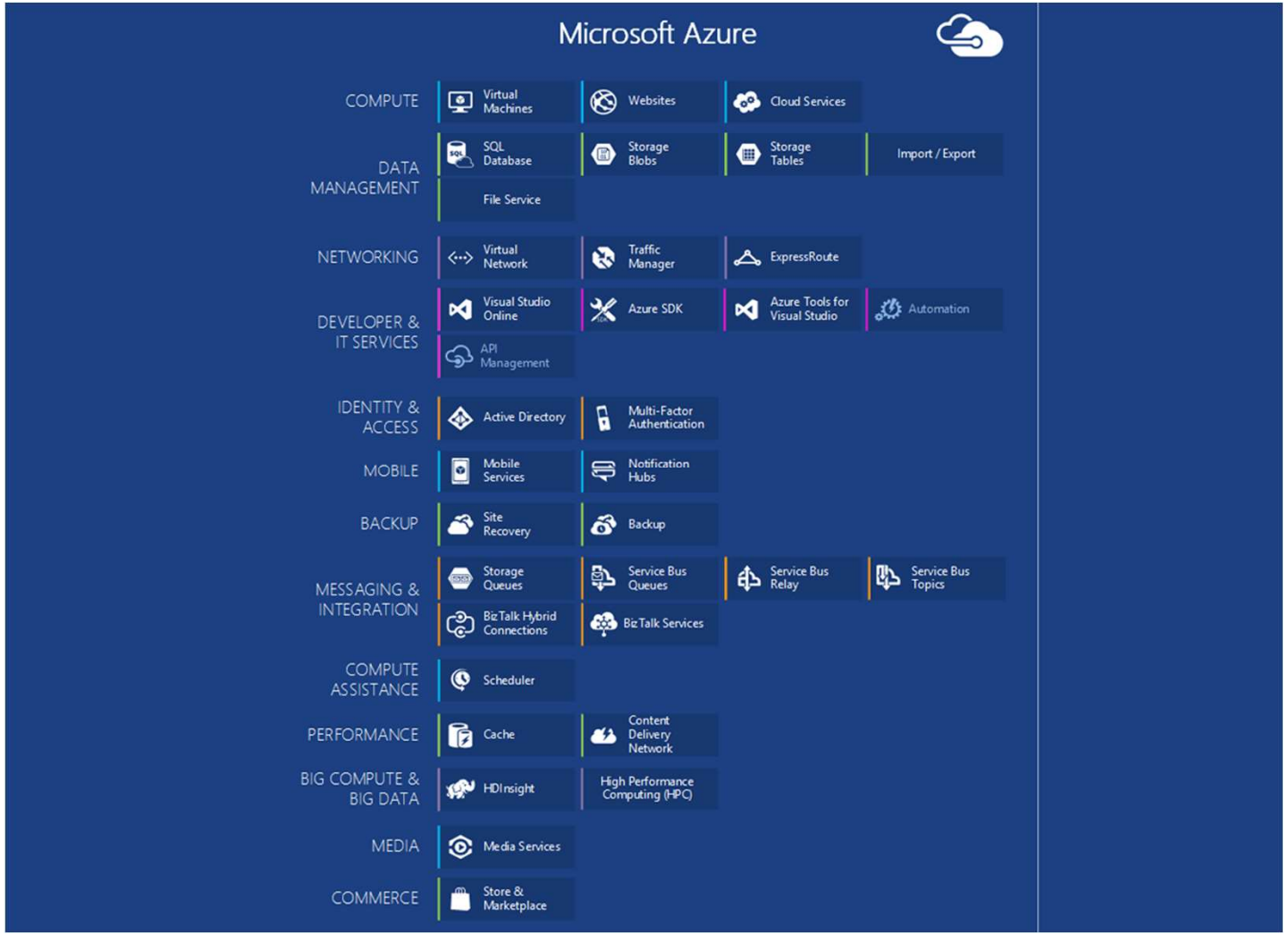
Hybrid Cloud Computing



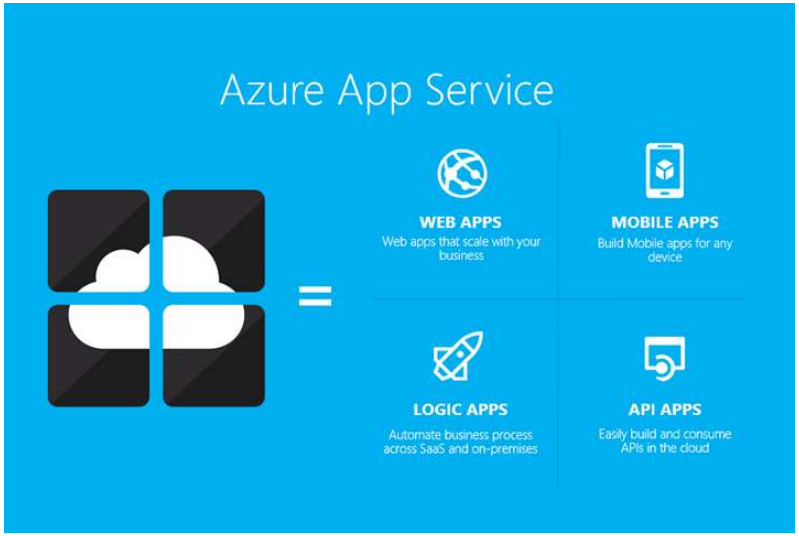
Azure Cloud

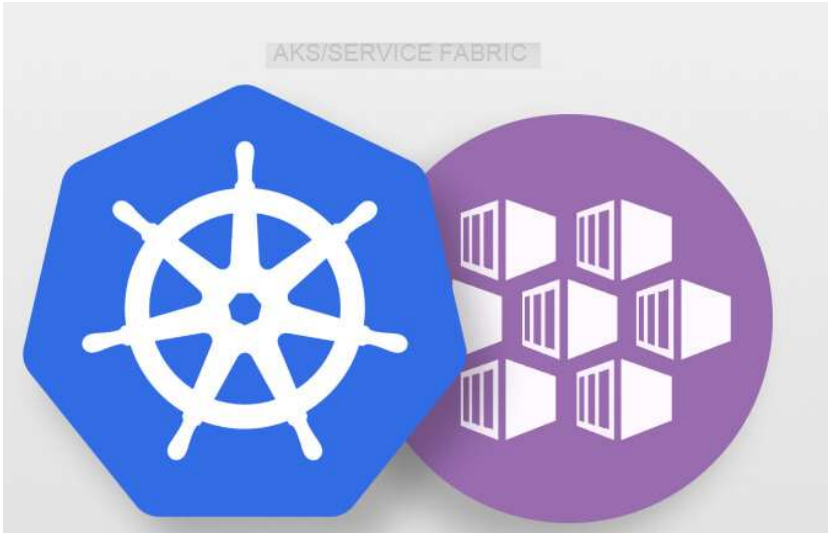

Platform Services
Security & Management
Security Center
Portal
Azure Active Directory
Azure AD B2C
Multi-Factor Authentication
Automation
Scheduler
Key Vault
Store/ Marketplace
VM Image Gallery & VM Depot
Media & CDN
Media Services
Media Analytics
Content Delivery Network
Integration
API Management
BizTalk Services
Logic Apps
Service Bus
Compute Services
Container Service
VM Scale Sets
Batch
RemoteApp
Dev/Test Lab
Application Platform
Web Apps
Mobile Apps
API Apps
Cloud Services
Service Fabric
Notification Hubs
Functions
Developer Services
Visual Studio
Mobile Engagement
VS Team Services
Xamarin
Application Insights
HockeyApp
Data
SQL Database
SQL Data Warehouse
DocumentDB
SQL Server Stretch Database
Redis Cache
Storage Tables
Azure Search
Intelligence
Cognitive Services
Bot Framework
Cortana
Analytics & IoT
HDInsight
Machine Learning
Stream Analytics
Data Catalog
Data Lake Analytics Service
Data Lake Store
IoT Hub
Event Hubs
Data Factory
Power BI Embedded
Hybrid Cloud
Azure AD Health Monitoring
AD Privileged Identity Management
Domain Services
Backup
Operational Analytics
Import/Export
Azure Site Recovery
StorSimple
Infrastructure Services
Compute
Virtual Machines
Containers
Storage
Blob
Queues
Files
Disks
Networking
Virtual Network
Load Balancer
DNS
Express Route
Traffic Manager
VPN Gateway
App Gateway
Datacenter Infrastructure

Azure Cloud

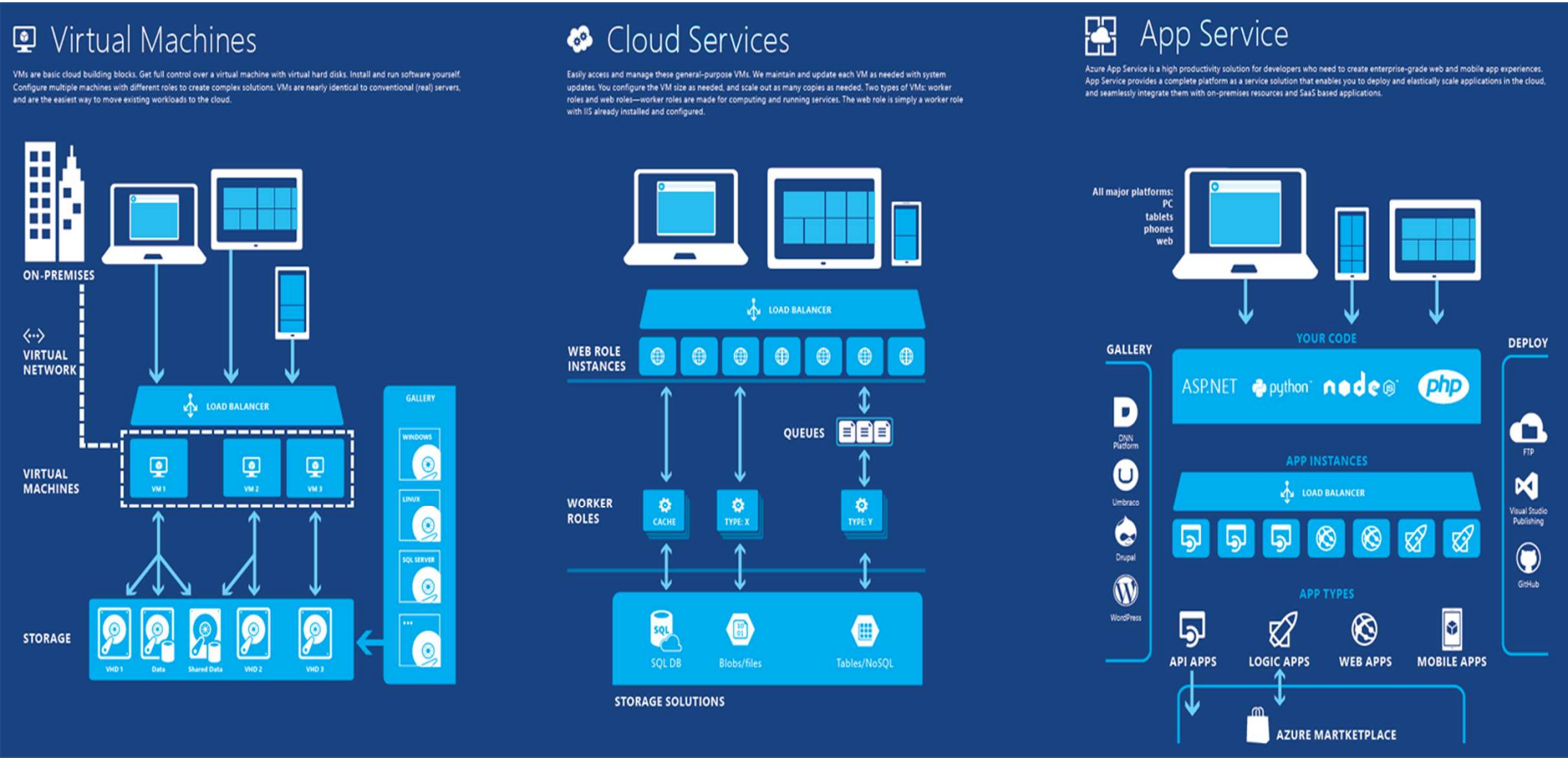

Microsoft Azure
COMPUTE
Virtual Machines
Websites
Cloud Services
DATA MANAGEMENT
SQL Database
Storage Blobs
Storage Tables
Import / Export
File Service
NETWORKING
Virtual Network
Traffic Manager
ExpressRoute
DEVELOPER & IT SERVICES
Visual Studio Online
Azure SDK
Azure Tools for Visual Studio
Automation
API Management
IDENTITY & ACCESS
Active Directory
Multi-Factor Authentication
MOBILE
Mobile Services
Notification Hubs
BACKUP
Site Recovery
Backup
MESSAGING & INTEGRATION
Storage Queues
Service Bus Queues
Service Bus Relay
Service Bus Topics
BizTalk Hybrid Connections
BizTalk Services
COMPUTE ASSISTANCE
Scheduler
PERFORMANCE
Cache
Content Delivery Network
BIG COMPUTE & BIG DATA
HDInsight
High Performance Computing (HPC)
MEDIA
Media Services
COMMERCE
Store & Marketplace

Azure Hosting Models

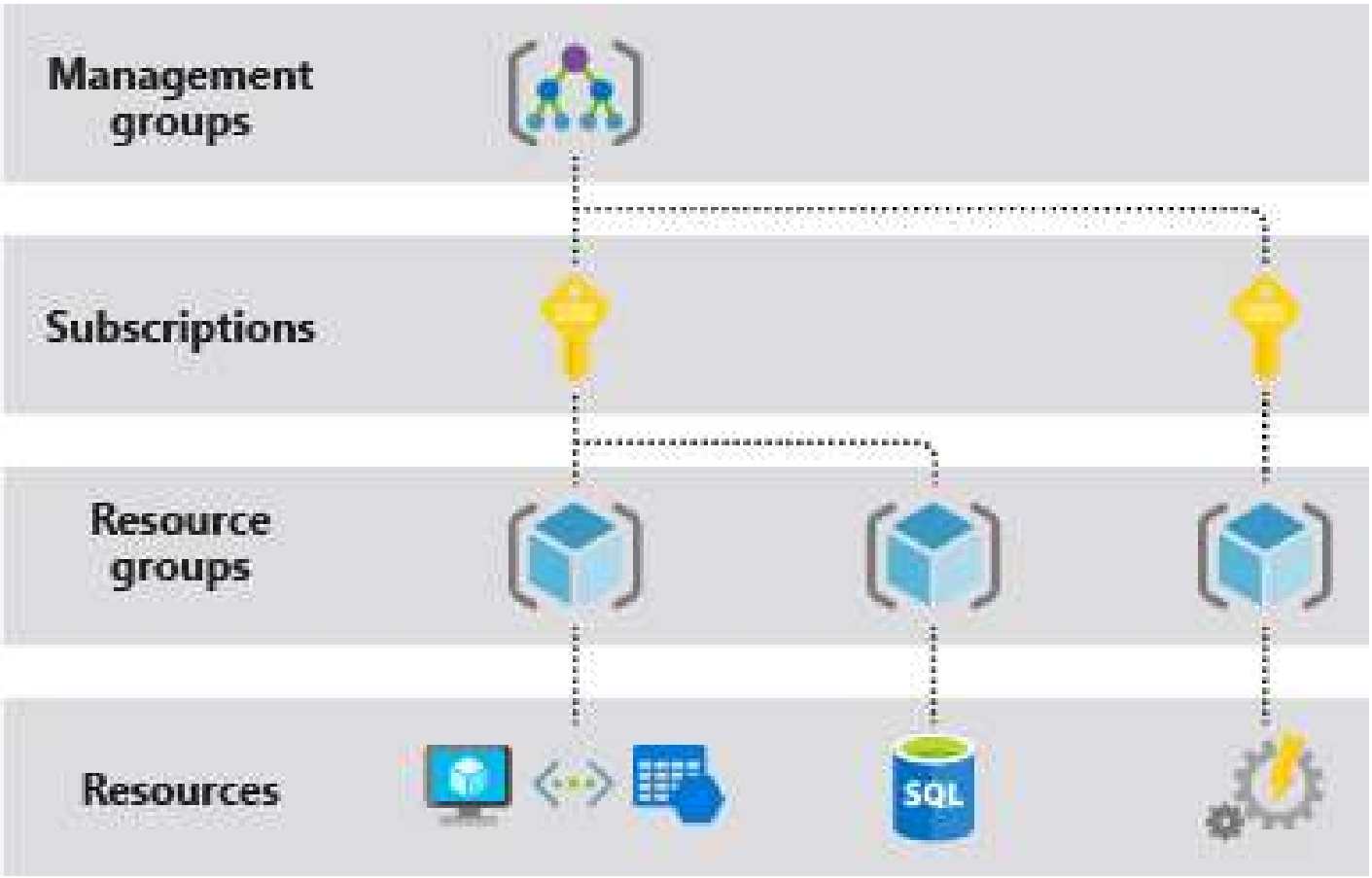




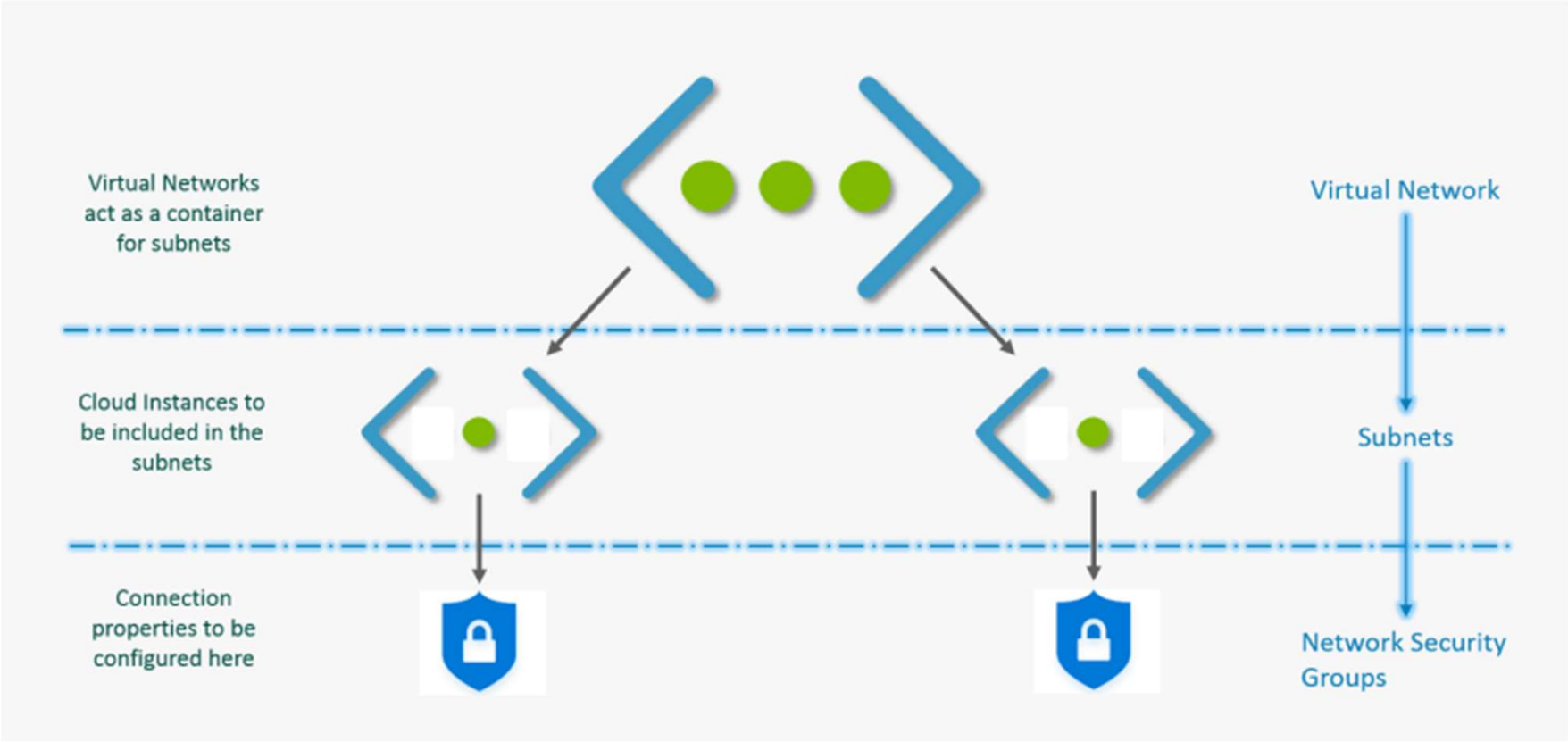
Azure Hosting Models



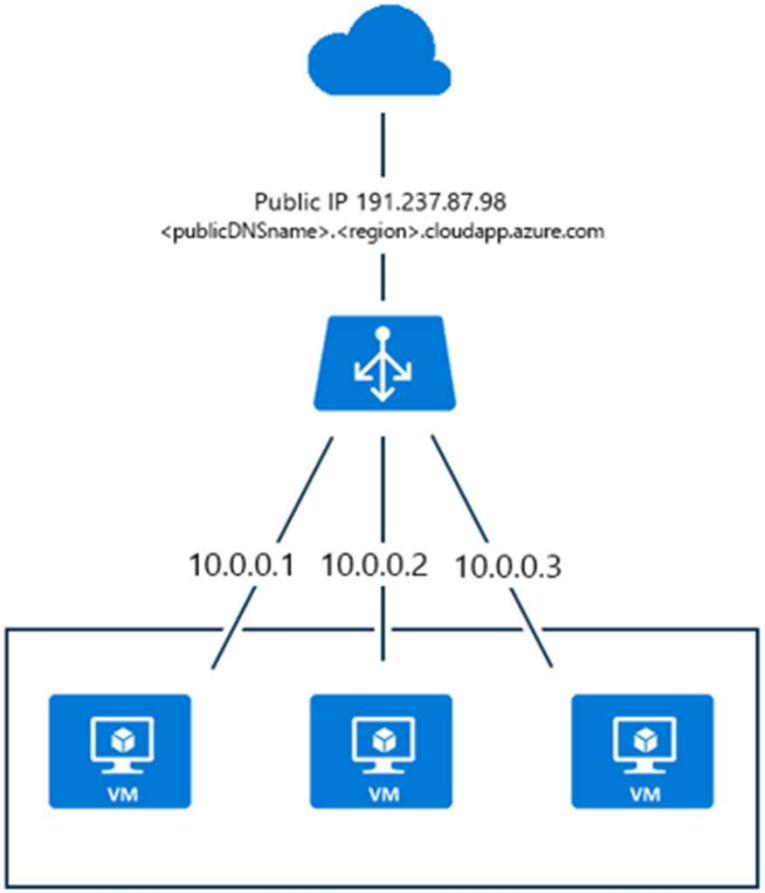
Understand scope

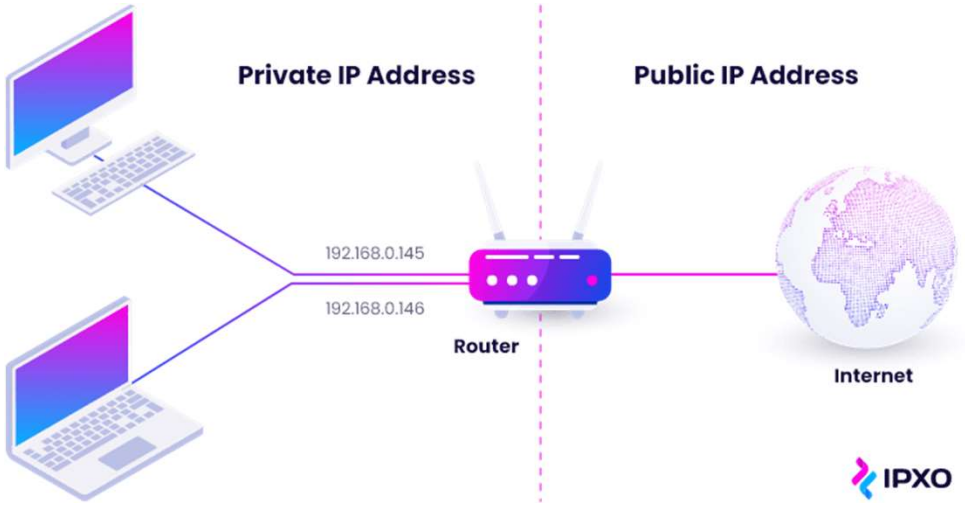


Azure VN


Virtual Networks act as a container for subnets
Cloud Instances to be included in the subnets
Connection properties to be configured here
Virtual Network
Subnets
Network Security Groups

Azure VN


Public IP 191.237.87.98
<publicDNSname>.<region>.cloudapp.azure.com
10.0.0.1
10.0.0.2
10.0.0.3
VM
VM
VM


Private IP Address
Public IP Address
192.168.0.145
192.168.0.146
Router
Internet
IPXO

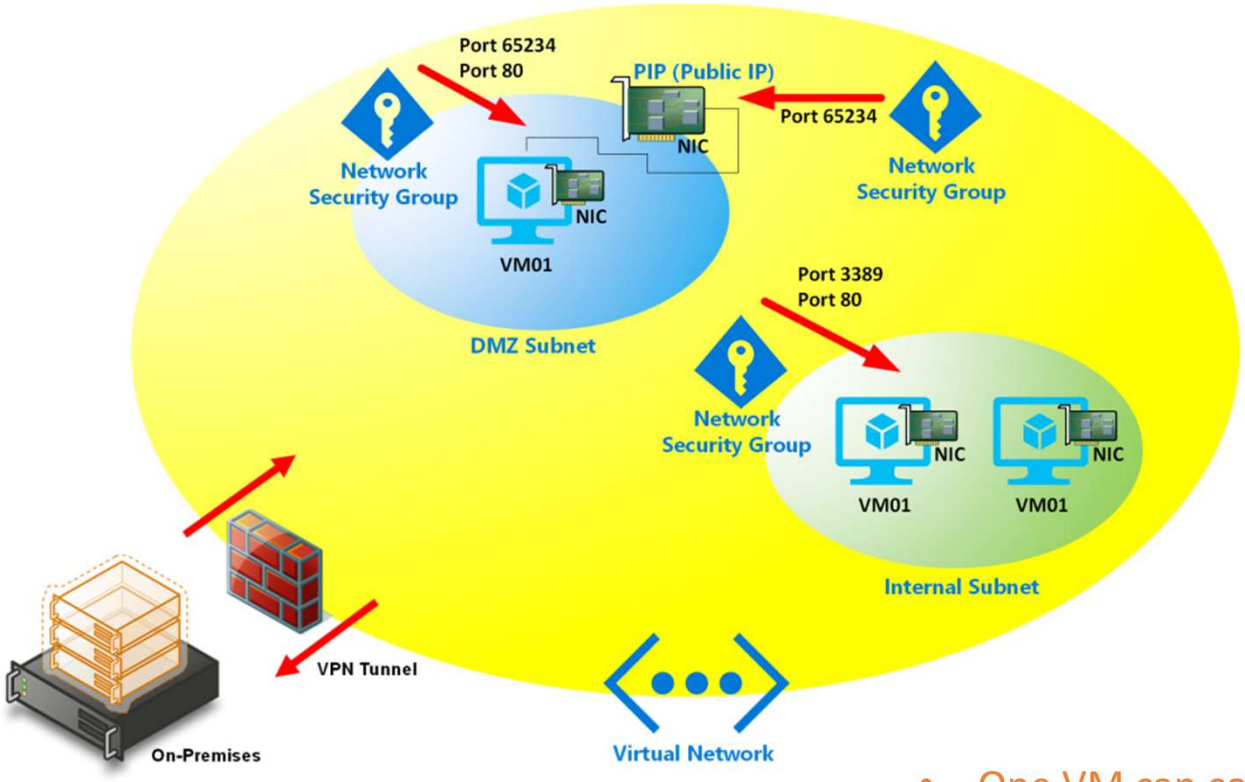
Azure VN

Private and public IP addresses – ARM

Public IP addresses	IP address association	Dynamic	Static
Virtual Machine	NIC	Yes	Yes
Load balancer	Front end configuration	Yes	Yes
VPN Gateway	Gateway IP configuration	Yes	No
Application Gateway	Front end configuration	Yes	No

Private IP addresses	IP address association	Dynamic	Static
Virtual Machine	NIC	Yes	Yes
Load balancer	Front end configuration	Yes	Yes
Application gateway	Front end configuration	Yes	Yes

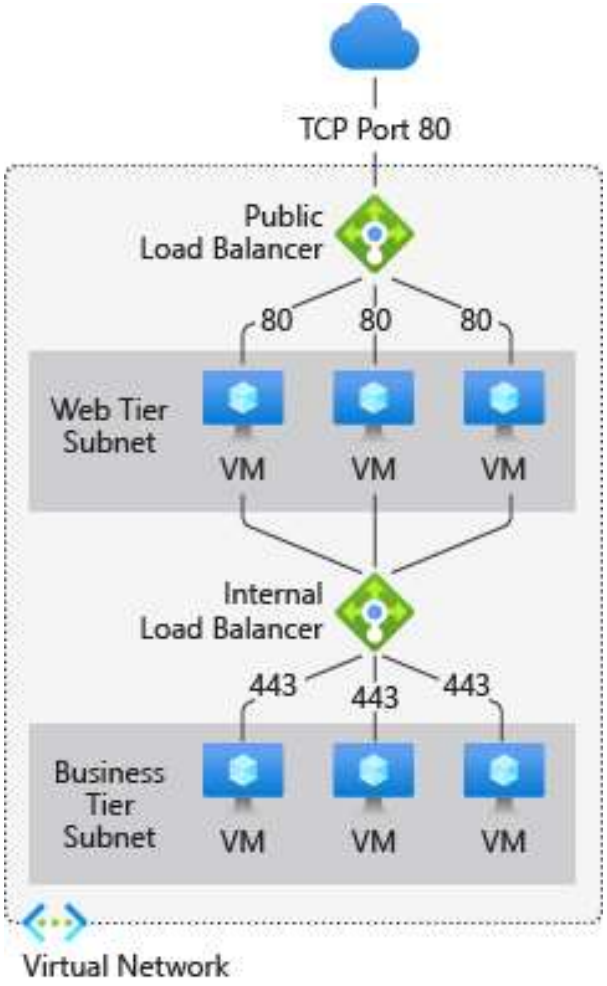
NIC & NSG

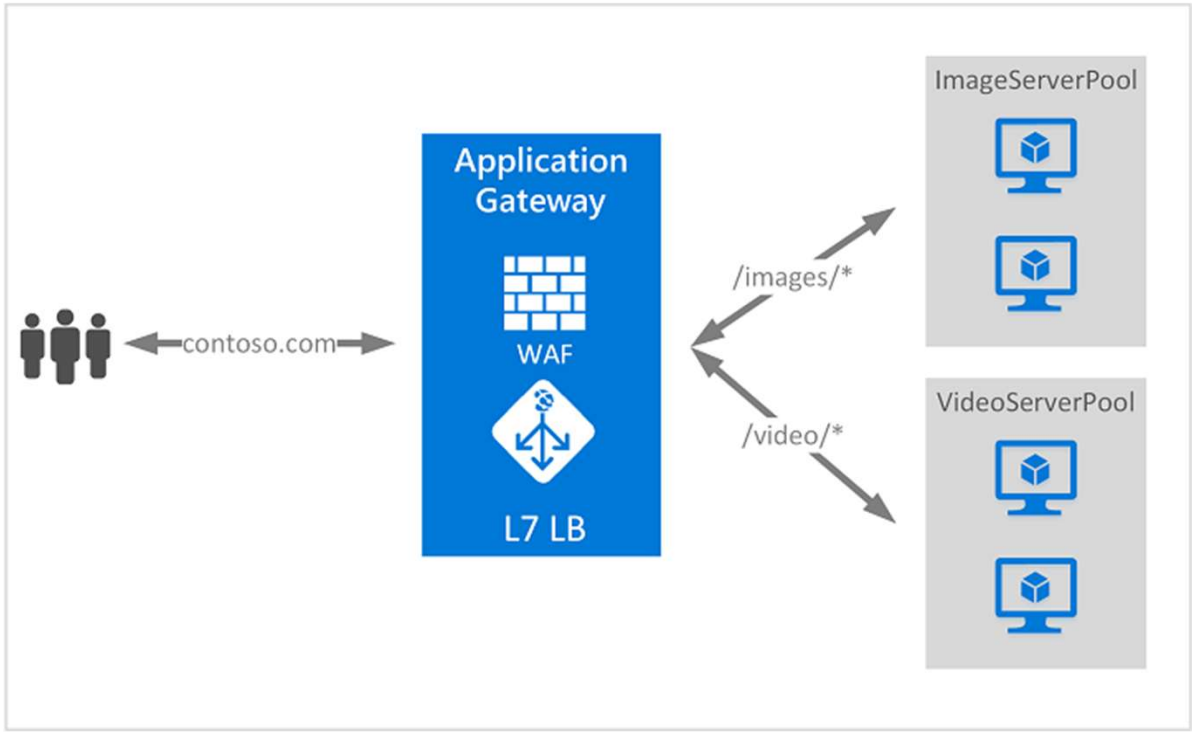


- One VM can communicate with another VM Trough NIC
- NIC has two IPS:

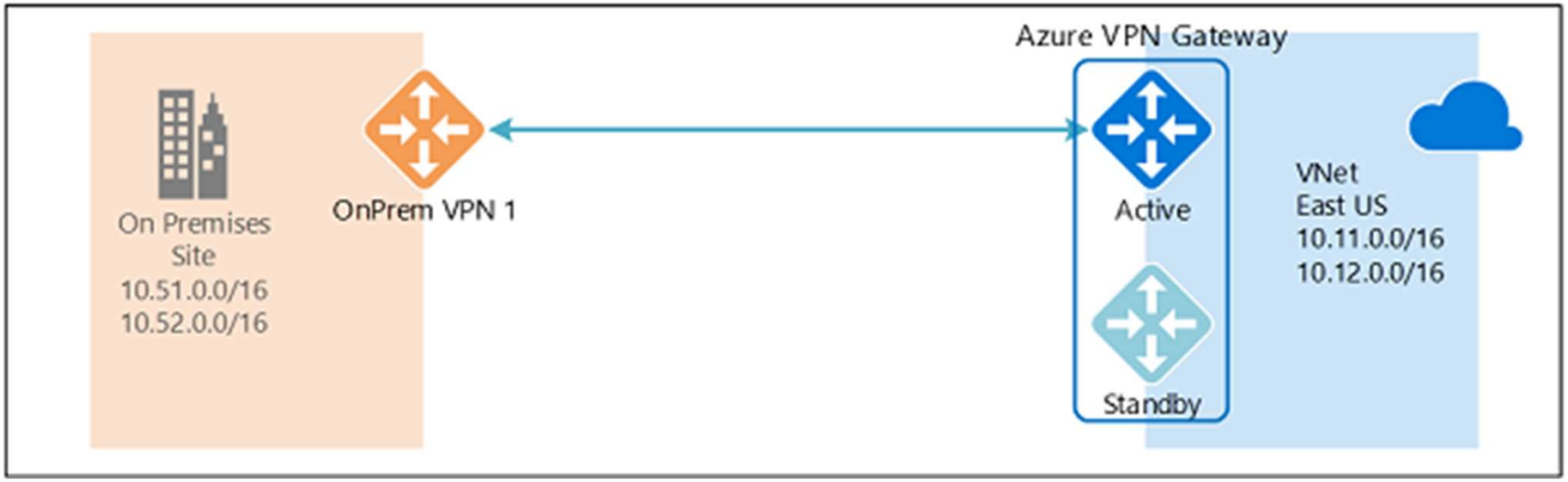
1. Private IP - Mandatory 2. Public IP - Optional

Azure LB & AG


TCP Port 80
Public
Load Balancer
80
80
80
Web Tier
Subnet
VM
VM
VM
Internal
Load Balancer
443
443
443
Business
Tier
Subnet
VM
VM
VM
Virtual Network


contoso.com
Application
Gateway
WAF
L7 LB
/images/*
/video/*
ImageServerPool
VideoServerPool

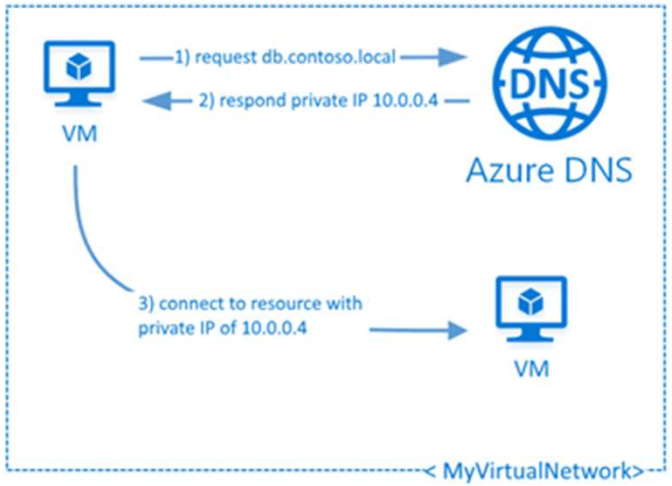
Azure VPN Gateways

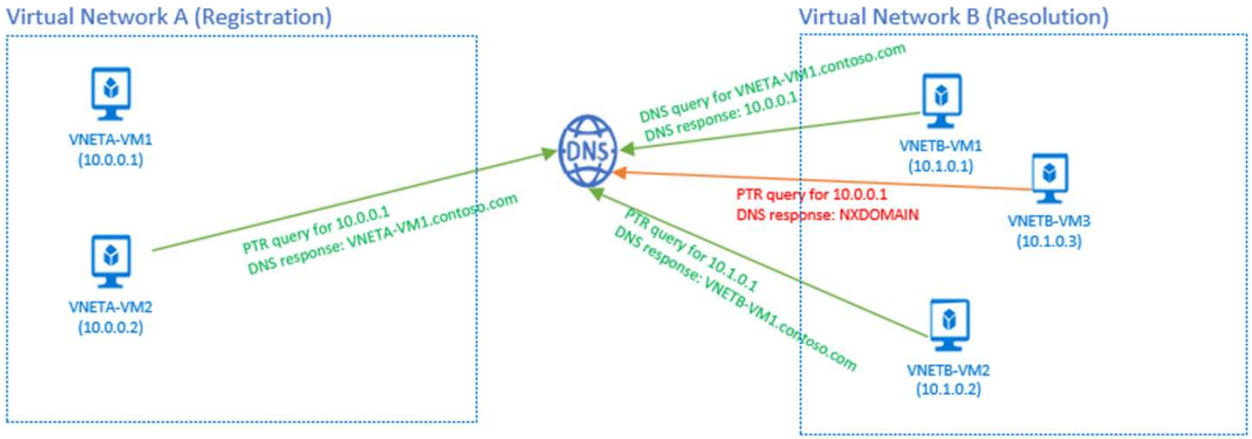


VPN Gateways

SKU	VPN Gateway/ExpressRoute Co-exist	ExpressRoute Gateway Throughput	VPN Gateway Throughput	VPN Gateway Max IPsec Tunnels
Basic	No	500 Mbps	100 Mbps	10
Standard	Yes	1000 Mbps	100 Mbps	10
Performance	Yes	2000 Mbps	200 Mbps	30

Azure DNS

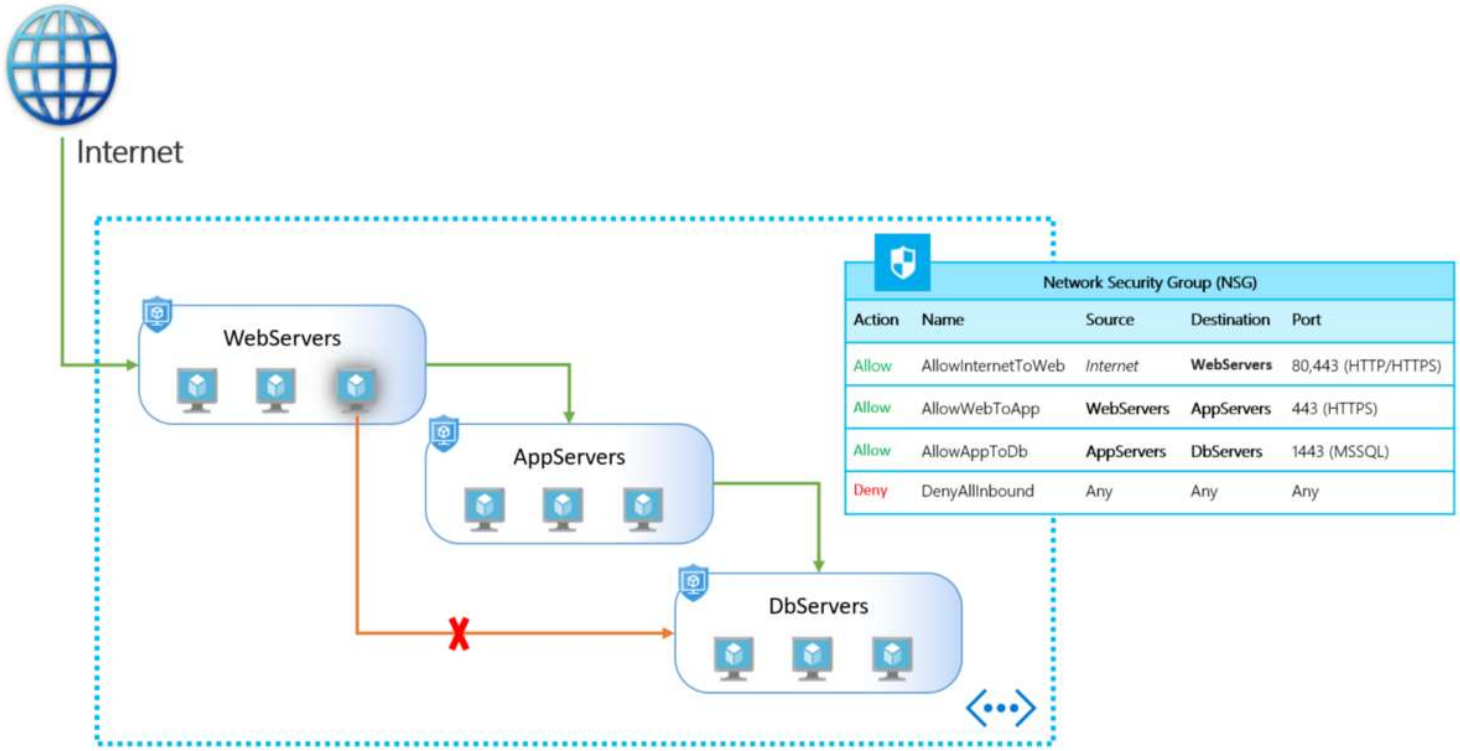




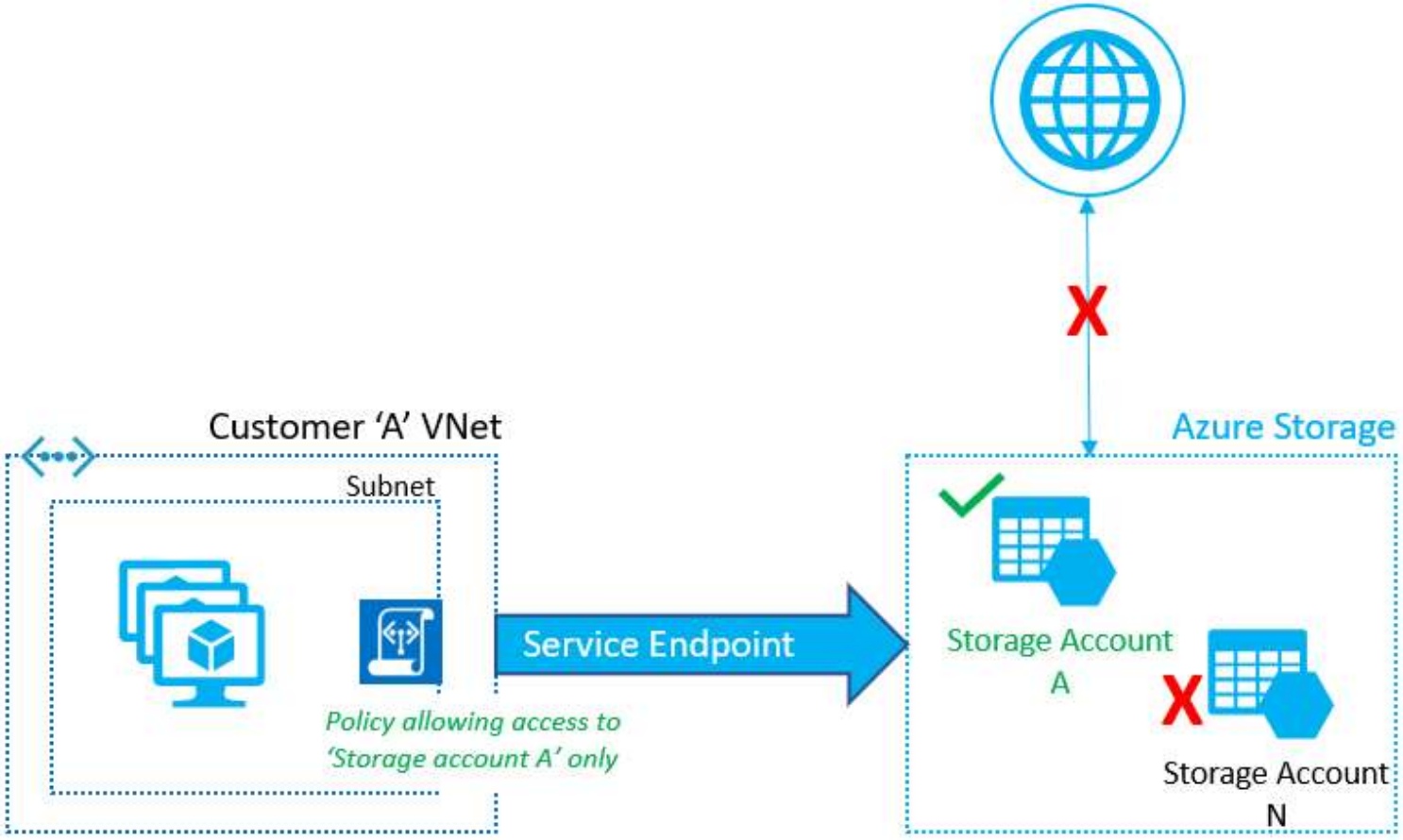
Private Zone records

VNETA-VM1 IN A 10.0.0.1 (auto registered)
VNETA-VM2 IN A 10.0.0.2 (auto registered)
VNETB-VM1 IN A 10.1.0.1 (manual record)
VNETB-VM2 IN A 10.1.0.2 (manual record)
VNETB-VM3 IN A 10.1.0.3 (manual record)

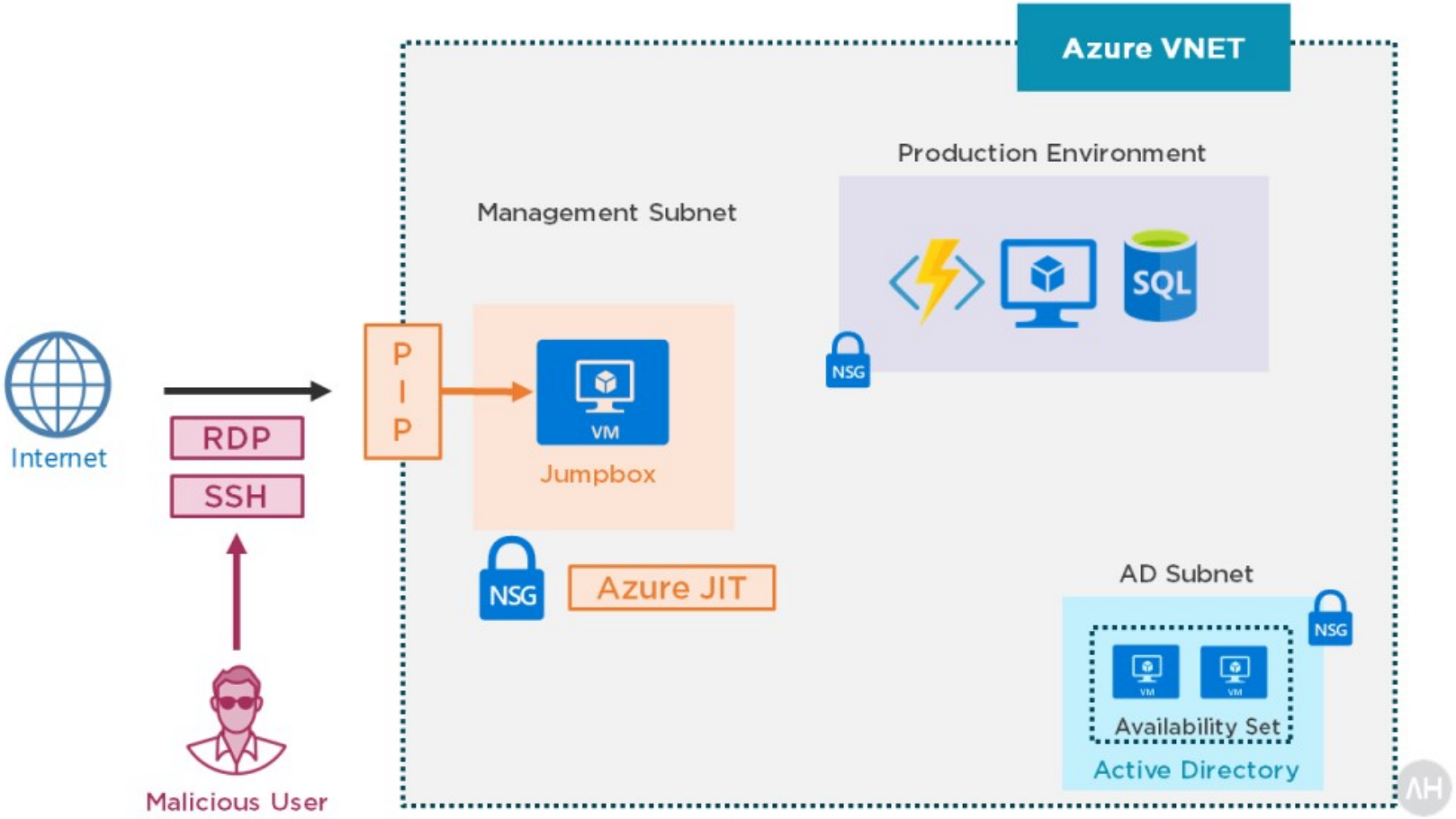
Application Security Groups



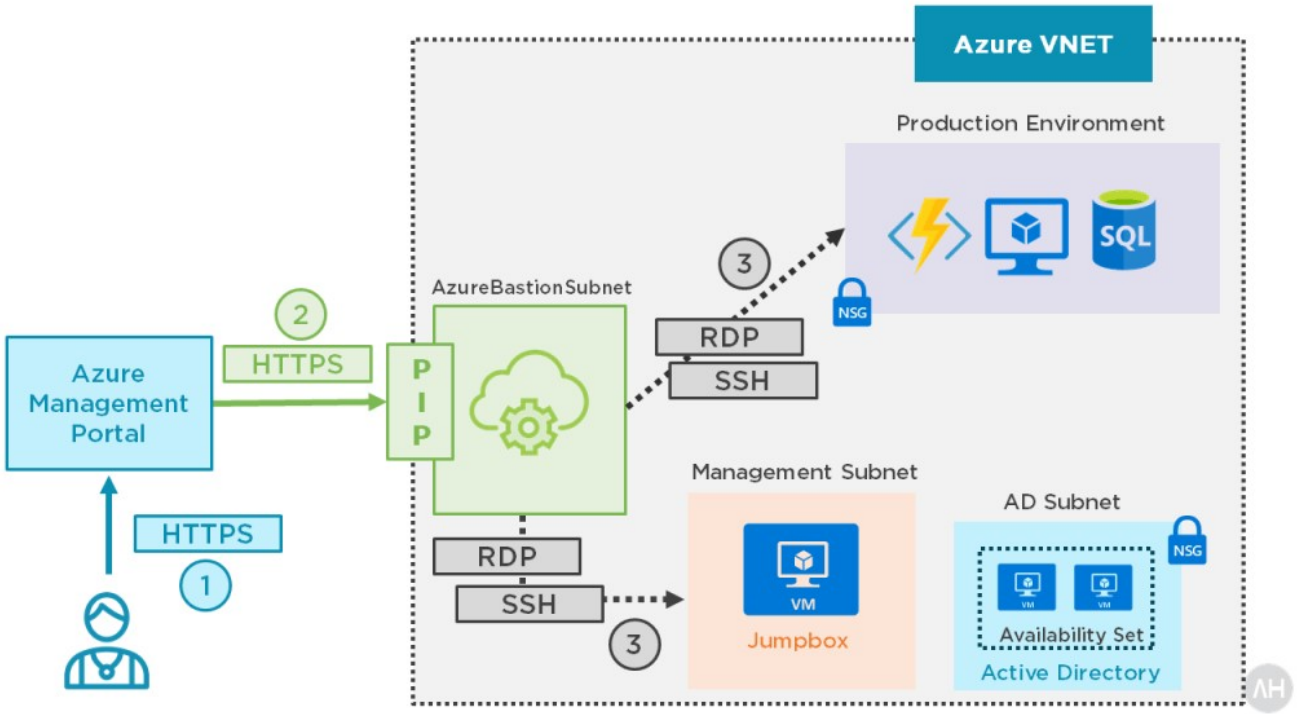
Service Endpoints

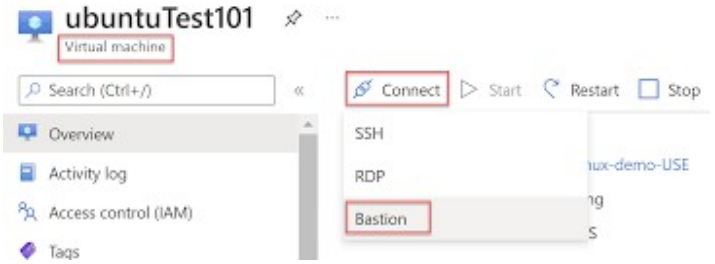


Azure Bastion- Why



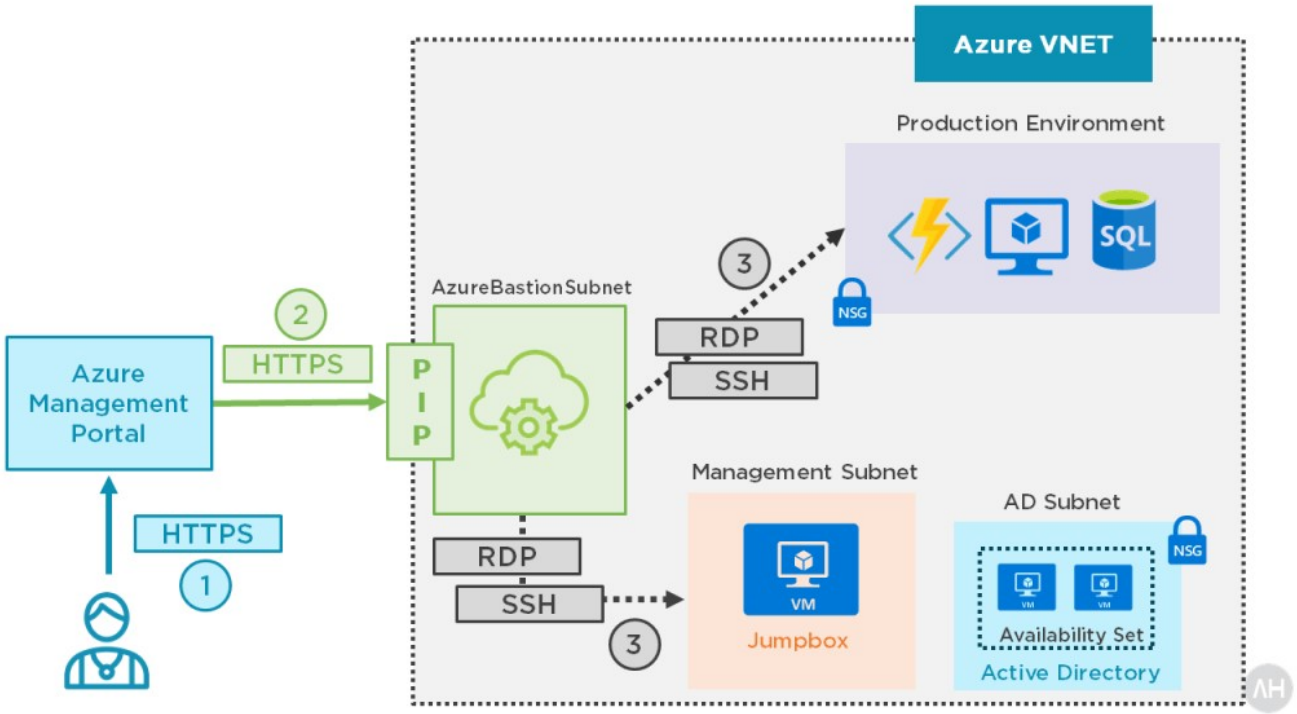
Azure Bastion

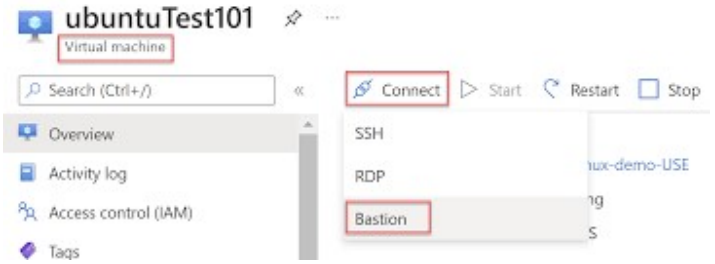




- Azure Bastion - PAAS Service
- Azure Bastion Secures RDP and SSH

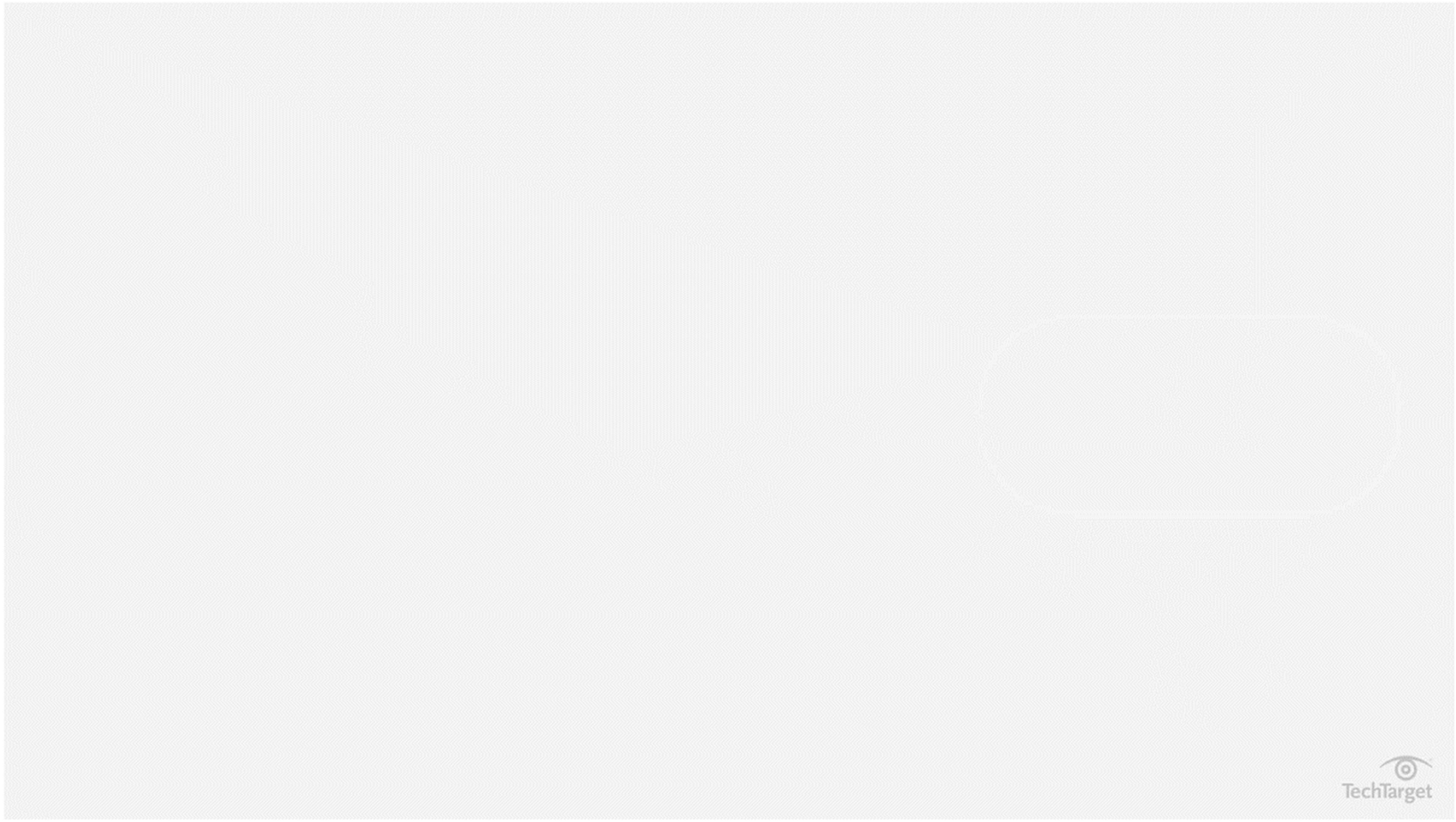
Azure Bastion



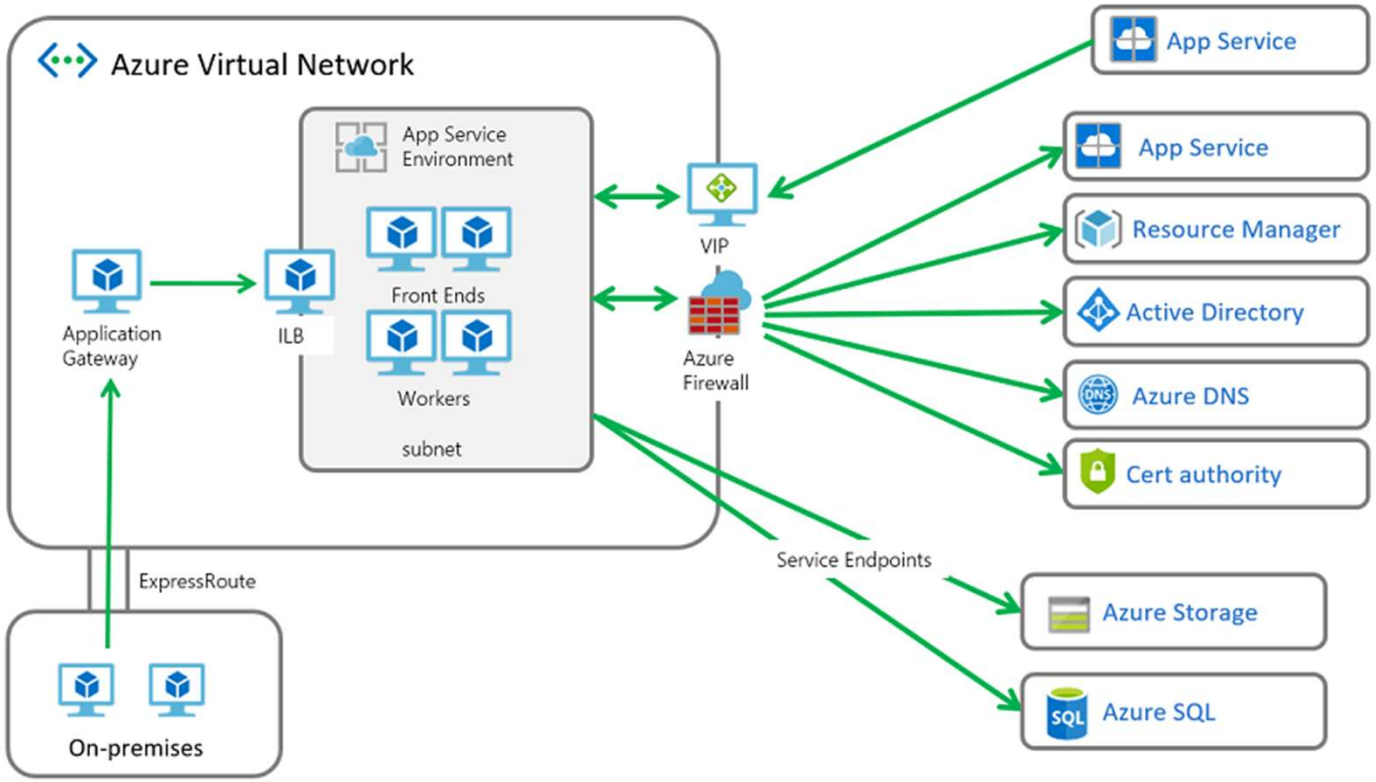


- Azure Bastion - PAAS Service
- Azure Bastion Secures RDP and SSH

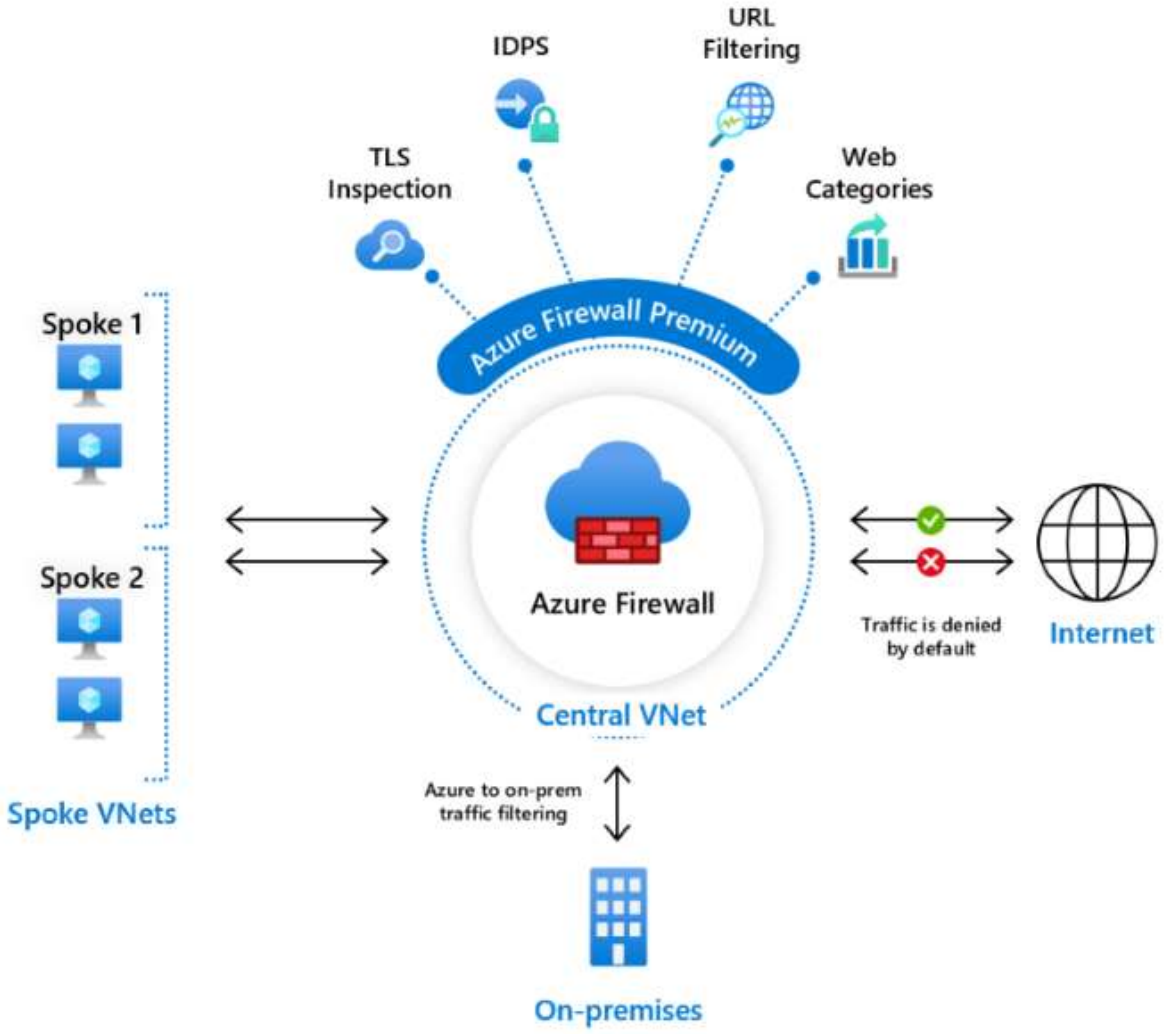
Firewall



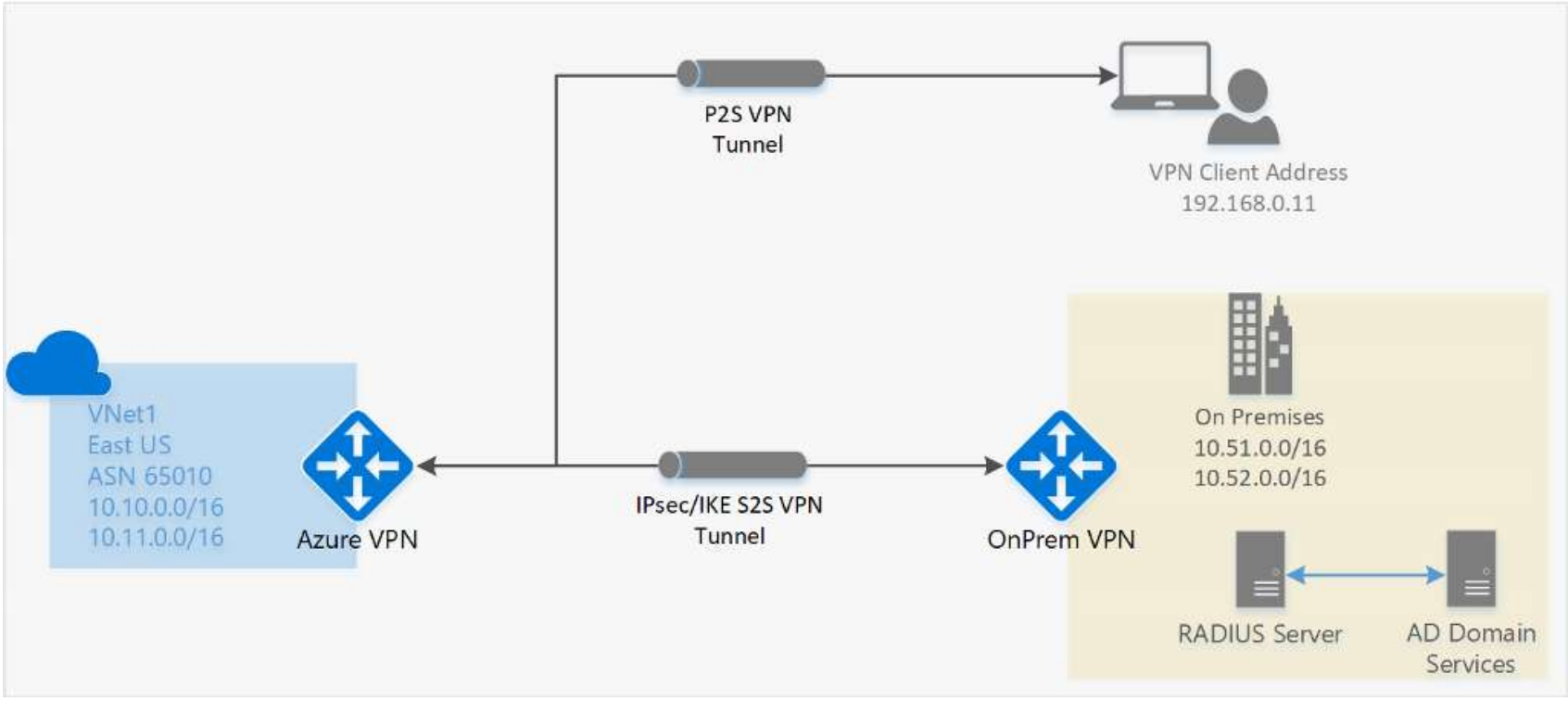
Azure Firewall



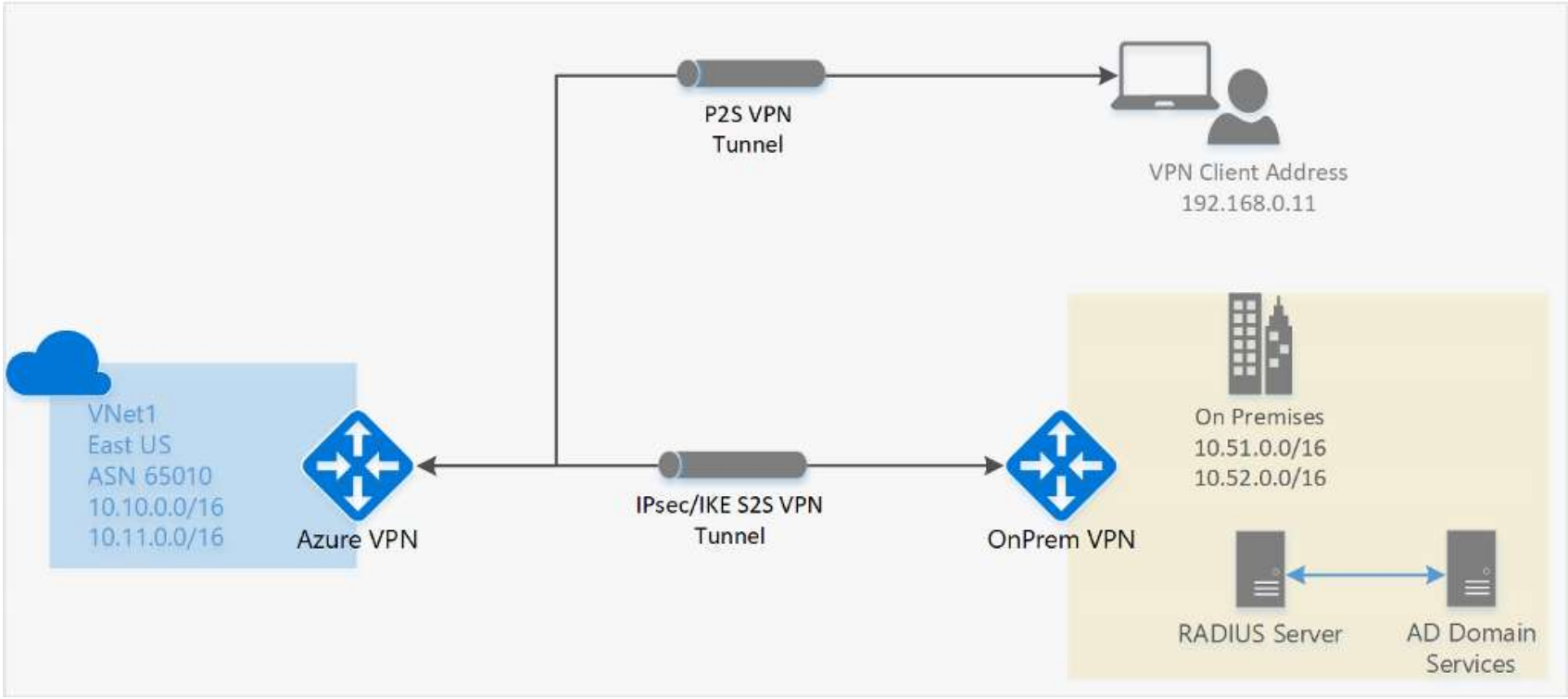
Azure Firewall



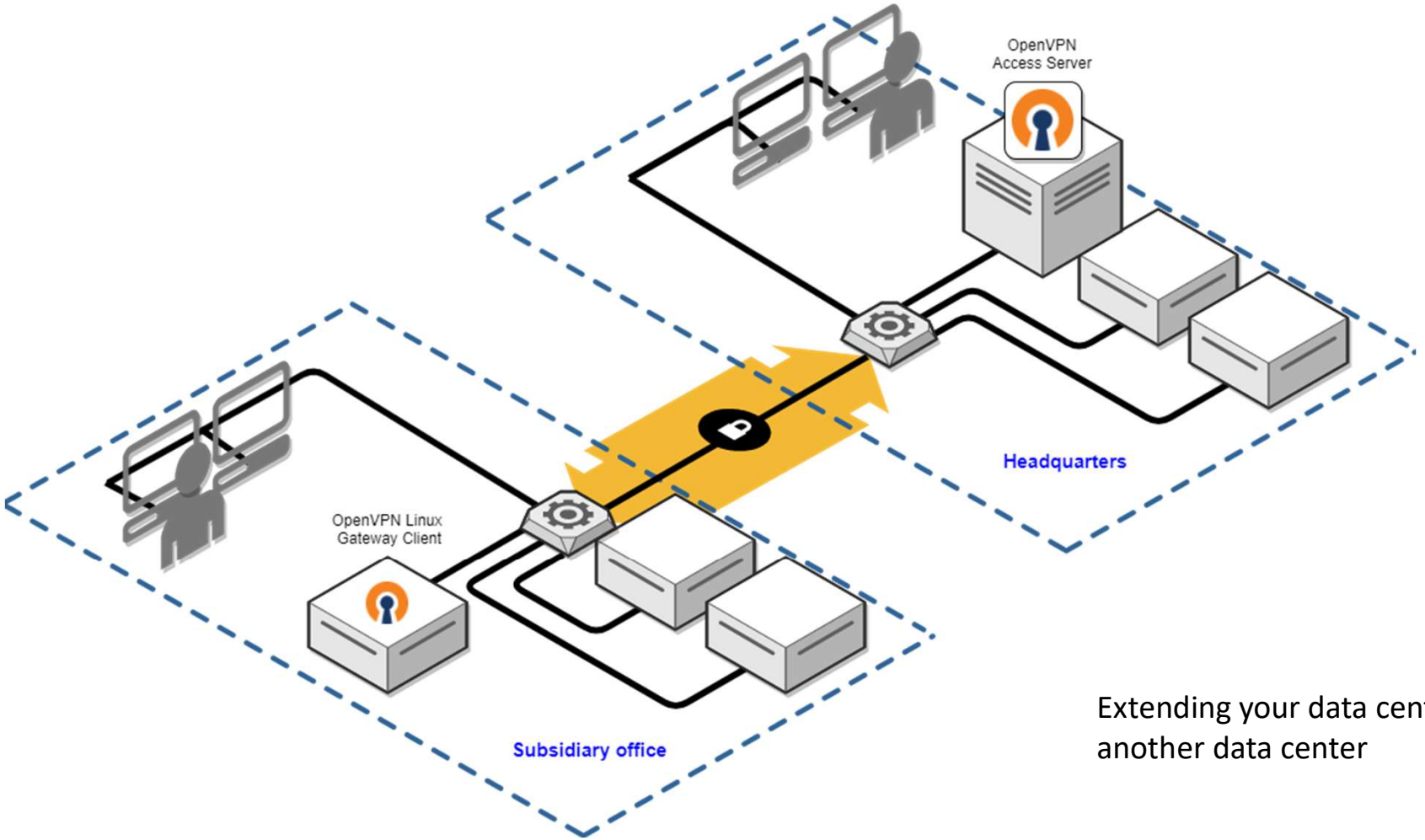
Azure VN Connectivity Pint to Site



Azure VN Connectivity Point to Site

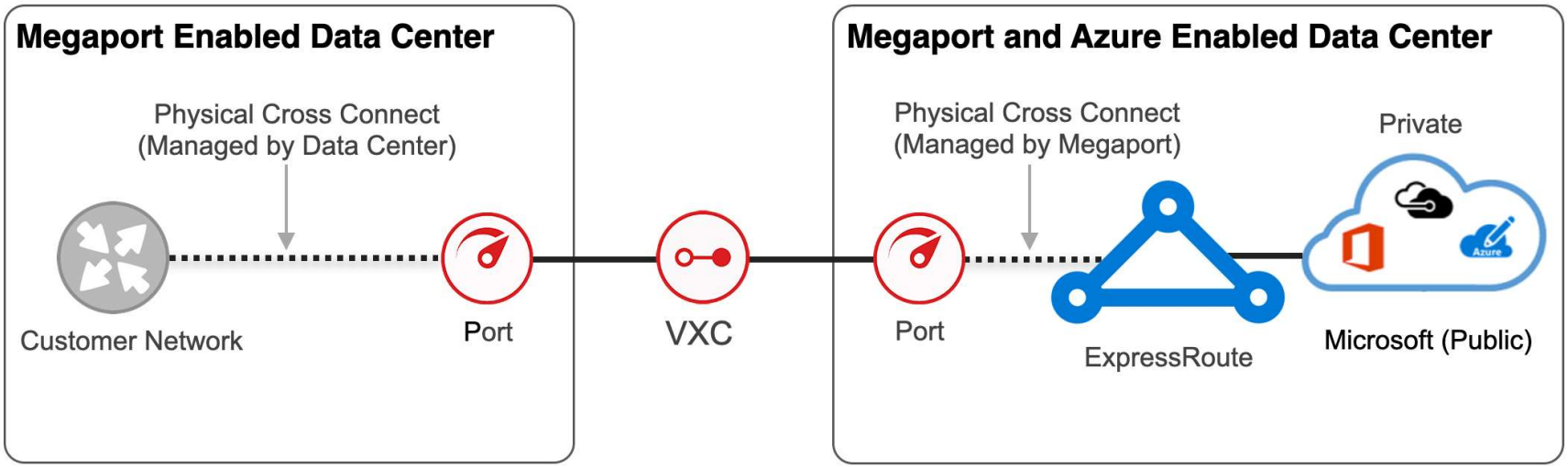


Azure VN Connectivity Site to Site

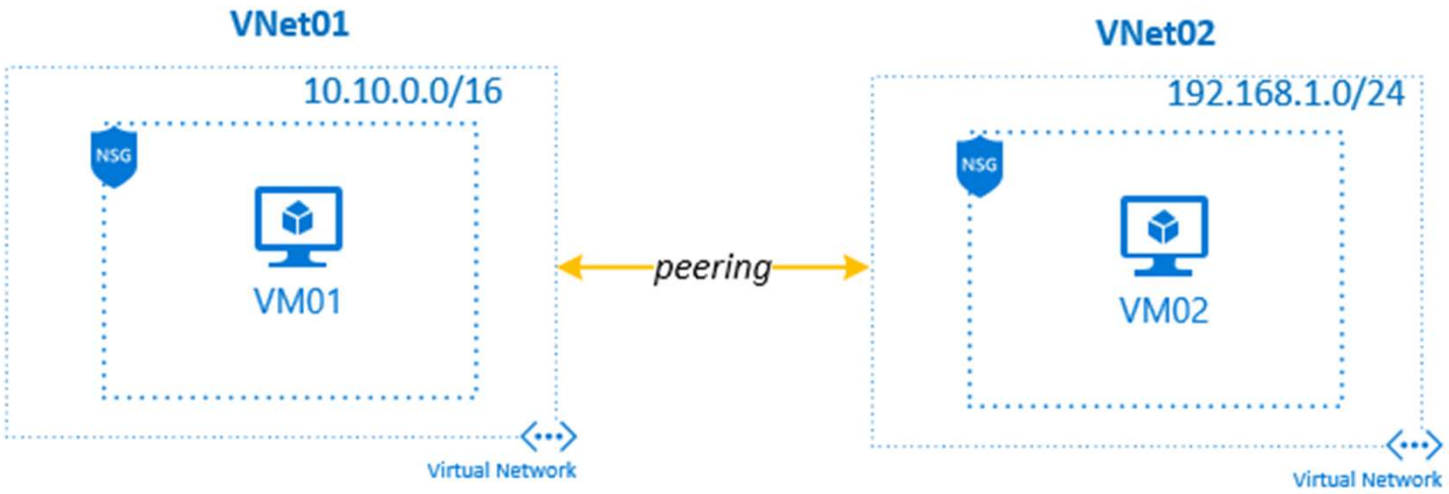


Extending your data center to cloud or another data center

Azure VN Connectivity Express Route



Azure VN Connectivity VNET Peering

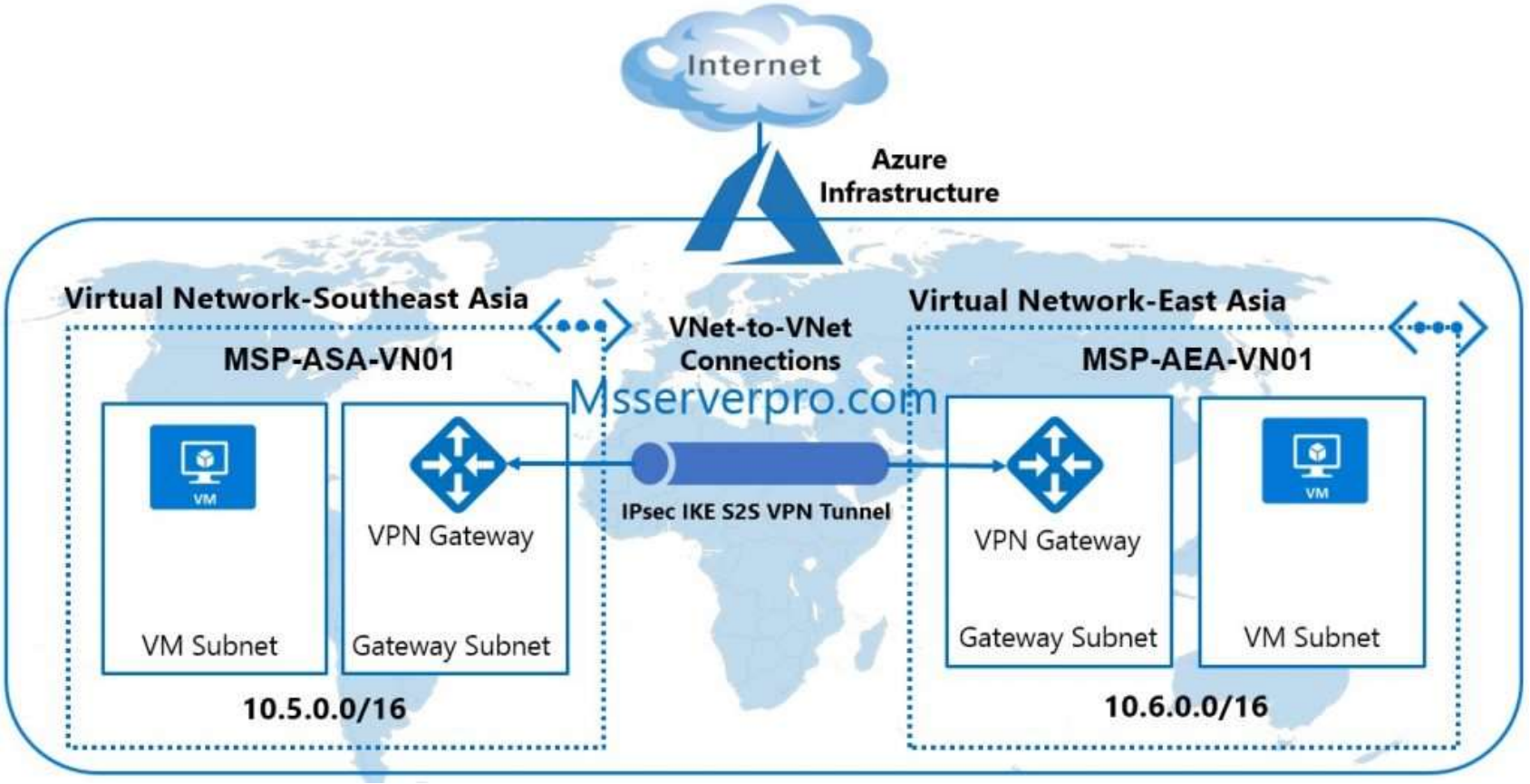


Azure VN Connectivity VNET To VNET Peering

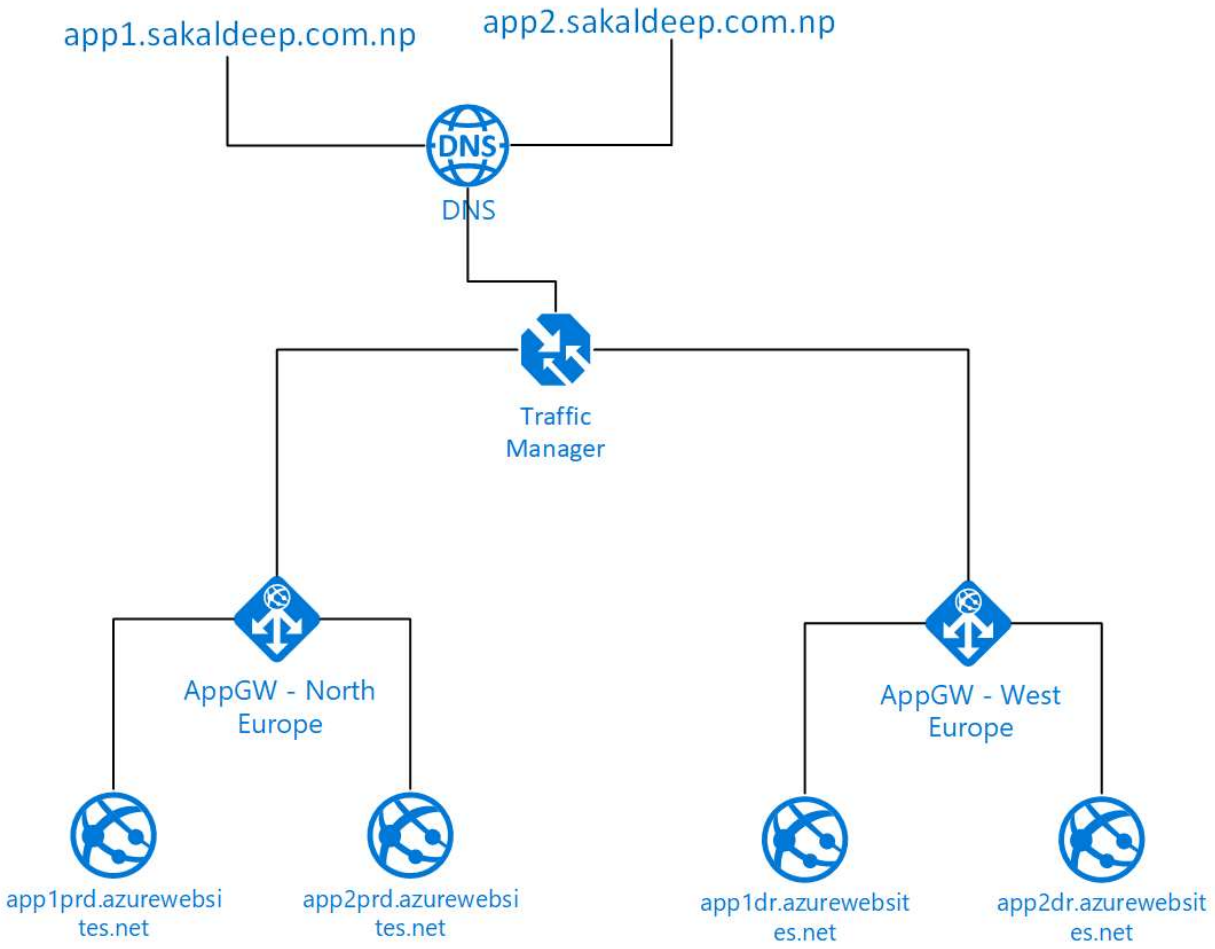
When a VNet to Vnet conection your vnet can be:

1. In same or diff regions
2. In same or diff subscriptions
3. In same or diff deployment models

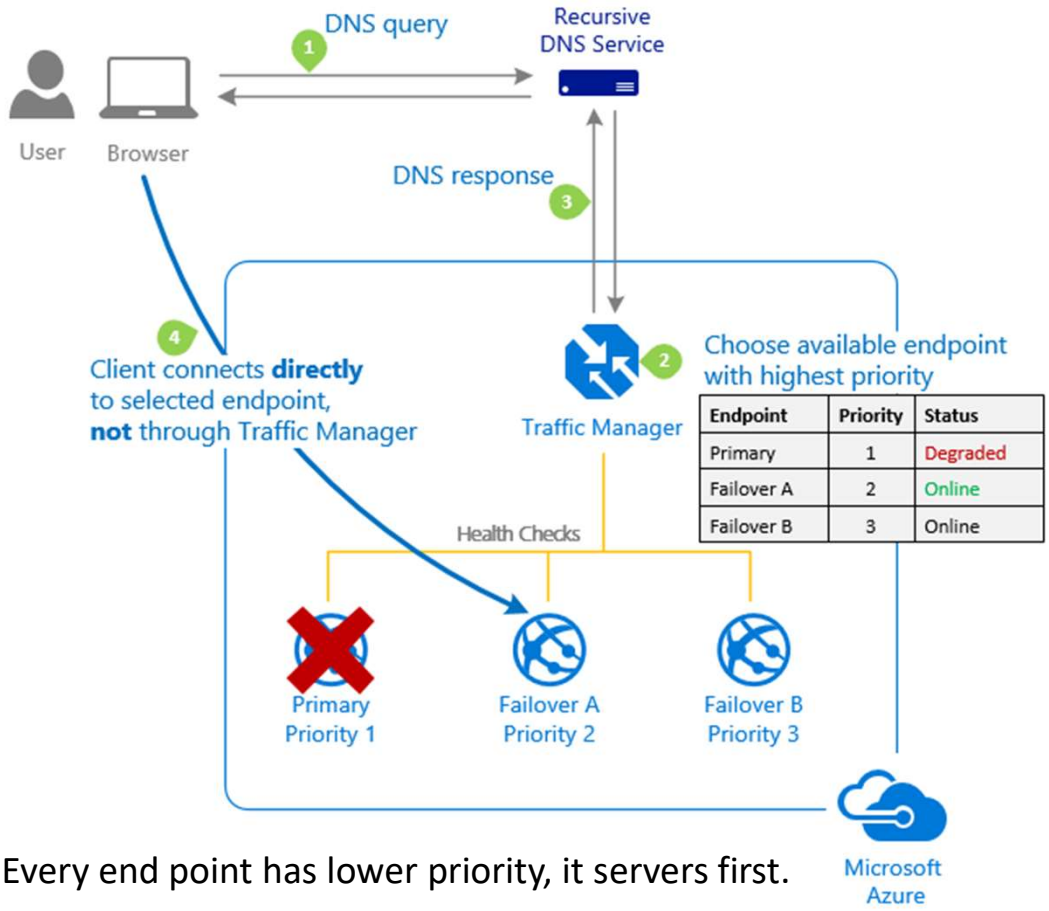
Azure VN Connectivity VNET To VNET Peering



Azure TM

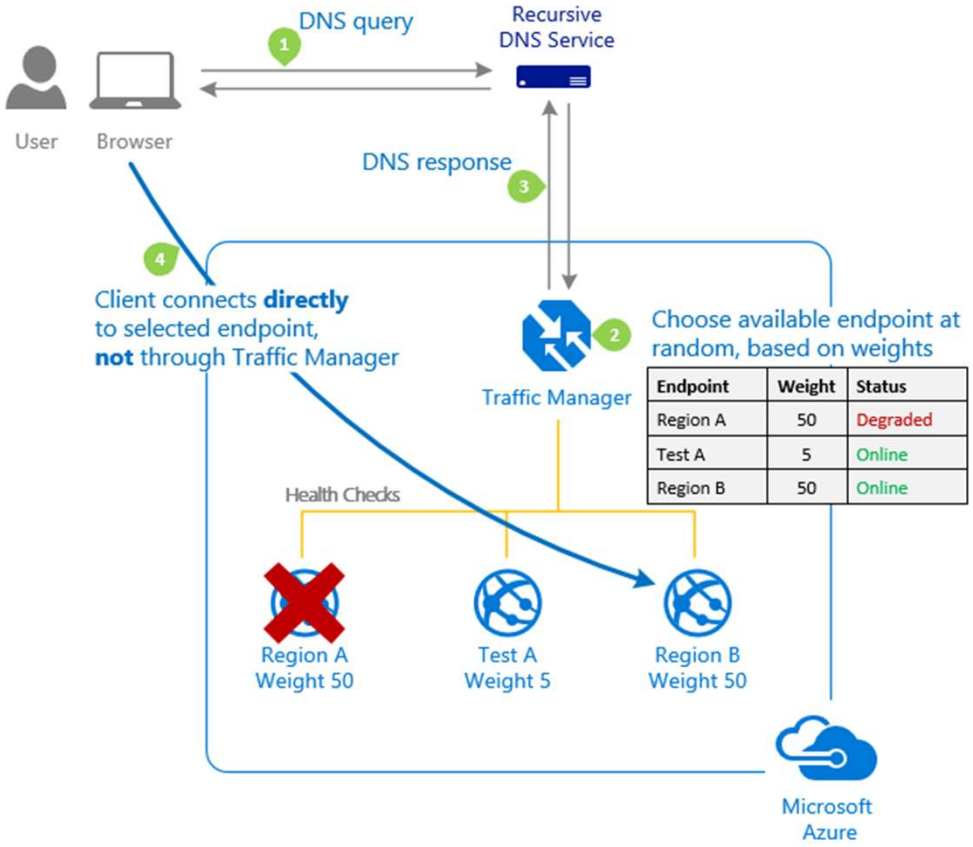

app1.sakaldeep.com.np
app2.sakaldeep.com.np
DNS
DNS
Traffic Manager
AppGW - North Europe
AppGW - West Europe
app1prd.azurewebsites.net
app2prd.azurewebsites.net
app1dr.azurewebsites.net
app2dr.azurewebsites.net

Azure Traffic Manager -Priority



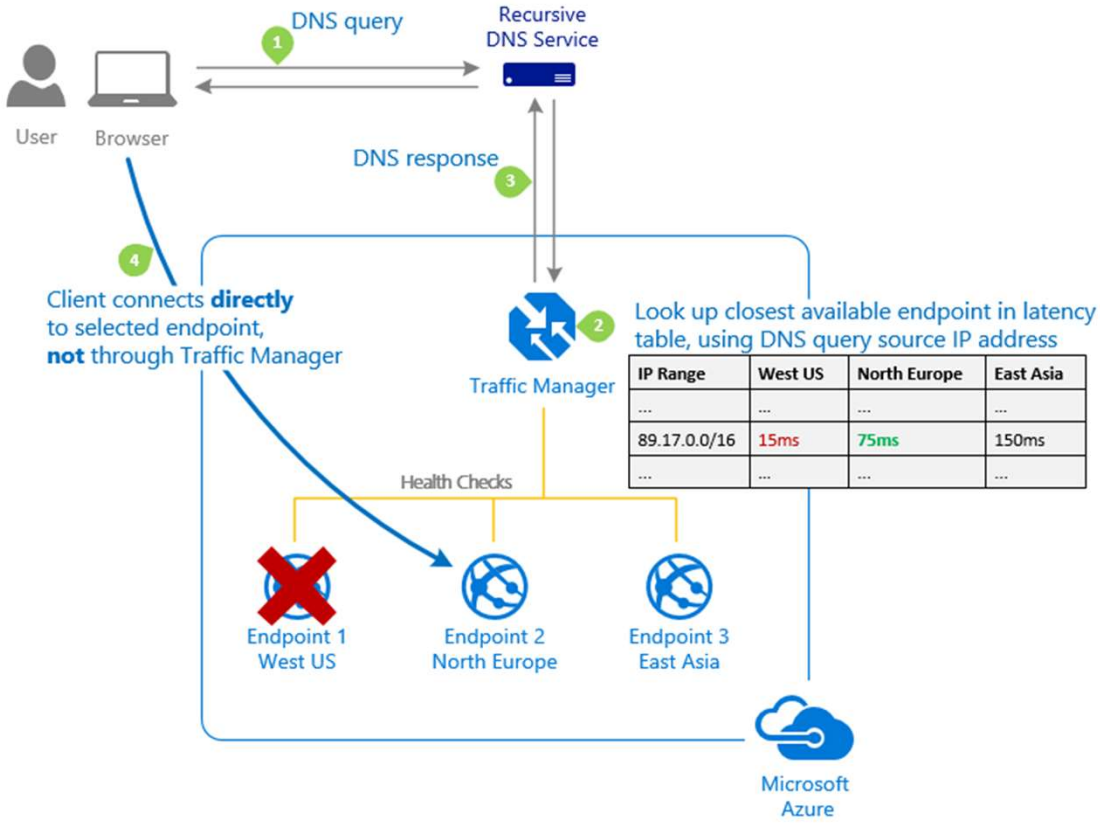
Every end point has lower priority, it servers first.

Azure Traffic Manager-weighted



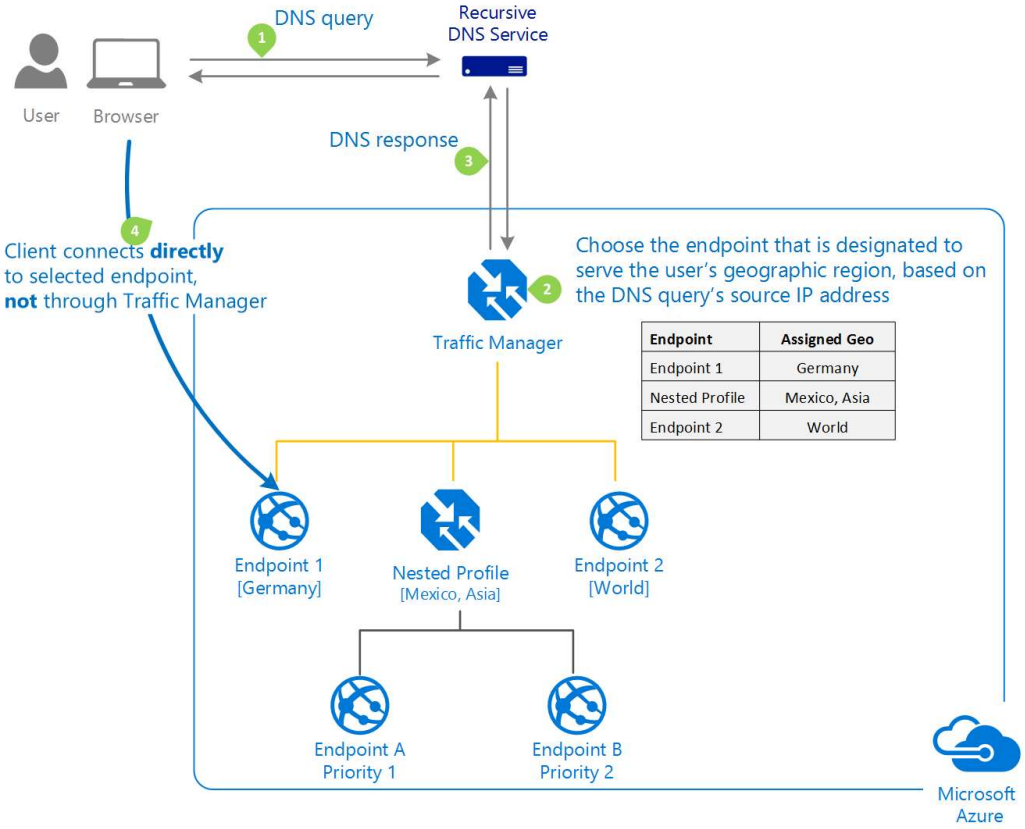
Two app Services- India -2 requests, US-1 request

Azure Traffic Manager-Performence



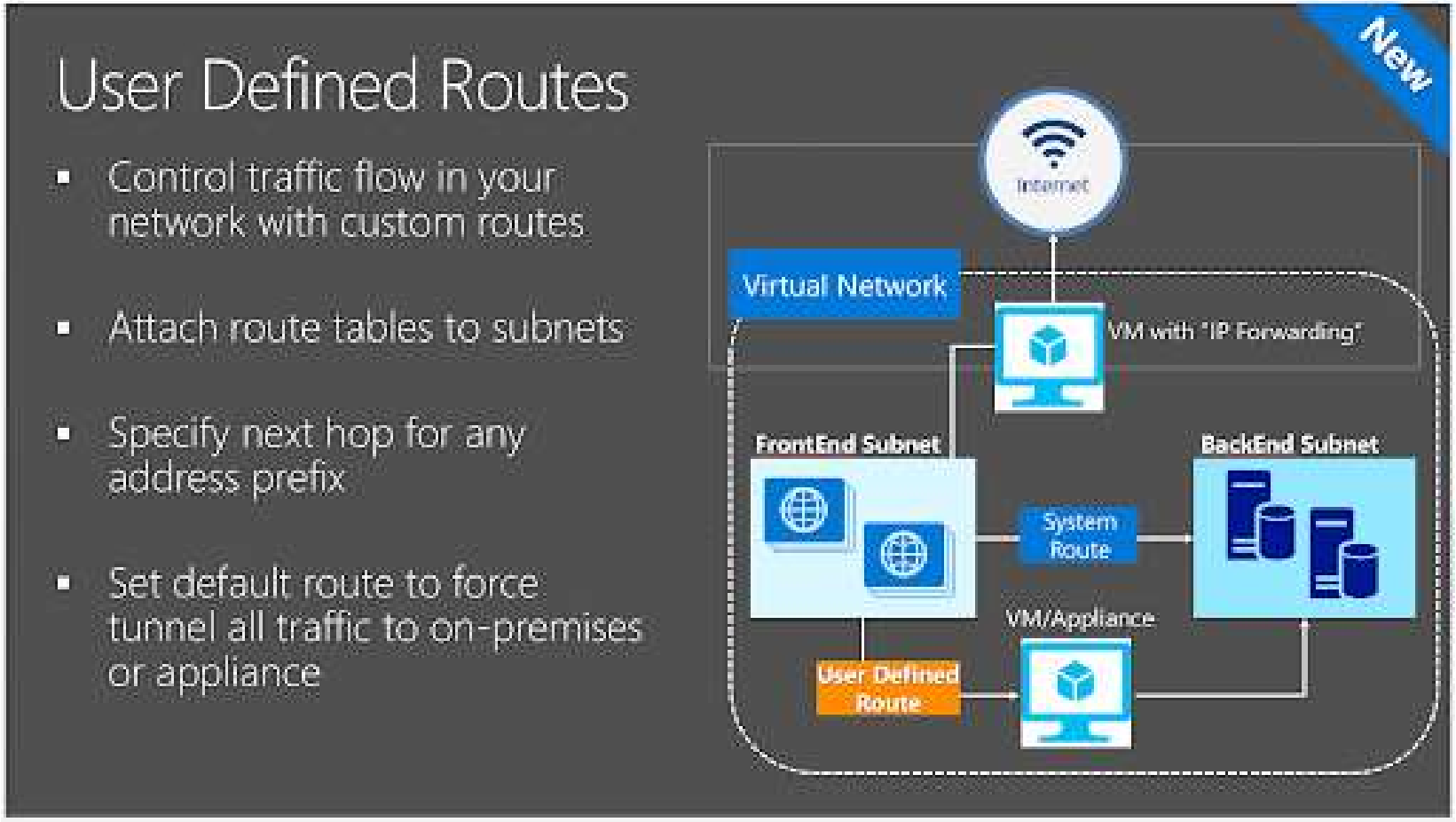
Select Performance routing when you have endpoints in different geographic locations and you want end users to use the "closest" endpoint for the lowest network latency.

Azure Traffic Manager-Geographic

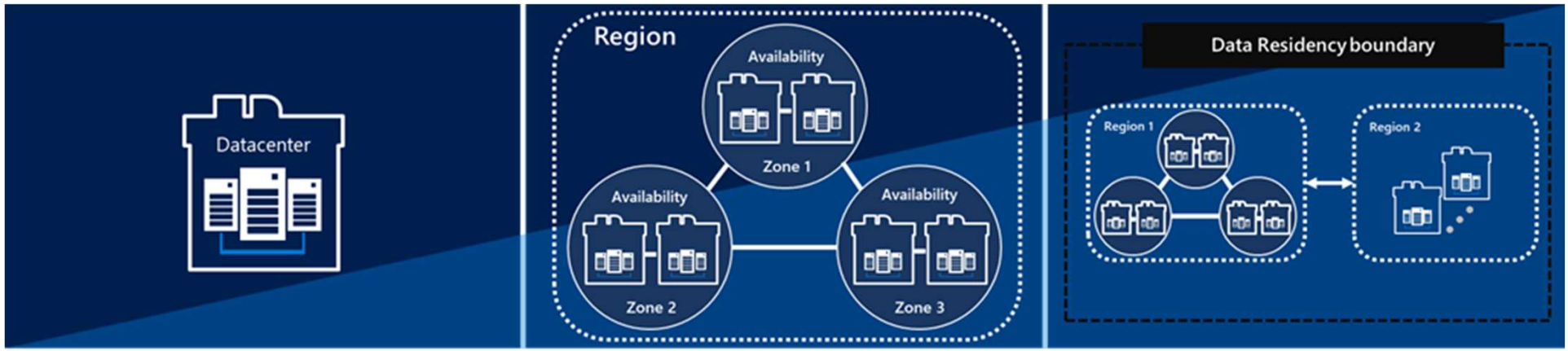


Suppose data is stored in India data center, when a request is came from US then data is loaded from India and sended to us.

User Defined Routes



Availability Set



Availability Sets

High Availability protection from hardware failures in a datacenter.

Availability Zones

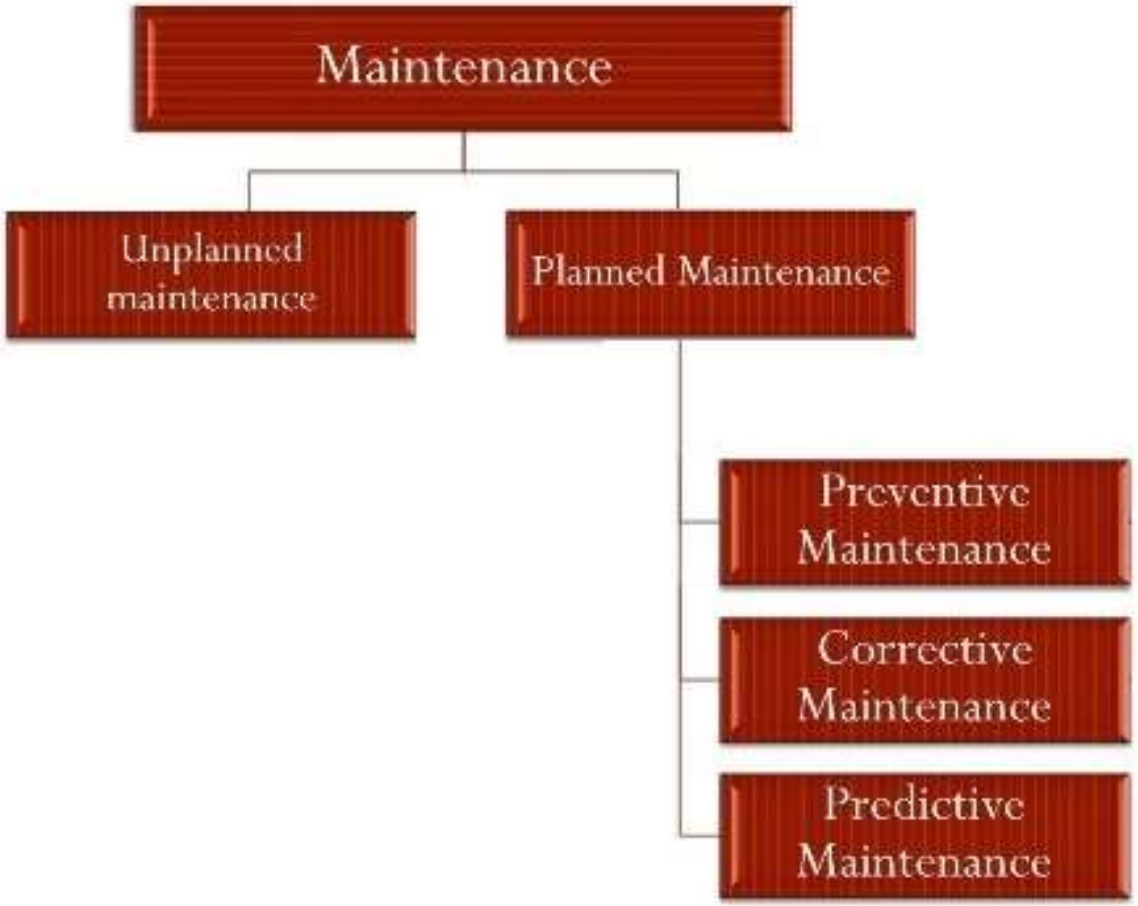
High Availability protection against loss of datacenters. Multiple datacenters per physically separated zone. Each zone features independent network, cooling, and power.

Region Pairs

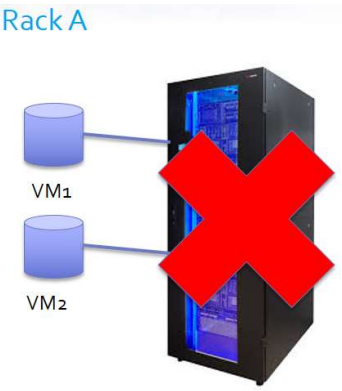
Protection for your data and applications from the loss of an entire region with Geo-redundant storage (GRS) and Azure Site Recovery.

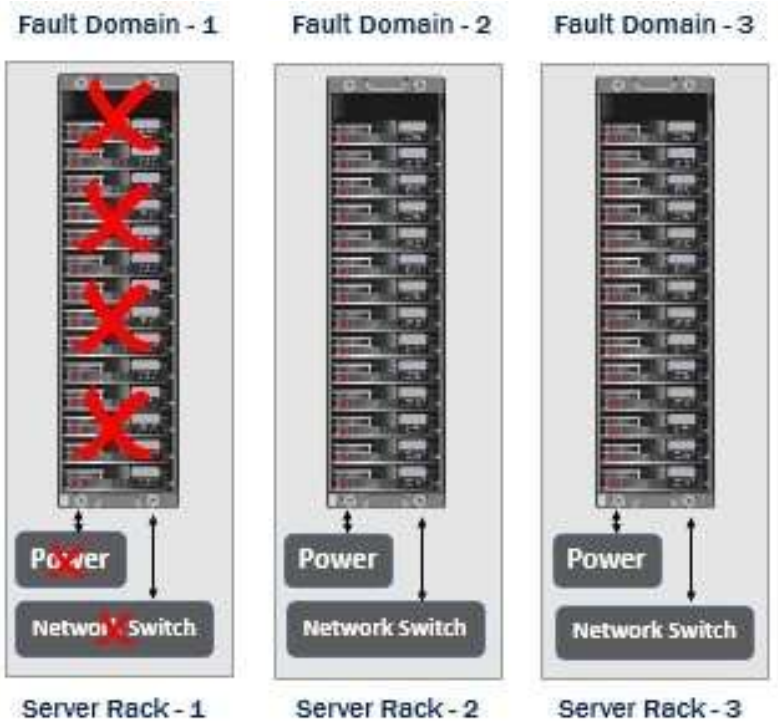
Availability Set

Availability Set



Availability Set





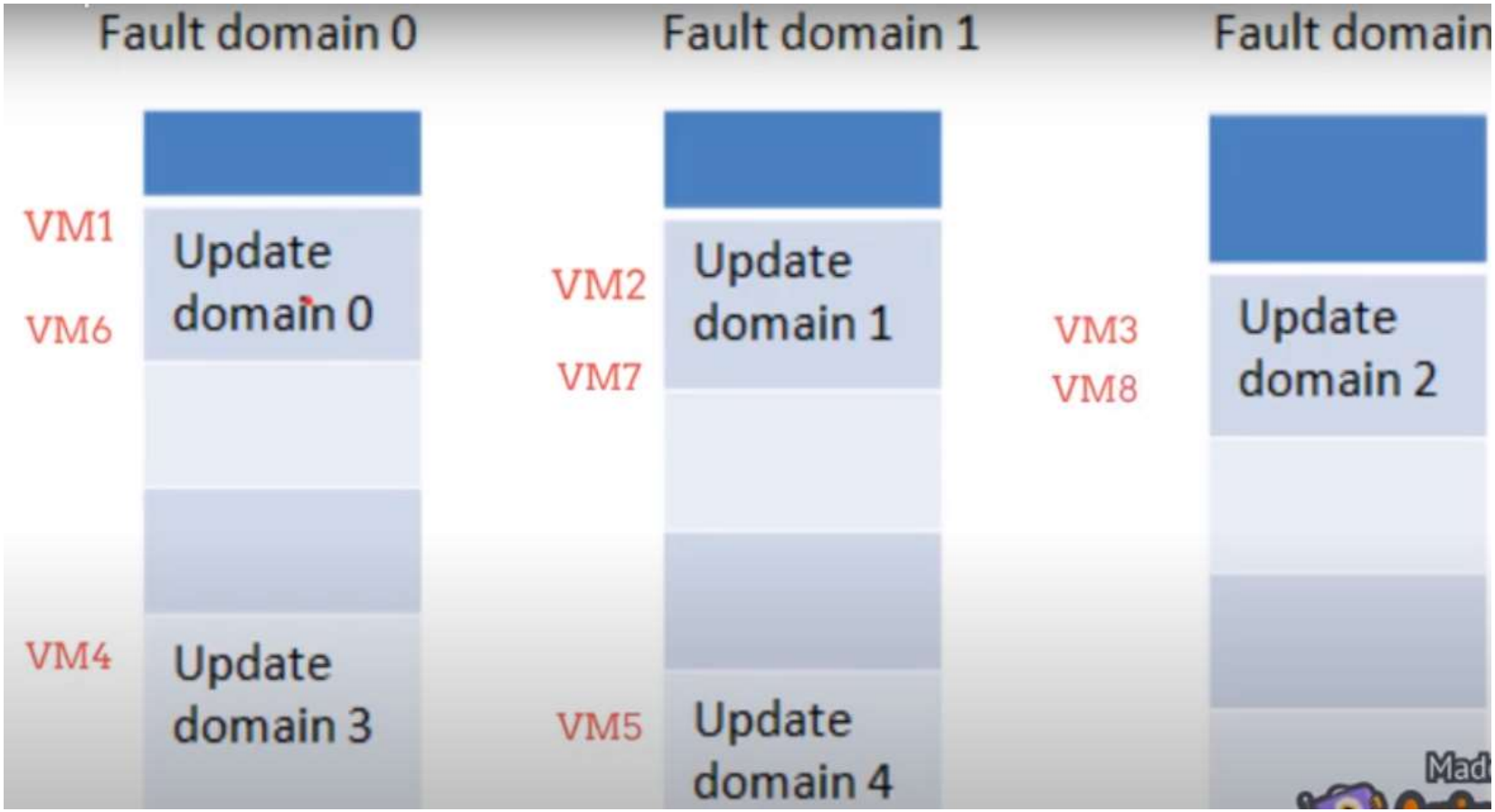
Availability Set

In the image below, we see an Availability Set with 16 virtual machines, and four update domains. This means that a maximum of four VMs can be down for maintenance at a given time, allowing the other 12 to carry the load. Once the first four return to service, another group will be available for maintenance. In conjunction with Fault Domains, this allows an Availability Set to ensure that undue burden is not placed on either rack.

Availability Set 1

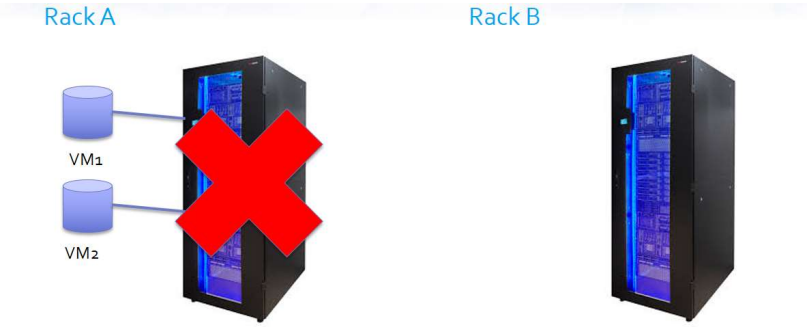
Update Domain 1	Update Domain 2	Update Domain 3	Update Domain 4
VM1 – updating	VM2	VM3	VM4
VM5 – updating	VM6	VM7	VM8
VM9 - updating	VM10	VM11	VM12
VM13 - updating	VM14	VM15	VM16

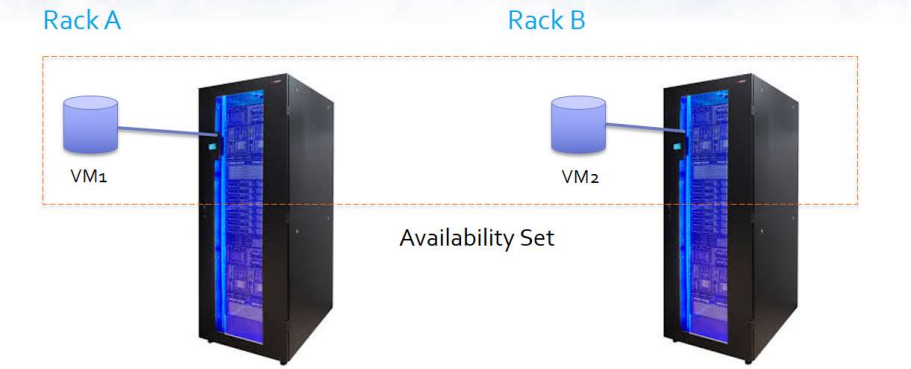
Availability Set (8 VM'S, 3-FD, 5-UD)



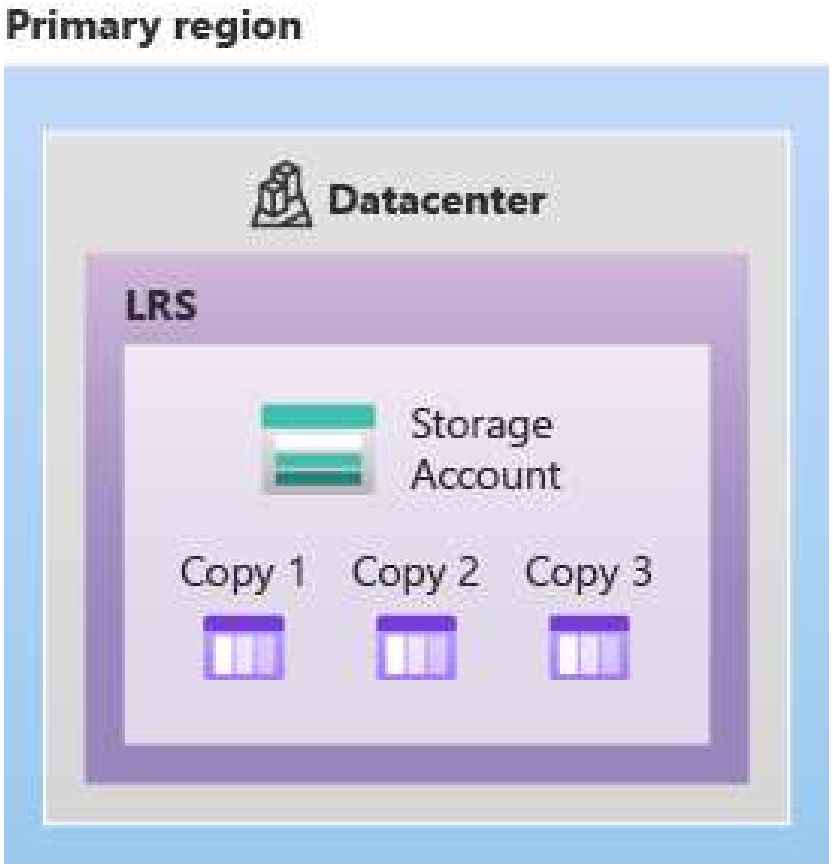
Availability Set

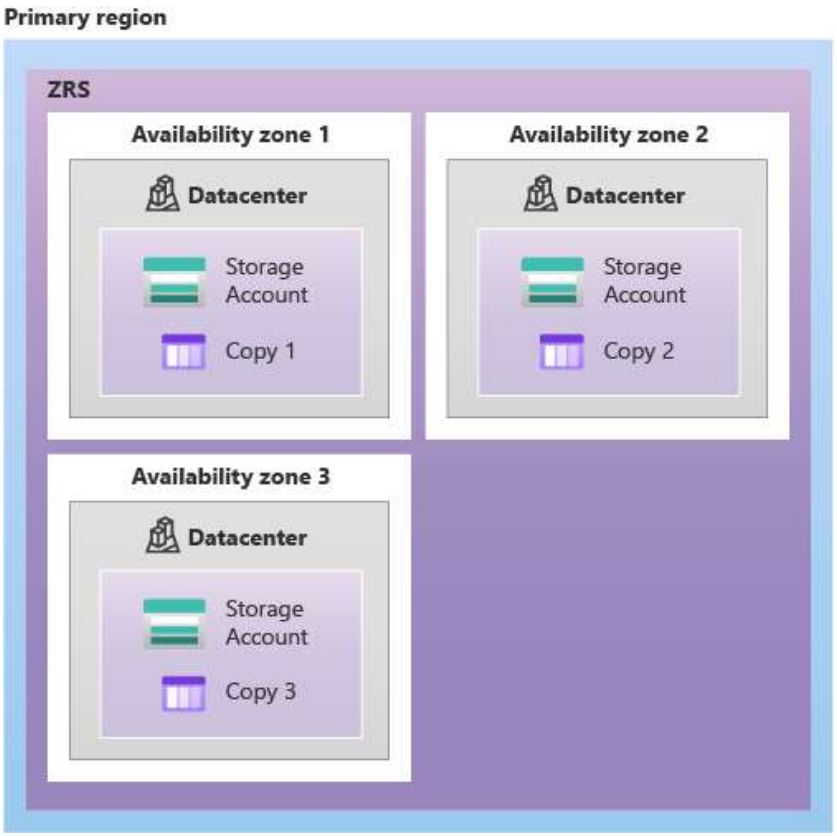
Step 1: Define Fault Domains (max-3) (logical grouping)
Step 2: Define Update Domain in Fault Domains
Step 3: Put VM's in update domains



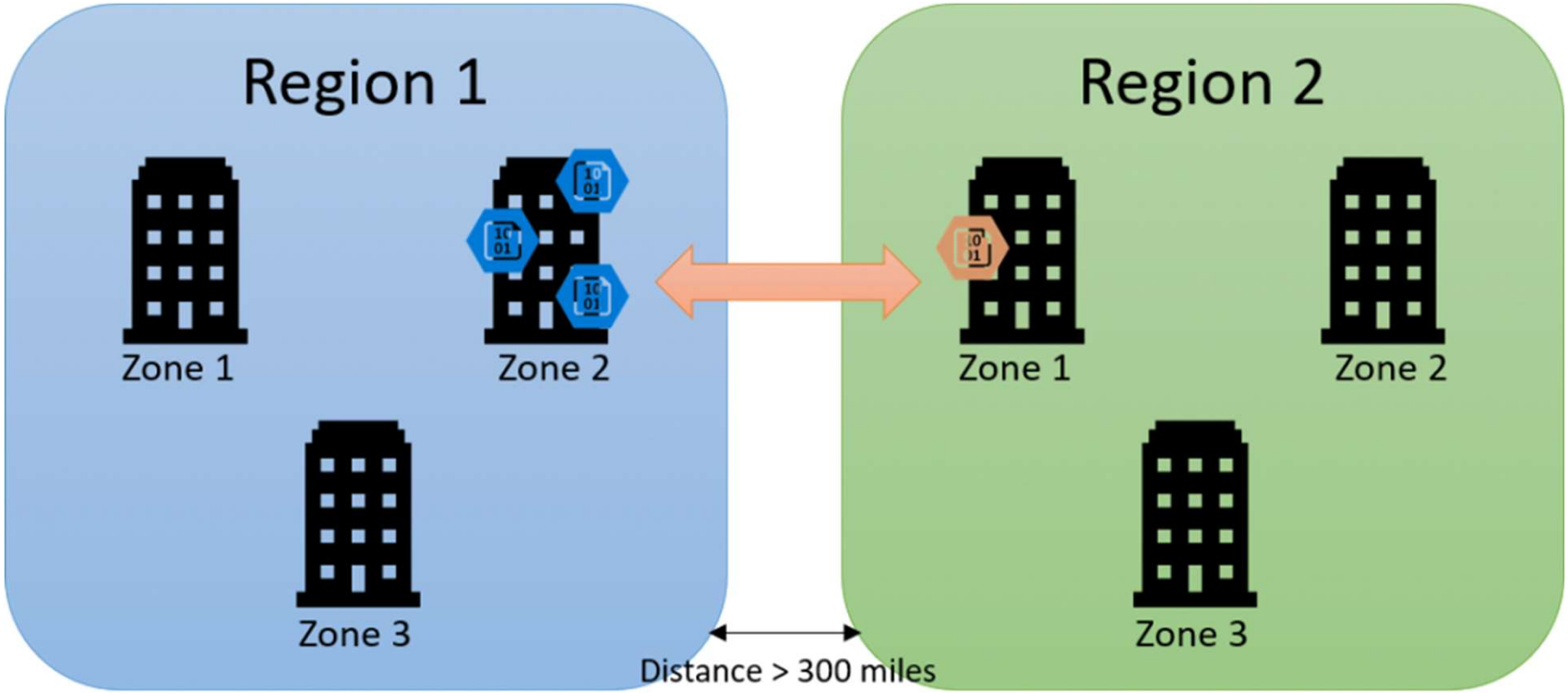


Availability Zone –LRS, ZRS



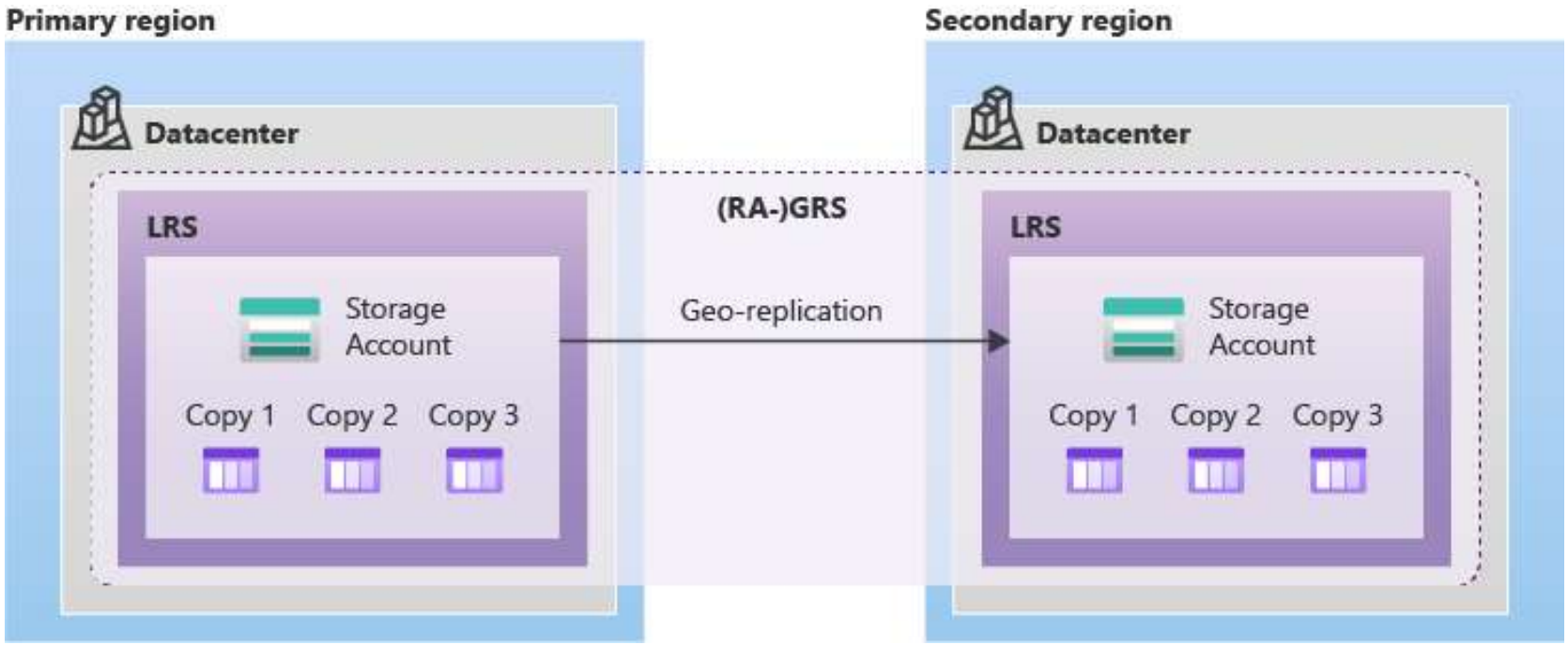


Availability Zone –GRS

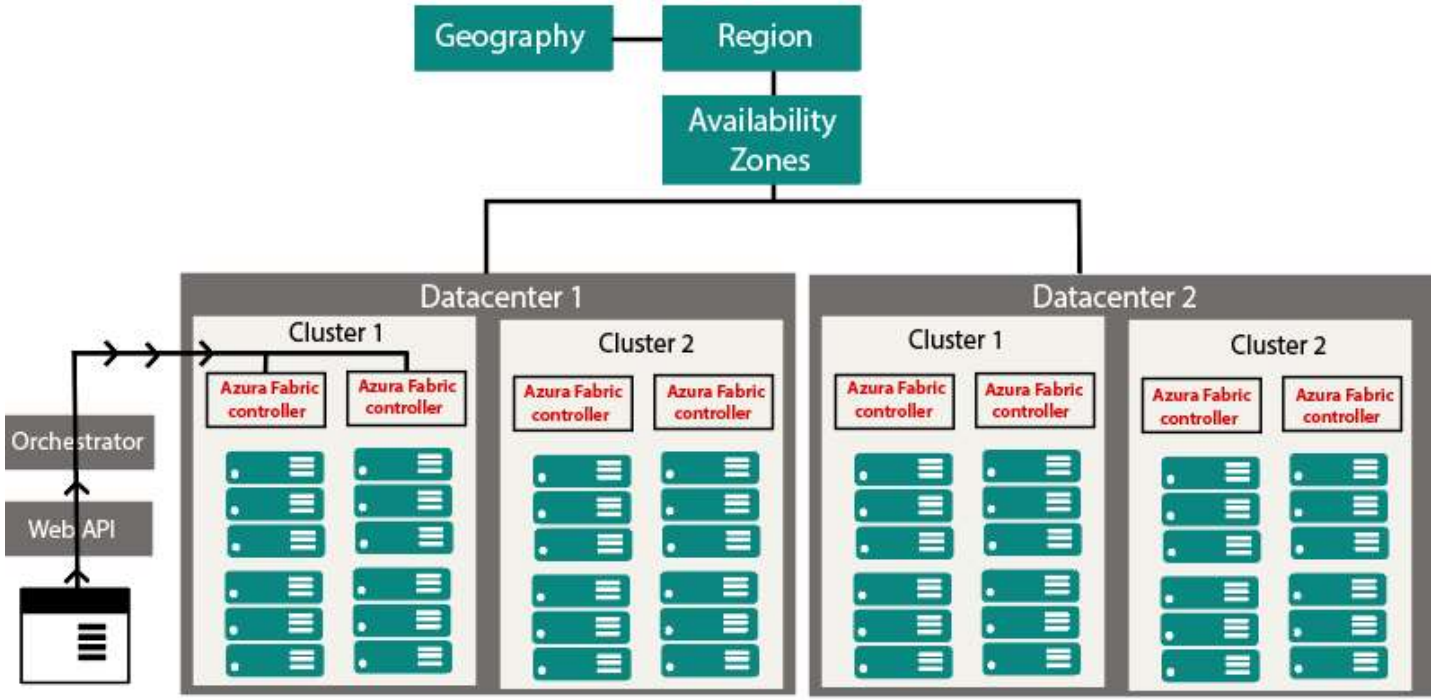


GRS replicates our data to another region, but data will be available to be read-only if Microsoft initiates a failure from primary to the secondary region.

Availability Zone –RAGRS

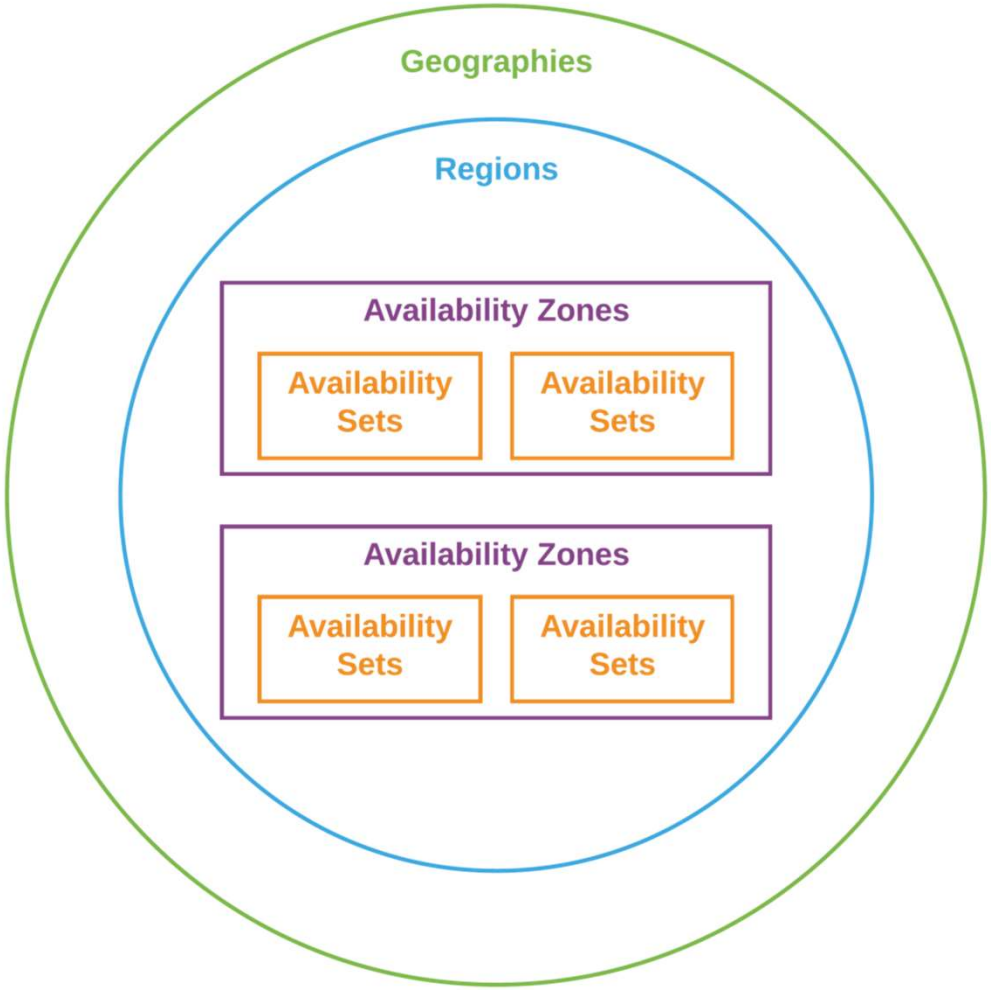


RAGRS replicates our data to another region, data will be available to be asynchronus

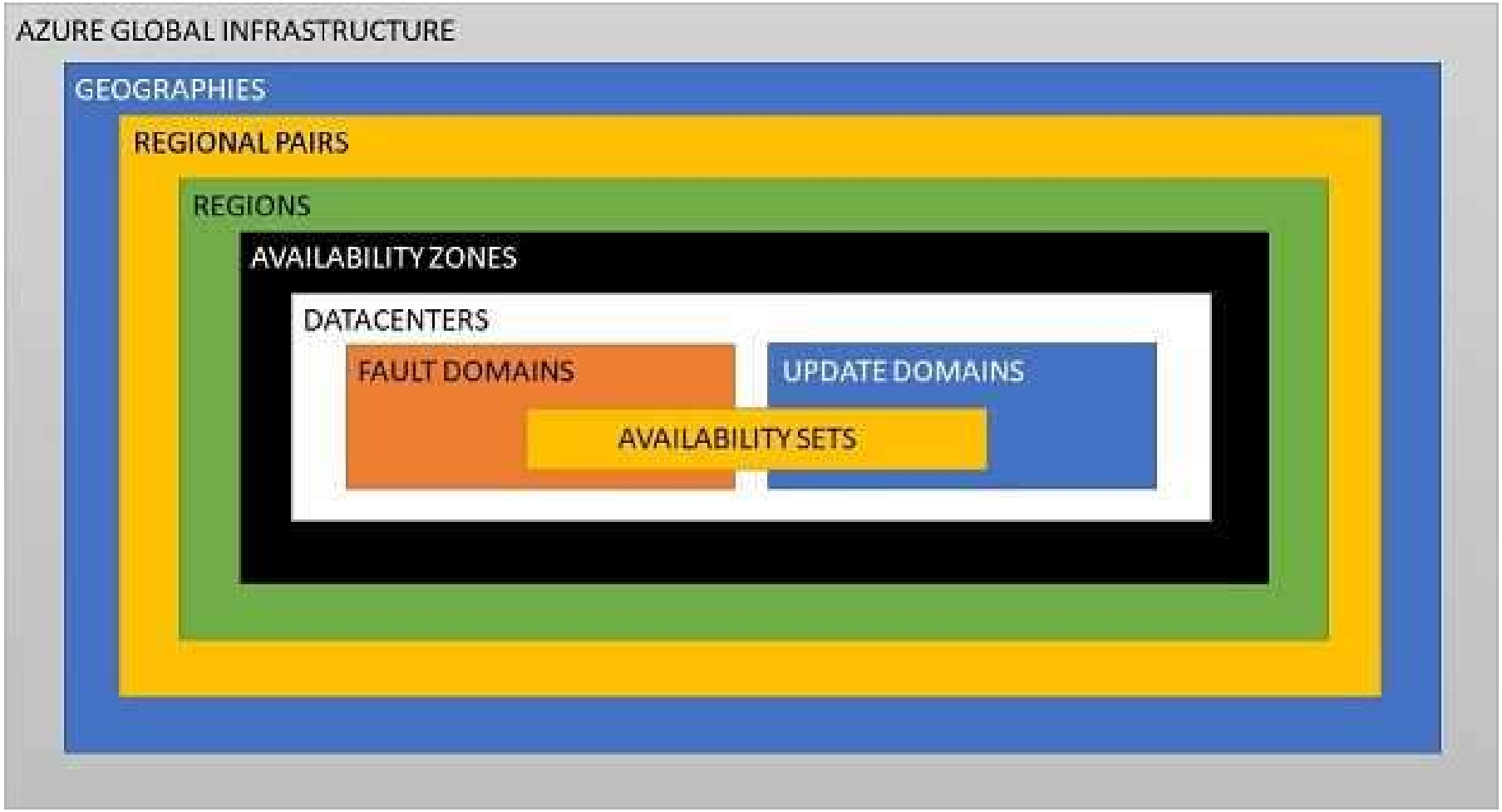


Geography	Regional Pair A	Regional Pair B
Canada	Canada Central	Canada East
China	China North	China East
India	Central India	South India
Japan	Japan East	Japan West
North America	East US	West US

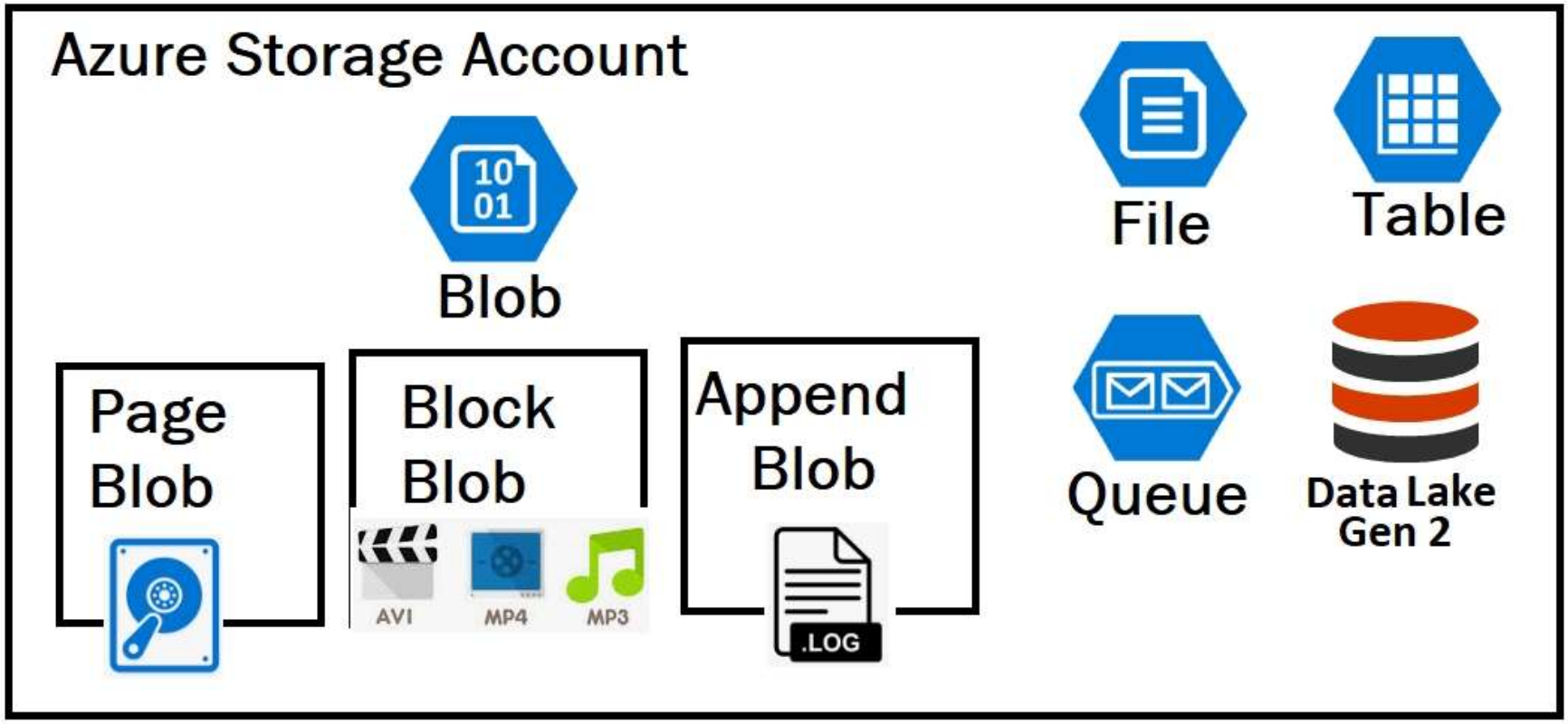
Availability Zone



Availability Zone



Azure Storage Account



Azure CDN

@pvergadia

Azure VM

Virtual Machine

- A virtual machine (VM) is an environment, usually a program or operating system, which does not physically exist but is created within another environment.
- Allows the ability to “run a computer within your computer”
- Can be viewed as a physical machine
  - Memory (RAM)
  - Ethernet connection
  - Storage (Hard disks)

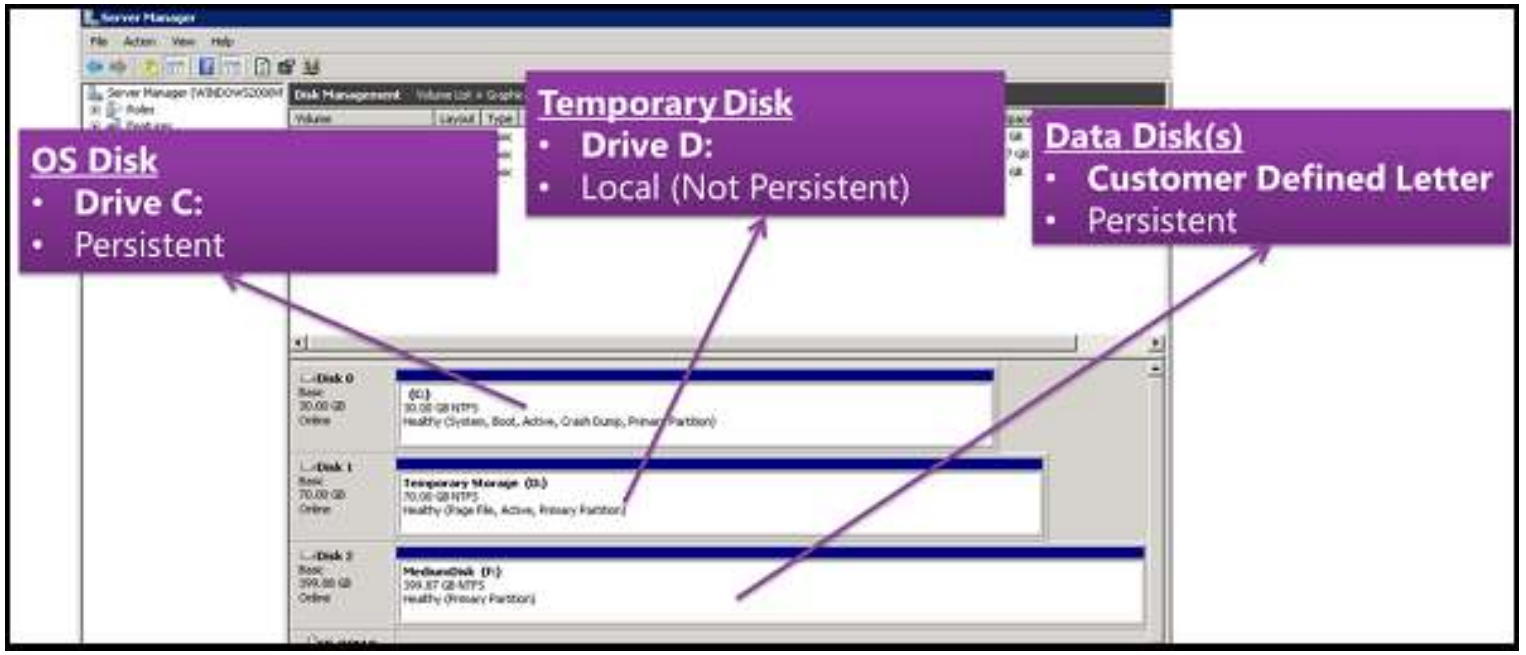
Azure VM

Terminology

- Host operating system (host OS)
  - The operating system of the physical computer on which the virtual machine was installed.
- Guest operating system (guest OS)
  - The operating system running inside the virtual machine.
- Snapshot
  - A snapshot is a copy of the virtual machine's current state.
  - Multiple snapshots can be saved to go back to at any given time.
- Image
  - The actual virtual machine

Azure VM

Azure VM Disks



OS Disk:- Our O.S (windows can be installed) (Page blobs)
Data Disk:- Our custom data will be stored (Data of our application) (optional) (HDD/SDD)
Temporary Disk:- Used for high input and output operations

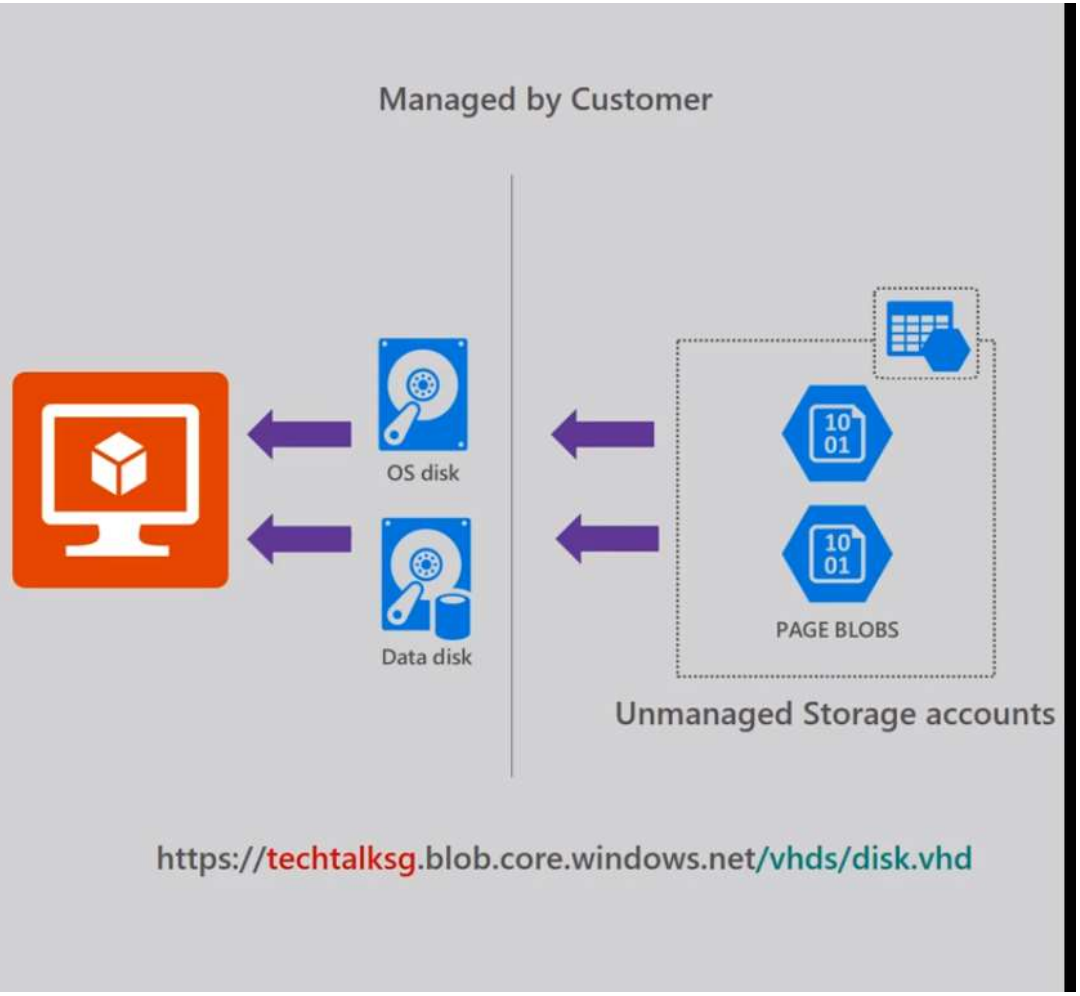
Azure VM

What are Unmanaged Disks?

Management - Disk Created and managed by customer

Proper Sizing - Storage Account is limited to 20000 IOPS

Sparse Storage (Standard)- only pay for actual data than a disk size



Azure VM

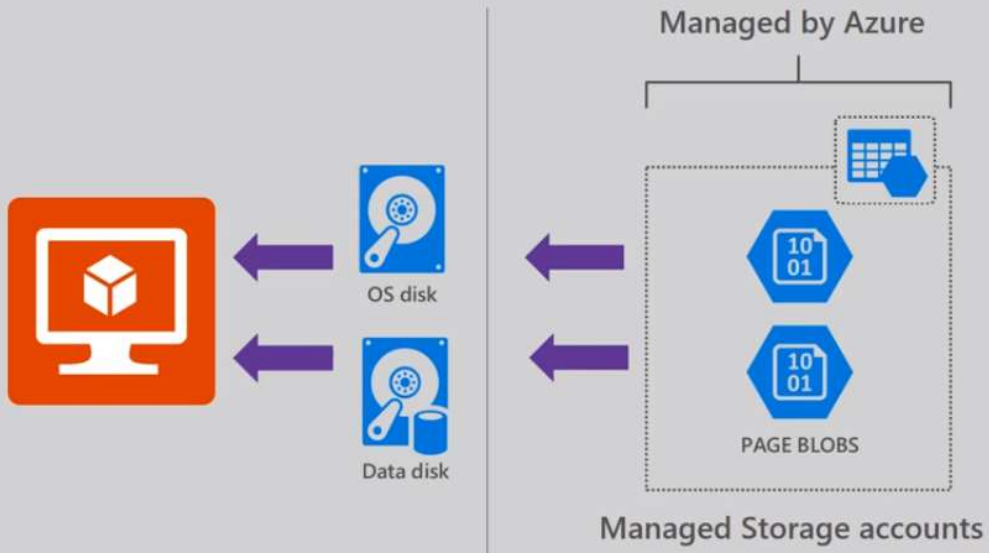
What are Managed Disks?

Simple - Abstracts storage accounts from customers

Granular access control – Top level ARM resource, apply Azure RBAC

Better performance - Storage account limits do not apply

Big scale - Up to 20,000 disks per region per subscription



Azure VM

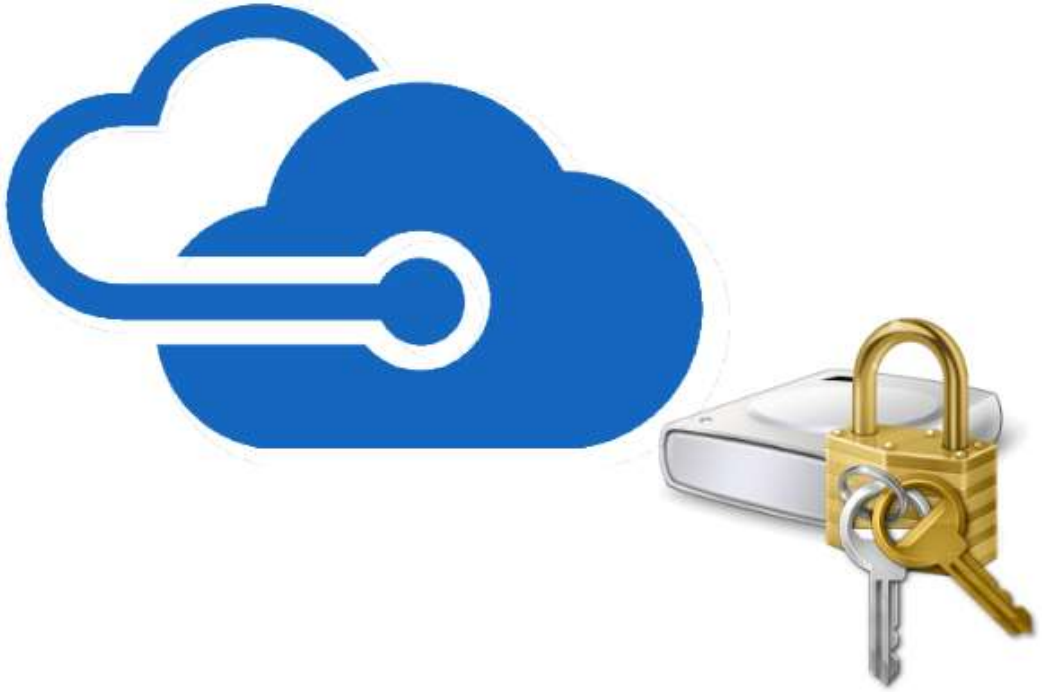
- Use Managed Disk for all the production IaaS workloads
- Use Managed Disks with Availability Set
- Not all Azure services support managed disk yet
- Some partner solutions still require unmanaged disk
- Migration to managed disk can be done by ConvertTo-AzureRmVMManagedDisk
- http://tech[illegible]azure-managed-disk/

used managed discs and if you've got availability set it makes perfect sense

Generalizing VM and Captureing VM Images

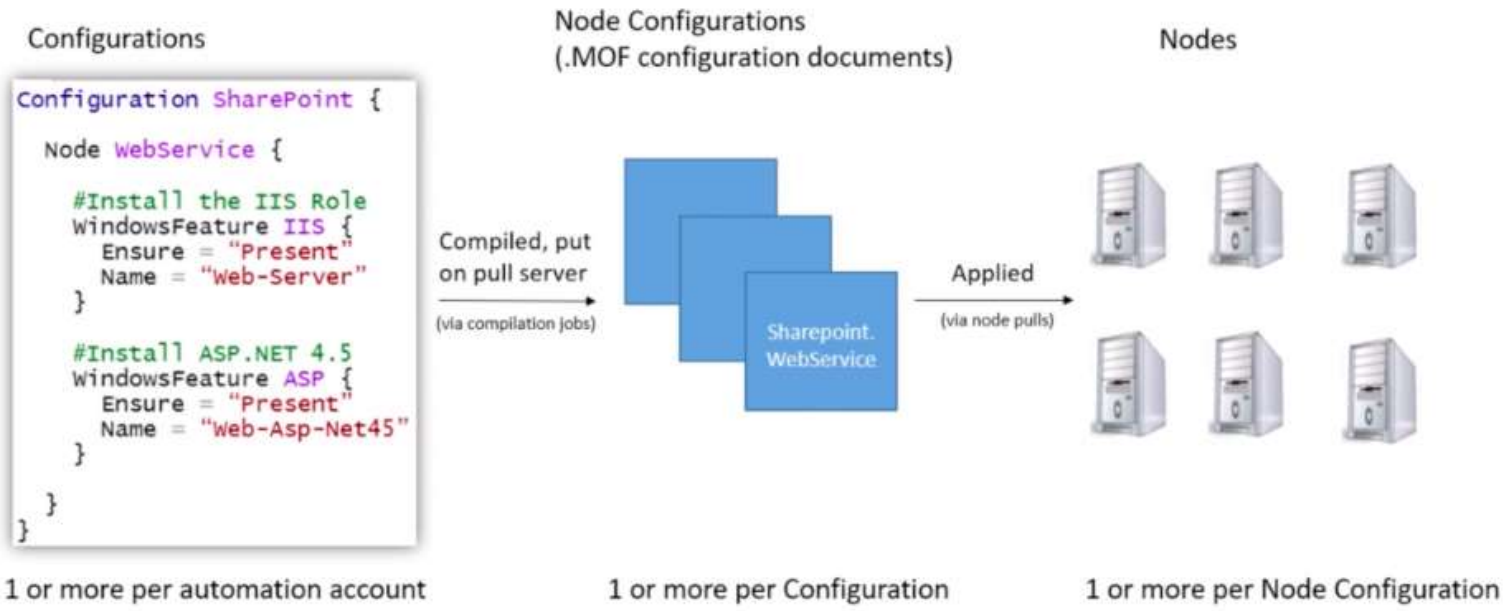
- If you want o create a vm instances, then these instances has differ from credentials and its own identity.
- So I want vm instances should be generalized or resuable
- Sol:- Creating vm instances taken from a one vm

Create an Azure VM with disk encryption



https://medium.com/@zaab_it/create-an-azure-vm-with-disk-encryption-36be9baab7ca

DSC

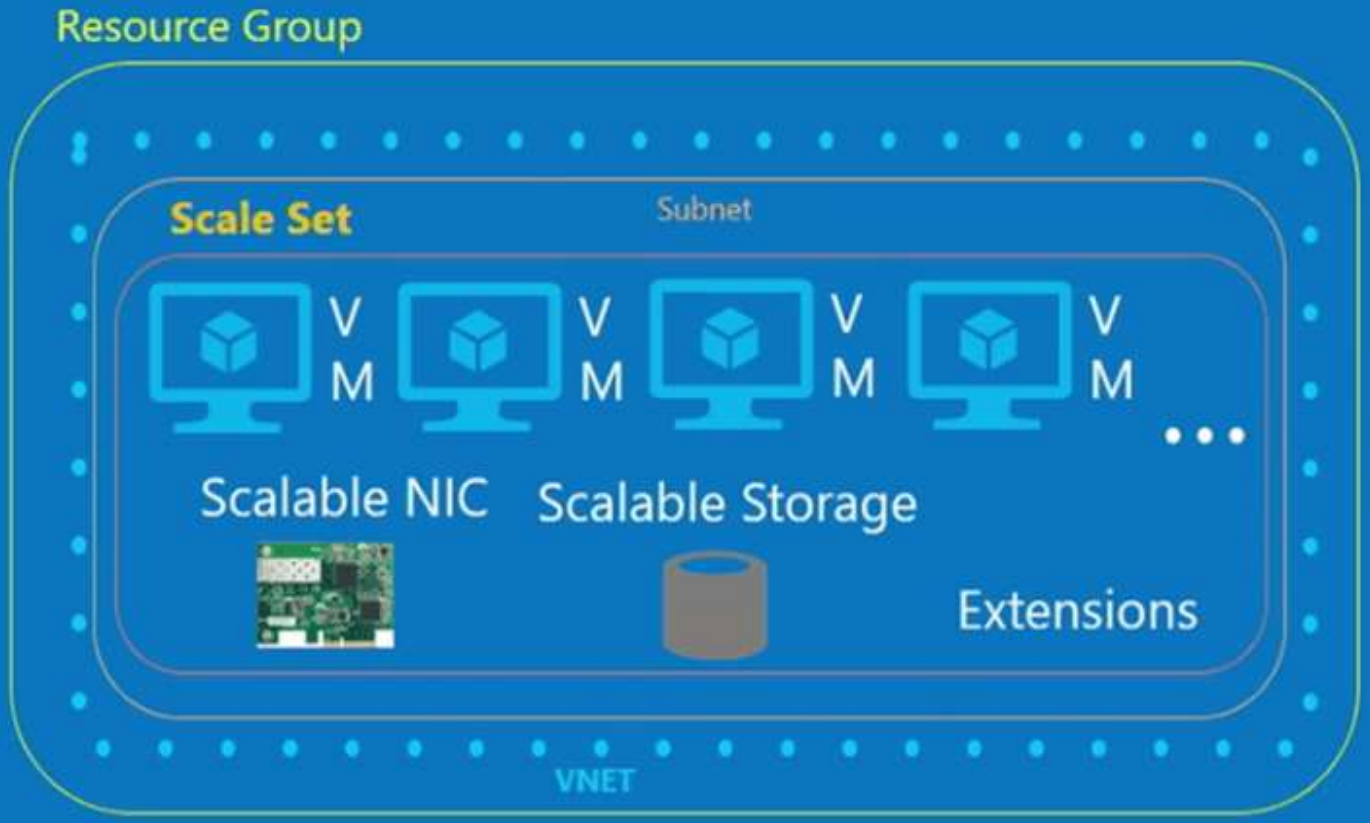


- Similar to ARM Template
- Instruction To O.S not to azure, so it is configurable to a particular state to the V.M

VM Scale Sets in ARM

Manage groups of identical VMs

- Auto-Scalable
- Fast
- Customizable
  - **Windows or Linux**
  - **VM extensions**
  - **Open PaaS platform**
- Ease of Management
  - **Focus on target instance count**
  - **Updateable**



How you buy affects how you manage

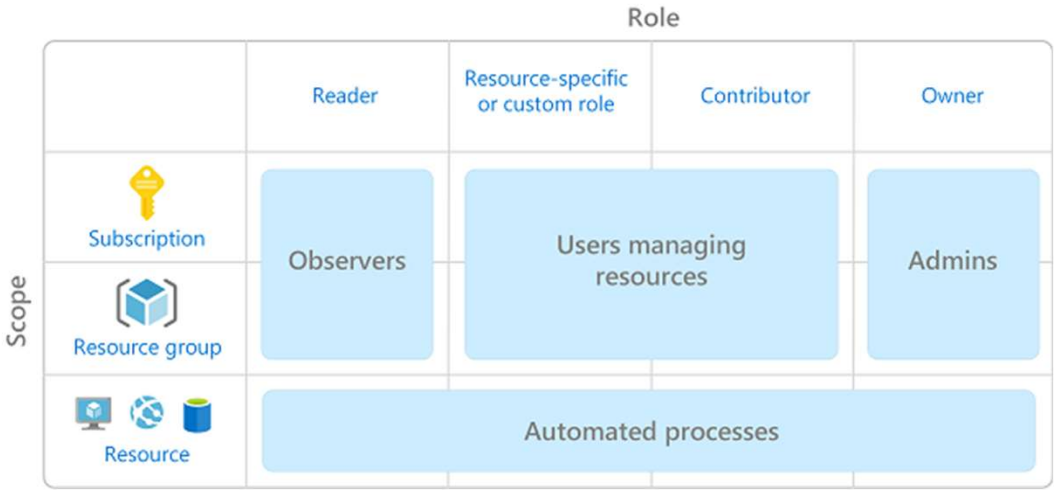
How do Azure offers vary?

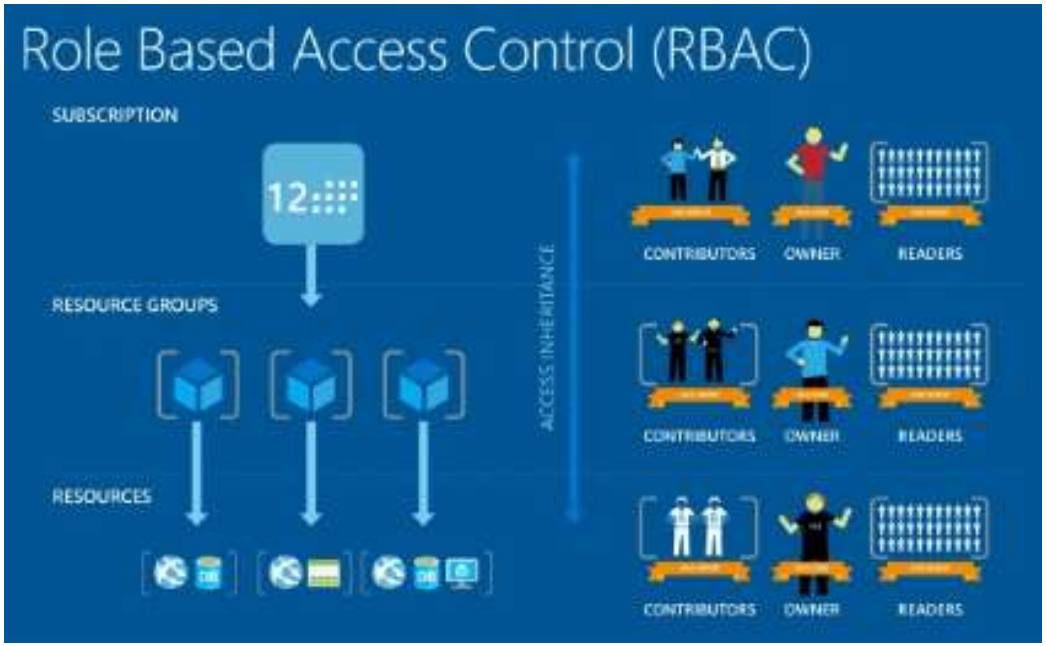
Direct vs. Partner vs. EA
Commitment vs. pay as you go
Credits & included quantities
Discounts – Overall and on specific resources

What offers are popular?

Free trial
Pay as you go
EA
Visual StudioMSDN
Sandbox

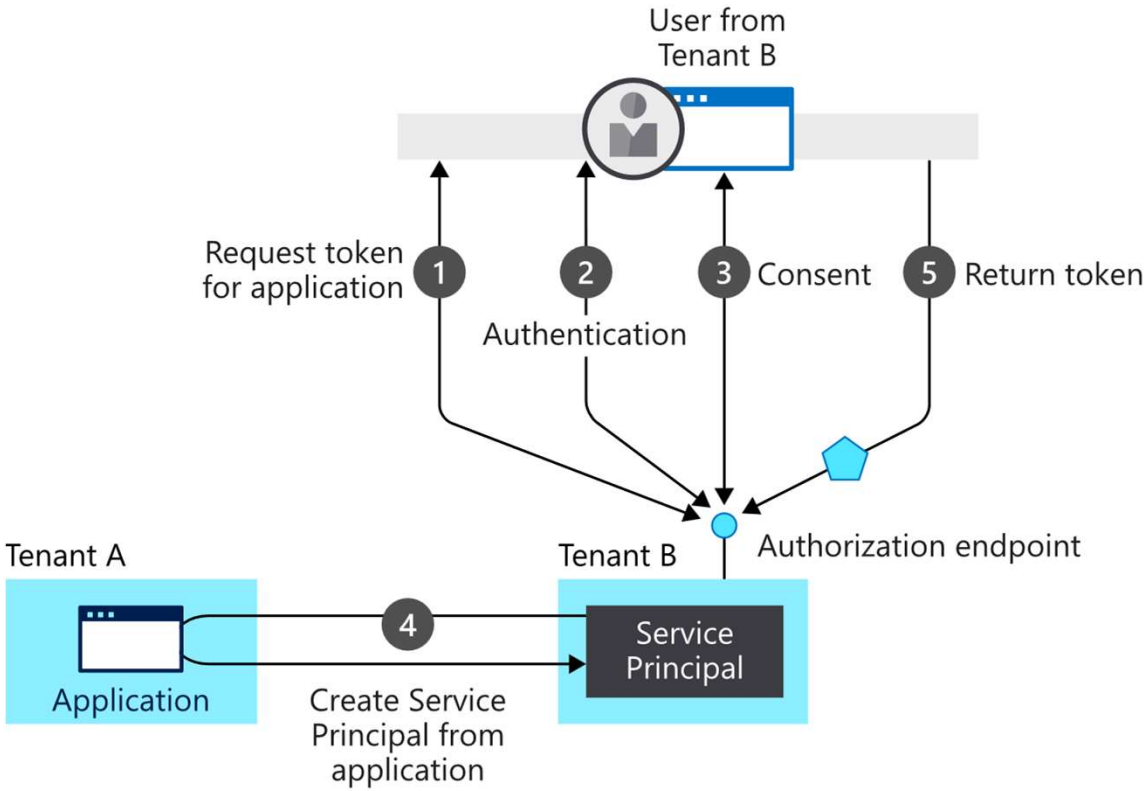
RABC


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

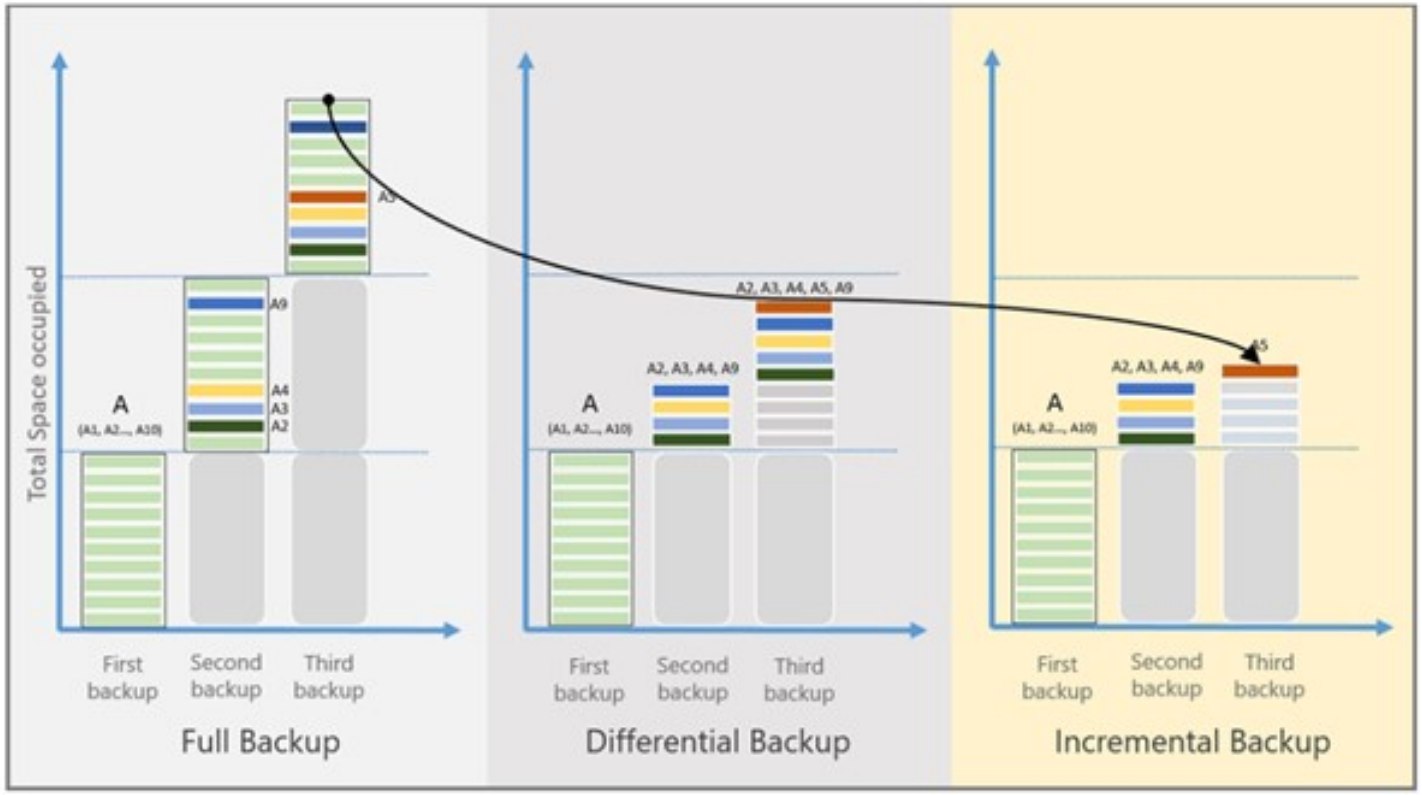

Role Based Access Control (RBAC)
SUBSCRIPTION
RESOURCE GROUPS
RESOURCES
ACCESS INHERITANCE
CONTRIBUTORS
OWNER
READERS
CONTRIBUTORS
OWNER
READERS
CONTRIBUTORS
OWNER
READERS

Register an application with the Microsoft identity platform

The Microsoft identity platform performs identity and access management (IAM) only for registered applications. Whether it's a client application like a web or mobile app, or it's a web API that backs a client app, registering it establishes a trust relationship between your application and the identity provider, the Microsoft identity platform.



Generalizing VM and Captureing VM Images

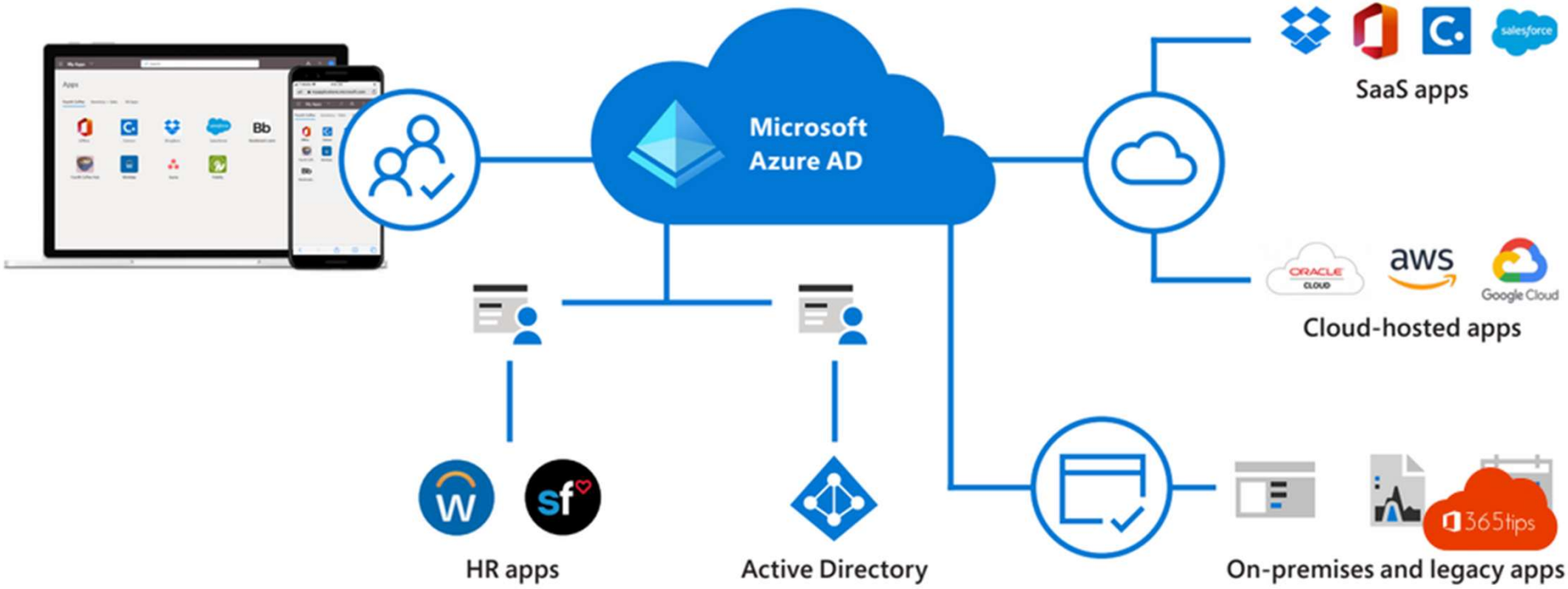


A

B-A
C-A

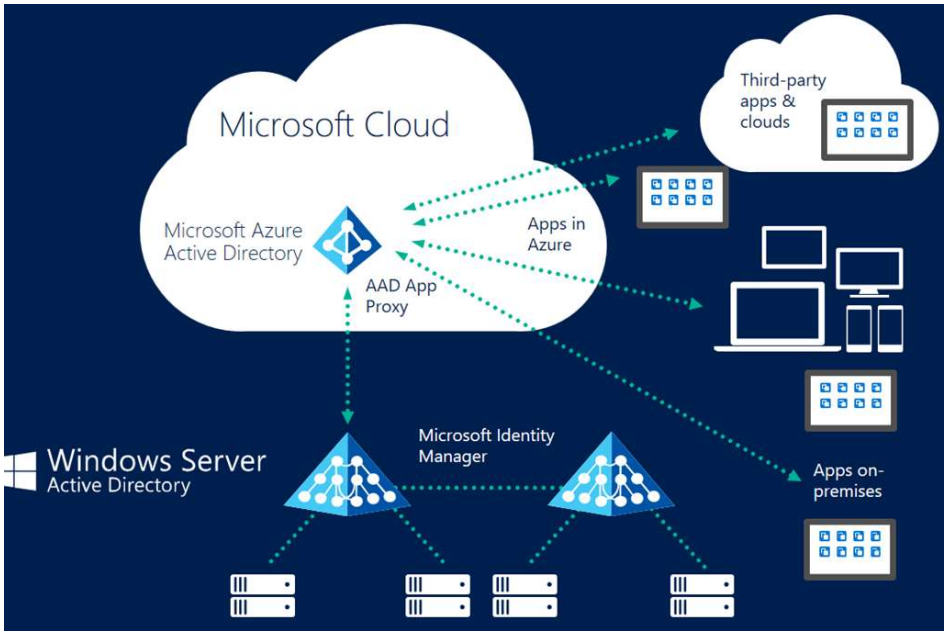
A
B-A
C-A

Azure AD



Azure Active Directory (Azure AD) is Microsoft's cloud-based identity and access management service, which helps your employees sign in and access resources in: ... Internal resources, such as apps on your corporate network and intranet, along with any cloud apps developed by your own organization.

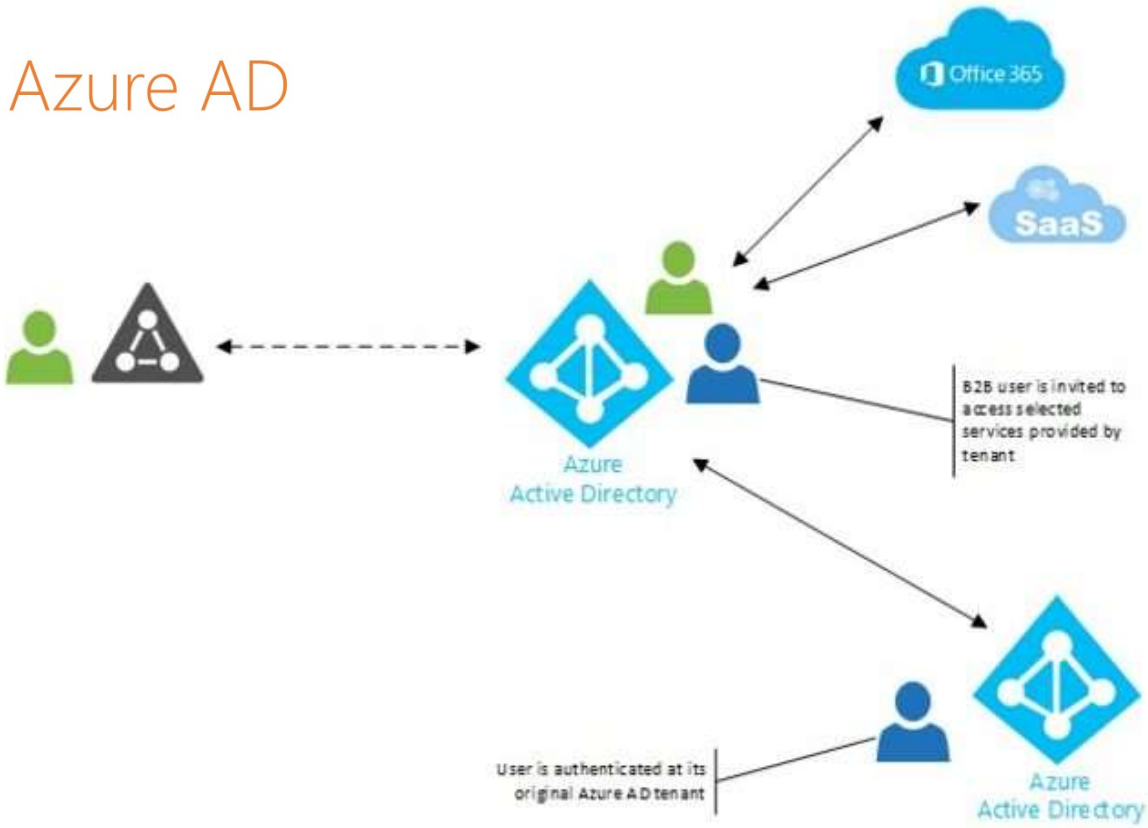
Azure AD



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

1. External resources, such as Microsoft 365, the Azure portal, and thousands of other SaaS applications.
2. Internal resources, such as apps on your corporate network and intranet, along with any cloud apps developed by your own organization. For more information about creating a tenant for your organization, see Quickstart: Create a new tenant in Azure Active Directory

Who Uses Azure AD

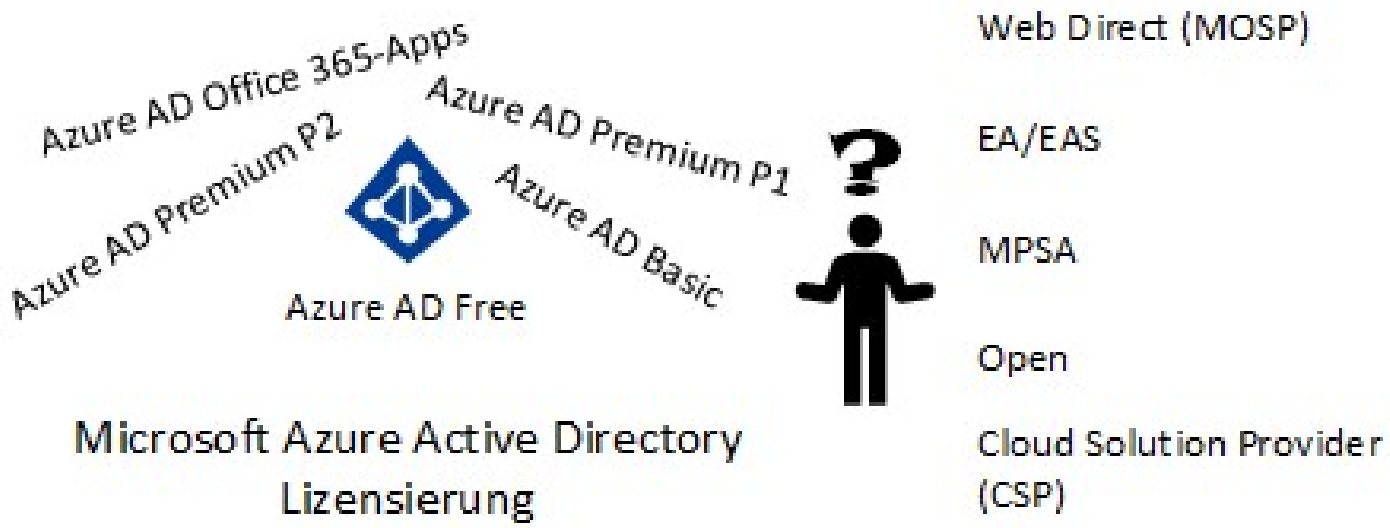


Who uses Azure AD?

Azure AD is intended for:

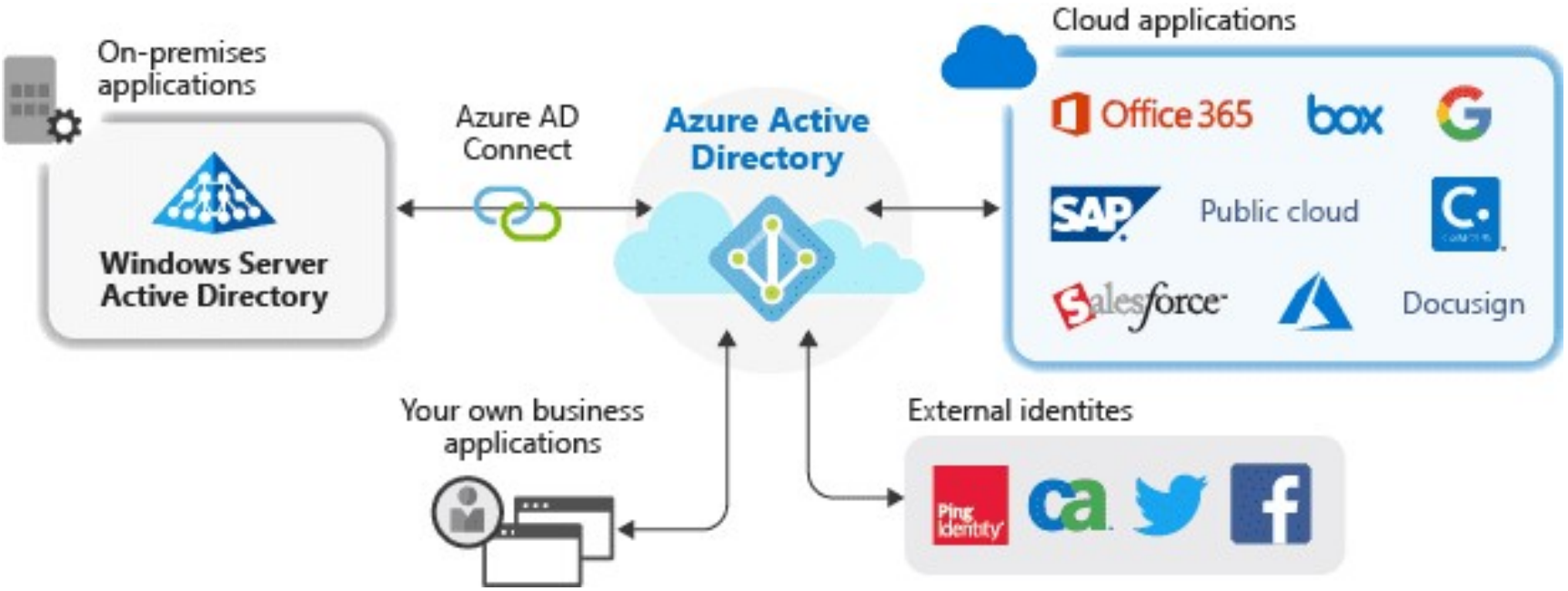
- **IT admins. App developers.**
- **]Microsoft 365, Office 365, Azure, or**
- **Dynamics CRM Online subscribers.**

What are the Azure AD licenses?

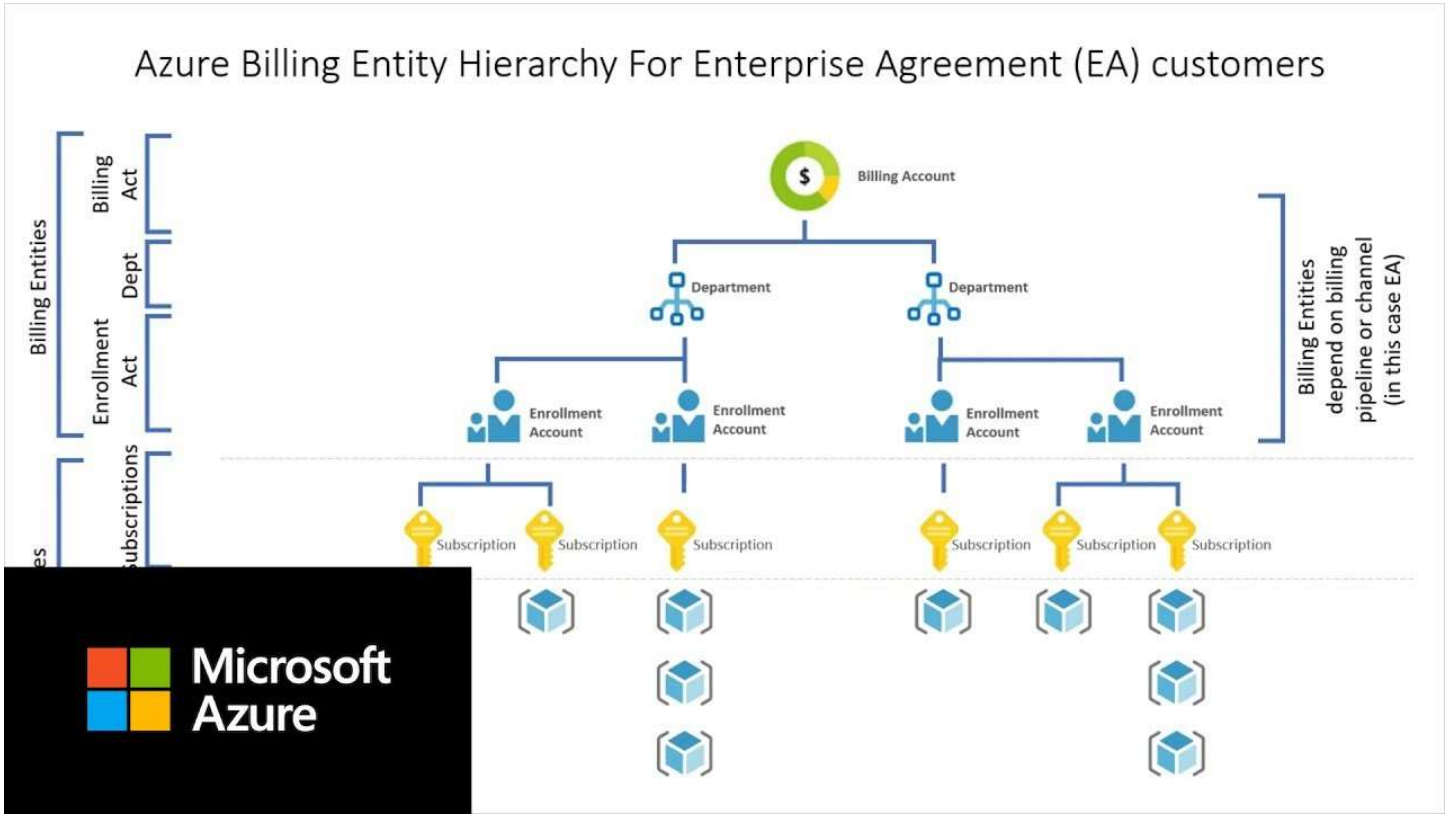


- **Azure Active Directory Free.**
- **Azure Active Directory Premium P1.**
- **Azure Active Directory Premium P2.**
- **"Pay as you go" feature licenses.**

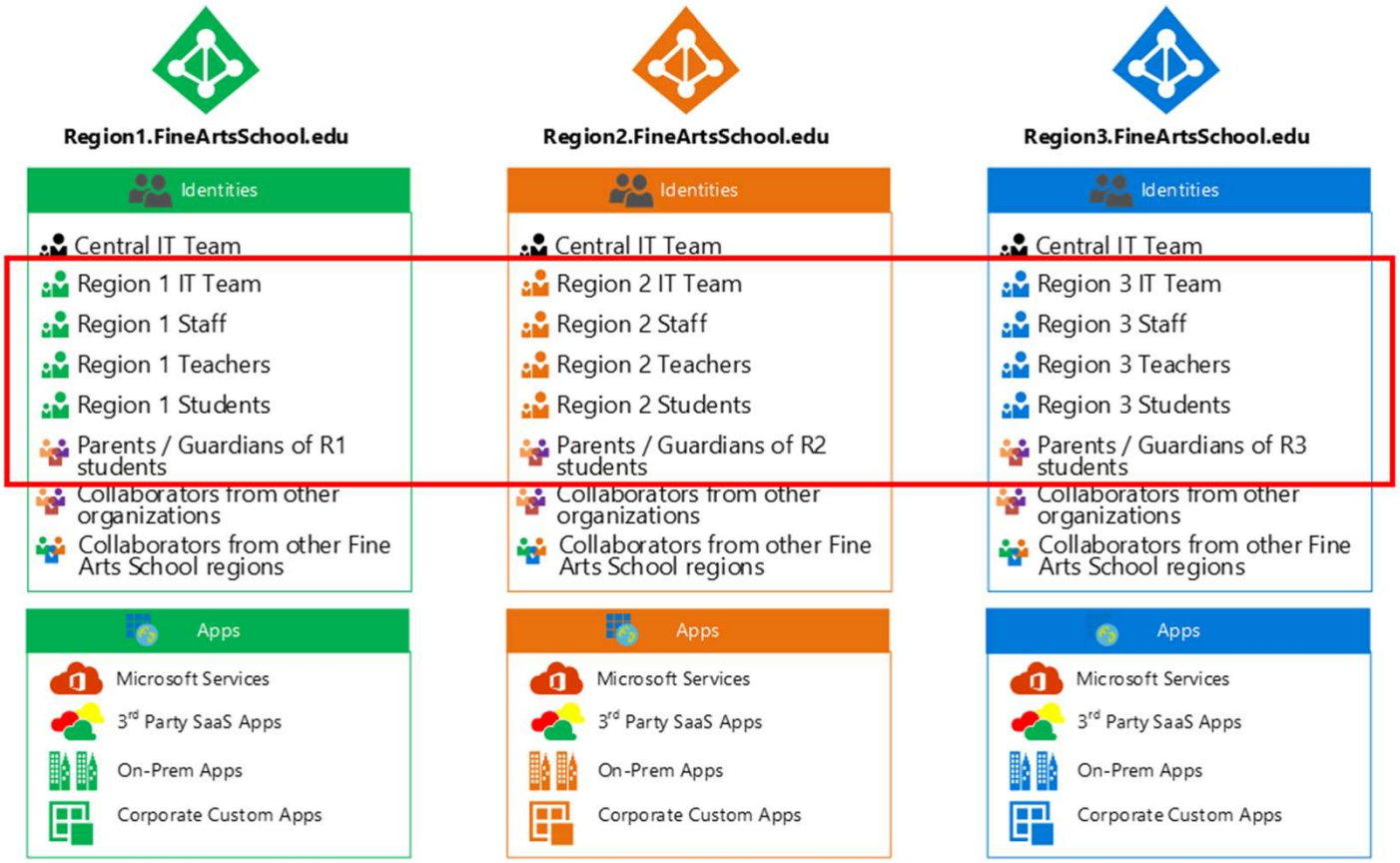
Managing Azure Directories



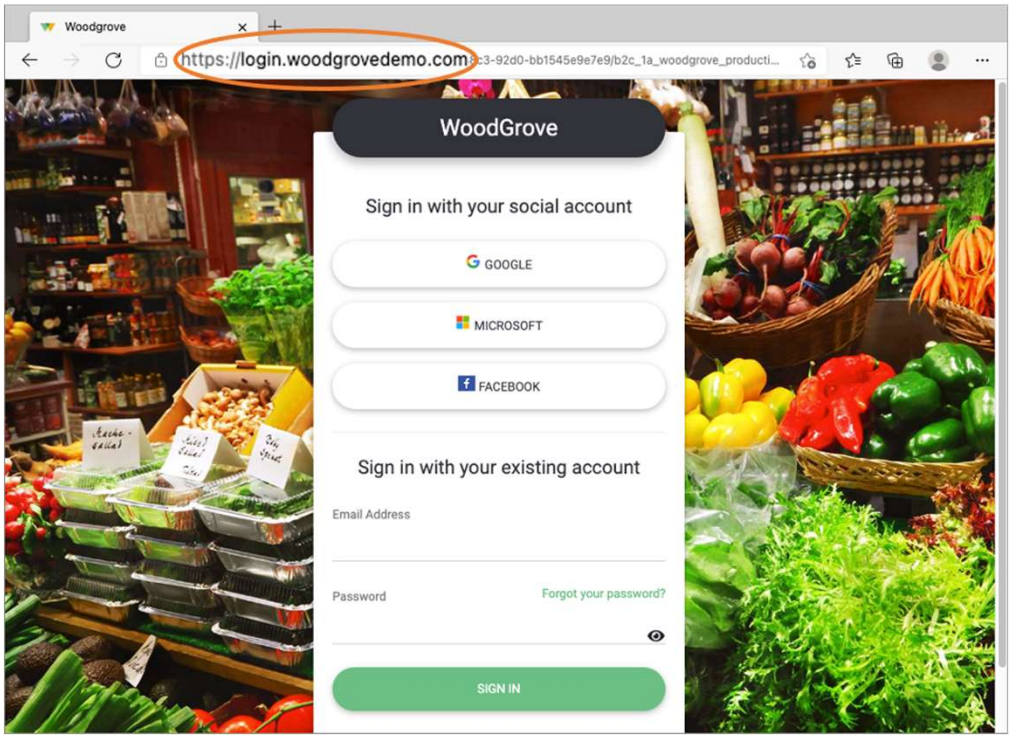
Access control in AD starts from a billing perspective

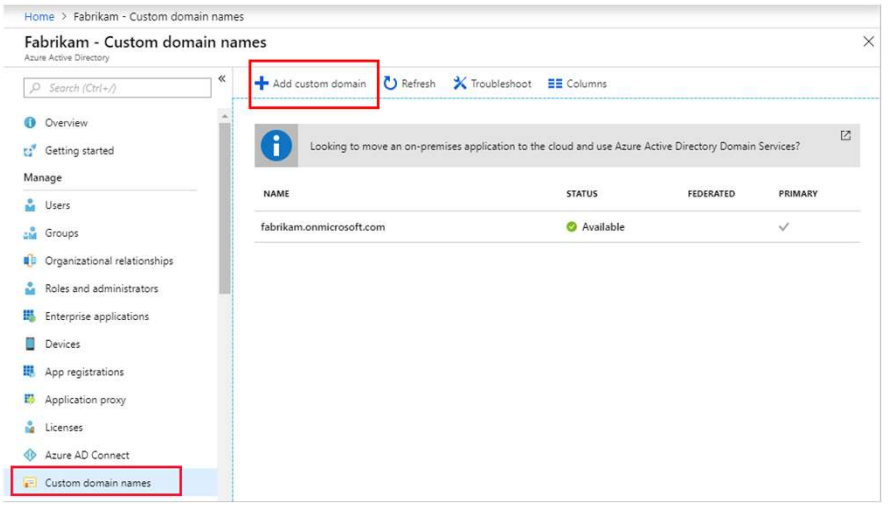


Managing Multiple AD Tenants

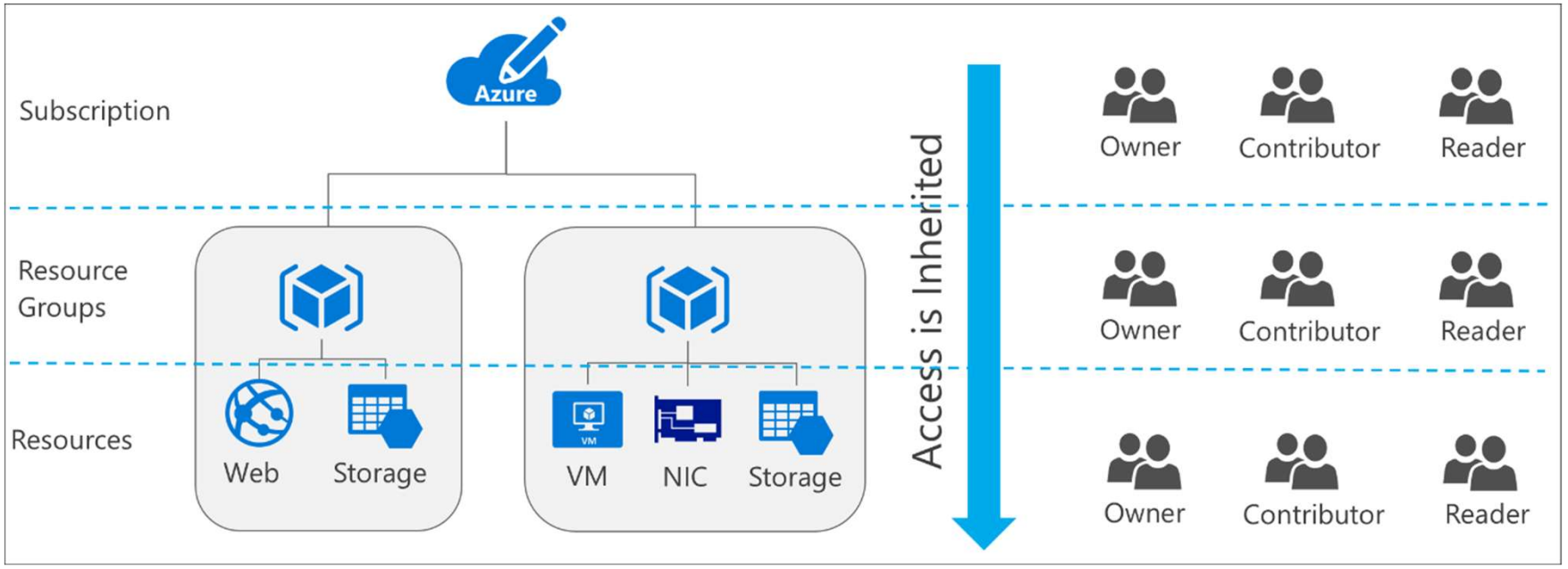


Adding a custom domain to AD

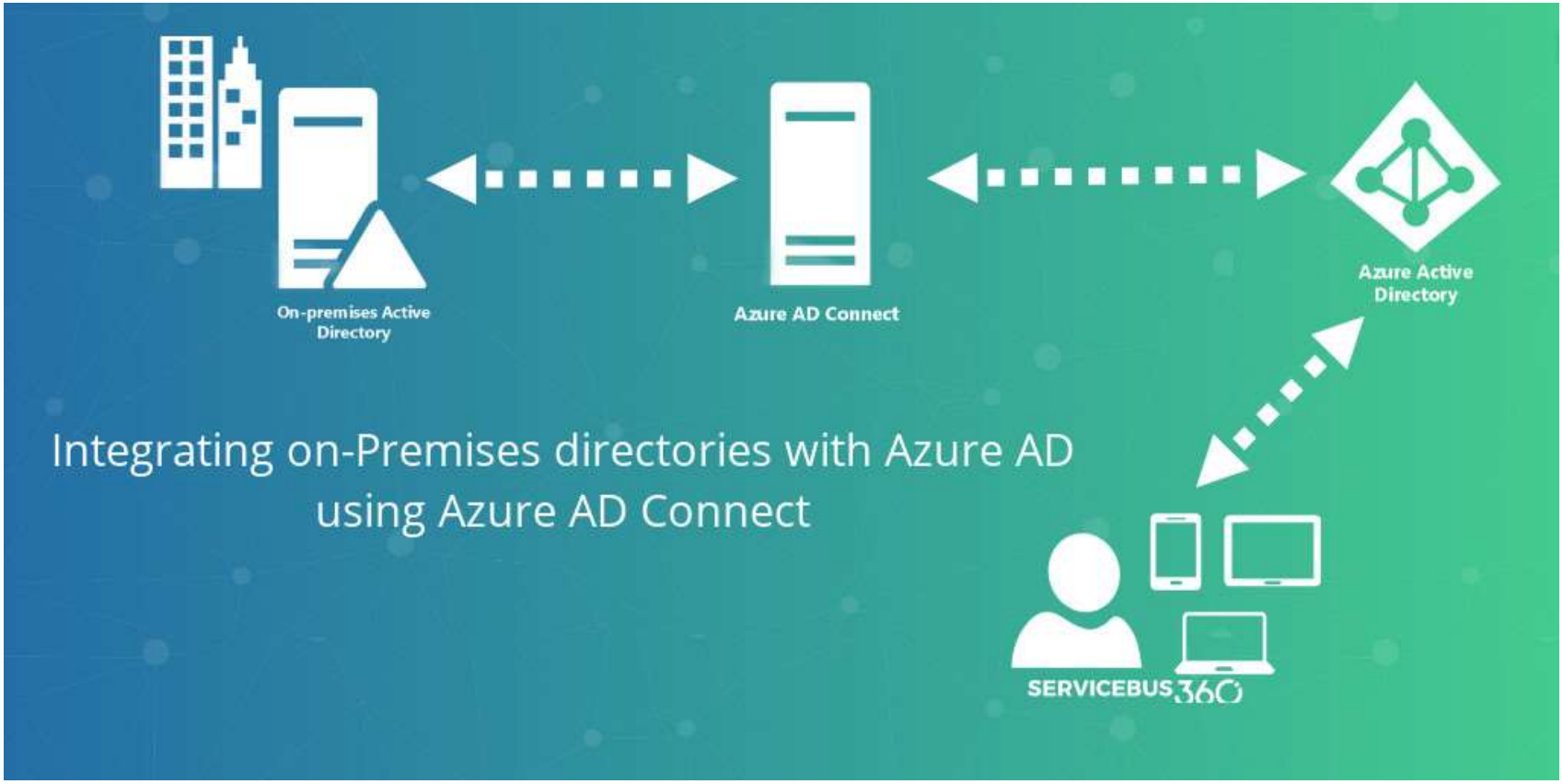




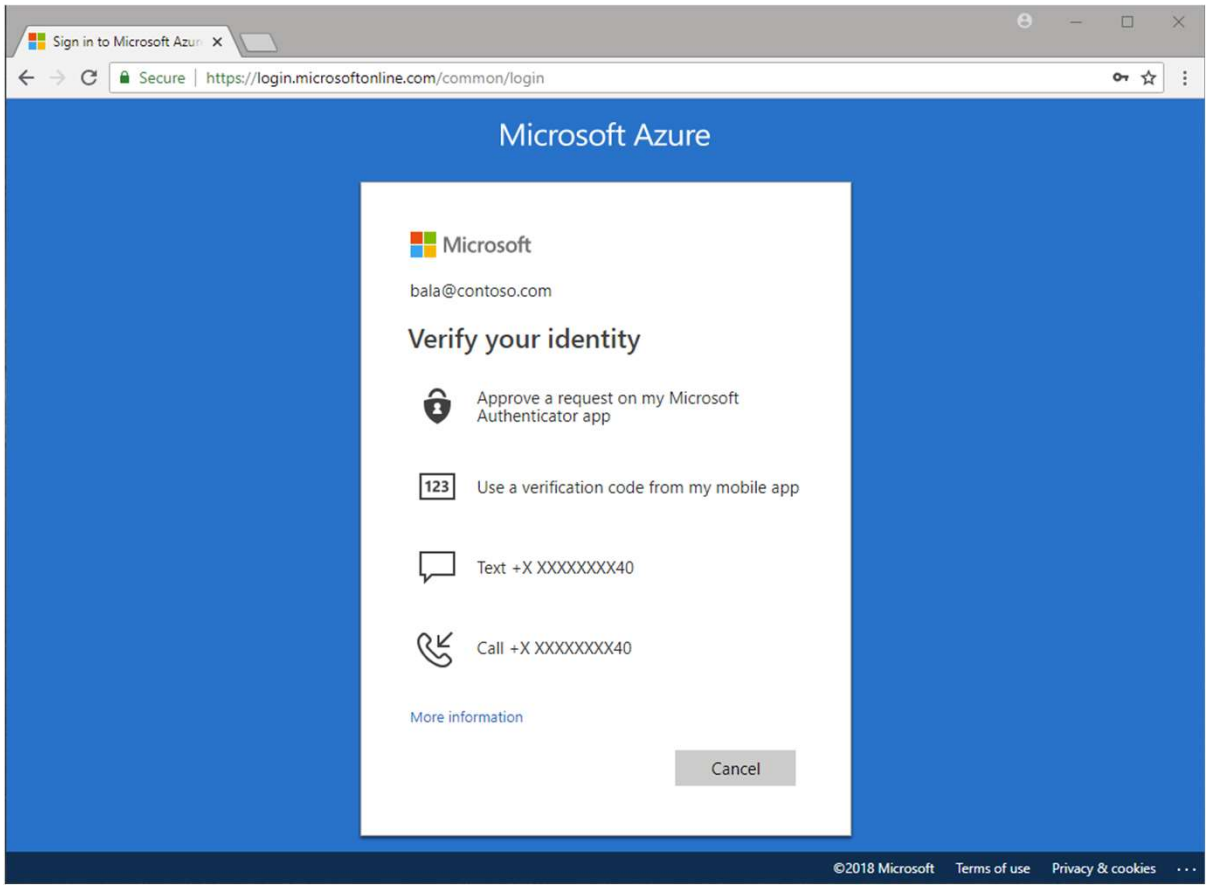
Configuring RABC



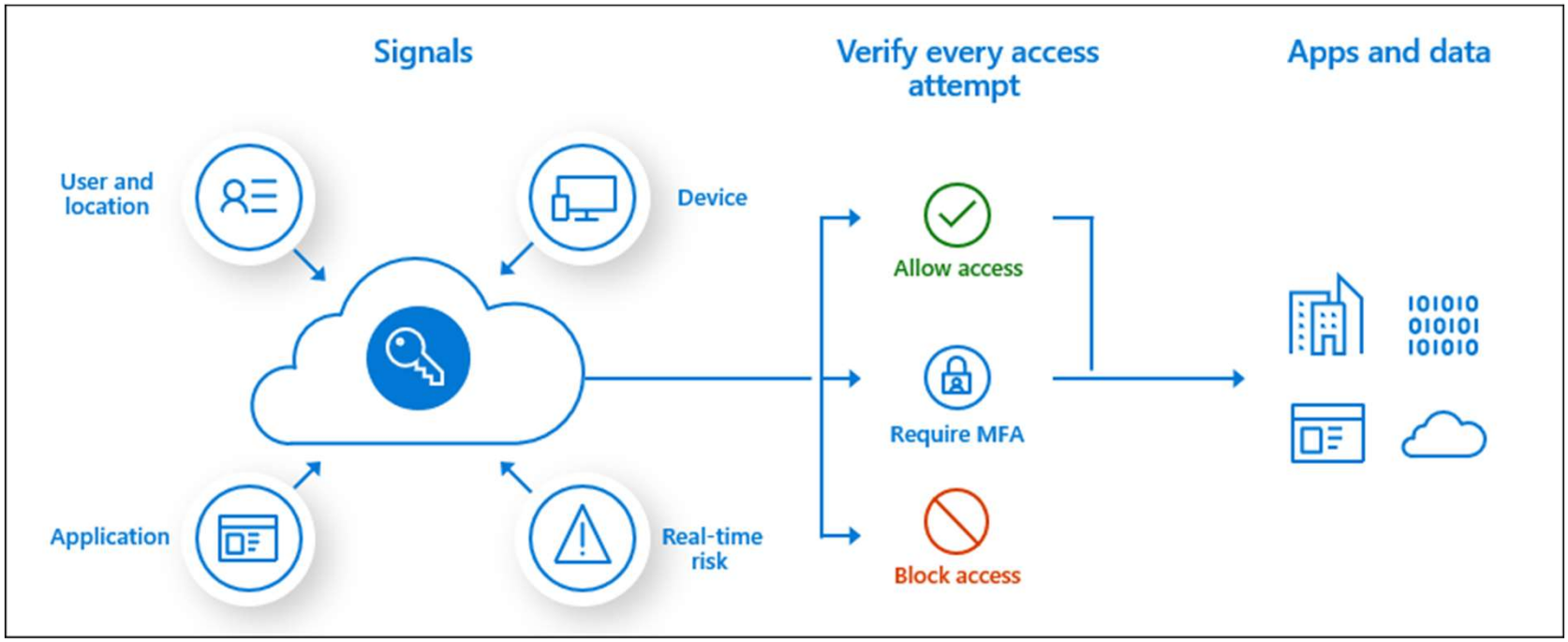
Integrating on premises with azure ad



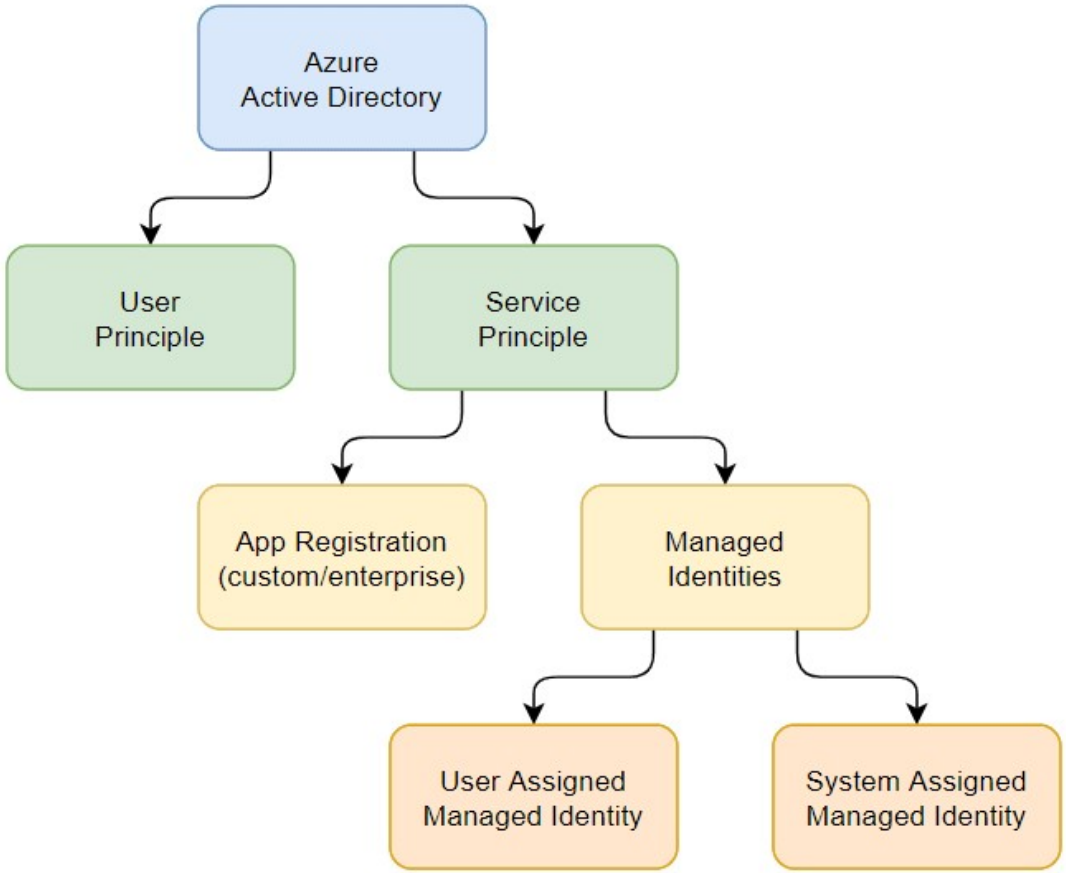
Azure multifactor authentication



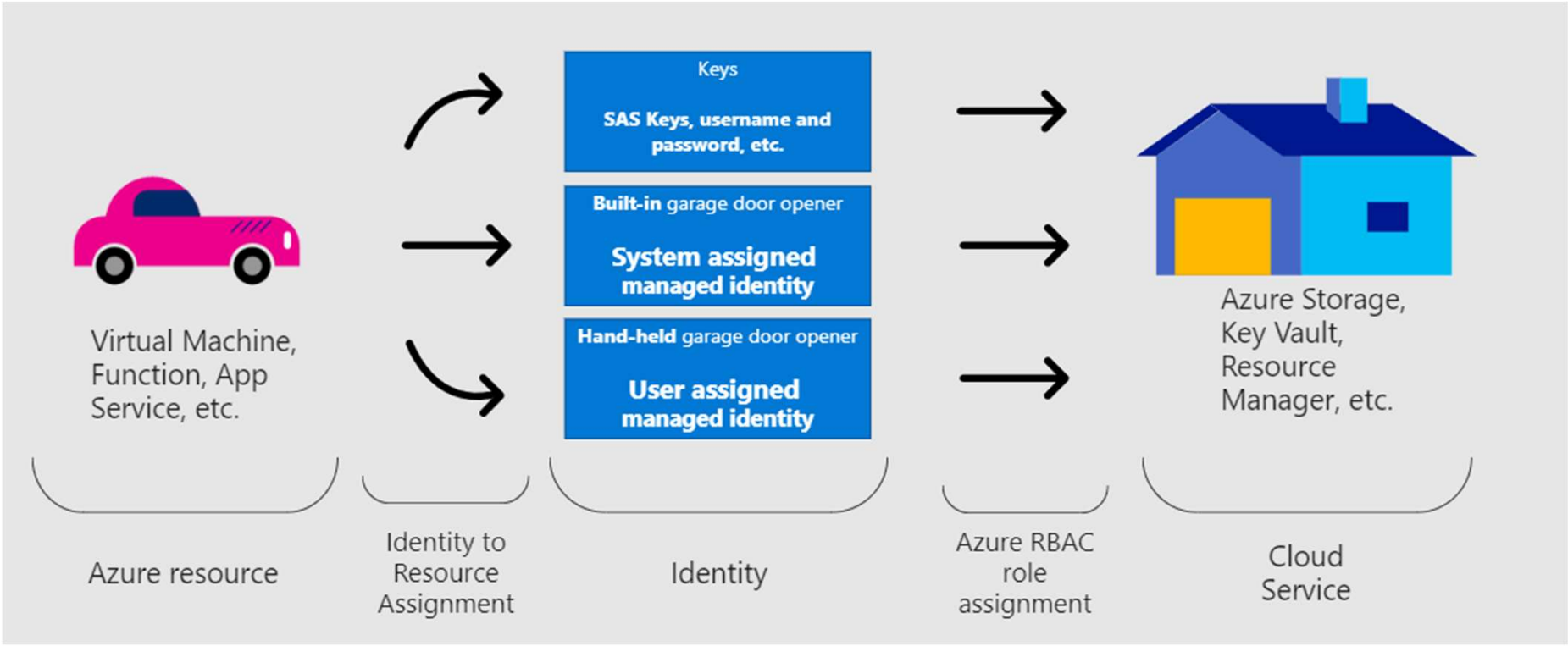
Azure conditional access policy



Azure identities



Azure identities



Azure identities

I can use Managed Identities when...

As a Developer, I want to build an application using

Source:

Azure Resources
Azure VMs
Azure App Services
Azure Functions
Azure Container instances
Azure Kubernetes Service
Azure Logic Apps
Azure
....

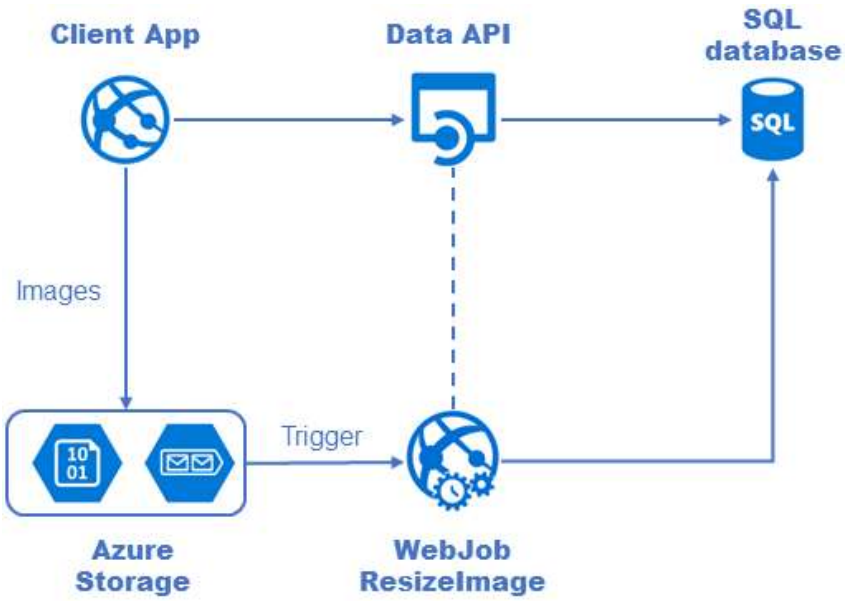
that accesses

Target:

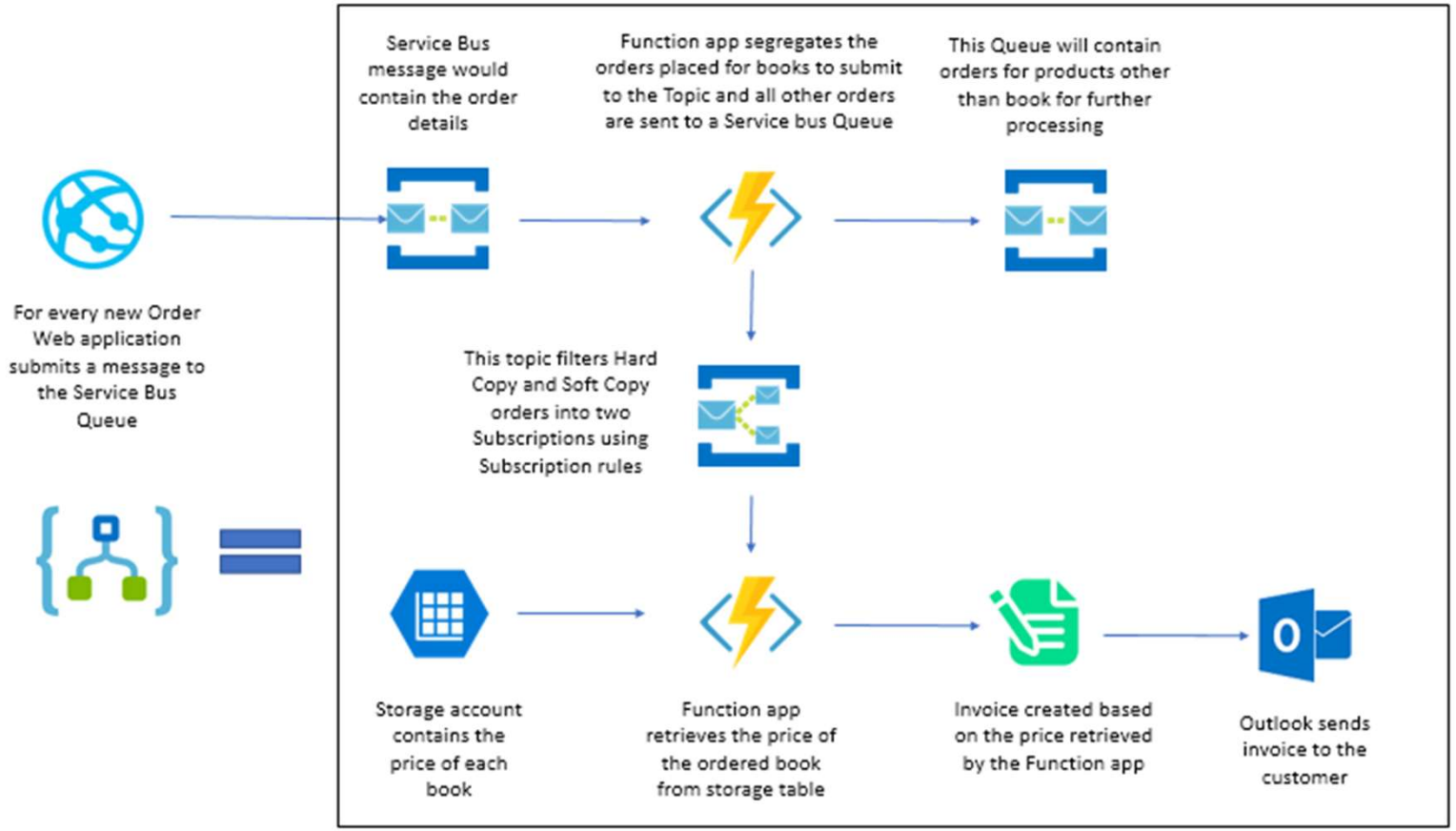
Azure Services that support Azure AD Authentication
Azure Key Vault
Azure Storage
Azure SQL
Azure Cosmos DB
Azure Machine Learning Service
....

without having to manage any credentials!

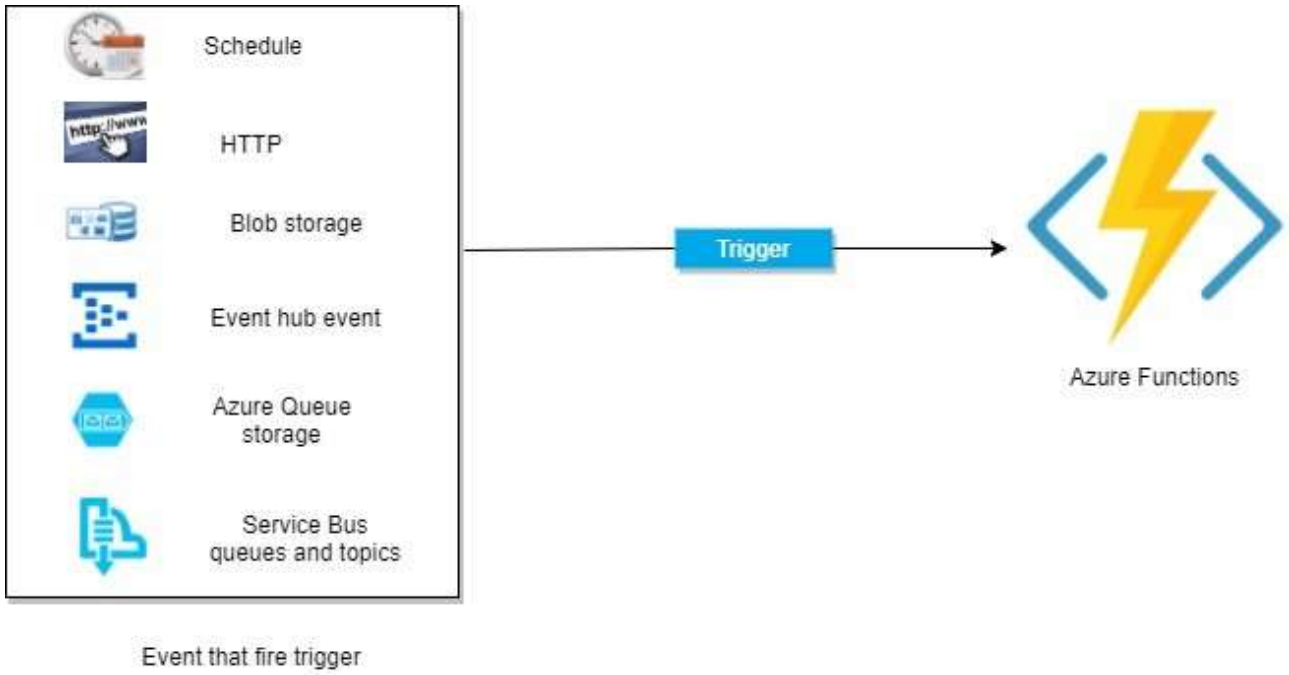
Azure identities



Azure Functions



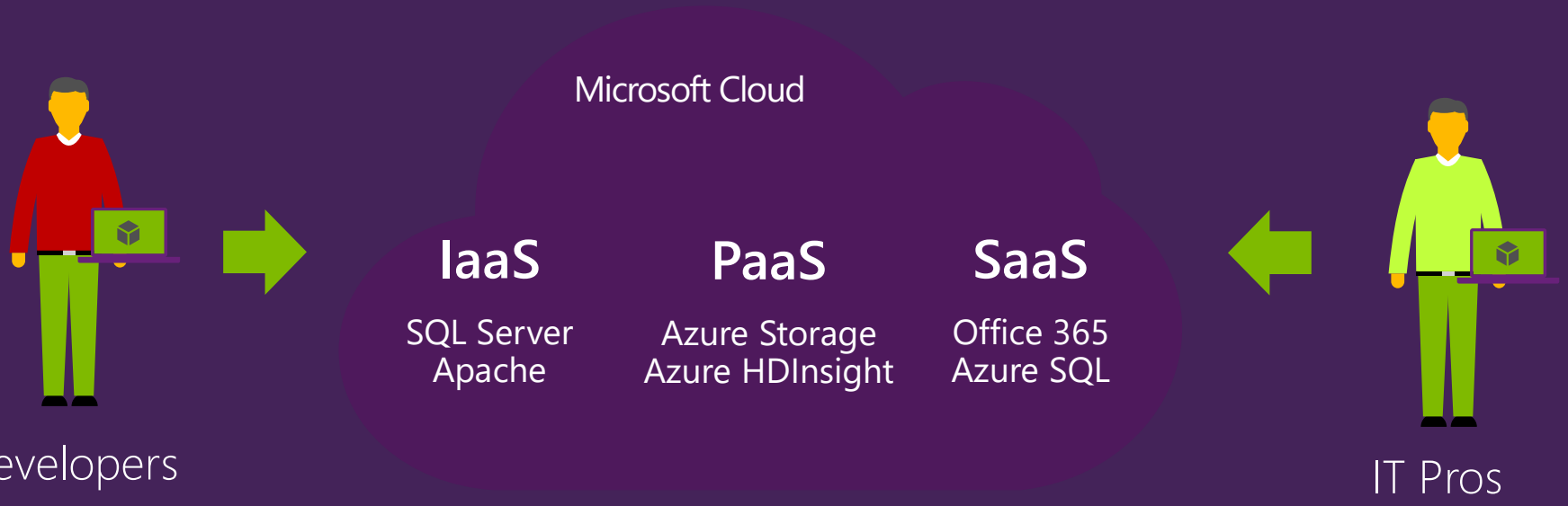
Azure Functions



https://www.serverless360.com/azure-functions

Azure Service Bus

Customers use Microsoft cloud in many ways



One common problem:

"How do I manage my keys and secrets?"

Key Management asks from our customers

"I want my data encrypted at rest, and …"

"I need to keep encryption keys in HSMs (FIPS140-2 Level 2+)."

"I need to control the lifecycle of my encryption keys."

"I want to control keys for my cloud apps from a single place."

"I need to keep encryption keys in country."

"I need to keep encryption keys on-premises."

"I need to keep encryption keys in dedicated HSMs."

Key Management options

Your on-premises HSMs | Per country Azure | Azure Key Vault

"I need to keep encryption keys in HSMs (FIPS140-2 Level 2+)."

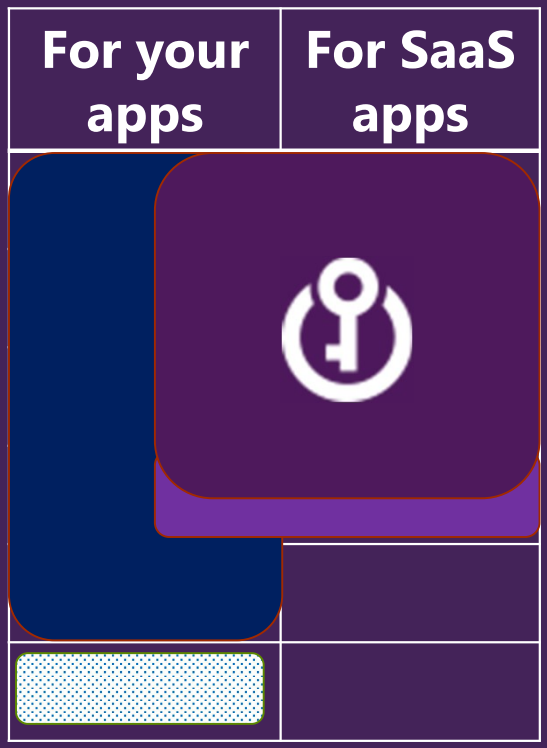
"I need to control the lifecycle of my encryption keys."

"I want to control keys for my cloud apps from a single place."

"I need to keep encryption keys in country."

"I need to keep encryption keys on-premises."

"I need to keep encryption keys in dedicated HSMs."



Secret management asks from our customers

"My app on Azure has passwords and cryptographic keys…"

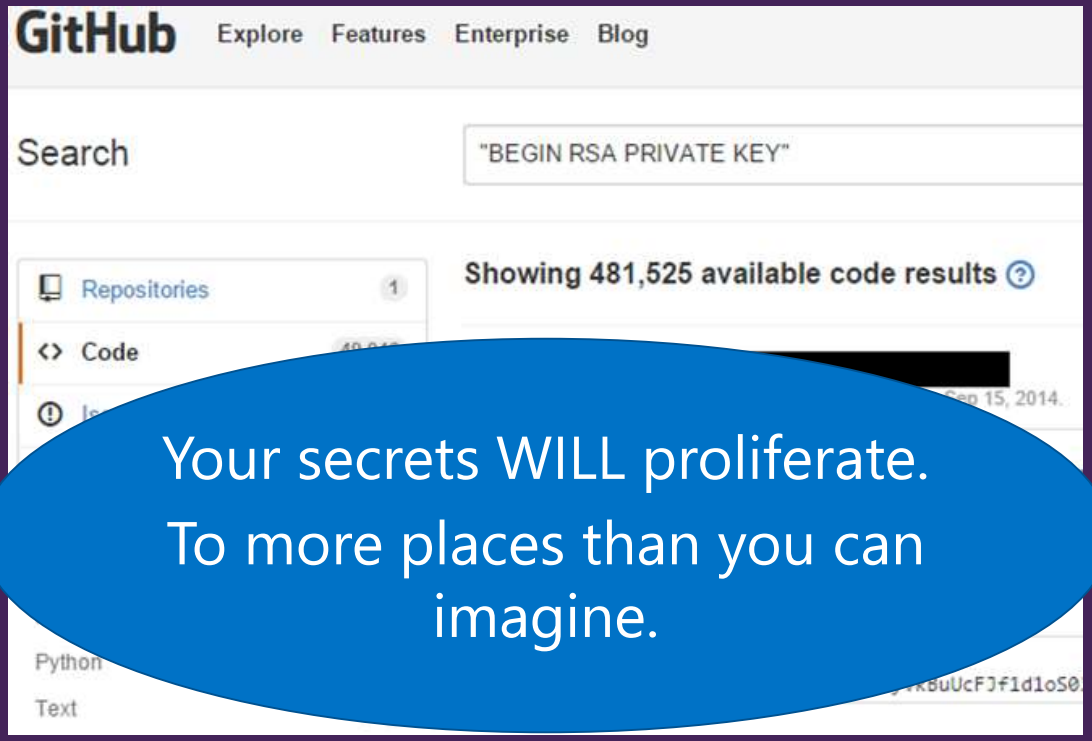
"I need a safe place to save these in Azure."

"I need to (re)use AD users and groups to manage access to secrets."

"I do NOT want to be in the news for a silly mistake"

Solution: Azure Key Vault

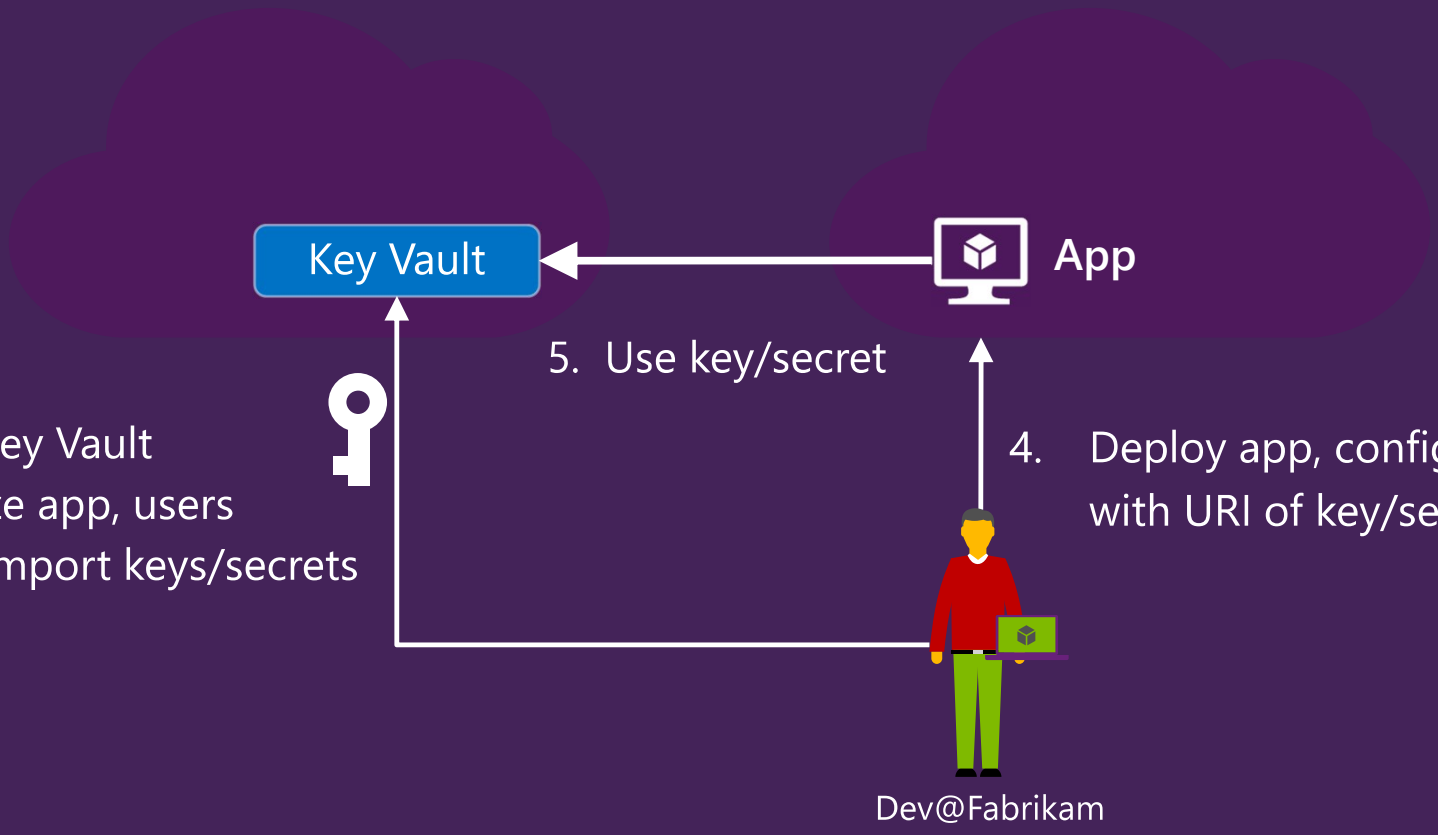
Today: Developer builds LOB application



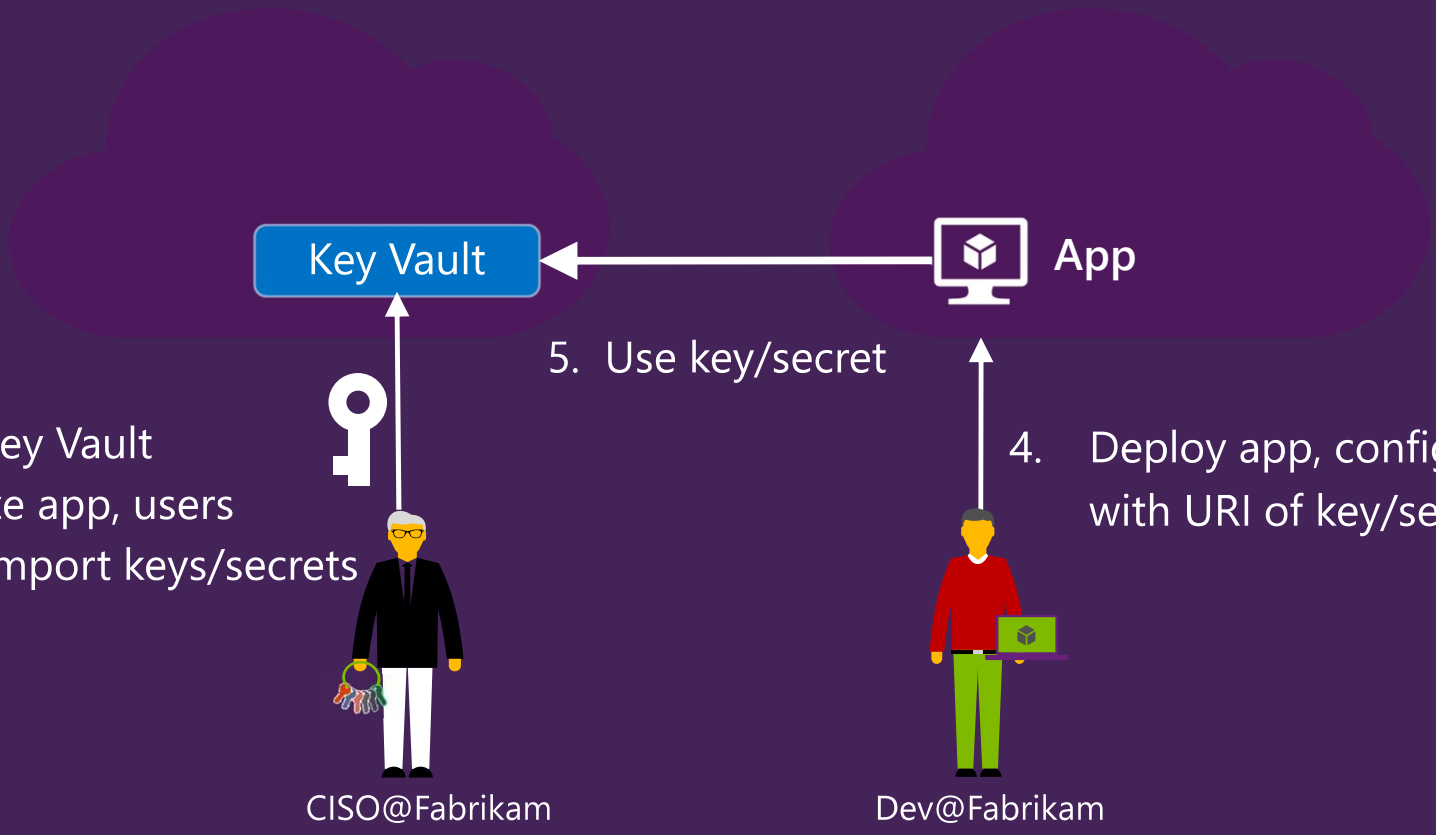
Your secrets WILL proliferate.

To more places than you can imagine.

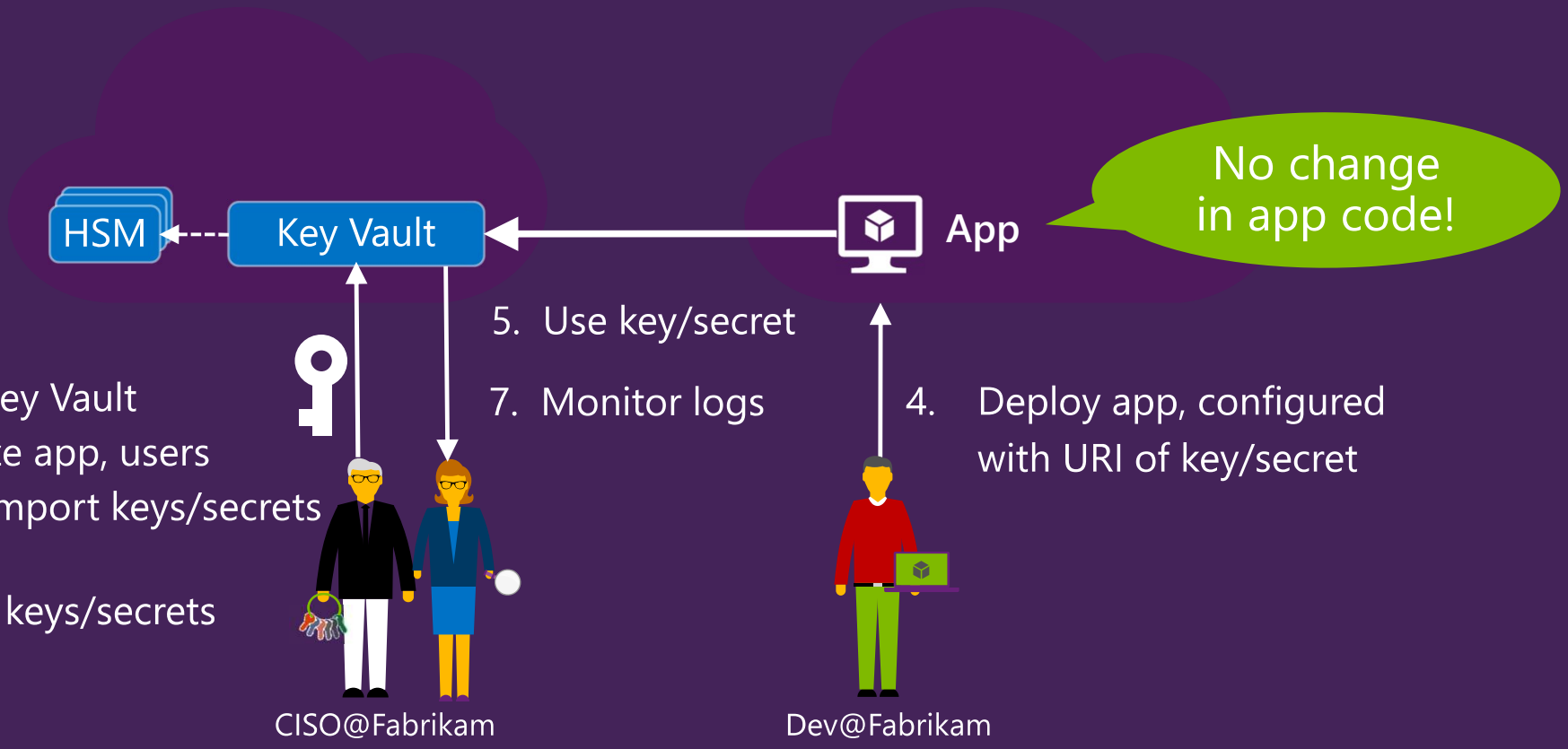
Phase 1: Developer builds LOB application



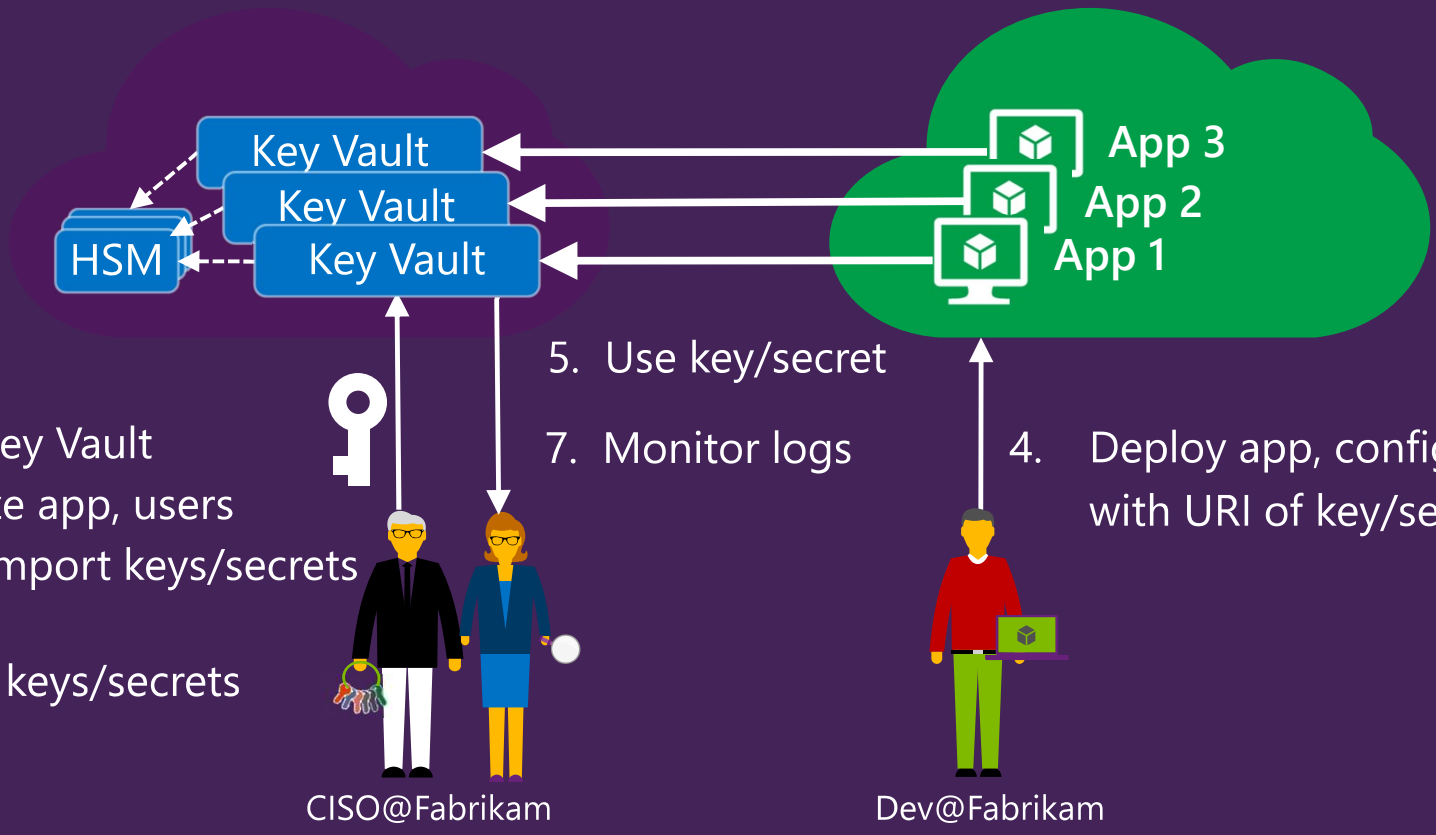
Phase 2: App moves into pilot



Phase 3: App moves into production



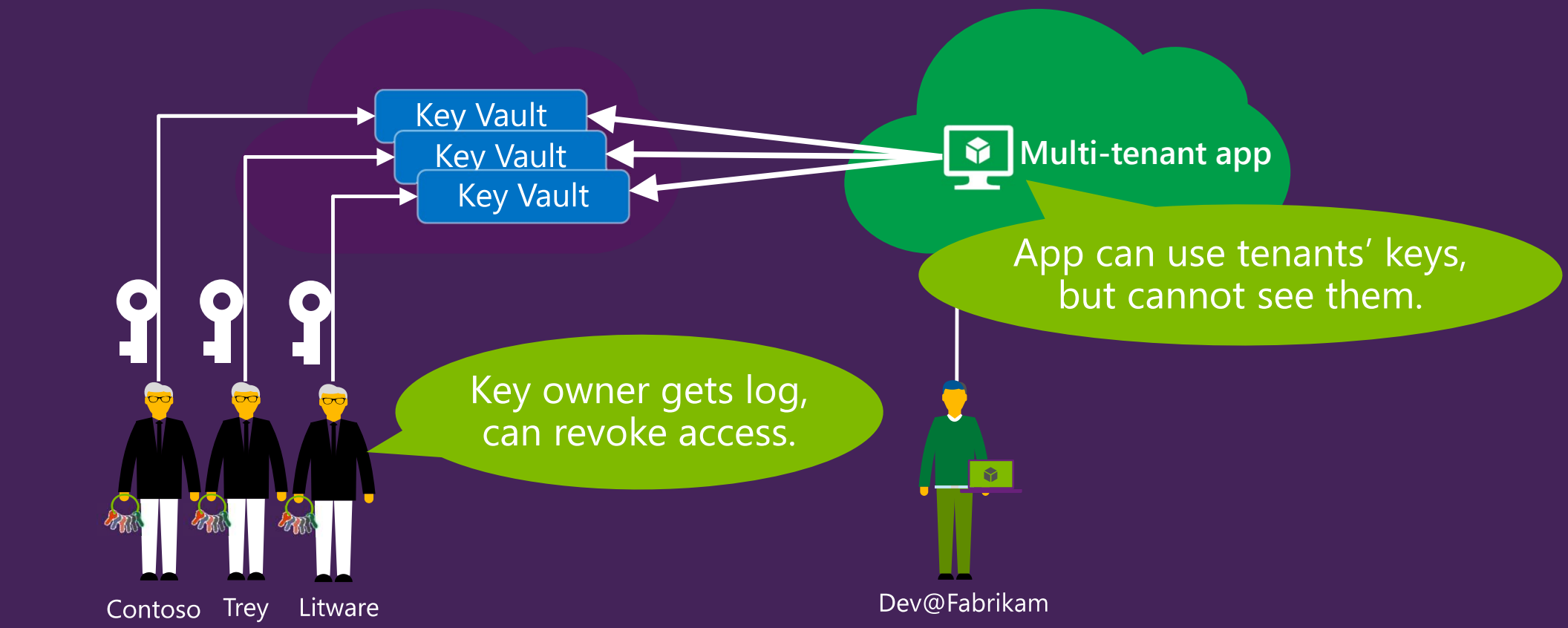
Phase 4: Scale, deploy more apps in minutes



1. Create Key Vault
2. Authorize app, users
3. Create/import keys/secrets

6. Manage keys/secrets

Multi-tenant app offers customer-managed keys



Your ORG is in control via Active Directory

- Users and apps authenticate to your key vaults using your organization's Azure AD
- Benefits for organizations:
  - Organizations can centrally revoke access to ALL key vaults in their organization.
  - If a user leaves, they instantly lose access to ALL key vaults in the organization.
  - Organizations can customize authentication via the options in Azure AD.

Objects in play

Secret

- **What:** Any sequence of bytes under 25KB. E.g. SQL connection string, PFX file, AES encryption key.
- **How used:** Authorized users/apps write and *read back* the secret value.

Key

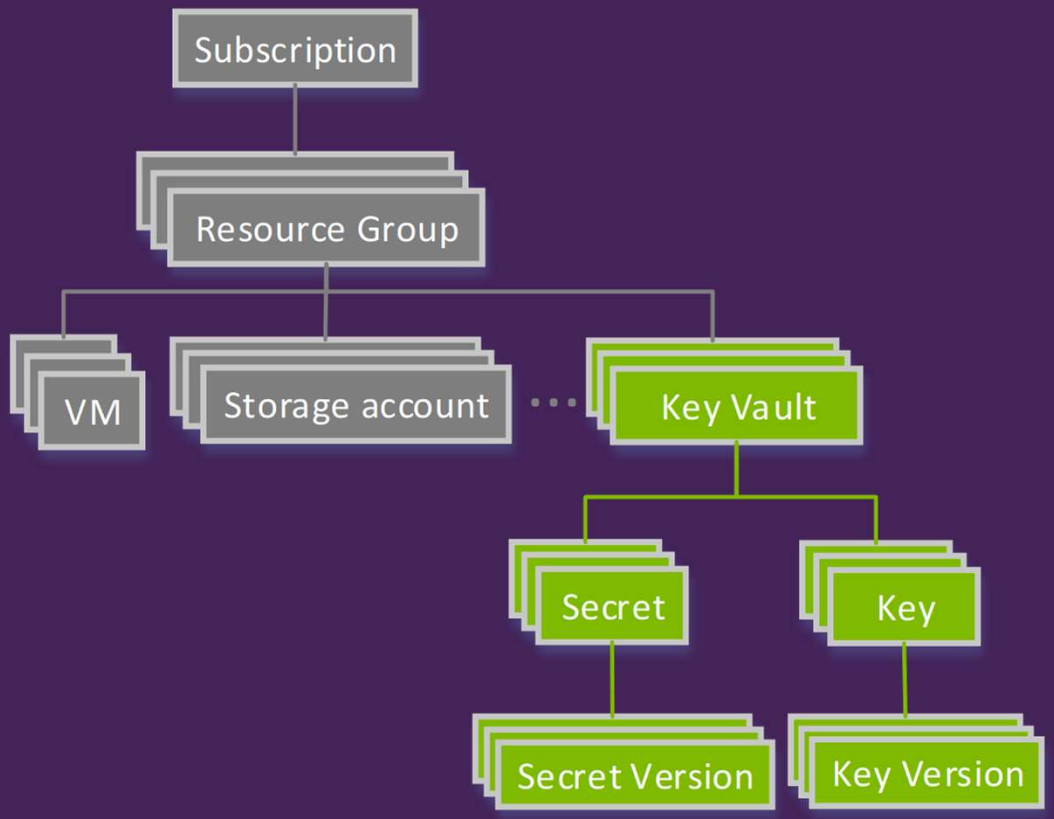
- **What:** A cryptographic key. RSA 2048.
- **How used:** *A key cannot be read back.* Caller must ask the service to decrypt / sign with the key.

Key Vault

- Container for related keys and secrets that are managed together.
- Unit of access control, unit of billing.
- An Azure resource, like a storage account.

Azure subscription, Resource groups, Azure AD Identities

Key Vault object model



Types of keys

HSM-protected key

- Operations on this key are performed inside HSMs (Thales nShield, FIPS 140-2 Level 2).

Software-protected key

- Operations on this key are performed in VMs on Azure (FIPS 140-2 Level 1 pending).
- When stored, they are encrypted with a key chain that terminates in HSMs.

Ways to use the Key Vault service

To create and manage a key vault

- Azure PowerShell
- Azure Resource Manager and Key Vault REST API + client SDK

To use a key vault

- Multiple applications pre-integrated with Key Vault
- If you are writing your own application, use Azure Key Vault REST API + client SDK

Authorization

Offline

- Key Vault owner sets ACL on key vault that specifies WHO can do WHICH operations.
- Each entry is the pair : {Azure AD identity, operations}.
- Key Operations: Create Key, Import Key, Delete Key, Encrypt, Decrypt, Wrap, Unwrap, Backup, Restore.
- Secret Operations: Get, Set, Delete, List.

At runtime

- Key Vault service checks caller's Azure AD token against permissions on the key vault, before performing operation.

Demo

TechEd
Europe 2014

Create a key vault
Create an Azure AD identity to access the key vault

Demo

TechEd
Europe 2014

Disk encryption in Azure VM
SQL Server Transparent Data Encryption

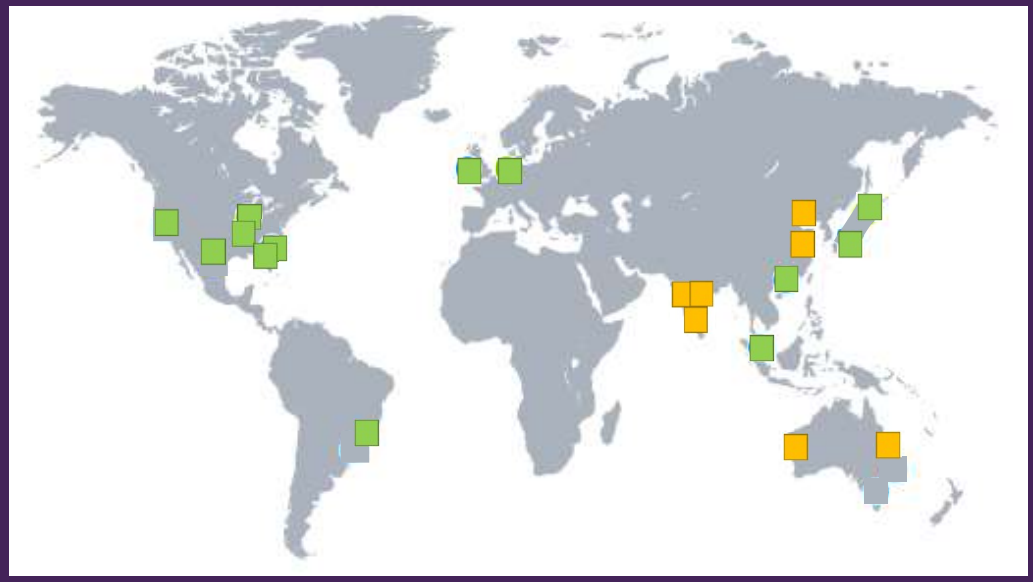
Current status

- Service was released in Public Preview in Jan 2015.
- Services leveraging Key Vault:
  - Azure RMS as BYOK
  - SQL Server Transparent Data Encryption
  - CloudLink SecureVM
  - Azure Storage client SDK
  - Azure VM certificate management
  - Azure VM volume encryption – announced
  - Office 365 Advanced Encryption – announced
- General Availability 'real soon now'
  - Until then, no SLA but team is operating as though we have one (service is operating at 99.9+)
  - Usage Logs coming in a future release.

Geo-availability and isolation

Available in

- 6 regions in US
- 2 regions in Europe
- 4 regions in Asia
- 1 region in South America
- All Azure regions over time.



Isolation

- Key Vaults, Keys, Secrets stay within region.
- Hardware ensures that cryptographic keys for a GEO cannot be used in data centers in other geos.

Preview Pricing

Pricing for Key Vault owners

Secrets and Software-protected keys	$0.015 / 10,000 operations
HSM Protected keys	$0.015 / 10,000 operations + $0.50 per key per month (every version counted separately)

Details: http://azure.microsoft.com/en-us/pricing/details/key-vault/

Pricing for Application owners

When an application uses a key vault, the owner of that key vault pays.

e.g. if a multi-tenant SaaS application uses key vaults supplied by their customers, the latter pay for usage of the key vault. The SaaS vendor pays zero.