Microsoft

Microsoft Academyadi

la partecipazione che ti premia

Azure Academy - Day 1

Extend Active Directory infrastructure in Microsoft Azure

Michele Sensalari
michele@sensalari.com

Michele

- Senior Consultant – Speaker – Trainer (22 anni)
- Dipendente 50% su tecnologie Microsoft Dipartimento di Informatica – Università degli Studi di Milano
- Freelance 50/70%
- Mi occupo di: AD, SCCM, W10, Win Server, AzureAD, O365, M365, Azure, Enterprise Mobility & Security
- Speaker da 12 anni di WPC e da 5 responsabile agenda ITPRO e Security
- Certificato MCT, MCSE, MCSA, MCITP
- Contatti:
  - michele@sensalari.com
  - michele.sensalari@overneteducation.it
  - Twitter: @ilsensa7
  - Linkedin: https://www.linkedin.com/in/michele-sensalari-4988b7/

Agenda – Day 1

- Introduzione alla Azure Academy
- Introduzione al cloud
- Active Directory -> Azure Active Directory
- Active Directory -> IAAS Virtual Machine AD
- Active Directory - > PAAS Azure AD Domain Services
- Azure Migrate (intro)

Introduzione alla Azure Academy

Programma e contenuti

- **21 Gennaio**: Extend Active Directory infrastructure in Azure – Michele Sensalari
- **18 Febbraio:** Disaster Recovery, Monitoring and Security – Michele Sensalari
- **17 Marzo:** Migrate your On-Premise App on Cloud – Michele Aponte
- **21 Aprile**: Manage Cognitive Services - Michele Aponte
- **19 Maggio**: Loading and Storing data in Azure – Ruggiero Lauria
- **16 Giugno**: Processing and Analysing Data in Azure – Ruggiero Lauria

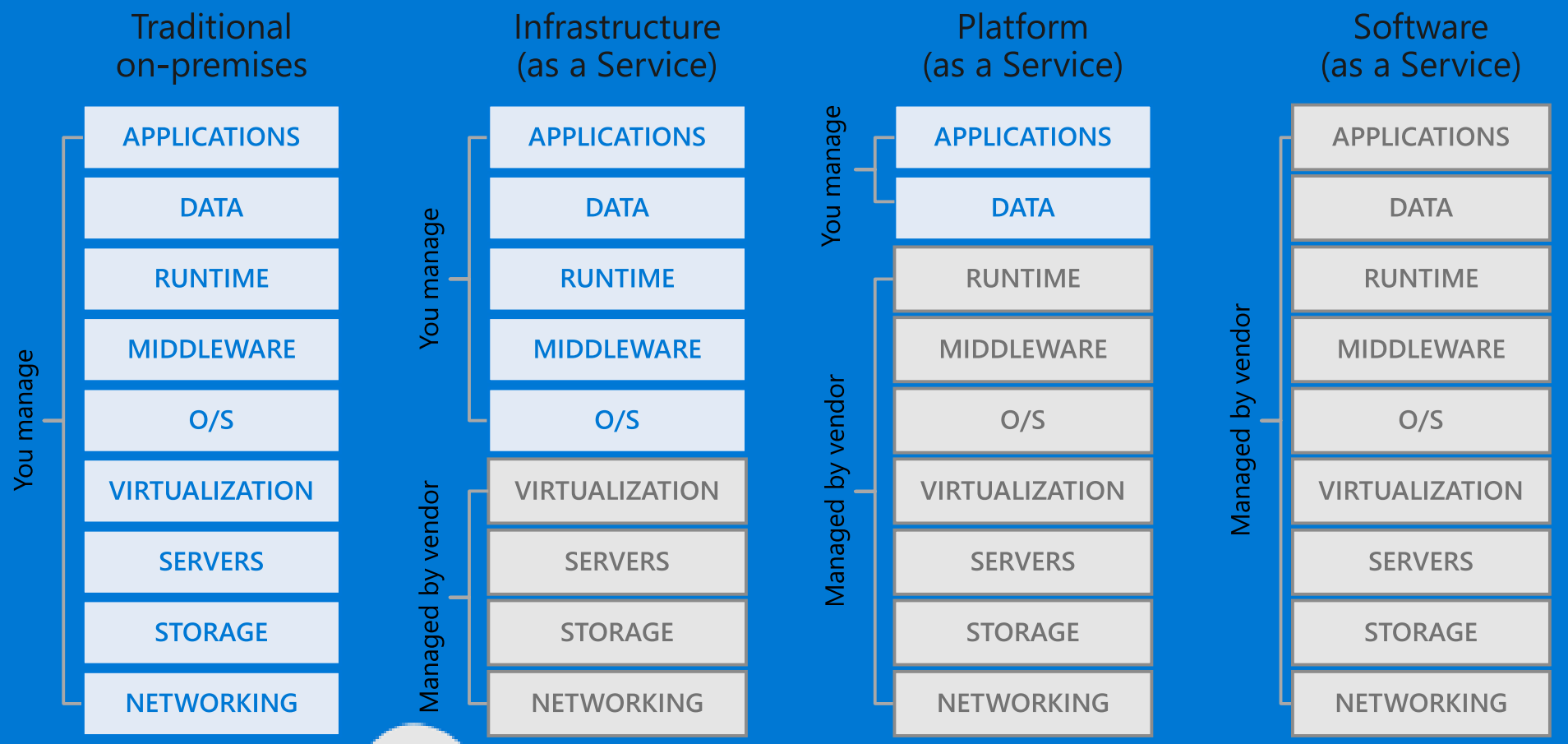
Introduzione al Cloud

Infrastructure as a Service (IaaS)

Platform as a Service (PaaS)

Software as a Service (SaaS)

Cloud Service Models



Why move to the cloud?

Cost effective

Pay-as-you-go pricing

Pay only for the resources you use

Scalable

Vertically scale resources

- Adding a faster CPU
- Adding memory

Horizontally scale

- Add more servers

Elastic

Automatically add or remove resources

Add resources when your application is most-heavily used

Remove resources when unnecessary

Current

Focus on building and deploying applications

Maintenance is done for you

- No more software patching, hardware setup, upgrades and IT management

Reliable

Your data is safe

Azure provides:

- Data backups
- Disaster recovery
- Data replication

Secure

Physical security

Digital security

Microsoft Azure

What is Azure?

Management

- Azure Monitor
- Log Analytics
- Azure Policy
- Azure Bluepirnts
- Azure Backup
- Site Recovery
- Azure Migrate
- Databox Family
- Cost Management

Platform as a Services (PaaS)

Compute/Containers

- Functions
- Kubernetes Service
- Container Instance
- Service Fabric

Web/Mobile

- Web Apps
- Logic Apps
- API Apps
- Mobile Apps
- Notification Hubs
- SignalR Service

DevOps/Developer

- Azure DevOps
- Lab Services
- Application Insights
- SDK

Integration

- API Management
- Logic Apps
- Service Bus
- Event Grid

IoT

- IoT Hub
- IoT Central
- Time Series Insights
- Azure Digital Twins
- IoT Edge

AI

- Cognitive Services
- Machine Learning Studio
- Machine Learning Service
- Bot Services
- Azure Search

Analytics

- SQL Data Warehouse
- Azure Databricks
- Apache Spark
- Stream Analytics
- Data Lake Storage Gen2

Data Services

- SQL Database
- SQL Data Warehouse
- Database for MySQL
- Cosmos DB
- Database for PostgreSQL
- Data Factory
- Database for MariaDB
- Azure Cache for Redis
- Database Migration Service
- Table Storage

Media/CDN

- Media Services
- Content Protection
- Video Indexer
- Content Delivery Network

Security

- Security Center
- Azure AD
- Azure AD for Domain Services
- Azure AD B2C
- DDoS Protection
- Key Vault
- Multi-Factor Authentication
- Azure ATP
- Role- based access control

Infrastructure as a Services (IaaS)

Compute

- Virtual Machine Scale Sets
- Linux Virtual Machine

Storage

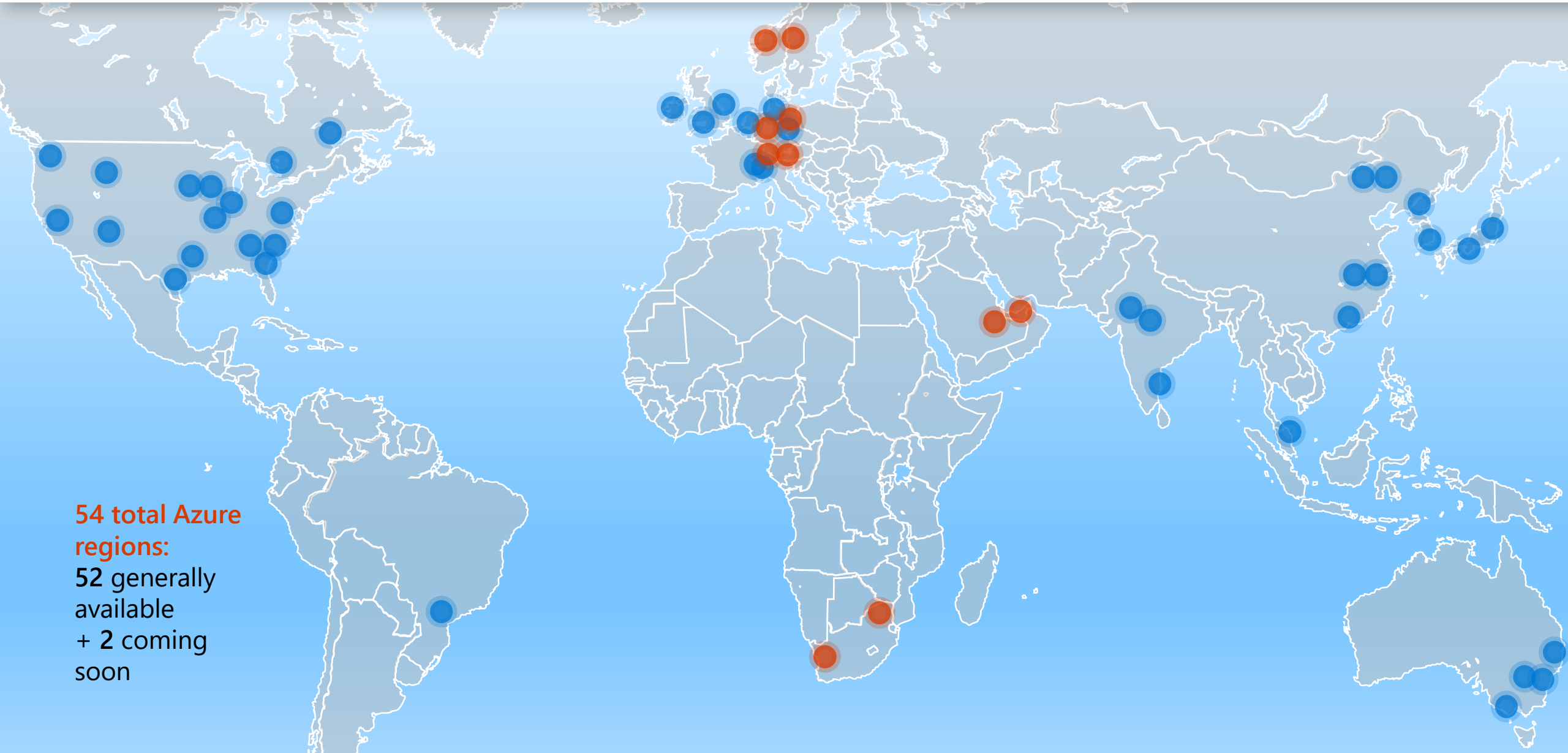
- Disk Storage
- Managed Disks

Networking

- Virtual Network
- VPN Gateway
- Express Route
- Load Balancer
- Azure Firewall
- Virtual WAN
- Network Watcher

Azure Datacenter Infrastructure

Azure Global Infrastructure

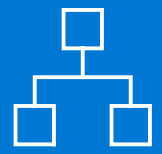


Compute

Azure Virtual machines

Windows or Linux VMs

Virtual Machine Scale Set



Networking

Azure Virtual Network

Connects VMs to VPN connections

Azure Load Balancer

Balances inbound and outbound connections

Azure Traffic Manager

Distributes network traffic across Azure regions

Storage

Azure blob storage

Stores objects like video files, JSON, images, IoT data

Azure file storage

Acts as a file server to share and access files

Azure table storage

NoSQL storage for unstructured data

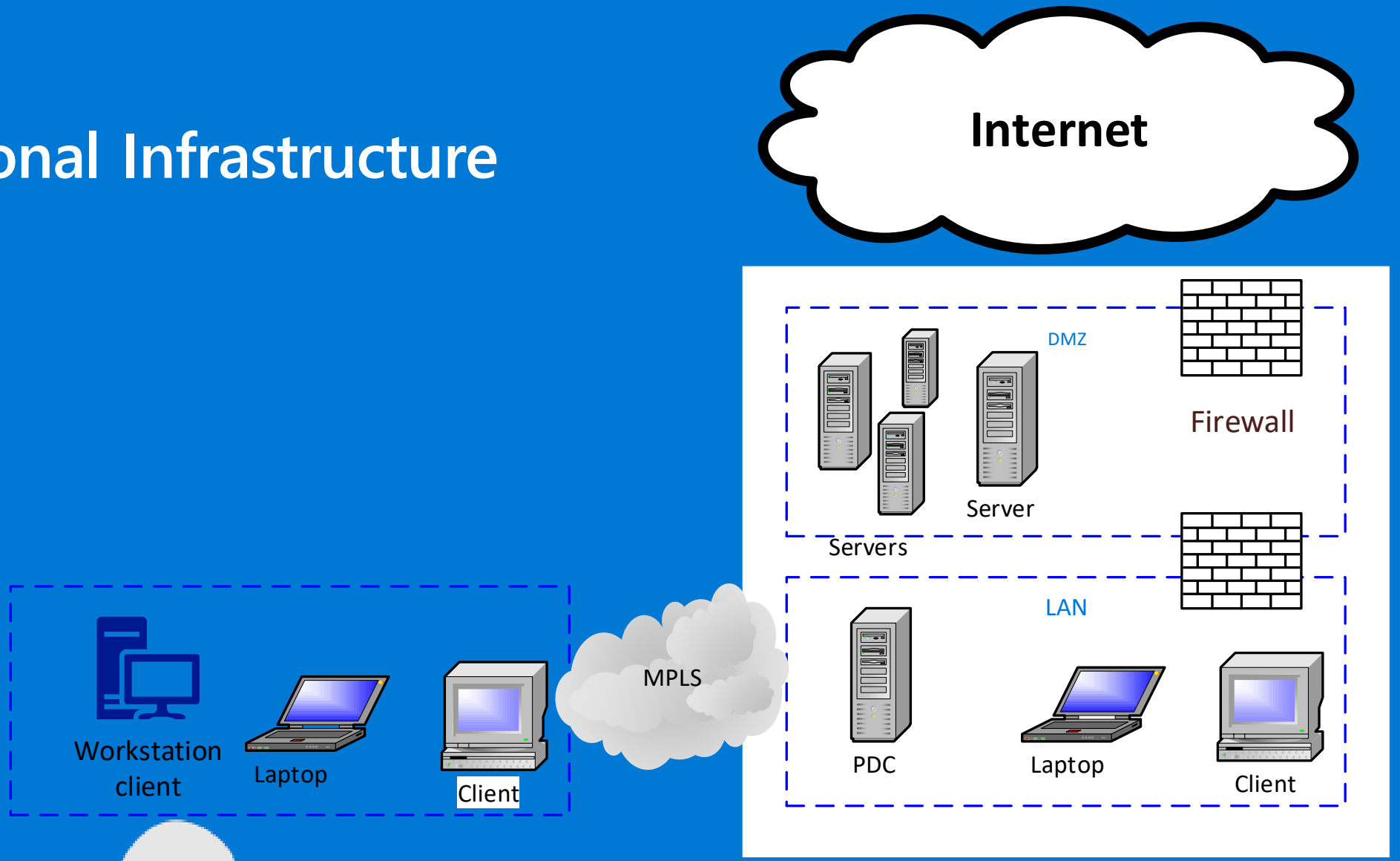
Security and management

Azure Security Center

Azure Sentinel

Active Directory -> Azure AD

Traditional Infrastructure



What is Azure Active Directory?

Azure AD is a multi-tenant, cloud-based directory and identify management service

Centralized directory store

Used by Azure and Office 365

Contains all the identities of users in your organization

Manage all your identities in the cloud

Govern access to all your apps in one place

Employ industry-leading security

What is Azure Active Directory?

- Single sign-on to any cloud or on-premises web app: Use a single identity for on-premises and cloud resources
- A full suite of identity management capabilities including multi-factor authentication, device registration, self-service password management, privileged account management, RBAC, monitoring, auditing, and alerting
- Extend AD to the cloud
- Compatible with iOS, Mac OS X, Android, and Windows devices
- Protect on-premises web applications with secure remote access
- Help protect sensitive data and applications

- Azure AD is primarily an identity solution, and designed for HTTP and HTTPS communications
- Queried using the REST API over HTTP and HTTPS. Instead of LDAP.
- Uses HTTP and HTTPS protocols such as SAML, WS-Federation, and OpenID Connect for authentication (and OAuth for authorization). Instead of Kerberos
- Includes federation services, and many third-party services (such as Facebook)
- Azure AD users and groups are created in a flat structure, and there are no Organizational Units (OUs) or Group Policy Objects (GPOs)

Azure Active Directory

254M

Azure AD

Monthly Active Users

100K+

Enterprise customers

Using Azure AD

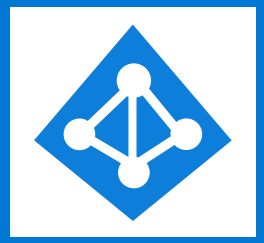
Oct 2019

Azure Active Directory Editions

Feature	Free	Office 365 Apps	Premium P1	Premium P2
Directory Objects	500,000 objects	No object limit	No object limit	No object limit
Single Sign-On	Up to 10 apps	Up to 10 apps	Unlimited	Unlimited
Core Identity and Access	X	X	X	X
B2B Collaboration	X	X	X	X
Identity & Access for O365		X	X	X
Premium Features			X	X
Hybrid Identities			X	X
Advanced Group Access			X	X
Conditional Access			X	X
Identity Protection				X
Identity Governance				X

https://azure.microsoft.com/en-us/pricing/details/active-directory/

Azure Active Directory



Azure Active Directory

Microsoft's Cloud-Based Identity and Access Management Service

AAD Tenant

A dedicated and trusted instance of Azure AD that represents a single organization

Custom Domains

Initial Domain will be x.onmicrosoft.com

- Cannot be changed or modified
- Can add and verify custom domain

Hybrid is the new normal

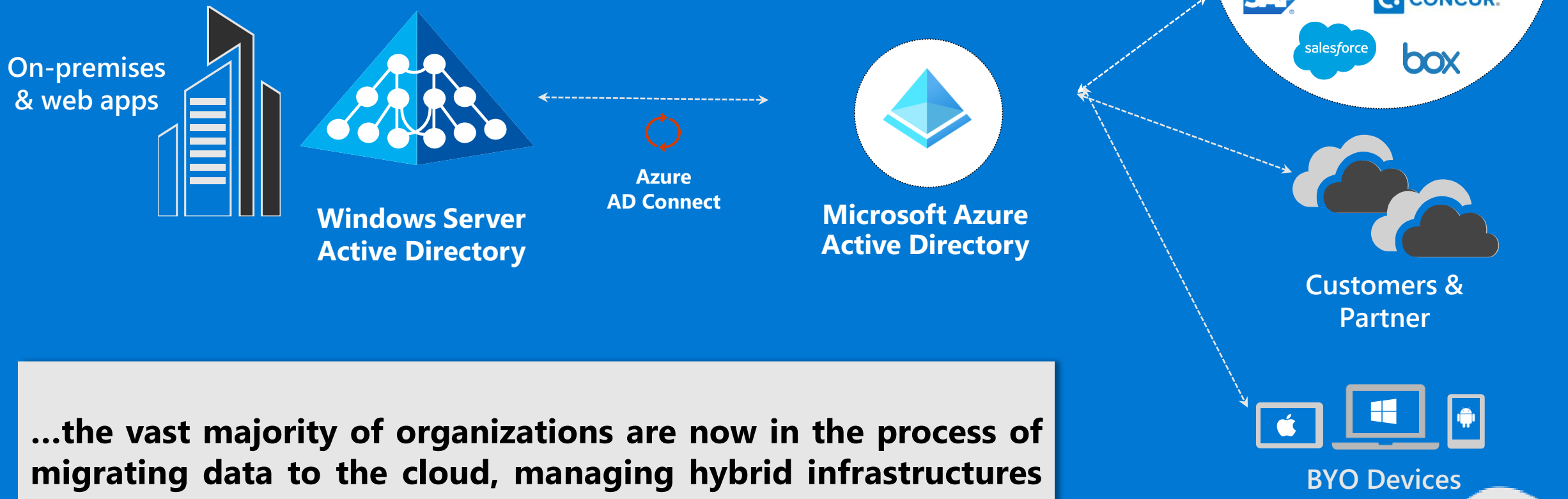
Secure access and governance of both cloud and on-prem apps

More usage of SaaS apps but still a significant number of on-prem apps

Orgs. modernizing apps but for many it won't happen

IT needs to secure and manage on-prem apps while providing a great user experience

Hybrid Environments



…the vast majority of organizations are now in the process of migrating data to the cloud, managing hybrid infrastructures in a complicated balance of legacy network components and traditional applications." Michael Xie, Forbes Magazine

Microsoft's Identity Services

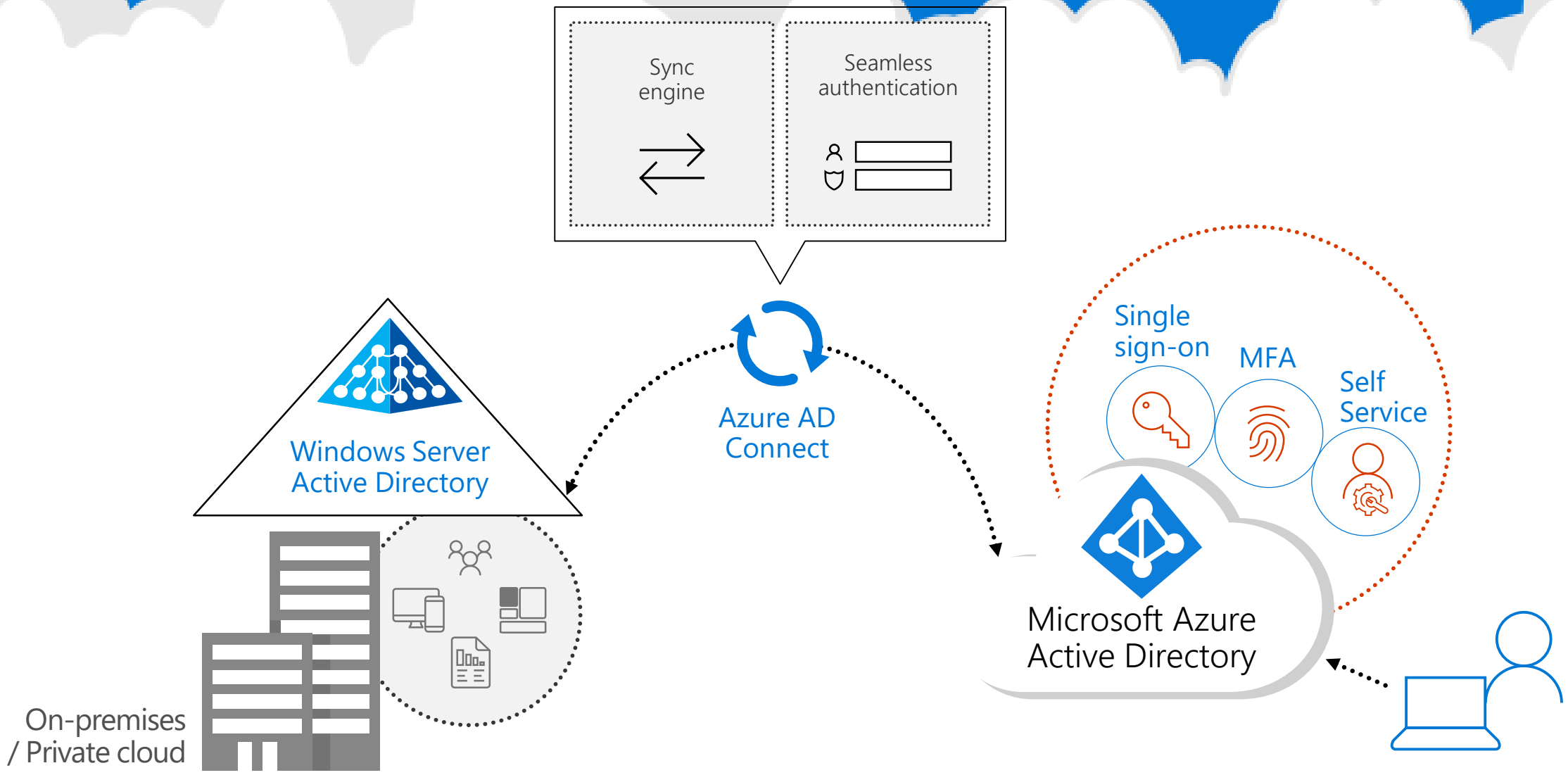
Active Directory

Azure Active Directory

Domain
Domain Controllers

Identity-as-a-Service

Azure AD Connect



Authentication options in Azure AD

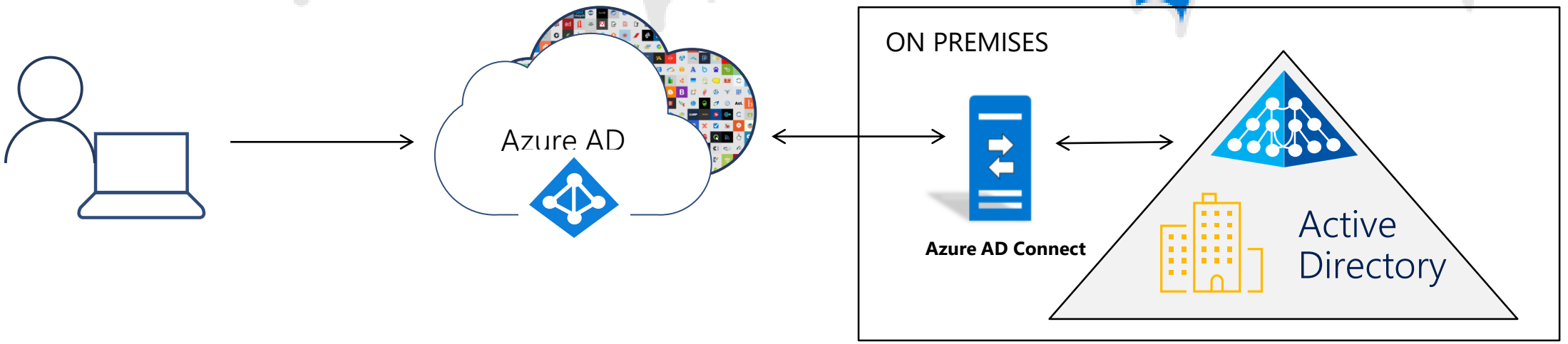
Cloud authentication

- Cloud-only
- Password Hash Sync + Seamless SSO
- Pass-through authentication + Seamless SSO

Federated authentication

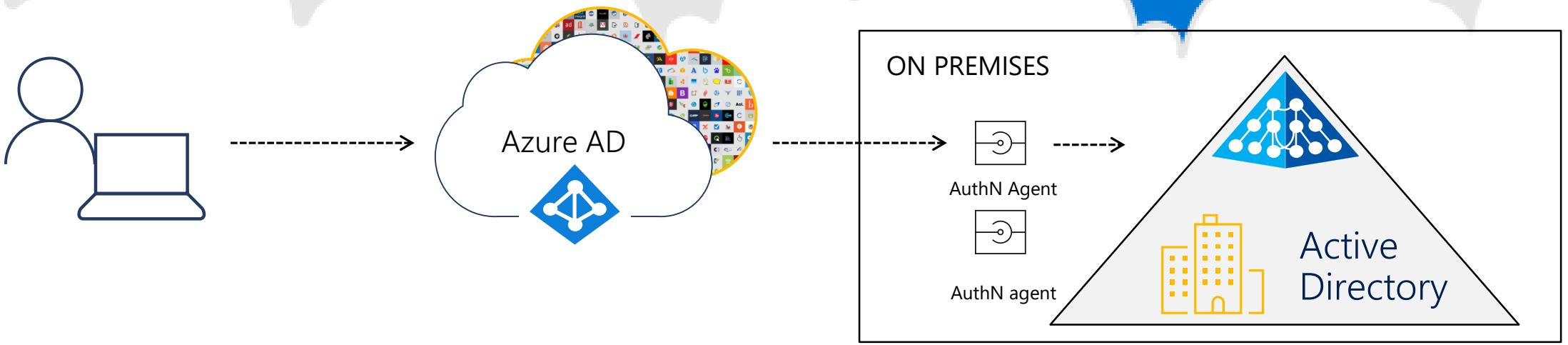
- AD FS
- Third party federation providers

Password Hash Sync



Great user experience	Secure and compliant	Easy to deploy & administer
Same passwords for cloud-based and on-premises apps	Only non-reversible hashes are stored in the cloud	No on-premises agent needed
Disaster recovery option incase other authN methods are unavailable	Leaked credential report available	Small on-premises footprint
	Integrated with Smart Lockout, Identity Protection and Conditional Access	

Pass thru Authentication



Great user experience

- Same passwords for cloud-based and on-premises apps
- Integrated with Self-Service Password Reset

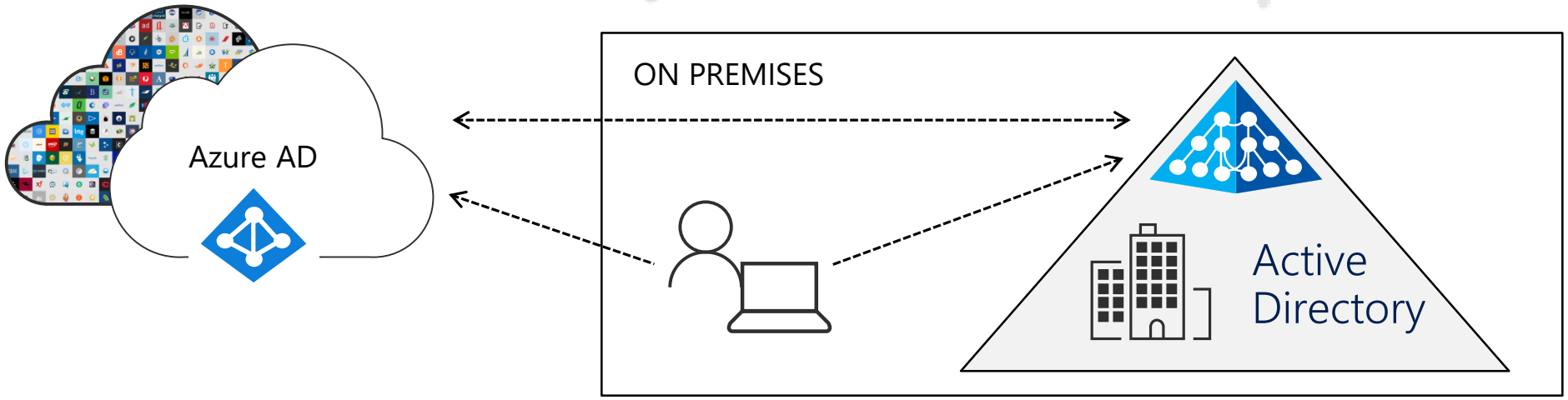
Secure and compliant

- Passwords remain on-premises
- No DMZ and no inbound firewall requirements
- Integrated with Smart Lockout, Identity Protection and Conditional Access

Easy to deploy & administer

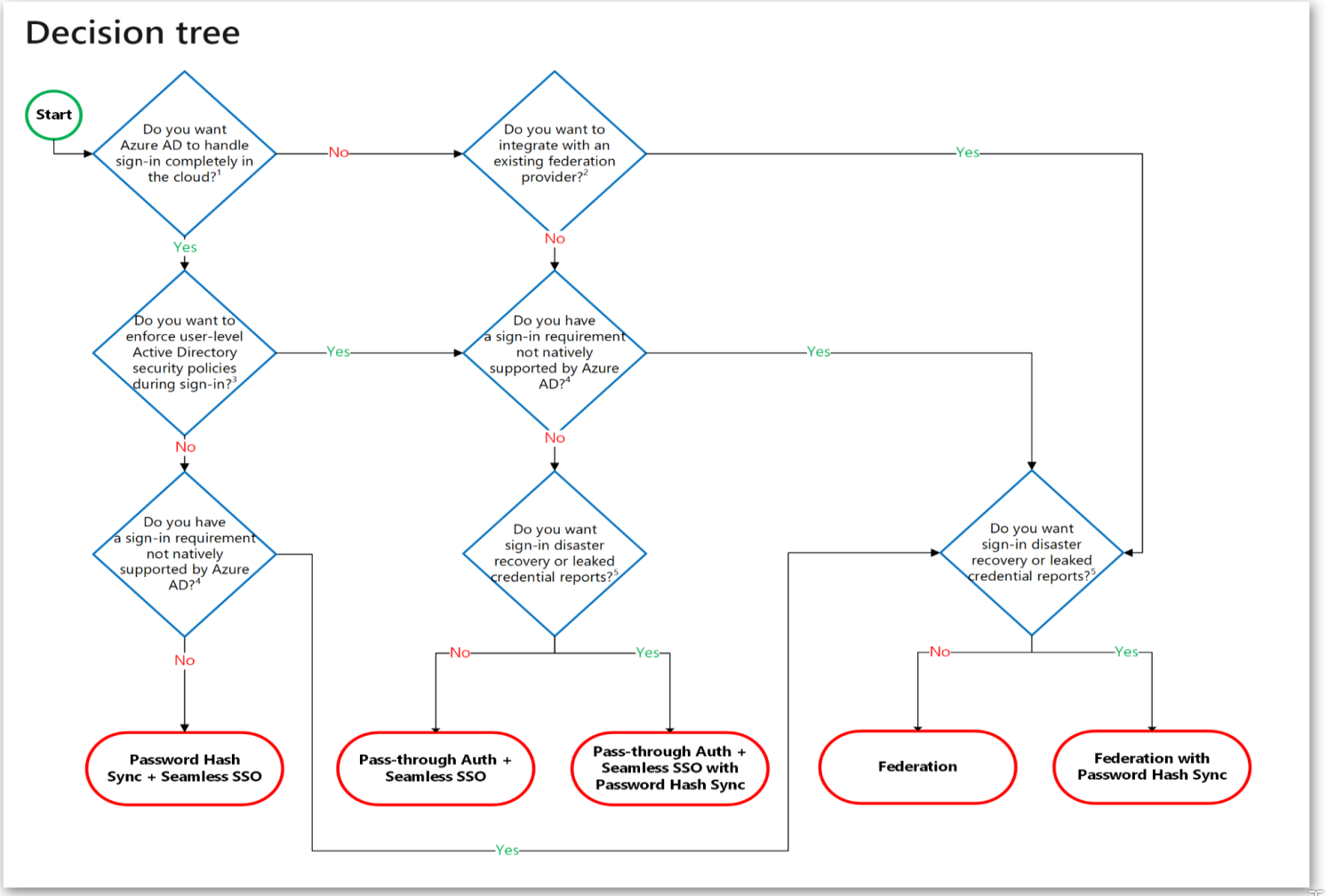
- Agent-based deployment
- High availability out-of-the-box
- No complex on-premises deployments or network config
- Zero management overhead

Seamless Single Sign On



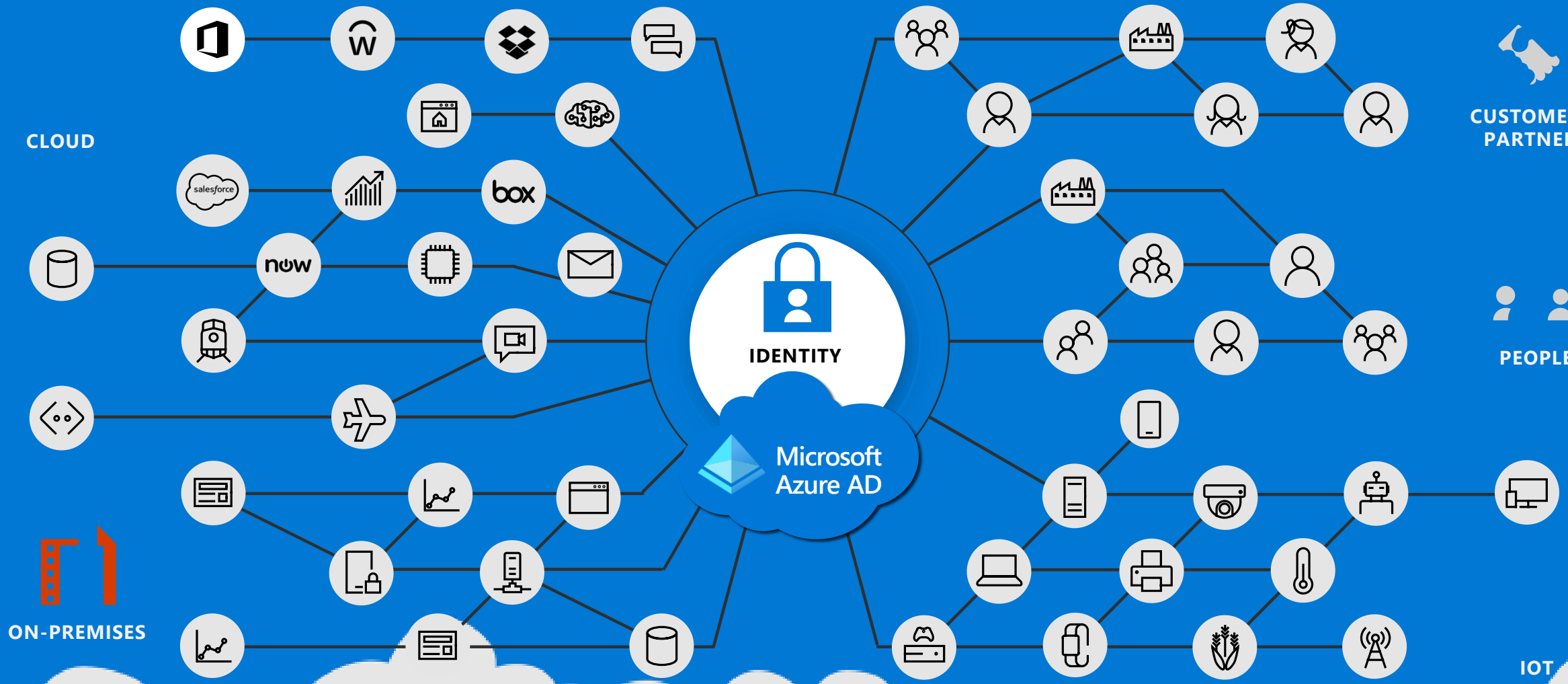
Easy to integrate	Easy to administer	Great user experience
Works with Password Hash Sync and Pass-through Authentication	No additional on-premise infrastructure	SSO experience from domain-joined devices within your corpnet
Supports Alternate Login ID	Register non-Windows 10 devices without AD FS	

Azure AD Authentication- Decision Tree



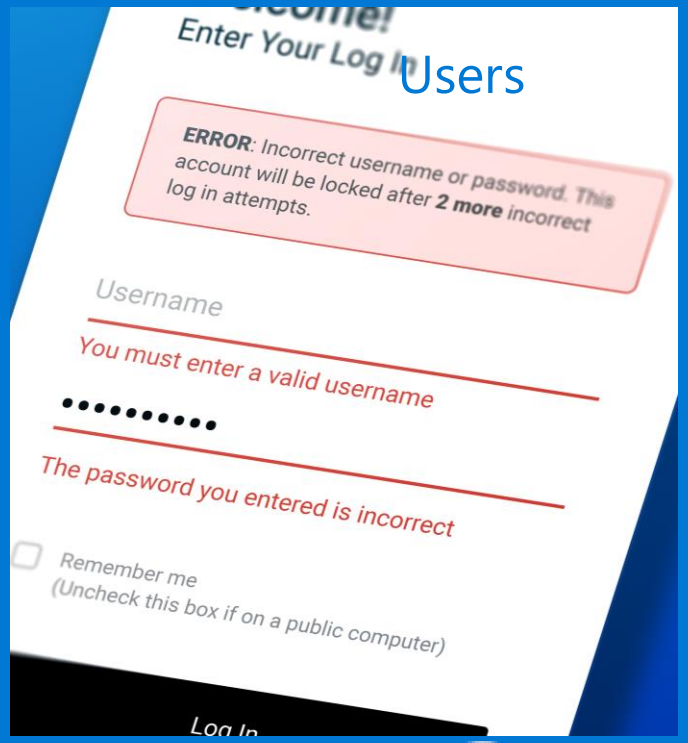
https://docs.microsoft.com/it-it/azure/security/fundamentals/choose-ad-authn

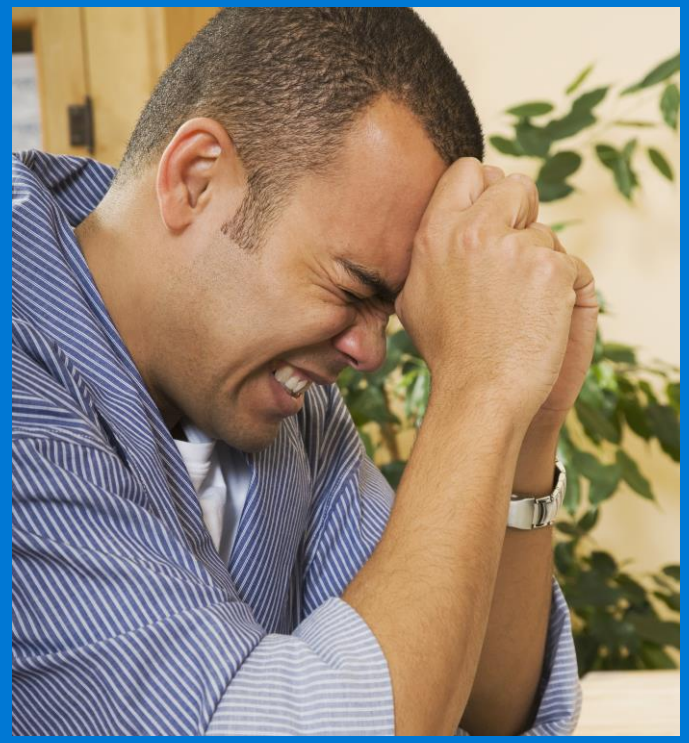
Identity is your control plane



Everybody hates passwords

Almost everyone hates passwords





Passwords are expensive and insecure

Password reuse across multiple accounts

Passwords are the weak link

Data breaches are expensive

Passwords generate tons of support calls

73%
of passwords are duplicates

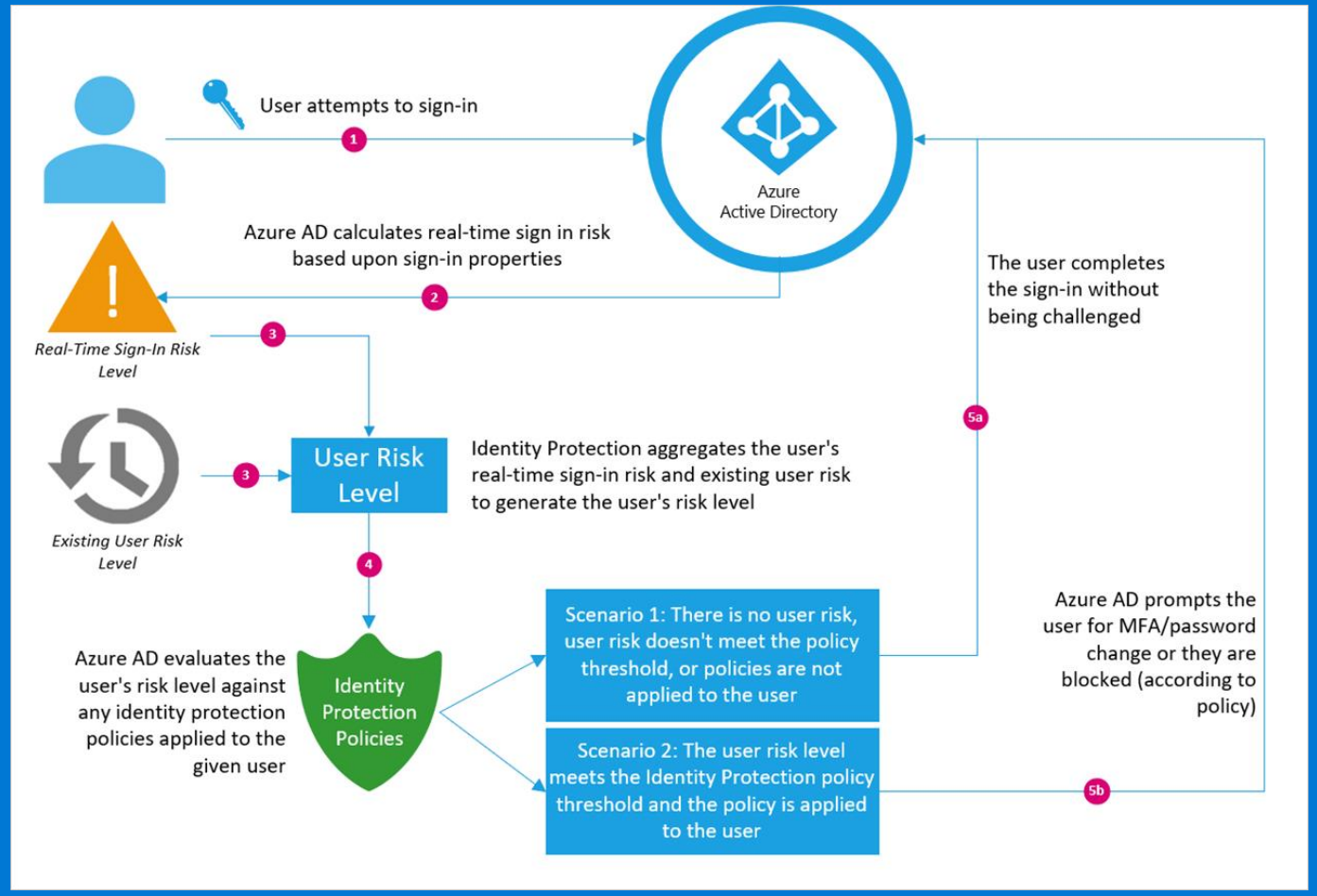
81%
of breaches leveraged passwords

$3.86
million, the average total cost of a data breach

#1 cost
for IT departments is forgotten passwords

Azure AD Identity Protection

- Proactively prevent compromised identities from being abused
- Automatically mitigate risk when suspicious activity is detected
- Investigate risky users and sign-ins to address potential vulnerabilities
- Be alerted when a user's risk reaches a specified threshold
- Export risk detection data to third-party utilities for further analysis.

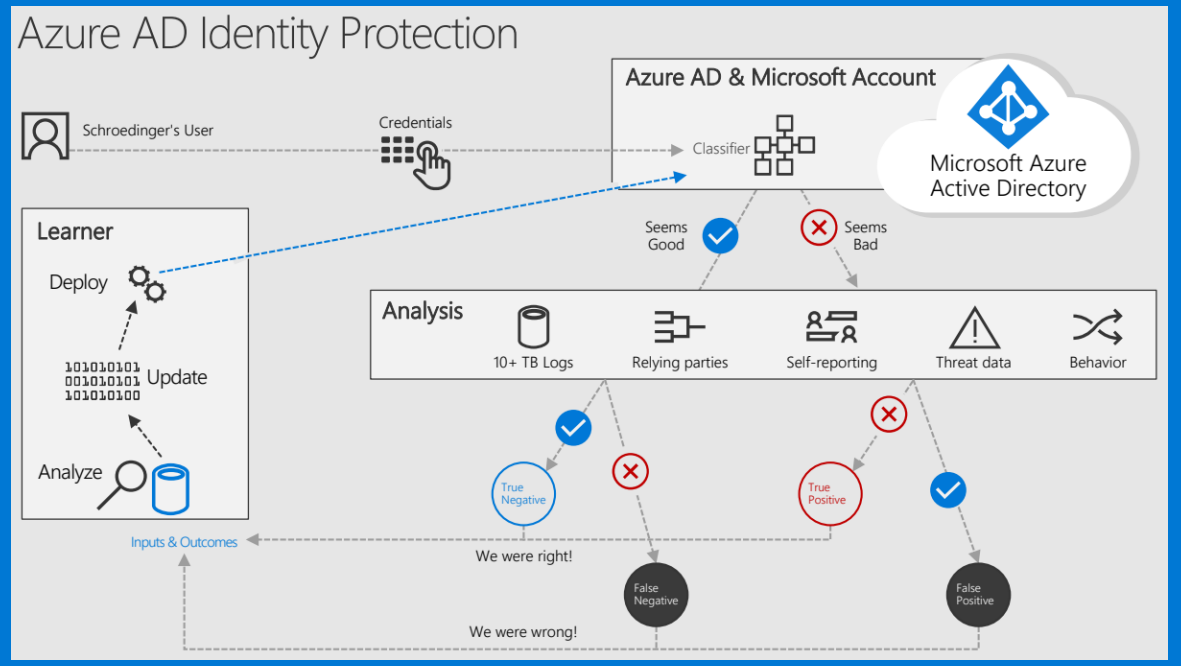


Azure Active Directory Identity Protection

Identity Protection identifies risks in the following classifications:

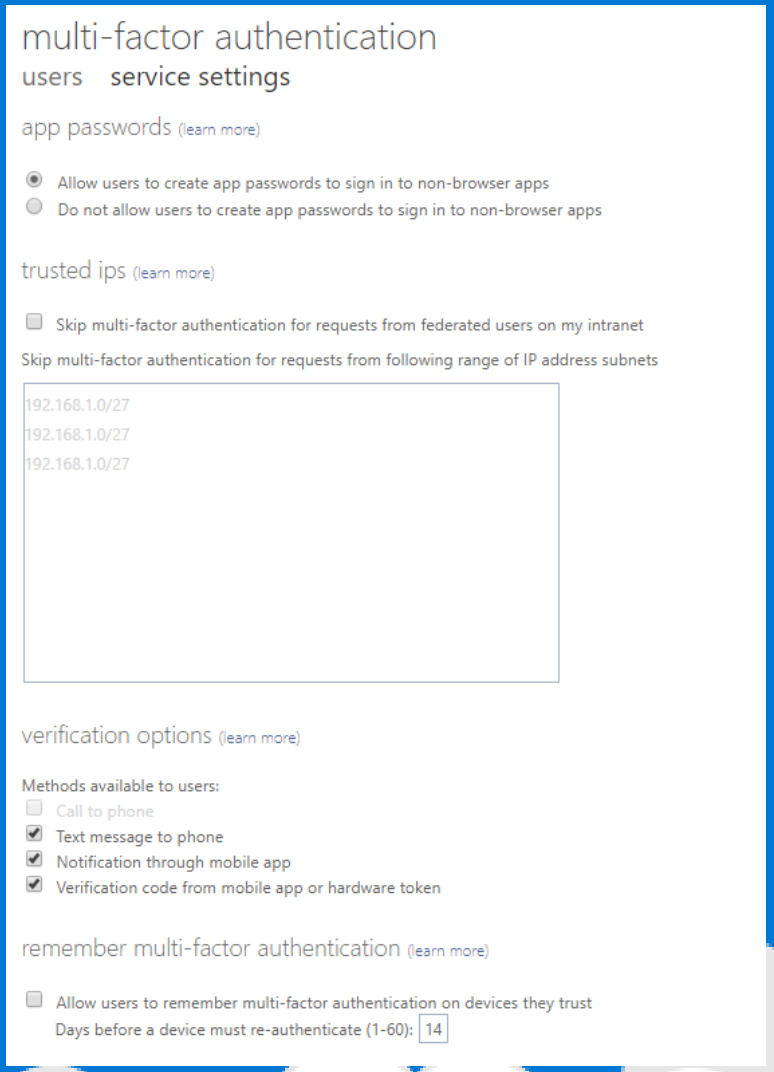
Risk detection type	Description
Atypical travel	Sign in from an atypical location based on the user's recent sign-ins.
Anonymous IP address	Sign in from an anonymous IP address (for example: Tor browser, anonymizer VPNs).
Unfamiliar sign-in properties	Sign in with properties we've not seen recently for the given user.
Malware linked IP address	Sign in from a malware linked IP address
Leaked Credentials	This risk detection indicates that the user's valid credentials have been leaked
Azure AD threat intelligence	Microsoft's internal and external threat intelligence sources have identified a known attack pattern

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



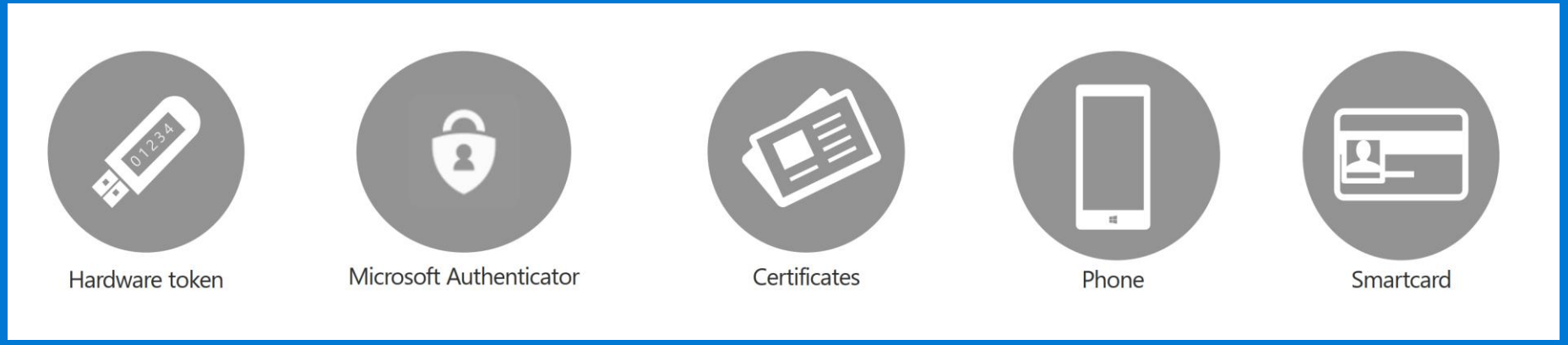
Implementing Multi-Factor Authentication

- Multi-factor Authentication (MFA) in Microsoft 365 helps increase security by requesting users to provide a username and a password while signing in and then use a second authentication method.
- The second authentication method might be acknowledging a phone call, text message, or an app notification on their smartphone
- You can also enable users who authenticate from a federated, on-premises directory for multi-factor authentication.
- The tenant administrator enables MFA in the Microsoft 365 admin center



Multi-Factor Authentication

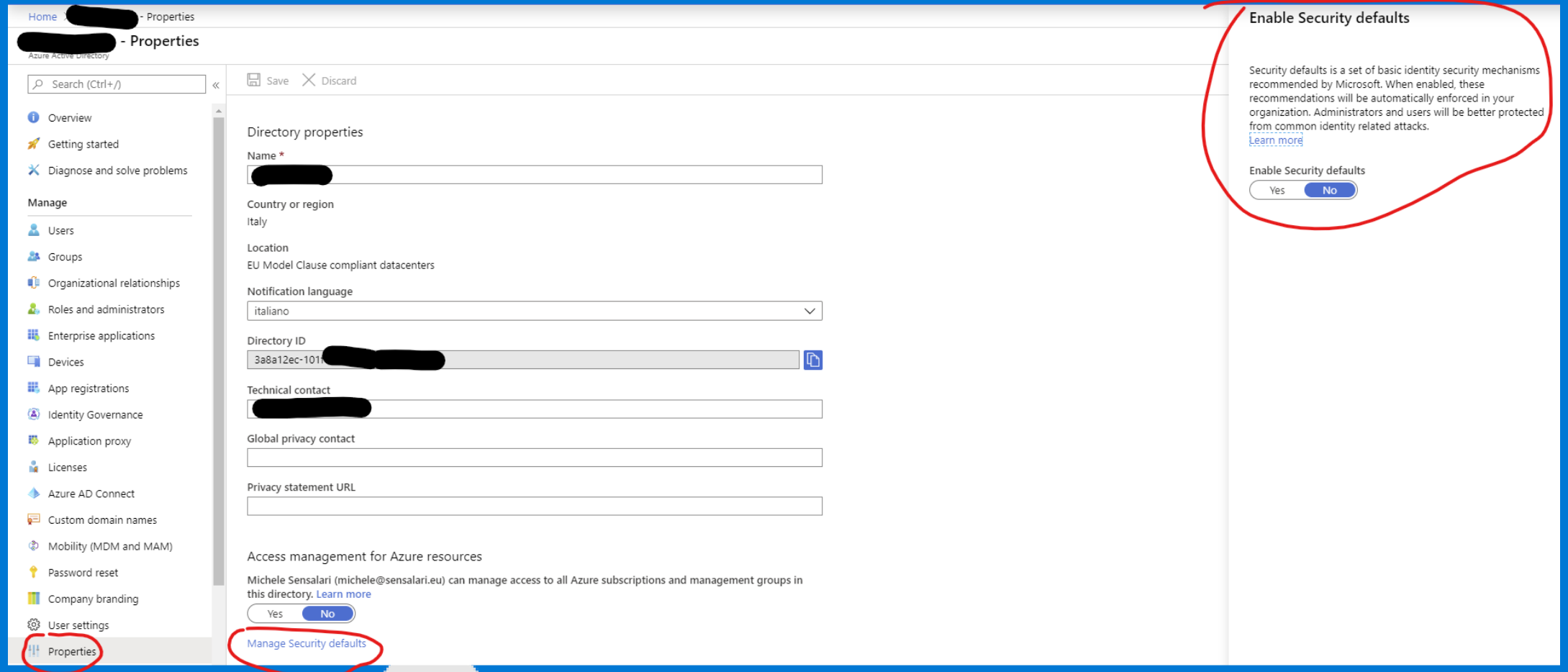
- Any two of more of the following factors:
  - Something you know: a password or pin
  - Something you have: a phone, smartcard, or hardware token
  - Something you are: facial recognition, fingerprint, or other biometric



You can reduce your odds of being compromised by up to 99.9% by implementing multi-factor authentication (MFA).

Source: Microsoft 2018 Security Research

Security Default



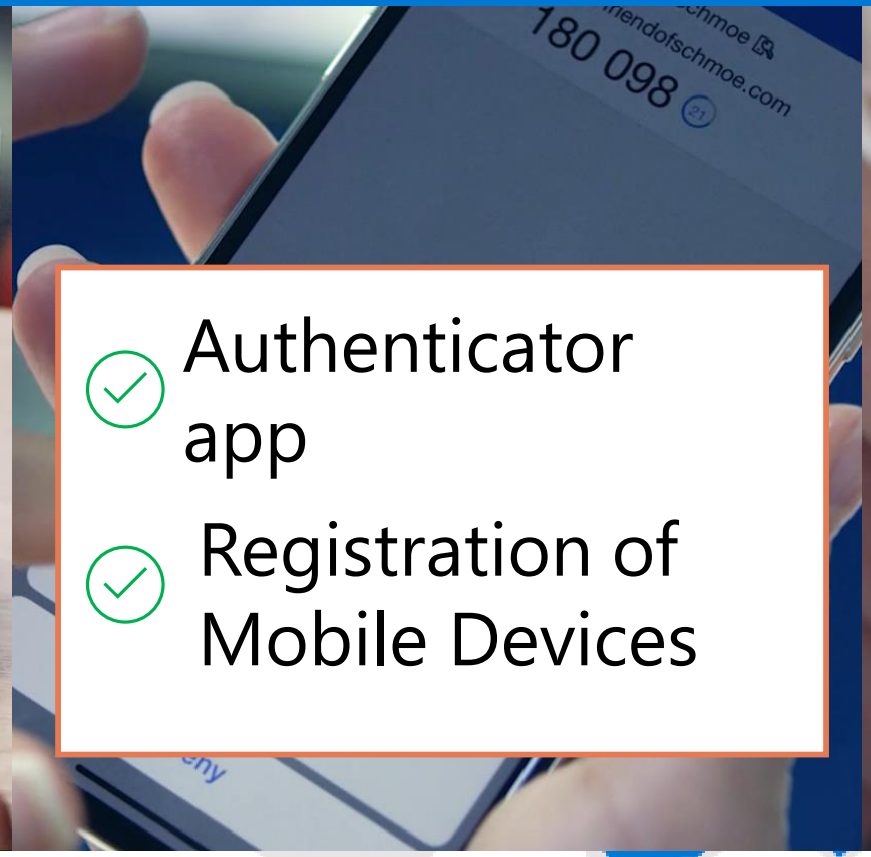
https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/concept-fundamentals-security-defaults#unified-multi-factor-authentication-registration

Passwordless foundation

Windows Hello

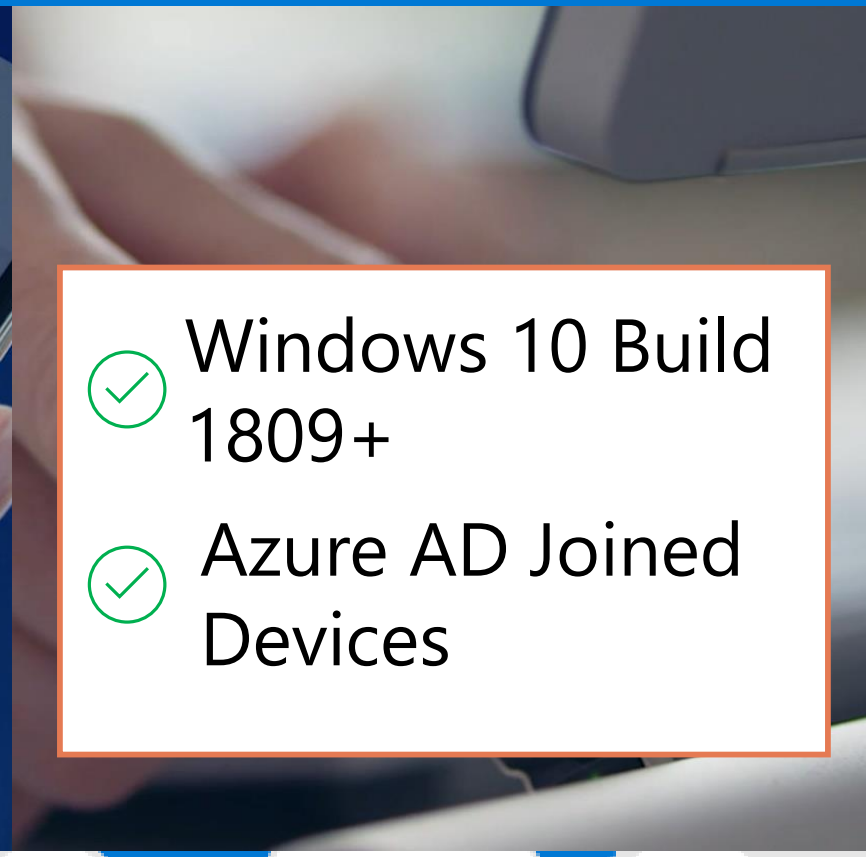
- Strong Credentials
- Registration of Windows Devices

Microsoft Authenticator



- Authenticator app
- Registration of Mobile Devices

FIDO2 Security Keys

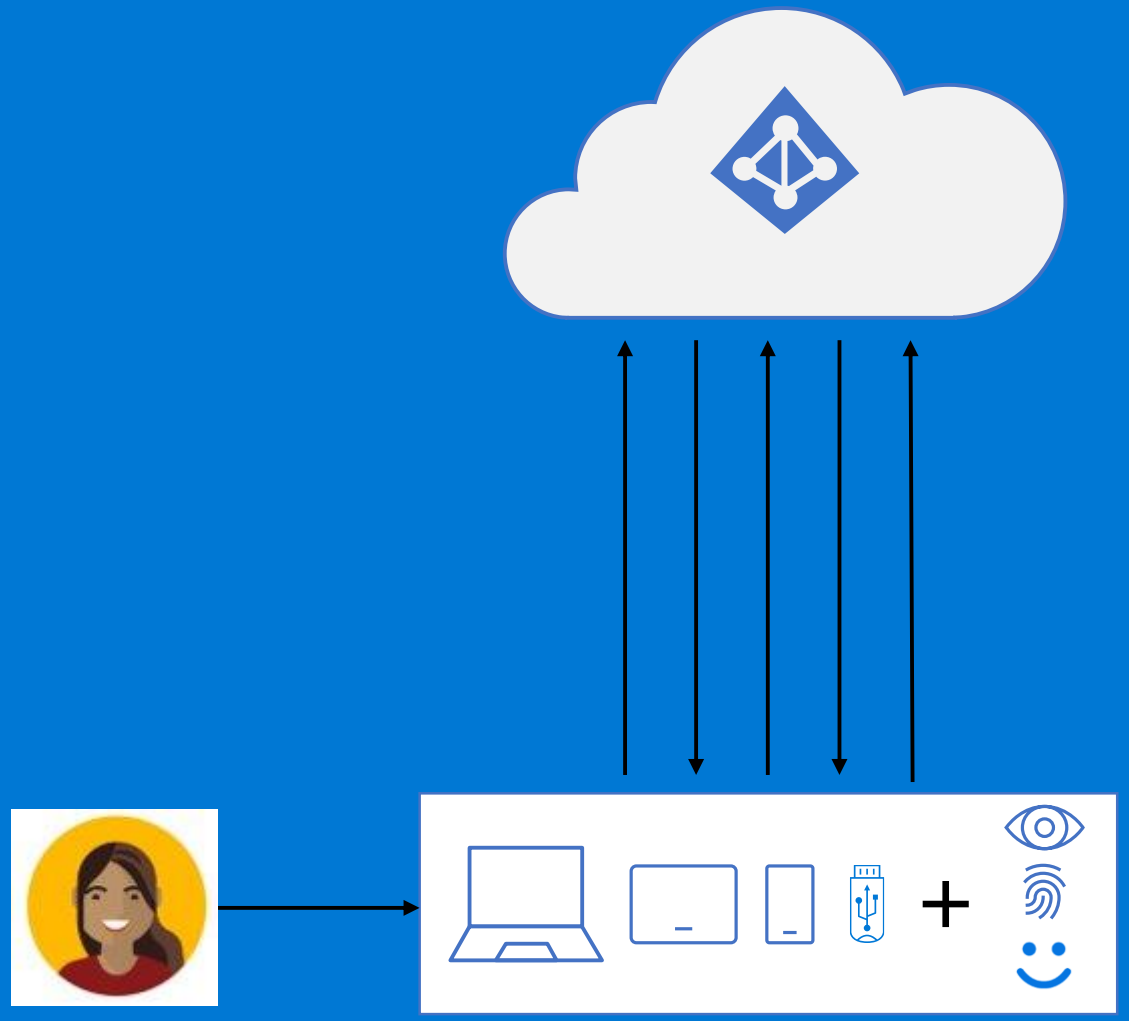


- Windows 10 Build 1809+
- Azure AD Joined Devices

Secure Authentication Flow

A simple, common architecture

- FIDO2: standard based Passwordless authentication
- Based on public-key technology
- Private-keys are securely stored on the device
- Requires a local gesture (e.g., biometric, PIN)
- Private-keys are bound to a single device and never shared



Windows Hello for Business

Microsoft’s premier passwordless experience

2016
Available since

FIDO2
Certified

9.3K enterprise deployments
with over 1.7M MAD

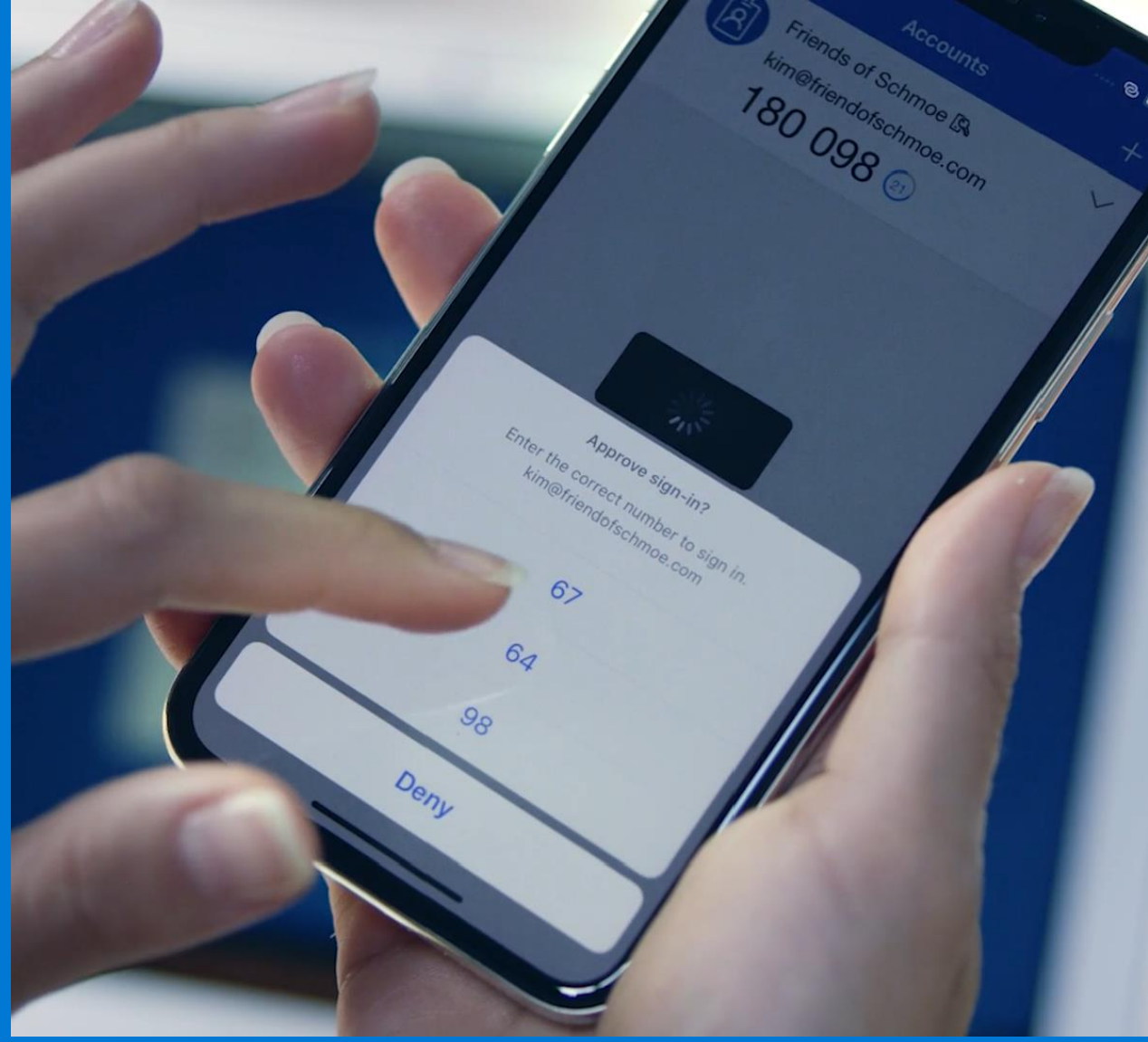
Microsoft Authenticator

Microsoft’s passwordless anywhere solution

2018
Available in public preview

~50K MAU
for passwordless sign-in

16M+ users of App
50M downloads



FIDO2 security keys

Microsoft's passwordless solution for shared devices

Currently only for Azure AD Joined devices

July 2019
Available in public preview

750+
enterprises expressed interest

2K+ tenants have enabled feature and registered keys

Upcoming

FIDO2 public preview expanding to Hybrid environments (Early 2020)

What will be included?

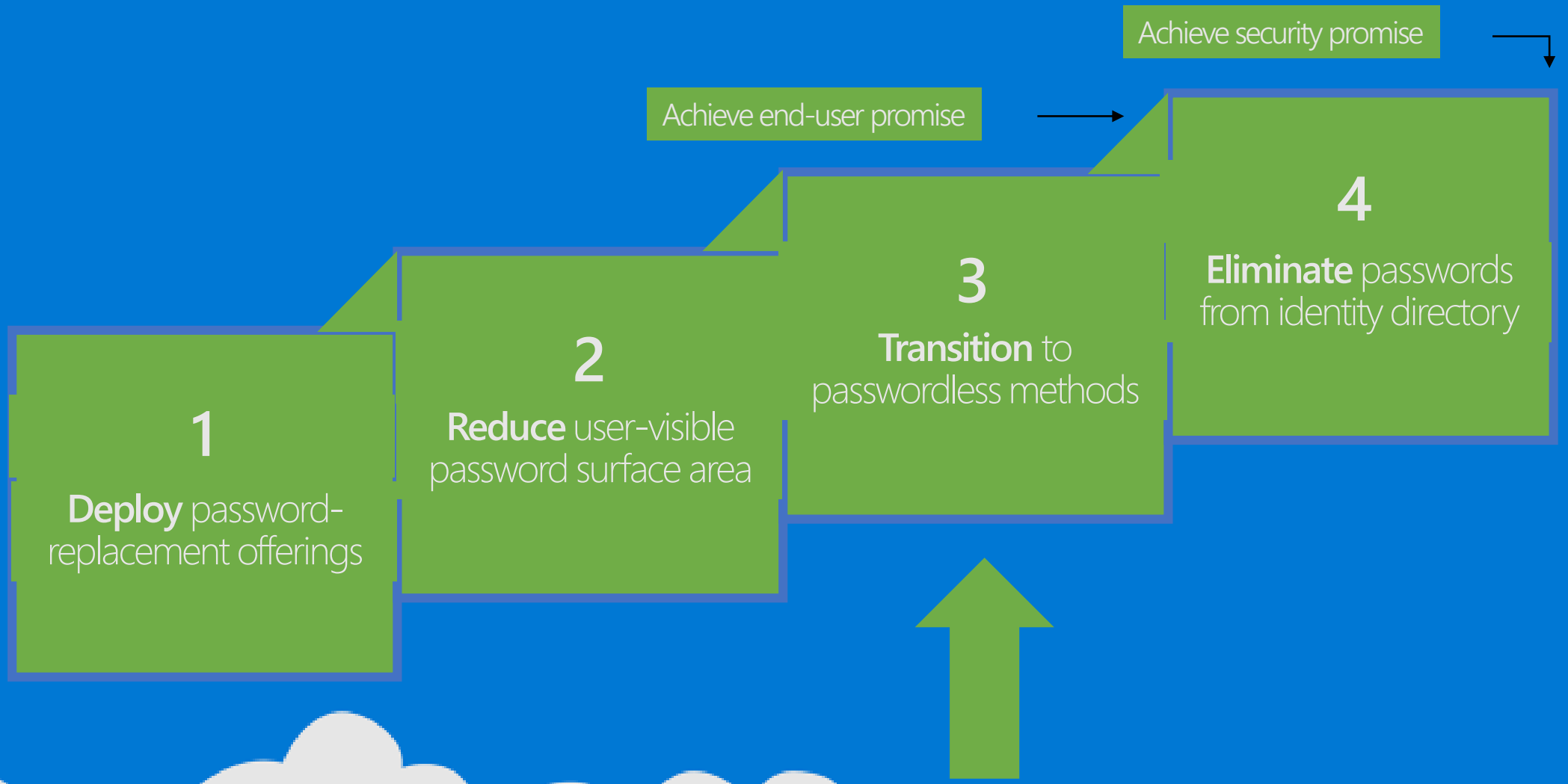
Passwordless sign-in using FIDO2 security keys

- Azure Active Directory Joined (AADJ)

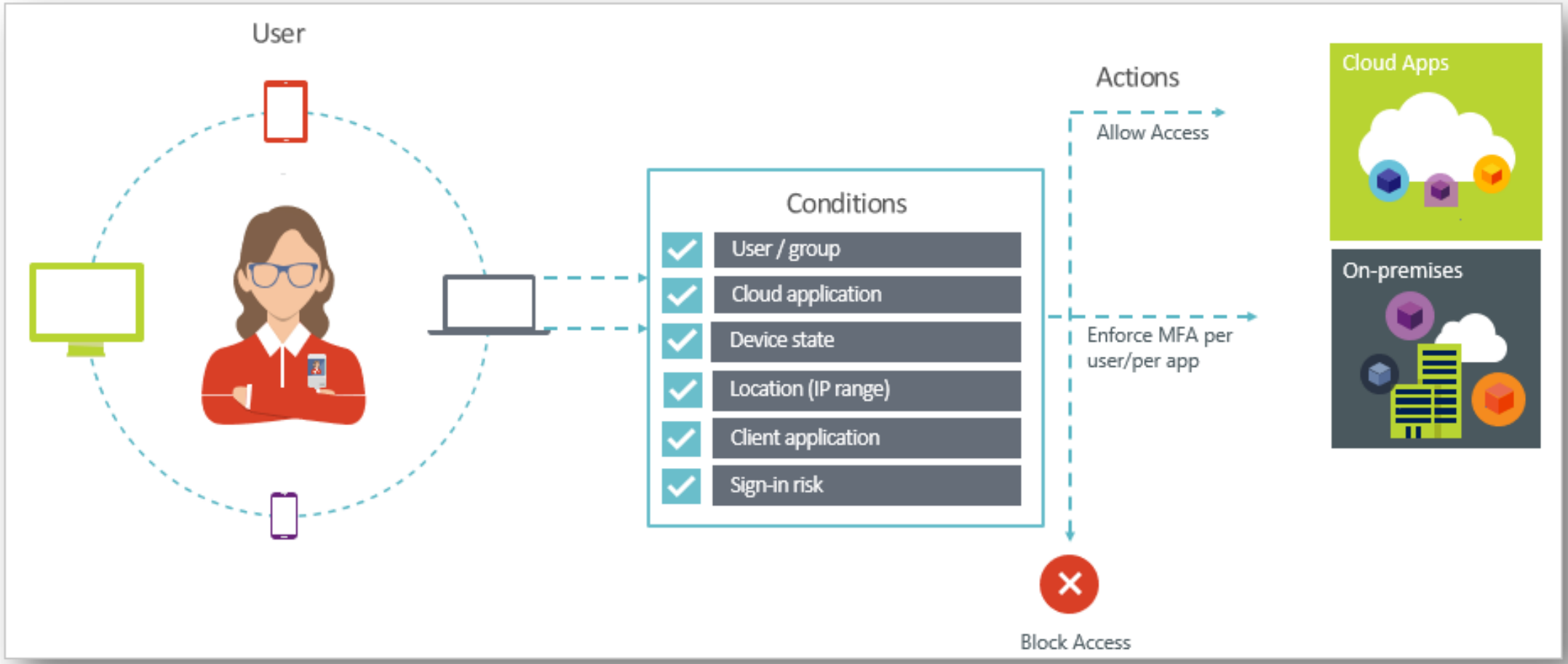
- Hybrid AADJ Windows 10 devices

Seamless SSO to Cloud and on-premises resources

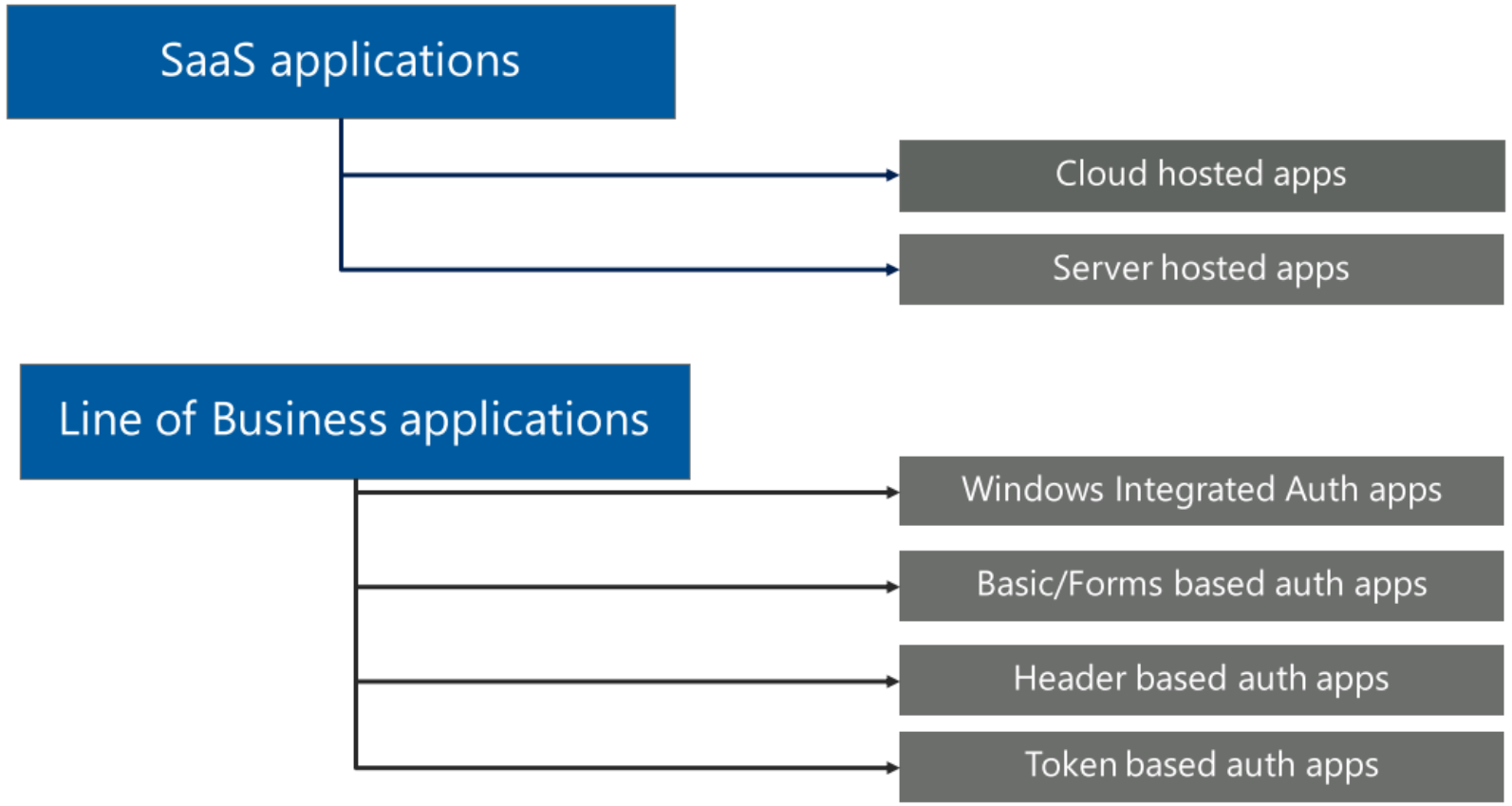
Microsoft Passwordless Journey



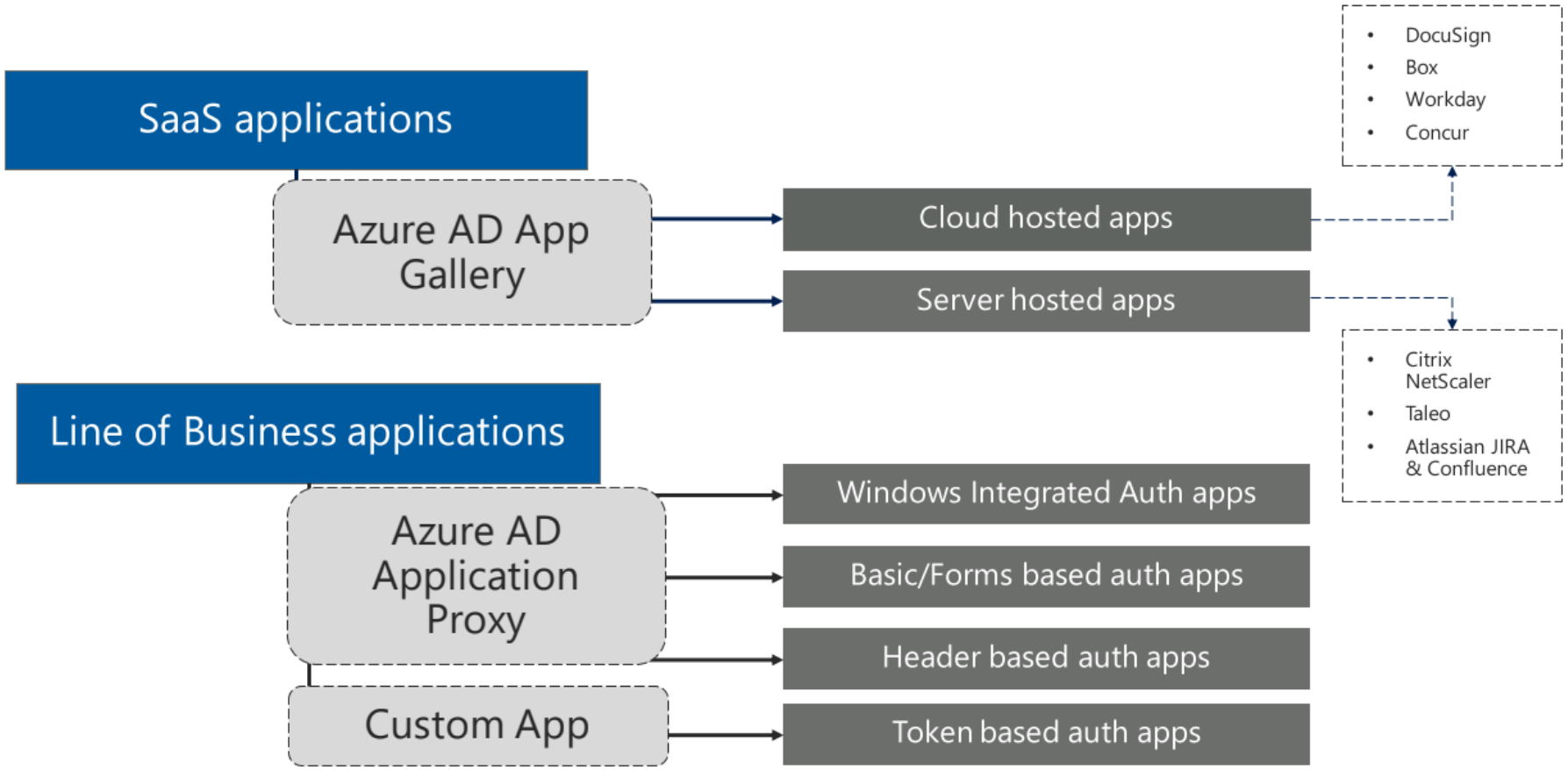
Azure AD Conditional Access



Azure AD Enterprise Applications

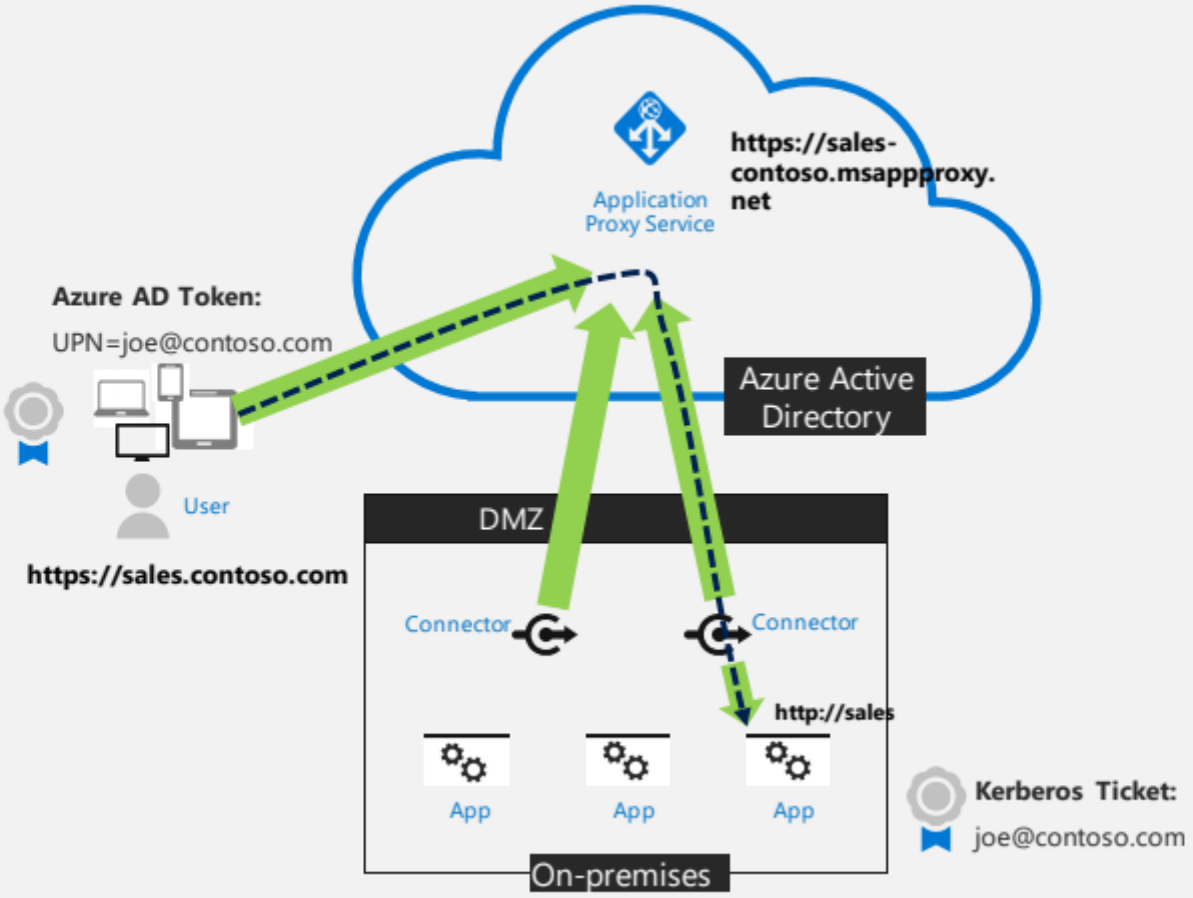


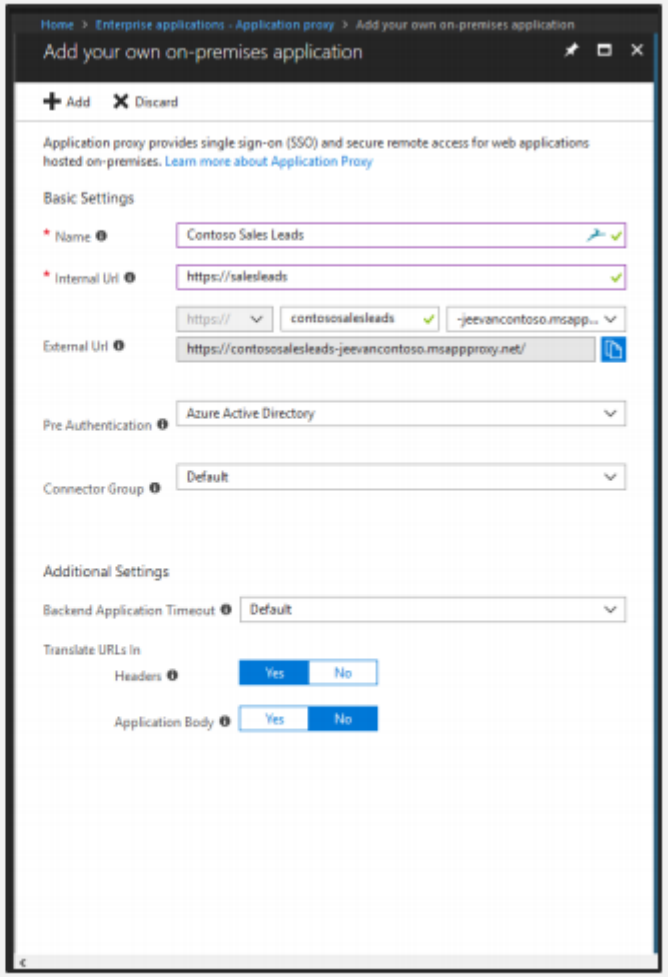
Azure AD Enterprise Applications



Azure AD Application Proxy

1. Make the internal hosted apps accessible to the workforce without VPN
2. Azure AD protected External URL
3. Azure AD authentication or Pre-Auth option for authentication
4. Ability to Translate Header
5. Ability to translate Body

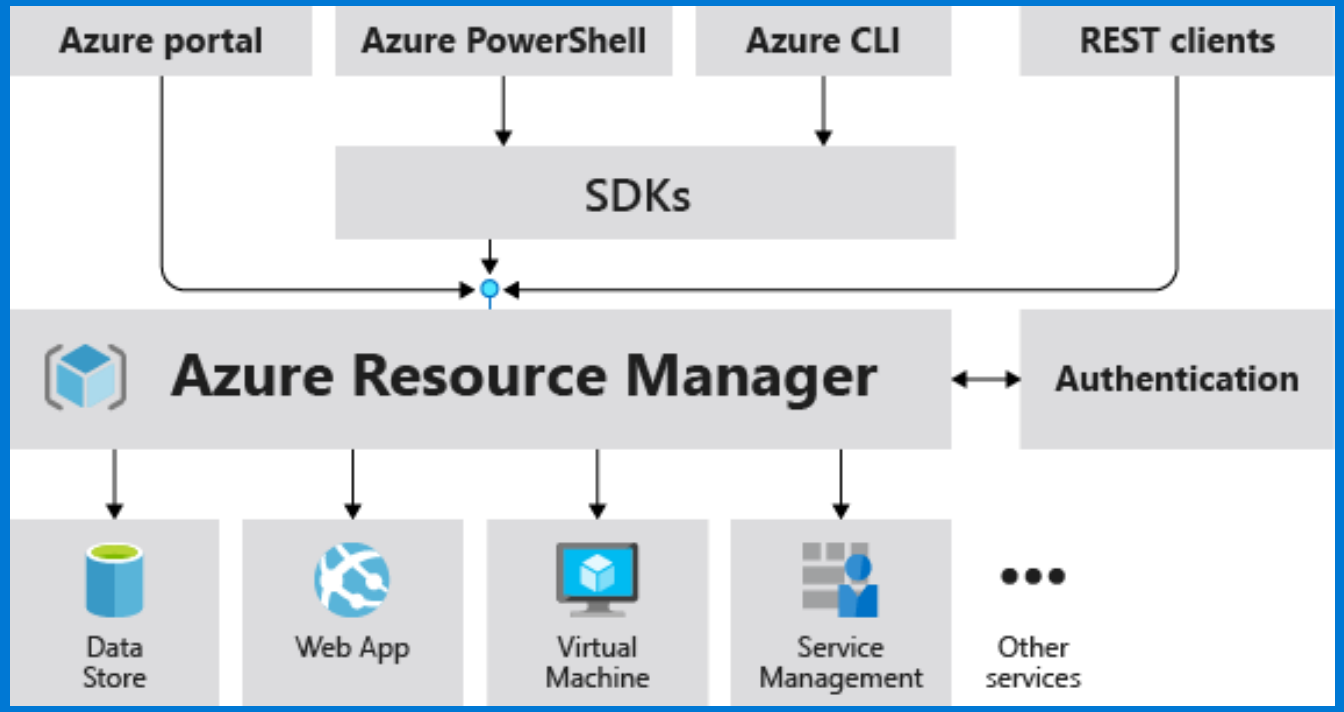




Active Directory -> IAAS VM ADDS

Azure Basic

Azure Resource Manager



How the Azure Resource Manager Works

Consistent management layer

See components as related and independent parts of your network

Deploy, manage, and monitor resources as a group

Provides security, auditing, and tagging

Azure Resource Manager

Resource

A manageable item available through Azure. VMs, web apps, databases, etc.

Resource group

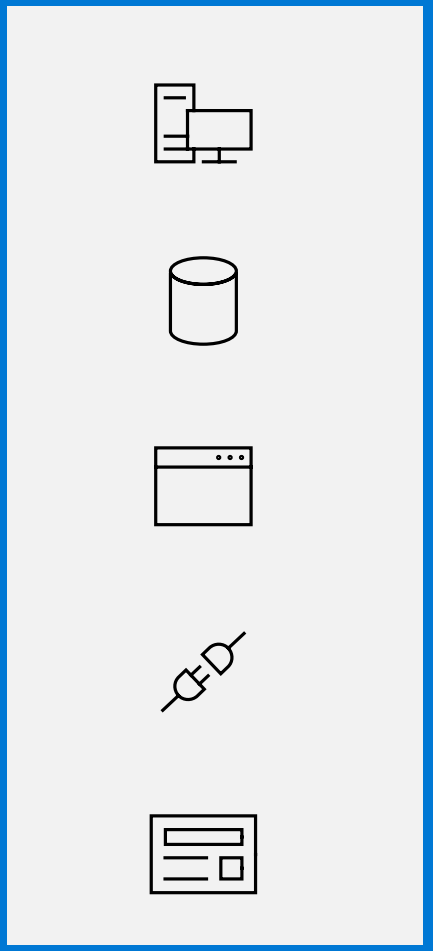
A container that holds related resources

You decide how to allocate resources to groups

Resource provider

A service that supplies the resources you can deploy and manage

Es. Microsoft.Compute, Microsoft.Storage, Microsoft.Web



Subscriptions

azuredeploy.json

```
},
 "resources": [
  {
   "type": "Microsoft.Storage/storageAccounts",
   "apiVersion": "2018-11-01",
   "name": "[variables('storageAccountName')]",
   "location": "[parameters('location')]",
   "sku": {
    "name": "[variables('storageAccountType')]"
   },
   "kind": "Storage",
   "properties": {}
  },
```

Azure Resource Manager Template

A JSON file that defines resources to deploy to a resource group

Defines dependencies between resources.

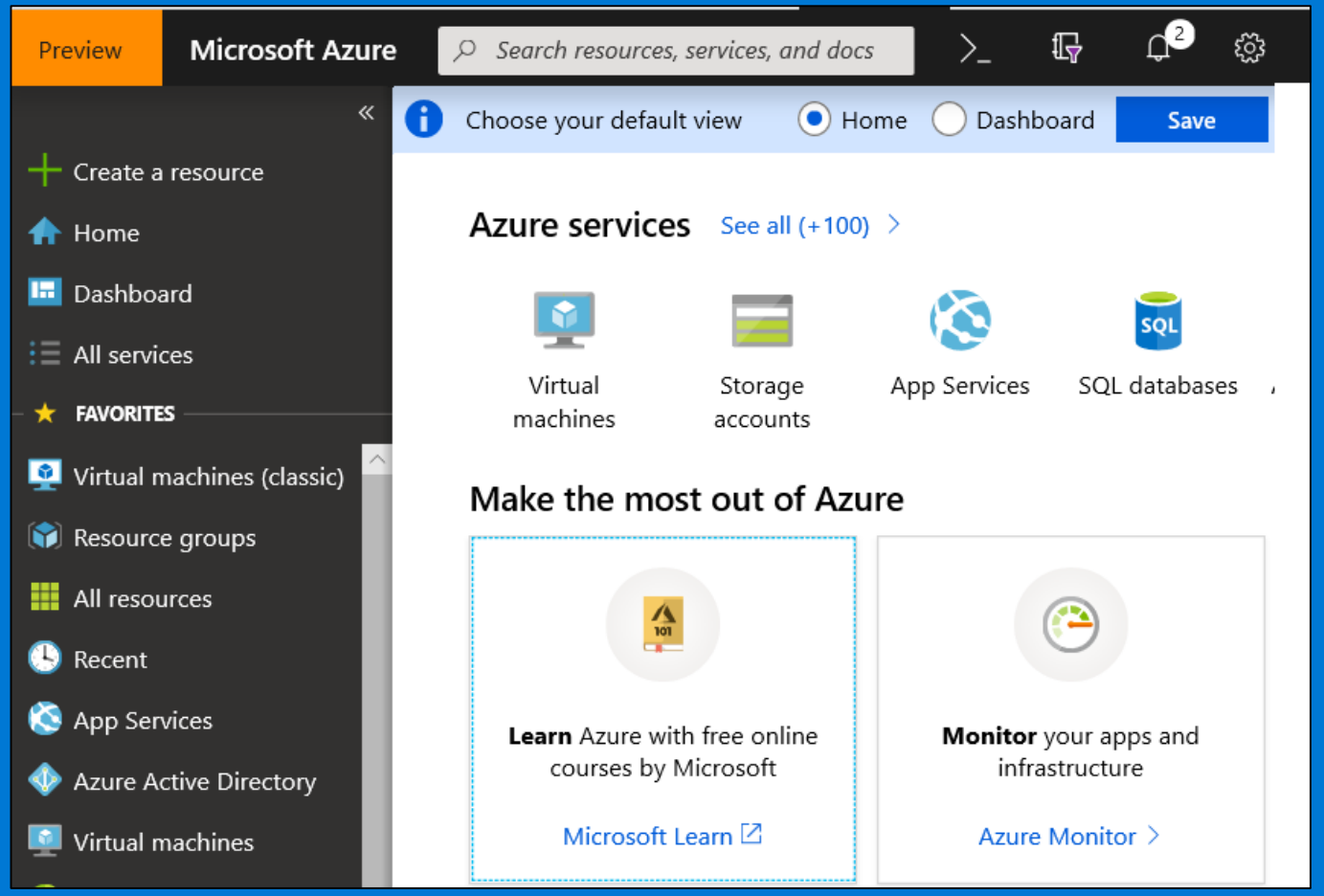
Benefits:

- Templates improve consistency
- Templates help express complex deployments
- Templates reduce manual, error-prone tasks
- Templates are code
- Templates promote reuse

Azure Tools

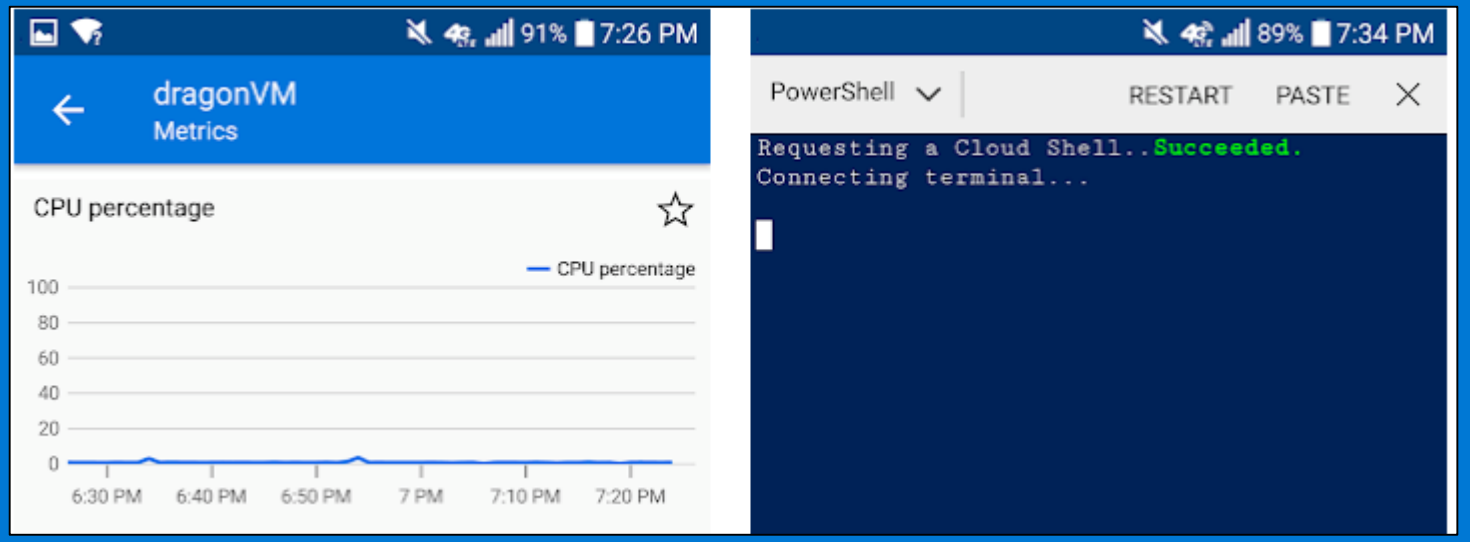
Azure Portal

- Search resources, services, and docs
- Manage resources
- Create customized dashboards and favorites
- Access the Cloud Shell
- Receive notifications



Azure Mobile App

- Stay connected to the cloud
- Check status and critical metrics anytime, anywhere
- Diagnose and fix issues quickly
- Run commands to manage your Azure resources



Azure PowerShell

- PowerShell 5.1 on Windows - PowerShell 6.x and higher on all other platforms (Mac, Windows, Linux)
- Frequently Updated
- Lets you connect to your Azure subscription and manage resources
- Adds the Azure-specific commands – new Az module
- Available inside a browser via the Azure Cloud Shell
- Available as a local installation on Linux, macOS, or Windows
- Has an interactive and a scripting mode
- Works in Azure Cloud Shell

Install-Module -Name Az -AllowClobber -Scope AllUsers

Get-Command -Verb Get -Noun AzVM* -Module Az.Compute

CommandType	Name	Version	Source
Alias	Get-AzVmssDiskEncryptionStatus	3.3.0	Az.Compute
Alias	Get-AzVmssVMDiskEncryptionStatus	3.3.0	Az.Compute
Cmdlet	Get-AzVM	3.3.0	Az.Compute
Cmdlet	Get-AzVMAccessExtension	3.3.0	Az.Compute
Cmdlet	Get-AzVMADDomainExtension	3.3.0	Az.Compute
Cmdlet	Get-AzVMAEMExtension	3.3.0	Az.Compute
Cmdlet	Get-AzVMBootDiagnosticsData	3.3.0	Az.Compute
Cmdlet	Get-AzVMChefExtension	3.3.0	Az.Compute
Cmdlet	Get-AzVMCustomScriptExtension	3.3.0	Az.Compute
Cmdlet	Get-AzVMDiagnosticsExtension	3.3.0	Az.Compute
Cmdlet	Get-AzVMDiskEncryptionStatus	3.3.0	Az.Compute
Cmdlet	Get-AzVMDscExtension	3.3.0	Az.Compute
Cmdlet	Get-AzVMDscExtensionStatus	3.3.0	Az.Compute
Cmdlet	Get-AzVMExtension	3.3.0	Az.Compute
Cmdlet	Get-AzVMExtensionImage	3.3.0	Az.Compute
Cmdlet	Get-AzVMExtensionImageType	3.3.0	Az.Compute
Cmdlet	Get-AzVMImage	3.3.0	Az.Compute
Cmdlet	Get-AzVMImageOffer	3.3.0	Az.Compute
Cmdlet	Get-AzVMImagePublisher	3.3.0	Az.Compute
Cmdlet	Get-AzVMImageSku	3.3.0	Az.Compute
Cmdlet	Get-AzVMRunCommandDocument	3.3.0	Az.Compute
Cmdlet	Get-AzVMSize	3.3.0	Az.Compute
Cmdlet	Get-AzVMSqlServerExtension	3.3.0	Az.Compute
Cmdlet	Get-AzVmss	3.3.0	Az.Compute
Cmdlet	Get-AzVmssDiskEncryption	3.3.0	Az.Compute
Cmdlet	Get-AzVmssRollingUpgrade	3.3.0	Az.Compute
Cmdlet	Get-AzVmssSku	3.3.0	Az.Compute
Cmdlet	Get-AzVmssVM	3.3.0	Az.Compute
Cmdlet	Get-AzVmssVMDiskEncryption	3.3.0	Az.Compute
Cmdlet	Get-AzVMUsage	3.3.0	Az.Compute

https://docs.microsoft.com/it-it/powershell/azure/get-started-azureps?view=azps-3.3.0

Azure CLI

- Cross-platform command-line program
- Runs on Linux, macOS, and Windows
- Can be used interactively or through scripts
- Commands are structured in _groups_ and _subgroups_
- Use find to locate commands
- Use --help for more detailed information

Install or update

The MSI distributable is used for installing or updating the Azure CLI on Windows. You don't need to uninstall any current versions before using the MSI installer.

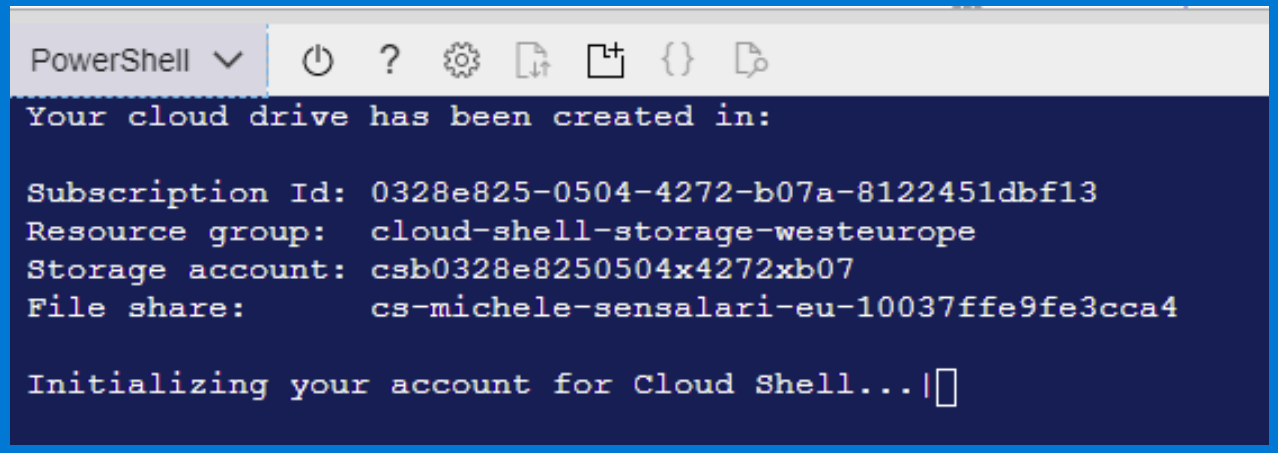
Download the MSI installer

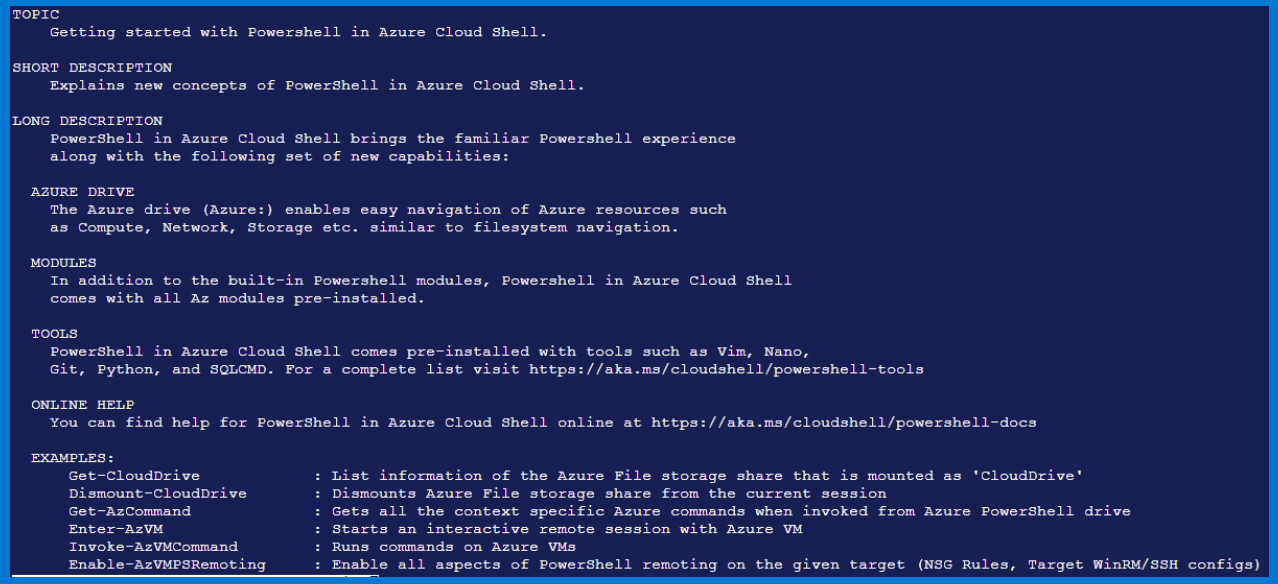
```
C:\Users\MicheleSensalari>az login
You have logged in. Now let us find all the subscriptions to which you have access...
```

```
C:\Users\MicheleSensalari>az find -h

Command
    az find : I'm an AI robot, my advice is based on our Azure documentation as well as the usage
    patterns of Azure CLI and Azure ARM users. Using me improves Azure products and documentation.

Arguments

Positional
    <CLI_TERM>  : An Azure CLI command or group for which you need an example.

Global Arguments
    --debug     : Increase logging verbosity to show all debug logs.
    --help -h   : Show this help message and exit.
    --output -o : Output format.  Allowed values: json, jsonc, none, table, tsv, yaml.  Default:
                  json.
    --query     : JMESPath query string. See http://jmespath.org/ for more information and examples.
    --verbose   : Increase logging verbosity. Use --debug for full debug logs.

Examples
    Give me any Azure CLI group and I'll show the most popular commands within the group.
        az find "az storage"


    Give me any Azure CLI command and I'll show the most popular parameters and subcommands.
        az find "az monitor activity-log list"


    You can also enter a search term, and I'll try to help find the best commands.
        az find "arm template"


For more specific examples, use: az find "az find"

Please let us know how we are doing: https://aka.ms/clihats
```

Azure Cloud Shell

- **Azure Cloud Shell** is a Interactive browser-based shell experience to manage and develop Azure resources.
- Offers either Bash or PowerShell
- Is temporary and provided on a per-session, per-user basis
- Requires a resource group, storage account, and Azure File share
- Authenticates automatically
- Integrated graphical text editor
- Is assigned one machine per user account
- Times out after 20 minutes





Azure Virtual Network

Resource Group

- Logical collection of resources.
- Resources can only exist in one resource group.
- Resource Groups cannot be renamed.
- Resource Groups can have resources of many different types (services).
- Resource Groups can have resources from many different regions.
- All the resources in your group should share the same lifecycle. You deploy, update, and delete them together. If one resource, such as a database server, needs to exist on a different deployment cycle it should be in another resource group.

- Each resource can only exist in one resource group.
- You can add or remove a resource to a resource group at any time.
- You can move a resource from one resource group to another group.
- A resource group can contain resources that reside 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. This interaction is common when the two resources are related but don't share the same lifecycle (for example, web apps connecting to a database).
- When creating a resource group, you need to provide a location for that resource group - Metadata

The Azure Virtual Network

- Azure Virtual Network enables you to create **private networks in the cloud** with full control over IP addresses, DNS servers, security rules, and traffic flows
- Virtual network names **must be unique within a resource group** but can be duplicated between a subscription or Azure region

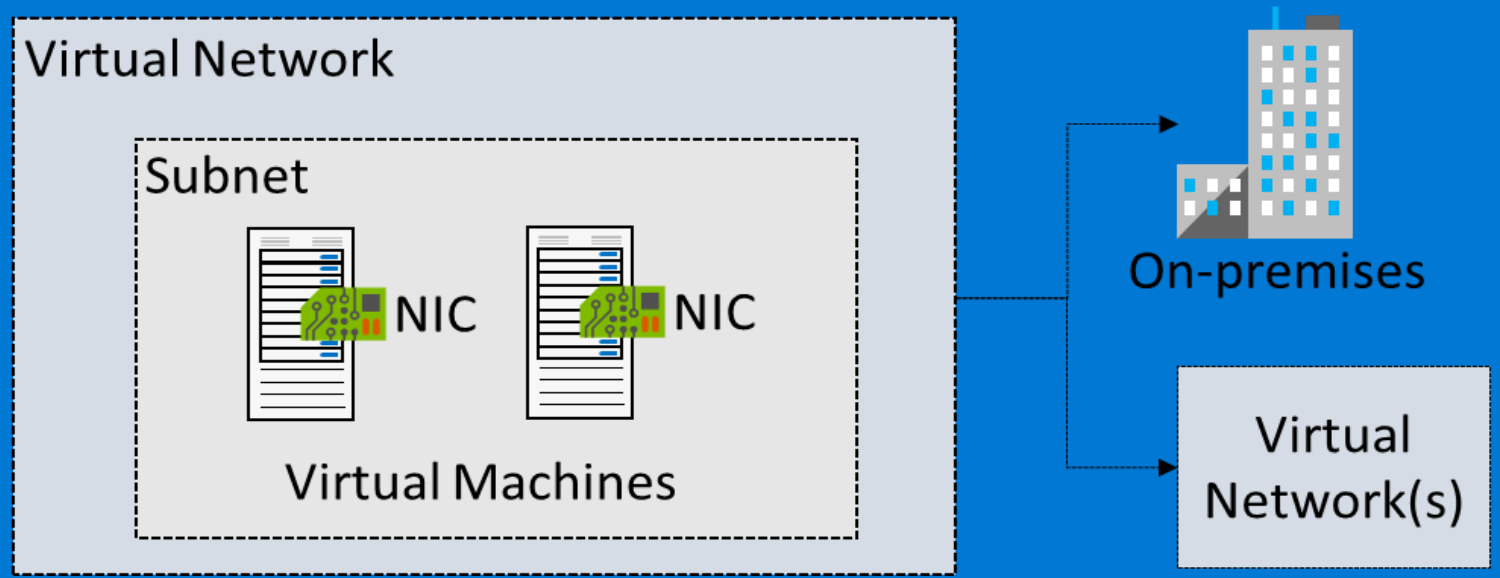
Regions

A **region** is an Azure data center within a specific geographic location. All Azure resources are created in an Azure region and subscription

A **resource** can only be created in a virtual network that exists in the same **region and subscription** as the resource

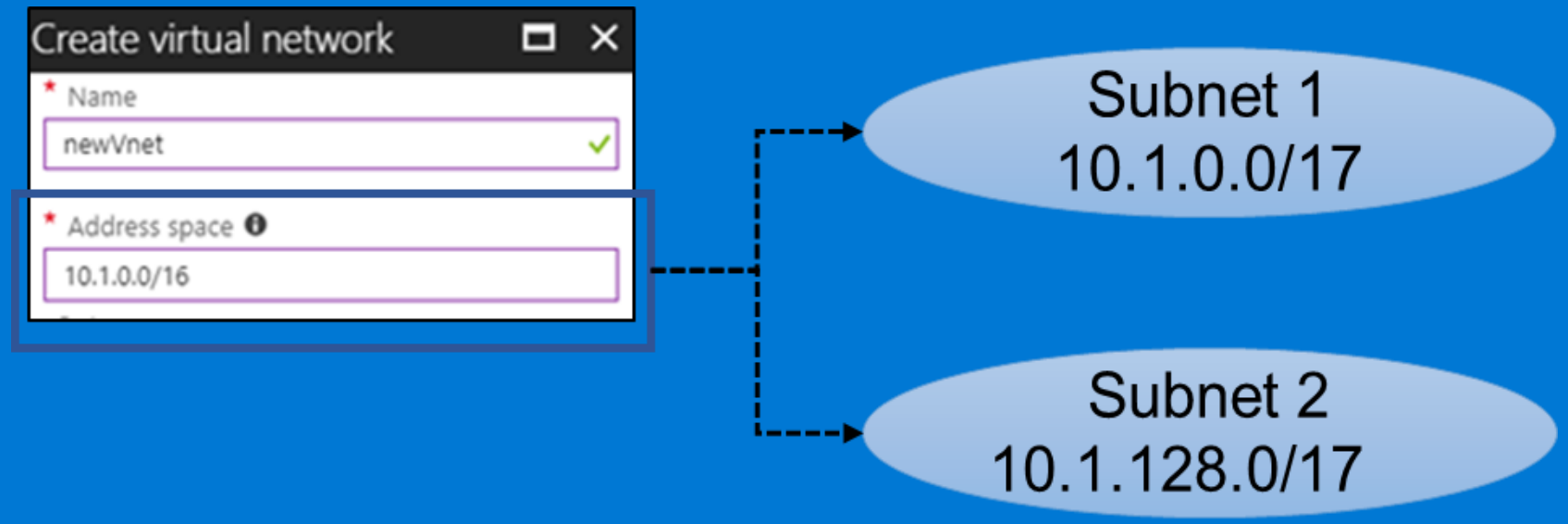
You can however, **connect virtual networks** that exist in different subscriptions and regions

Virtual Networks



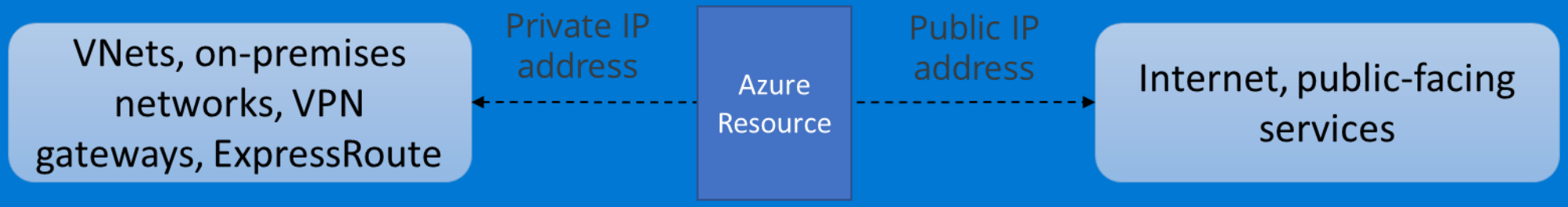
- Logical representation of your own network
- Create a dedicated private cloud-only VNet
- Securely extend your datacenter With VNets
- Enable hybrid cloud scenarios

Subnets



- A virtual network can be segmented into one or more subnets
- Subnets provide logical divisions within your network
- Subnets can help improve security, increase performance, and make it easier to manage the network
- Each subnet must have a unique address range - cannot overlap with other subnets in the virtual network in the subscription

IP Addressing



- **Private IP addresses** are used within an Azure virtual network (VNet), and your on-premises network, when you use a VPN gateway or ExpressRoute circuit to extend your network to Azure
- **Public IP addresses** is used for communication with the Internet, including Azure public-facing services

Public IP Addresses

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

A public IP address resource can be associated with virtual machine network interfaces, internet-facing load balancers, VPN gateways, and application gateways.

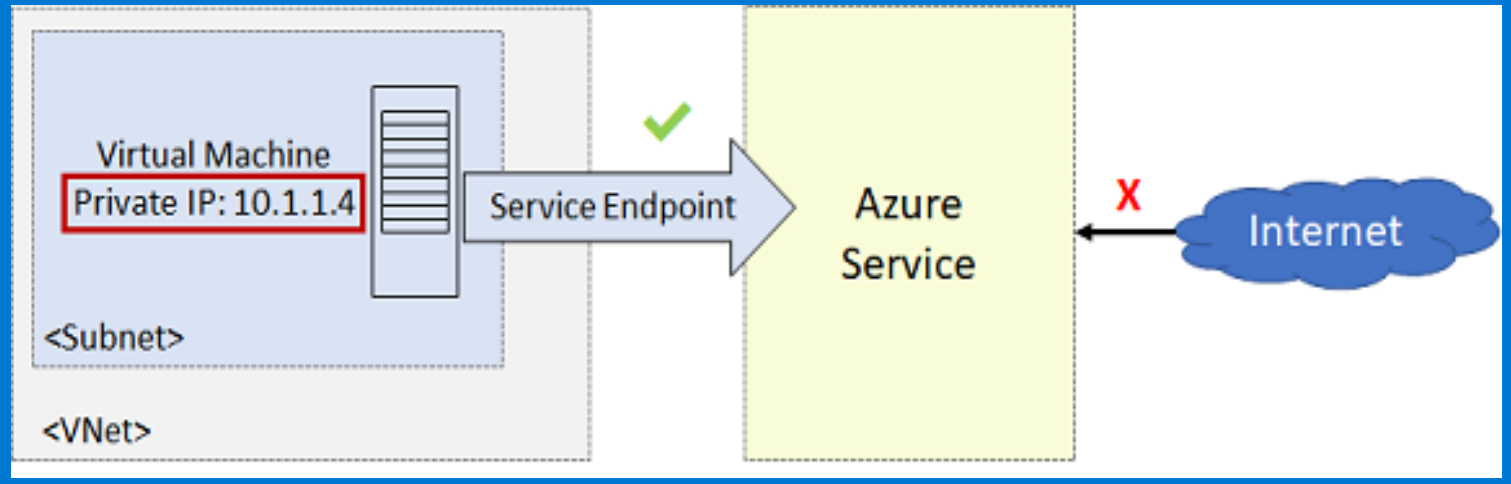
Private IP Addresses

Private IP Addresses	IP address association	Dynamic	Static
Virtual Machine	NIC	Yes	Yes
Internal Load Balancer	Front-end configuration	Yes	Yes
Application Gateway	Front-end configuration	Yes	Yes

Dynamic (default). Azure assigns the next available unassigned or unreserved IP address in the subnet's address range

Static. You select and assign any unassigned or unreserved IP address in the subnet's address range

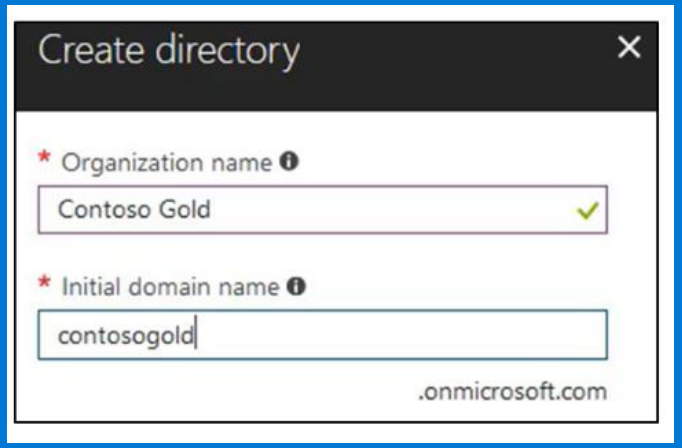
Service Endpoints

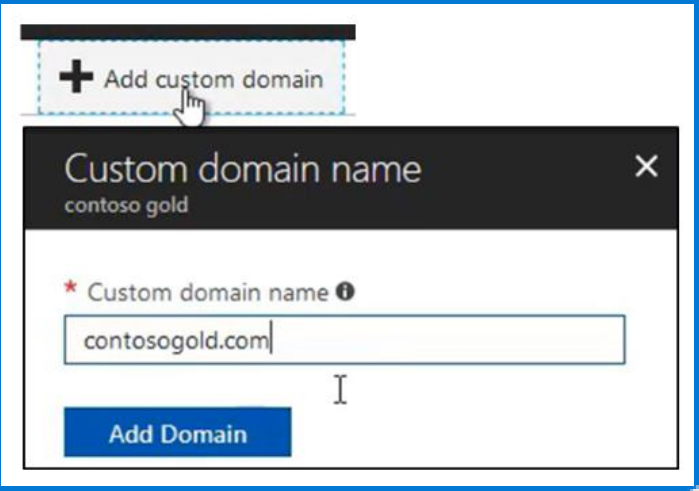


- Endpoints limit network access to specific subnets and IP addresses
- Improved security for your Azure service resources
- Optimal routing for Azure service traffic from your virtual network
- Endpoints use the Microsoft Azure backbone network
- Simple to set up with less management overhead

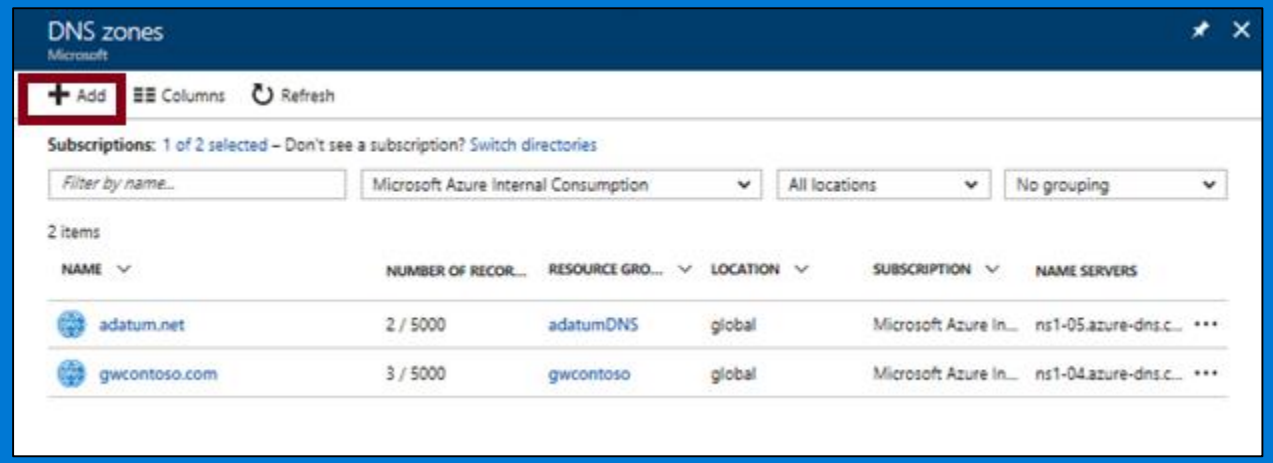
Domains and Custom Domains

- When you create an Azure subscription an Azure AD domain is created for you
- The domain has initial domain name in the form *domainname.onmicrosoft.com*
- You can customize/change the name
- After the custom name is added it must be verified



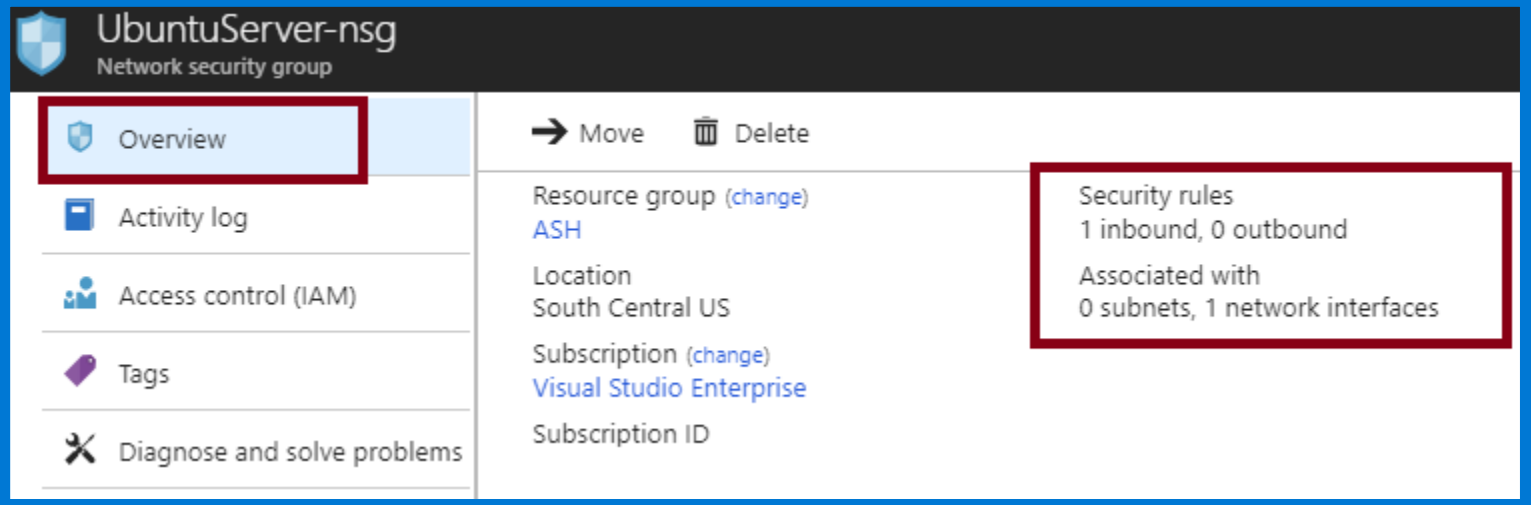


Azure DNS Zones



- A DNS zone hosts the DNS records for a domain
- The name of the zone must be unique within the resource group
- Where multiple zones share the same name, each instance is assigned different name server addresses
- Only one set of addresses can be configured with the domain name registrar

Network Security Groups (NSG)



- You can limit network traffic to resources in a virtual network using a NSG
- A NSG contains a list of security rules that allow or deny inbound or outbound network traffic
- An NSG can be associated to a subnet or a network interface

VPN Connections—Hybrid Networking Scenarios

Cloud		Customer	Segment & workloads
	Secure point-to-site connectivity Virtual network (Point-to-Site)		• **Developers** • Small scale deployments • Connect from anywhere
	Secure site-to-site VPN connectivity Virtual network (Site-to-Site)		• **SMB, Enterprises** • Connect to Azure compute • IaaS and PaaS workloads
	Private site-to-site connectivity ExpressRoute		• **SMB & Enterprises** • Mission critical workloads • Backup/DR, media, HPC • Connect to all hardware

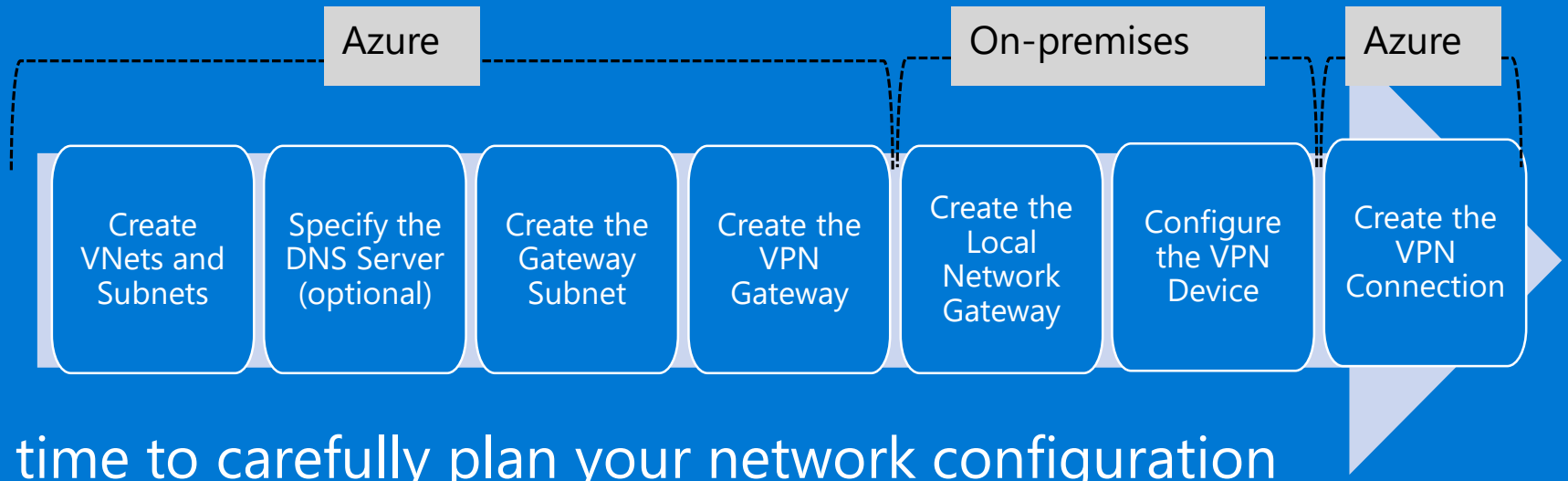
Site-to-Site VPN to Azure VNet (VPN Gateway)

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

You can also use a VPN gateway to send encrypted traffic between Azure virtual networks over the **Microsoft network**

Each virtual network can only have **one VPN gateway**, but you can create multiple connections to the same gateway

Implement VNet-to-VNet Connections



- Take time to carefully plan your network configuration
- The on-premises part is necessary only if you are configuring Site-to-Site
- Always verify and test your connections

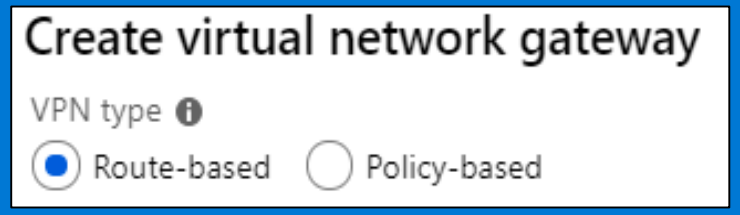
Gateway SKUs

SKU	S2S/VNet-to-VNet Tunnels	P2S SSTP Connections	P2S IKEv2 Connections	Aggregate Throughput Benchmark
Basic	Max. 10	Max. 128	Not Supported	100 Mbps
VpnGw1	Max. 30	Max. 128	Max. 250	650 Mbps
VpnGw2	Max. 30	Max. 128	Max. 500	1 Gbps
VpnGw3	Max. 30	Max. 128	Max. 1000	1.25 Gbps

✔ **The Basic SKU is considered a legacy SKU**

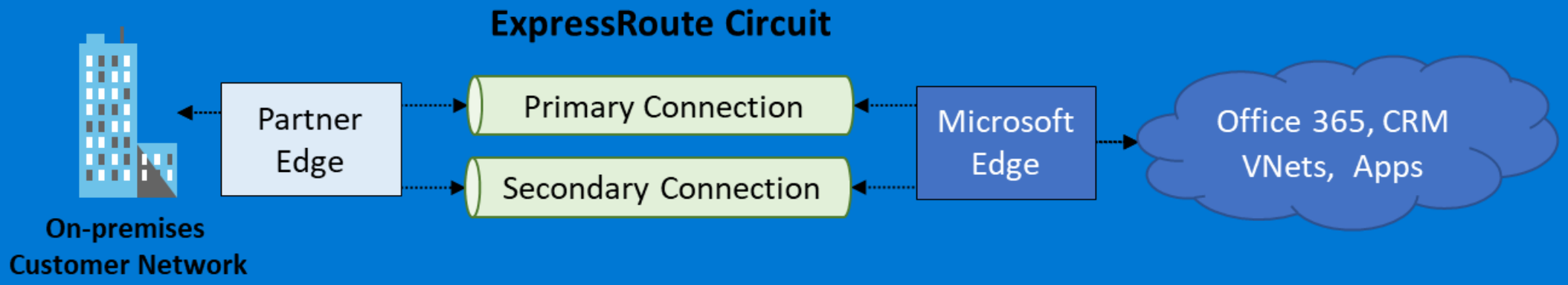
VPN Types

- Policy-based VPNs encrypt and direct packets through IPsec tunnels based on the IPsec policies
  - Can only be used on the Basic gateway SKU
  - You can have only 1 tunnel
  - You can only use Policy-based VPNs for S2S connections
- Route-based VPNs use *routes* in the IP forwarding or routing table to direct packets



Most VPN Gateway configurations require a Route-based VPN

What is Azure ExpressRoute?



Use Azure ExpressRoute to **create private connections between Azure data centers and infrastructure on your environment**. ExpressRoute connections don't go over the public Internet, and they offer more reliability, faster speeds and lower latencies than typical Internet connections

ExpressRoute or Site-to-Site VPN Gateway?

- ExpressRoute is a direct, private connection from your WAN to Microsoft Services
- ExpressRoute is a direct, private connection from your WAN to Microsoft Services
- A VPN Gateway has bandwidth is typically capped at under 1Gbps aggregate, whereas ExpressRoute can go all the way up to 10Gbps
- Pricing varies depending on the service you choose

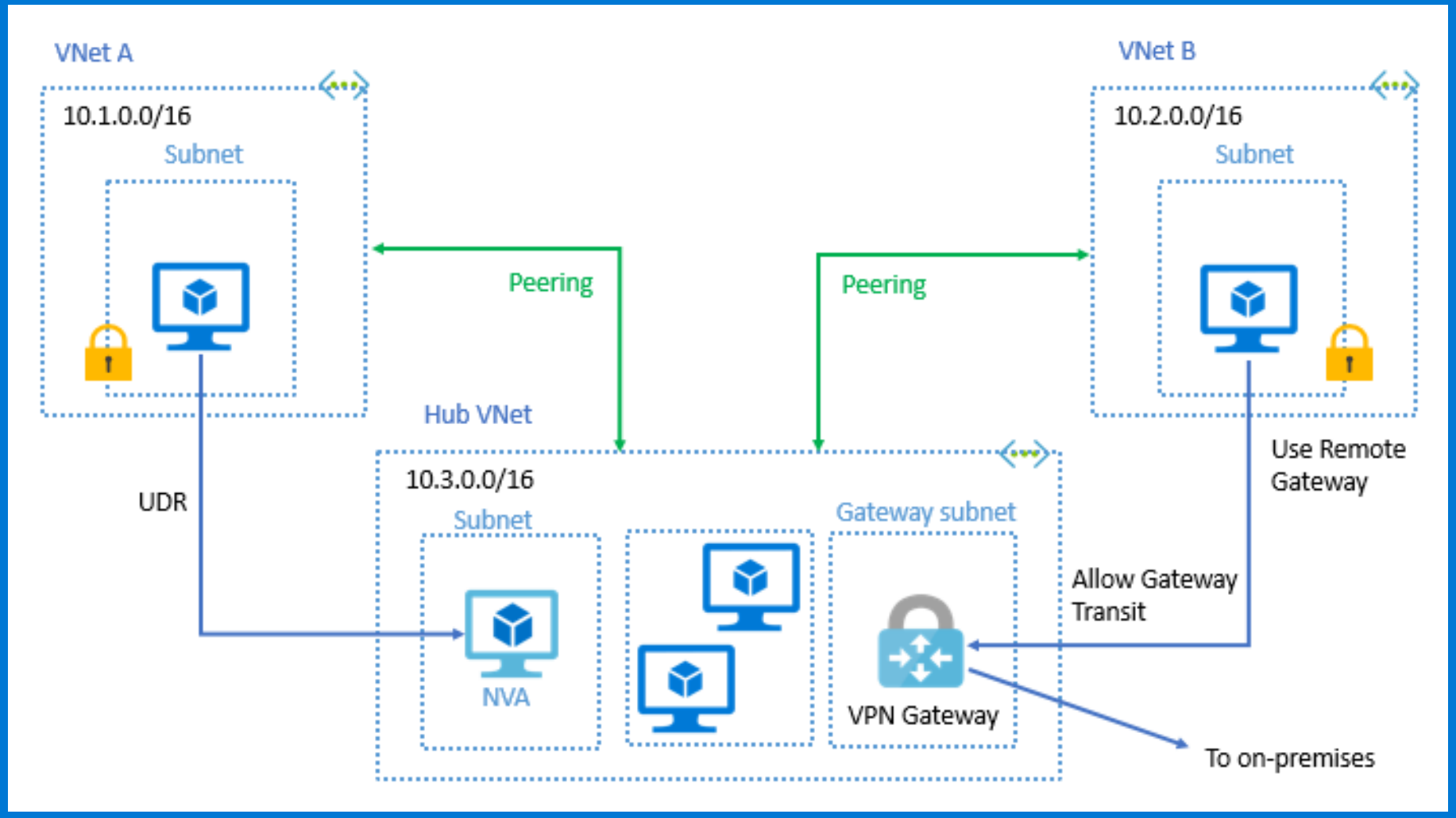
Virtual Network to Virtual Network (VNet Peering)

Virtual network peering enables you to seamlessly connect two Azure virtual networks. Once peered, the virtual networks appear as one, for connectivity purposes

- VNet peering—connecting VNets within the same Azure region
- Global VNet peering—connecting VNets across Azure regions

After virtual networks are peered, resources in either virtual network can directly connect with resources in the peered virtual network

VNet Peering



Azure Load Balancer

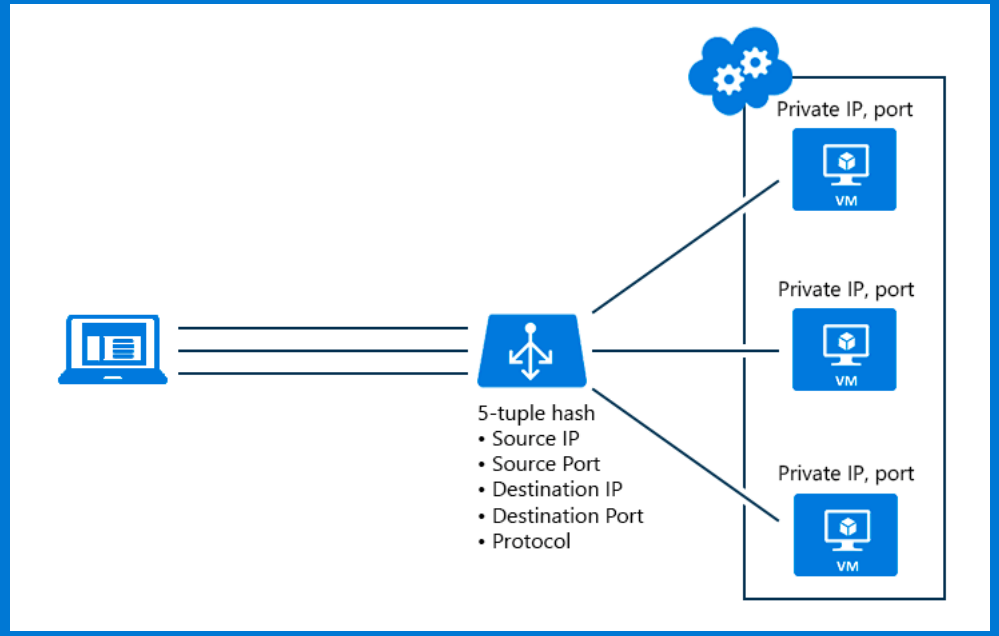
Allows you to scale your applications and create **high availability** and **resiliency** for your services and applications

Public

A public Load Balancer maps the public IP address and port number of incoming traffic to the private IP address and port number of the VM and vice versa.

Internal

An internal Load Balancer directs traffic only to resources that are inside a virtual network or that use a VPN to access Azure infrastructure.



Public Load Balancer

A public Load Balancer maps the **public IP address** and port number of incoming traffic to the **private IP address** and port number of the VM

Automatic reconfiguration

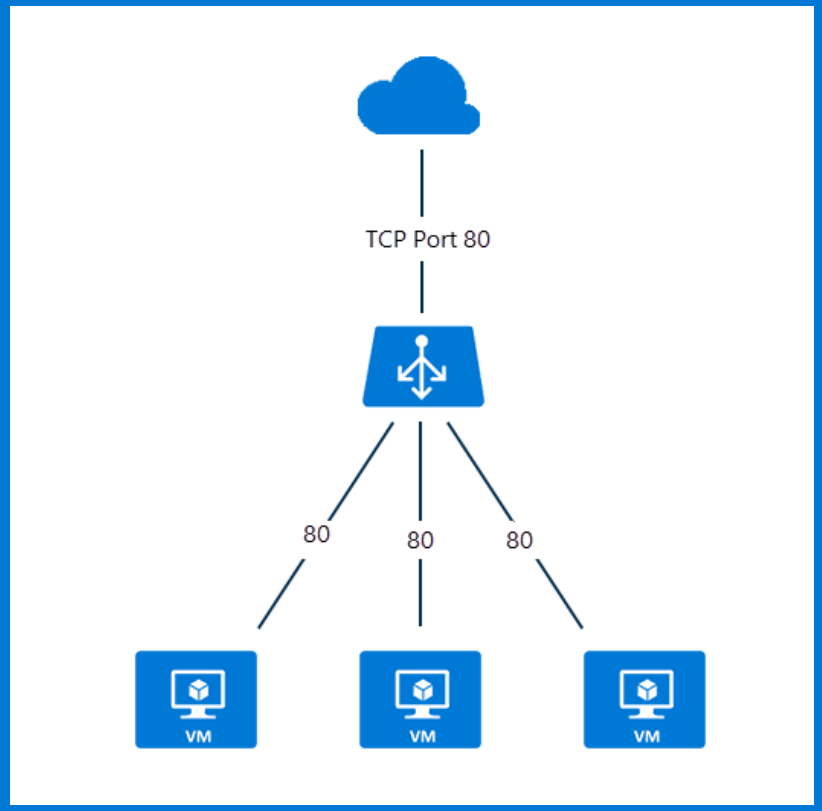
Instantly reconfigures itself as you scale instance up or down

Outbound connections (SNAT)

All outbound flows from private IP addresses inside your virtual network to public IP addresses on the internet can be translated to a frontend IP address of the Load Balancer

Default Distribution Mode

Azure Load Balancer distributes traffic evenly amongst multiple VM instance



Internal Load Balancer

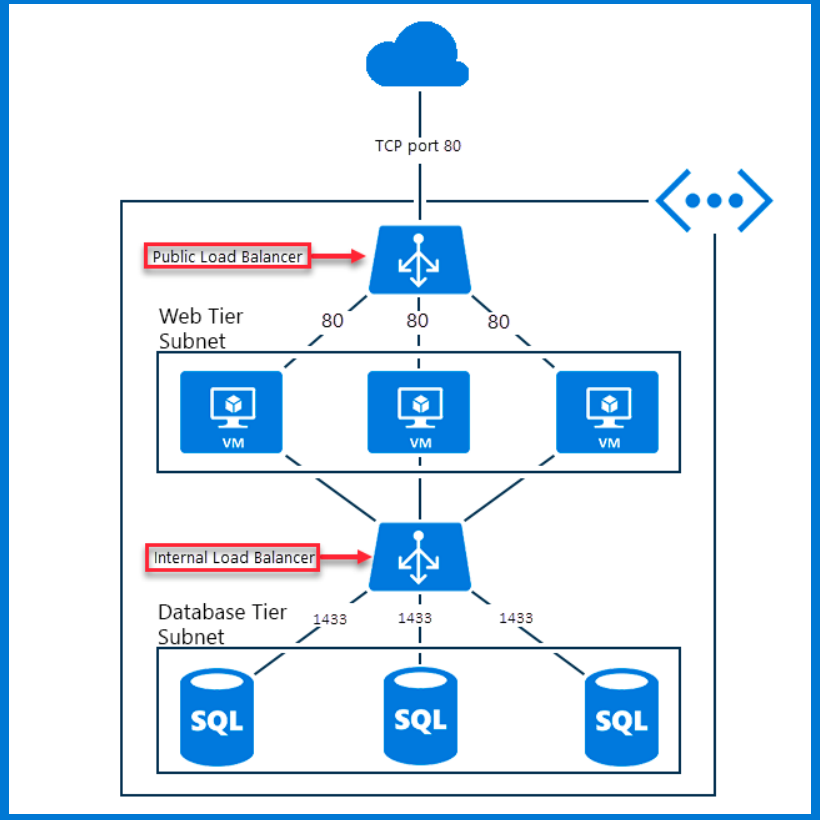
An internal Load Balancer directs traffic only to resources **inside a virtual network** or that use a VPN to access Azure infrastructure

Within a virtual network

Cross-premises virtual network

Multi-tier applications

Line-of-business applications



Azure Traffic Manager

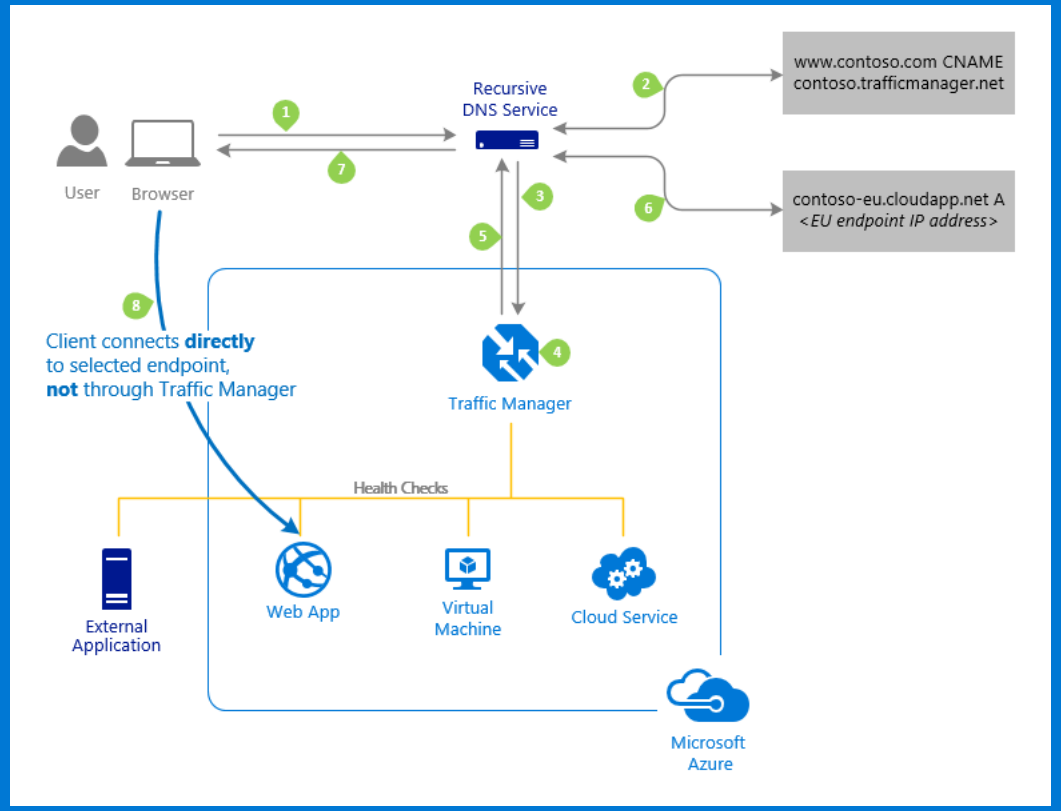
Azure Traffic Manager is a **DNS-based traffic load balancer** that enables you to distribute traffic optimally to services across global Azure regions

Global DNS load balancing

Automatic failover when an endpoint goes down

Combine with hybrid applications
Supports external, non-Azure endpoints so that it can be used with hybrid cloud and on-premises deployments

Distribute traffic for complex deployments
Use nested Traffic Manager profiles for sophisticated, flexible rules for complex deployments



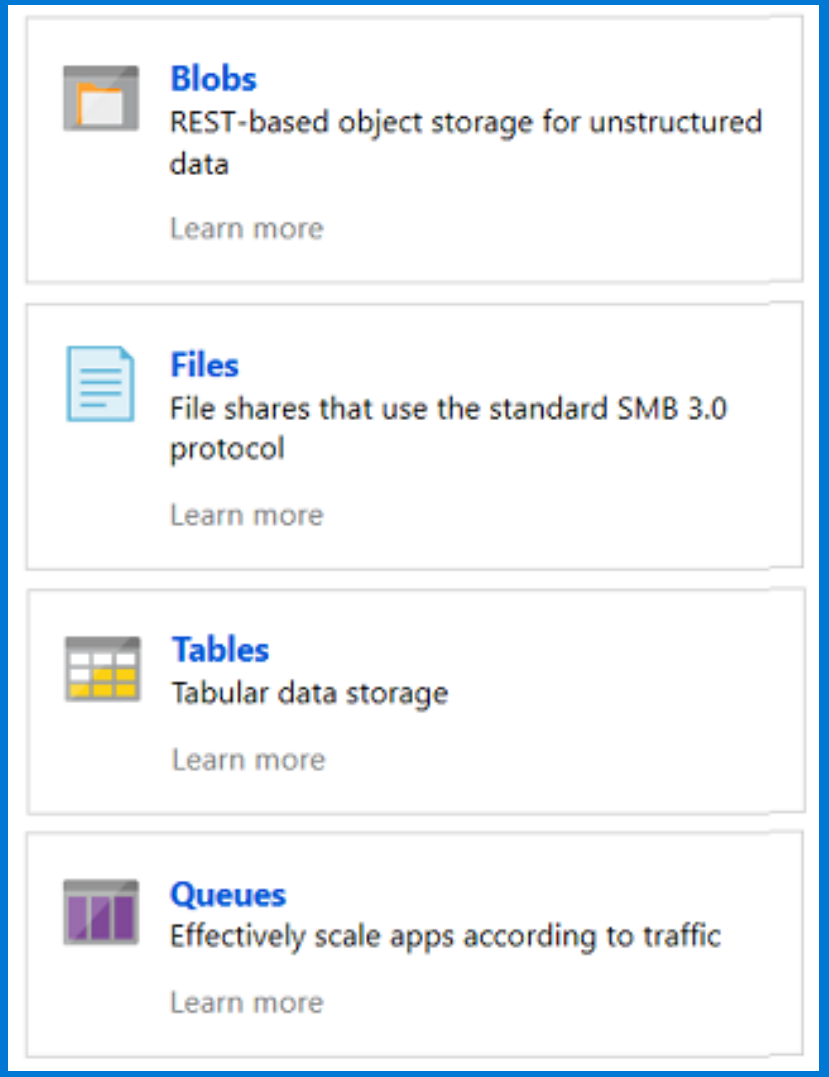
Azure Storage

Azure Storage

- A service that you can use to store files, messages, tables, and other types of information
- Durable, secure, scalable, managed, accessible
- Manage data with multiple storage accounts
- Three categories of Azure storage:
  - Storage for virtual machines – Disks and File Shares
  - Unstructured data – Blobs and Data Lake Store
  - Structured data - Tables, Cosmos DB, and Azure SQL DB
- Standard storage backed by magnetic drives (HDD) is lowest cost
- Premium storage backed by solid state drives (SSD)

Azure Storage Services

- **Azure Blobs**: A massively scalable object store for text and binary data
- **Azure Files**: Managed file shares for cloud or on-premises deployments
- **Azure Tables**: A NoSQL store for schema less storage of structured data
- **Azure Queues**: A messaging store for reliable messaging between application components



Storage Account Types

Storage account type	Supported services	Supported tiers	Replication options
Blob storage	Blob (block blobs and append blobs only)	Standard	LRS, GRS, RA-GRS
General-purpose V2	Blob, File, Queue, Table, and Disk	Standard, Premium	LRS, GRS, RA-GRS, ZRS, ZGRS (preview), RA-ZGRS (preview)
General-purpose V1	Blob, File, Queue, Table, and Disk	Standard, Premium	LRS, GRS, RA-GRS
Block blob storage	Blob (block blobs and append blobs only)	Premium	LRS
File Storage	Files only	Premium	LRS

✔ All storage accounts are encrypted using Storage Service Encryption (SSE) for data at rest

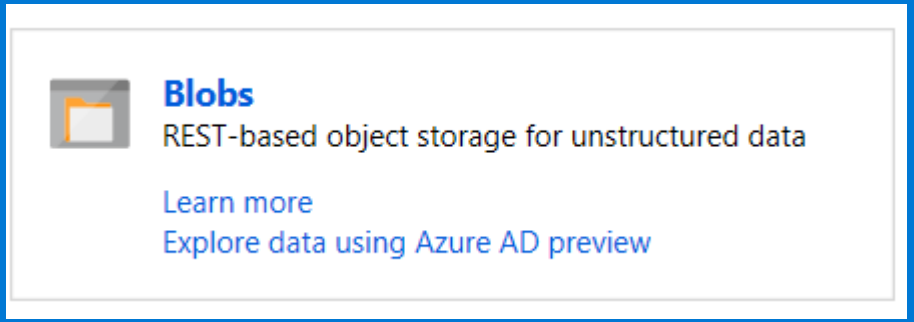
Accessing Storage

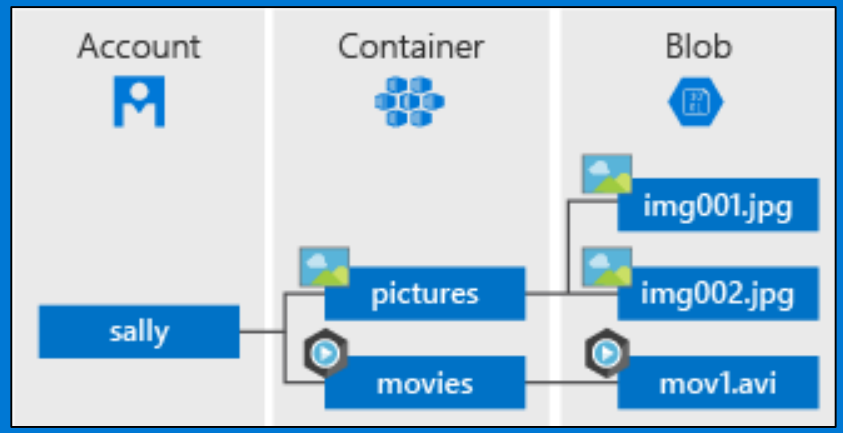
CNAME record	Target
blobs.contoso.com	contosoblobs.blob.core.windows.net

- Every object has a unique URL address
- The storage account name forms the subdomain of that address
- The subdomain and domain name forms an *endpoint*
  - **Blob service**: http://*mystorageaccount*.blob.core.windows.net
  - **Table service**: http://*mystorageaccount*.table.core.windows.net
  - **Queue service**: http://*mystorageaccount*.queue.core.windows.net
  - **File service**: http://*mystorageaccount*.file.core.windows.net
- If you prefer you can configure a custom domain name

Blob Storage

- Stores unstructured data in the cloud
- Can store any type of text or binary data
- Also referred to as *object storage*
- Common uses:
  - Serving images or documents directly to a browser
  - Storing files for distributed access
  - Streaming video and audio
  - Storing data for backup and restore, disaster recovery, archiving
  - Storing data for analysis by an on-premises or Azure-hosted service

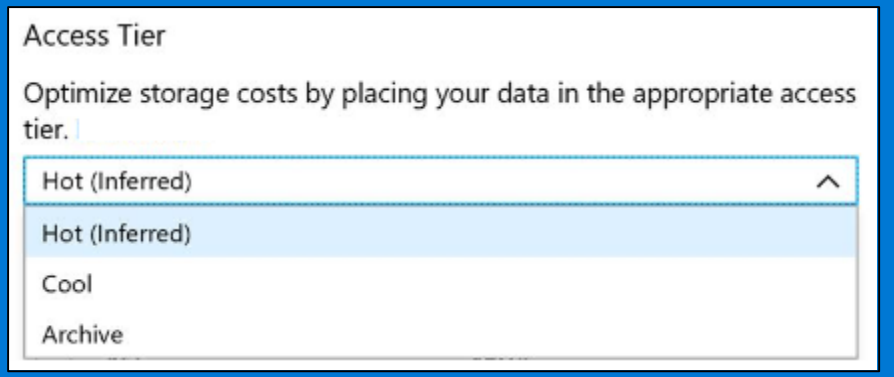




Blob Performance Tiers

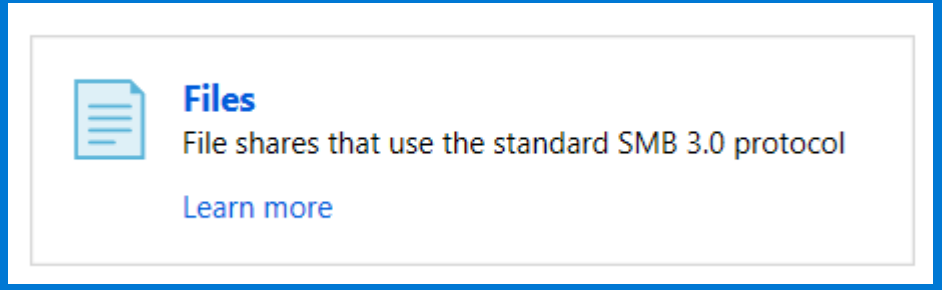
- **Hot tier** - Optimized for frequent access of objects in the storage account
- **Cool tier** - Optimized for storing large amounts of data that is infrequently accessed and stored for at least 30 days
- **Archive** - Optimized for data that can tolerate several hours of retrieval latency and will remain in the Archive tier for at least 180 days

✔ You can switch between these access tiers at any time.



Azure Files

- **Managed file shares in the cloud that are accessible via SMB**
- **Common uses:**
  - Replace and supplement
  - Lift and shift
  - Azure File Sync
  - Shared applications
  - Diagnostic data
  - Tools and utilities



Files vs Blobs

Feature	Description	When to use
Azure Files	SMB interface, client libraries, and a REST interface that allows access from anywhere to stored files.	• Lift and shift an application to the cloud. • Store shared data across multiple virtual machines. • Store development and debugging tools that need to be accessed from many virtual machines.
Azure Blobs	Client libraries and a REST interface that allows unstructured data (flat namespace) to be stored and accessed at a massive scale in block blobs.	• Support streaming and random-access scenarios. • Access application data from anywhere.

Azure Virtual Machine

Location and Pricing

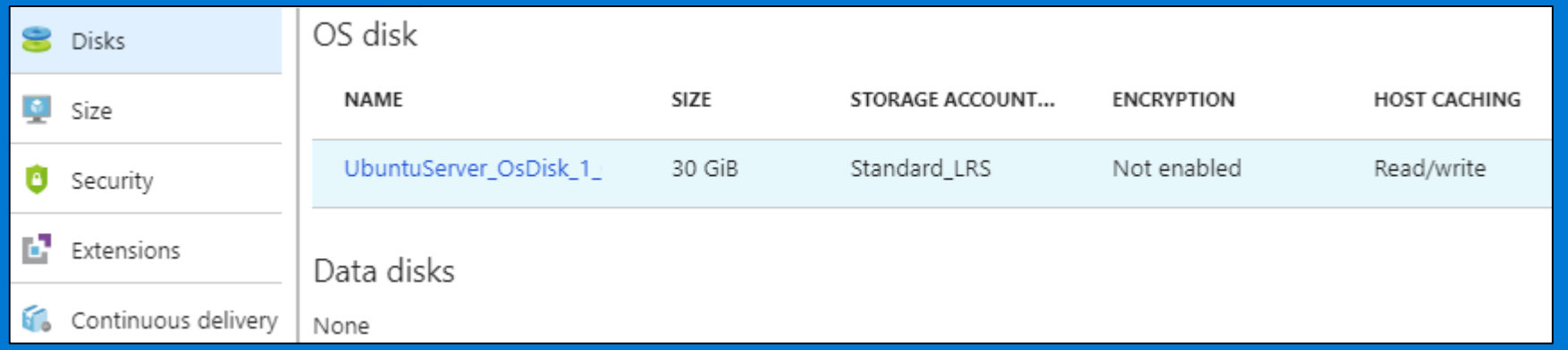
- Location
  - Each region has different hardware and service capabilities
  - Locate virtual machines as close as possible to your users
  - Locate virtual machines to ensure compliance and legal obligations
- Pricing
  - Compute costs
  - Storage costs (consumption-based and reserved instances)

54 Azure regions
Available in 140 countries

Virtual Machine Sizing

VM Type	Sizes	Purpose
General Purpose	B, Dsv3, Dv3, DSv2, Dv2, Av2, DC	Testing and development, small to medium databases, and low to medium traffic web servers.
Compute Optimized	Fsv2, Fs, F	Medium traffic web servers, network appliances, batch processes, and application servers.
Memory Optimized	Esv3, Ev3, M, GS, G, DSv2, Dv2	Relational database servers, medium to large caches, and in-memory analytics.
Storage Optimized	Lsv2, Ls	Ideal for VMs running databases.
GPU	NV, NVv2, NC, NCv2, NCv3, ND, NDv2 (Preview)	Ideal for model training and inferencing with deep learning.
High Performance Compute	H	Fastest and most powerful CPU virtual machines with optional high-throughput network interfaces.

Virtual Machine Disks



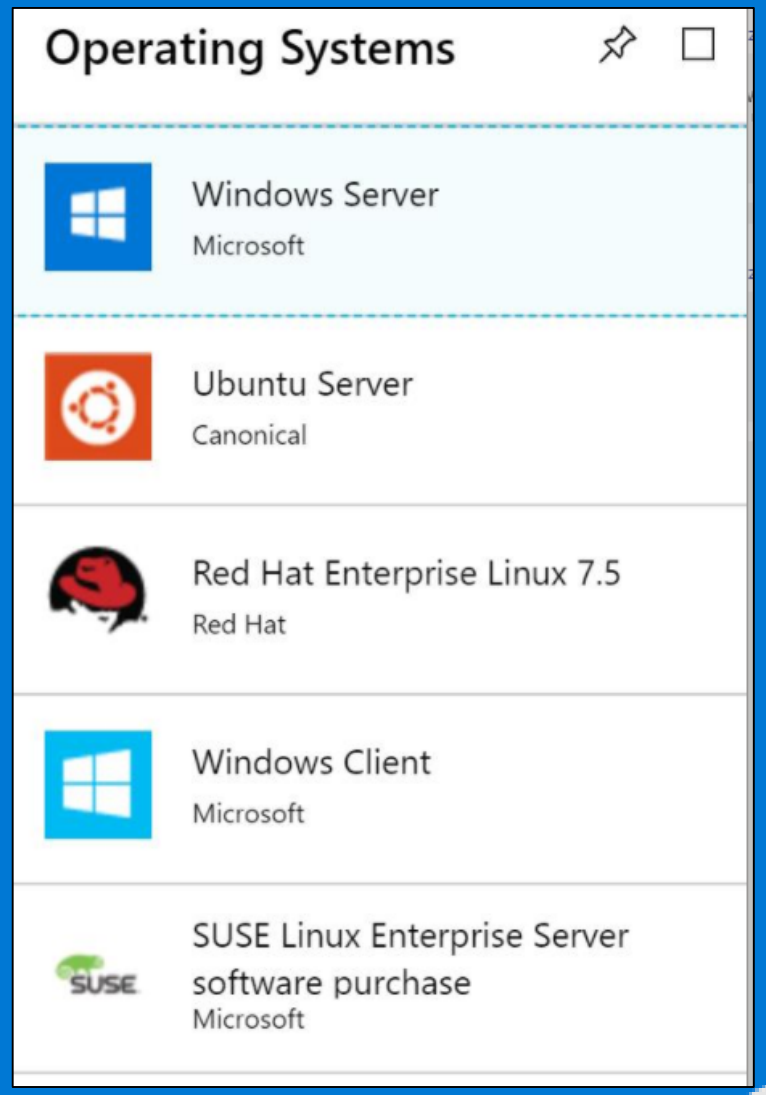
- **Operating System Disks** are SATA drives, labeled as C:
- **Temporary Disks** provides short term storage
- **Data Disks** are SCSI drives and depend on your virtual machine type

Storage Options

- Premium storage offers high-performance, low-latency SSD disk support
- Use premium storage for virtual machines with input/output (I/O)-intensive workloads
- Two types of disks: Unmanaged and Managed
  - Unmanaged disks require you to manage the storage accounts and VHDs
  - Managed disks are maintained by Azure (recommended)

Supported Operating Systems

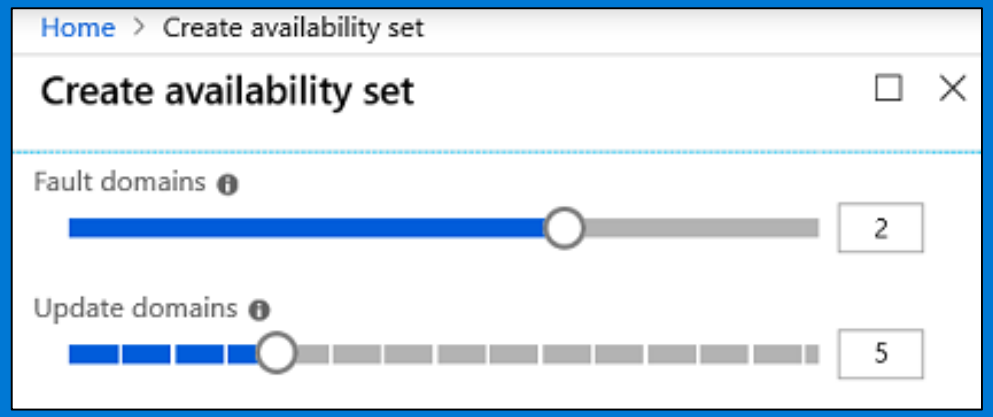
- Windows Server includes many common products, requires a license, doesn't support OS upgrades
- Linux distributions are supported, upgrade of the OS is supported



Maintenance vs. Downtime

- When the platform predicts a failure, it will issue an **unplanned hardware maintenance** event. Action: Live migration.
- **Unexpected Downtime** is when a virtual machine fails unexpectedly. Action: Automatically migrate (heal).
- **Planned Maintenance** events are periodic updates made to the Azure platform. Action: No action.

Availability Sets

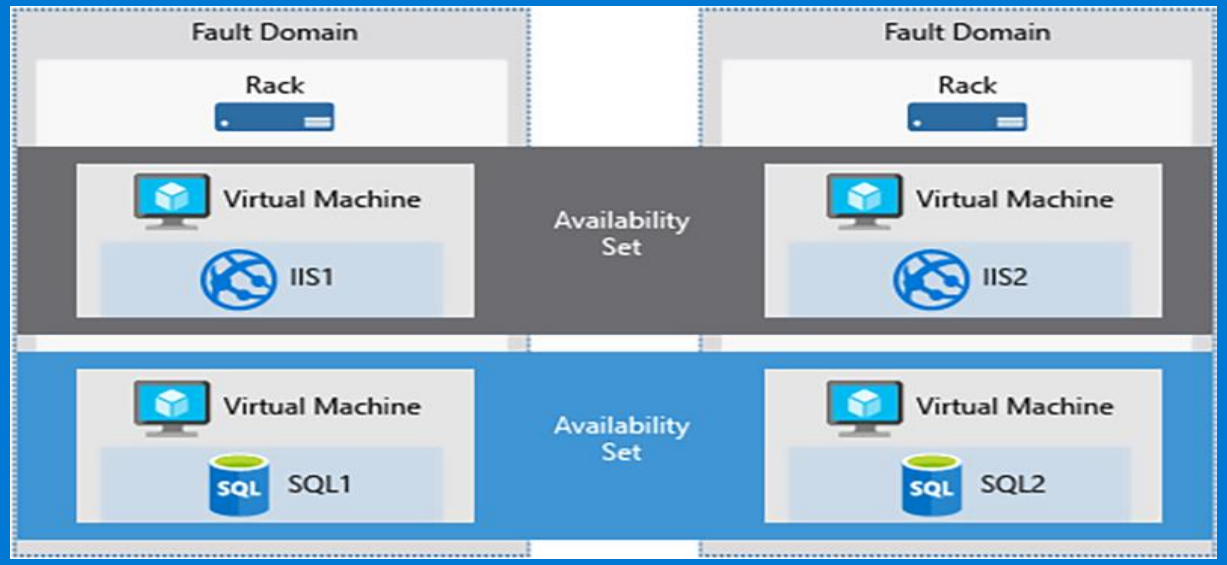


Two or more instances in two or more availability zones = 99.99% uptime

- Configure multiple virtual machines in an Availability Set
- Configure each application tier into separate Availability Sets
- Combine a Load Balancer with Availability Sets
- Use managed disks with the virtual machines

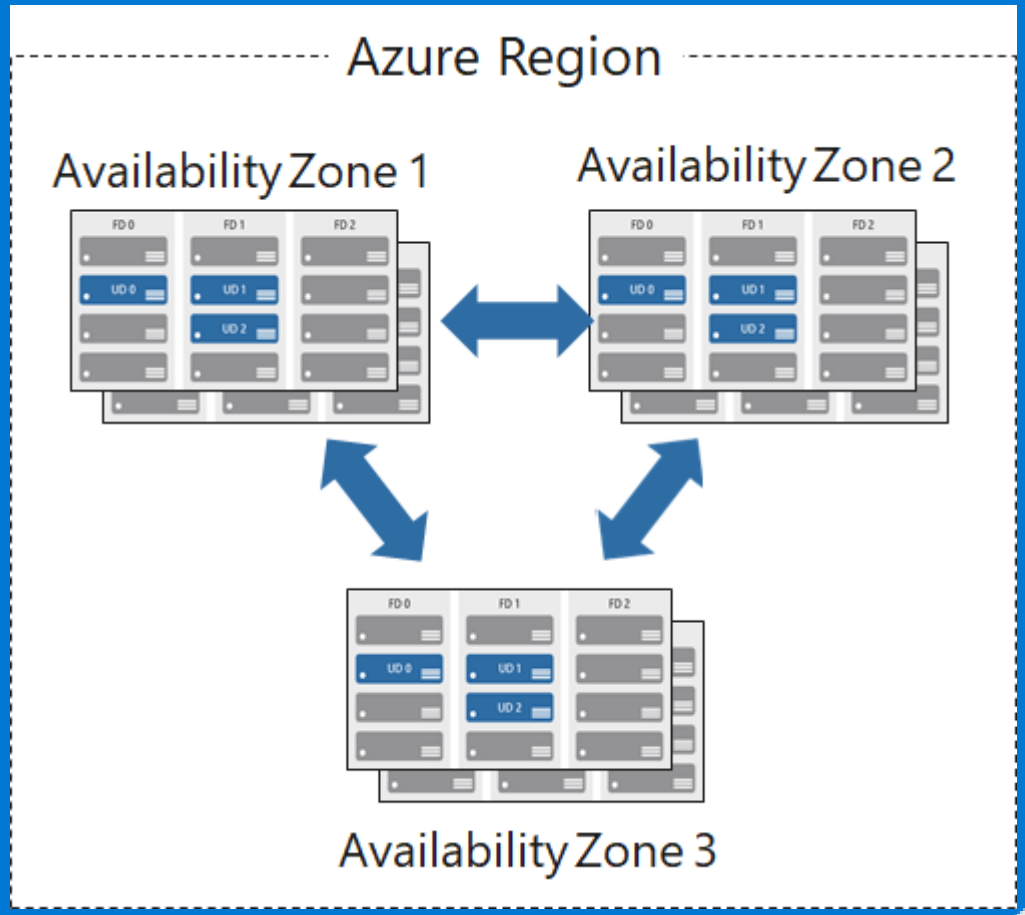
Update and Fault Domains

- **Update domains** lets Azure to perform incremental or rolling upgrades across a deployment. During planned maintenance, only one update domain is rebooted at a time.
- **Fault Domains** are a group of virtual machines that share a common set of hardware, switches, that share a single point of failure. VMs in an availability set are placed in at least two fault domains.

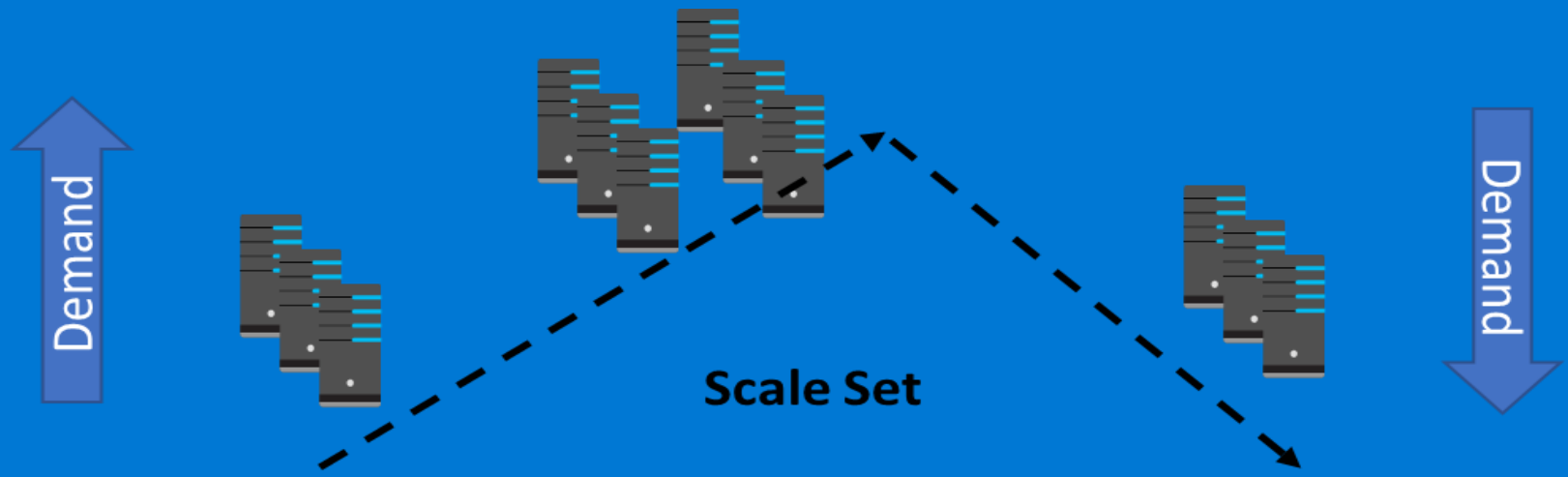


Availability Zones

- Unique physical locations in a region
- Includes datacenters with independent power, cooling, and networking
- Protects from datacenter failures
- Combines update and fault domains



Scale Sets



- Scale sets deploy a set of **identical** VMs
- No pre-provisioning of VMs is required
- As demand goes up VMs are added
- As demand goes down VM are removed
- The process can be manual, automated, or a combination of both

Azure Spot Instance (Preview)

- Using Spot VMs allows you to take advantage of our unused capacity at a significant cost savings. At any point in time when Azure needs the capacity back, the Azure infrastructure will evict Spot VMs. Therefore, Spot VMs are great for workloads that can handle interruptions like batch processing jobs, dev/test environments, large compute workloads, and more.
- The amount of available capacity can vary based on size, region, time of day, and more. When deploying Spot VMs, Azure will allocate the VMs if there is capacity available, but there is no SLA for these VMs. A Spot VM offers no high availability guarantees. At any point in time when Azure needs the capacity back, the Azure infrastructure will evict Spot VMs with 30 seconds notice.

https://docs.microsoft.com/en-us/azure/virtual-machines/linux/spot-vms

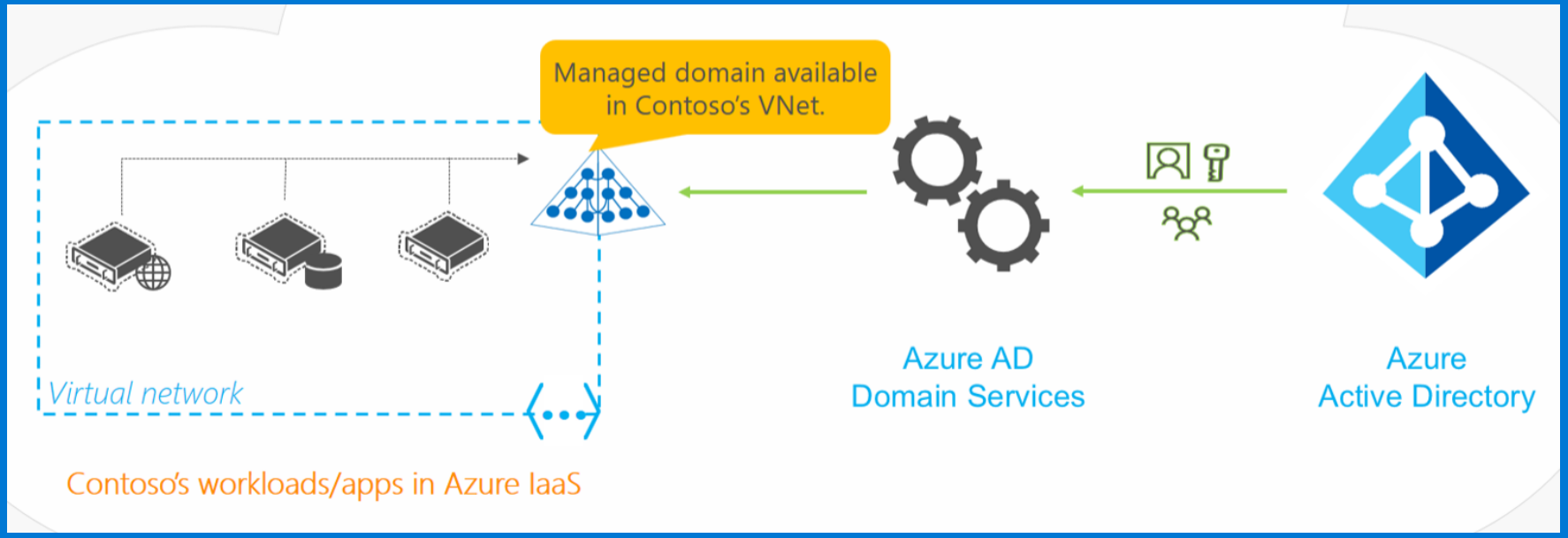
Active Directory -> Azure AD Domain Services

Azure Active Directory (AD) Domain Services

- Azure AD Domain Services provides managed domain services such as domain join, group policy, LDAP, Kerberos/NTLM authentication that are fully compatible with Windows Server Active Directory.
- You can consume these domain services without the need for you to deploy, manage, and patch domain controllers in the cloud.
- Azure AD Domain Services integrates with your existing Azure AD tenant, thus making it possible for users to log in using their corporate credentials. Additionally, you can use existing groups and user accounts to secure access to resources, thus ensuring a smoother 'lift-and-shift' of on-premises resources to Azure Infrastructure Services.
- Azure AD Domain Services functionality works seamlessly regardless of whether your Azure AD tenant is cloud-only or synced with your on-premises Active Directory

Azure Domain Services for Cloud Only Organizations

A cloud-only Azure AD tenant (often referred to as 'managed tenants') does not have any on-premises identity footprint. In other words, user accounts, their passwords, and group memberships are all native to the cloud - that is, created and managed in Azure AD

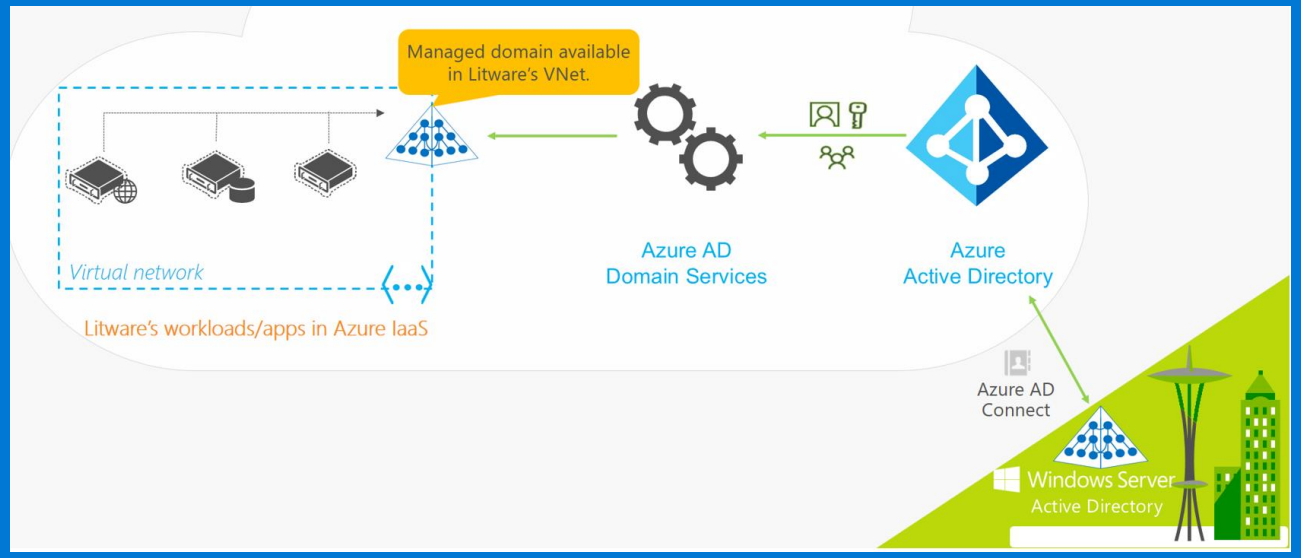


Azure Domain Services for Cloud Only Organizations

- Company’s administrator does not need to manage, patch, or monitor this domain or any domain controllers for this managed domain.
- There is no need to manage AD replication for this domain. User accounts, group memberships, and credentials from Contoso's Azure AD tenant are automatically available within this managed domain.
- Since the domain is managed by Azure AD Domain Services, Contoso's IT administrator does not have Domain Administrator or Enterprise Administrator privileges on this domain

Azure Domain Services for Hybrid Organizations

Organizations with a hybrid IT infrastructure consume a mix of cloud resources and on-premises resources. Such organizations synchronize identity information from their on-premises directory to their Azure AD tenant. As hybrid organizations look to migrate more of their on-premises applications to the cloud, especially legacy directory-aware applications, Azure AD Domain Services can be useful to them.



Azure Domain Services – Benefits

- Simple – You can satisfy the identity needs of virtual machines deployed to Azure Infrastructure services with a few simple clicks. You do not need to deploy and manage identity infrastructure in Azure or setup connectivity back to your on-premises identity infrastructure.

- Integrated – Azure AD Domain Services is deeply integrated with your Azure AD tenant. You can now use Azure AD as an integrated cloud-based enterprise directory that caters to the needs of both your modern applications and traditional directory-aware applications.

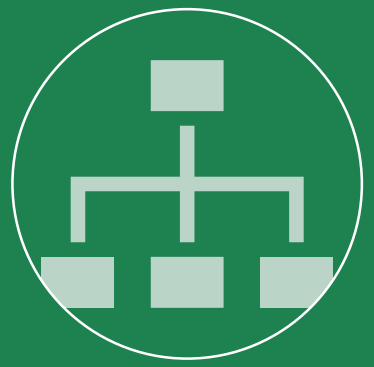
- Compatible – Azure AD Domain Services is built on the proven enterprise grade infrastructure of Windows Server Active Directory. Therefore, your applications can rely on a greater degree of compatibility with Windows Server Active Directory features. Not all features available in Windows Server AD are currently available in Azure AD Domain Services. However, available features are compatible with the corresponding Windows Server AD features you rely on in your on-premises infrastructure. The LDAP, Kerberos, NTLM, Group Policy, and domain join capabilities constitute a mature offering that has been tested and refined over various Windows Server releases.

- Cost-effective – With Azure AD Domain Services, you can avoid the infrastructure and management burden that is associated with managing identity infrastructure to support traditional directory-aware applications. You can move these applications to Azure Infrastructure Services and benefit from greater savings on operational expenses.

Azure AD Domain Services

Managed domain services

- No need to
  - deploy
  - manage
  - patch domain controllers for classic application authentication



Classic Active Directory features

- Domain join
- Group policy
- LDAP
- Kerberos/NTLM authentication

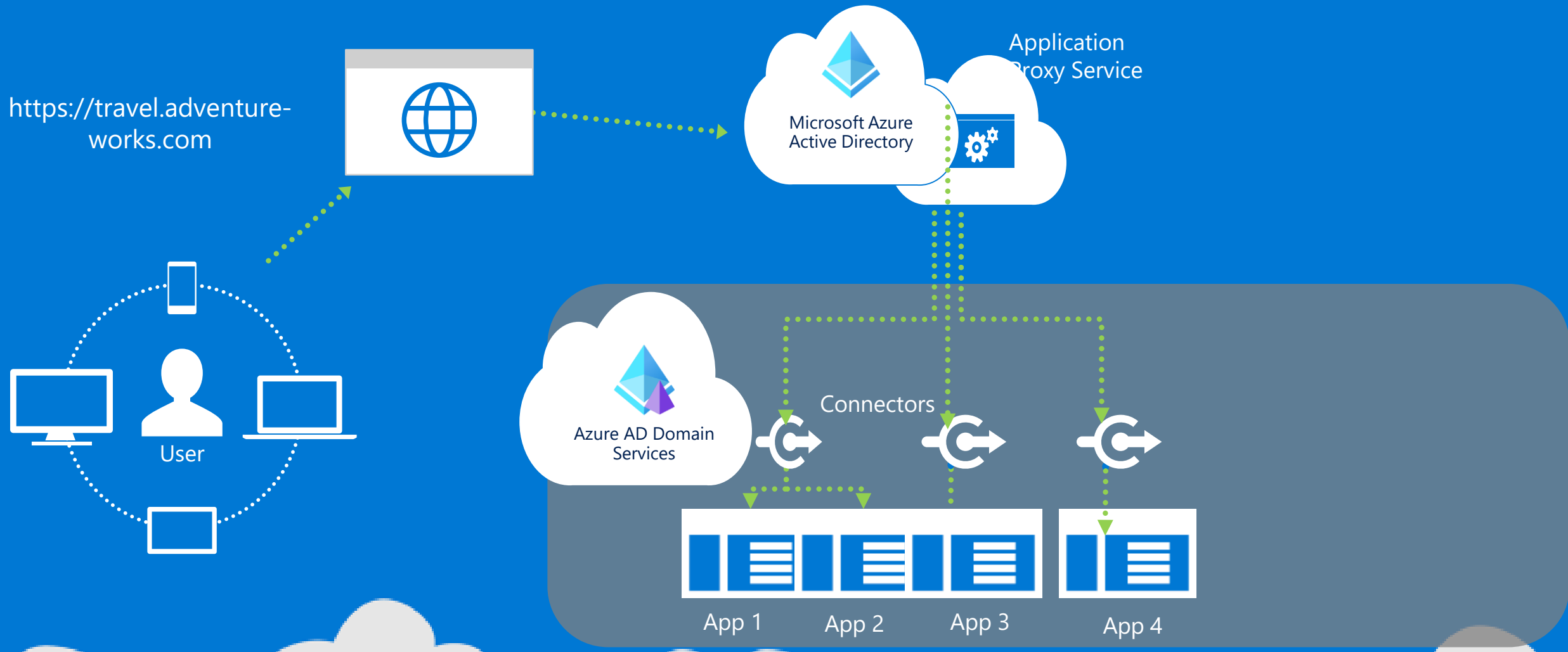
Integrates with your Azure AD tenant

- Users sign in using their existing credentials.

Secure

- Delegated Administration
- No Domain or Enterprise Administrators

AAD Application Proxy + Domain Services



Azure Migrate

I am ready to transform but have questions

Is the cloud secure for my apps?

Which apps make sense to run in the cloud? Can I trust my business-critical app to a cloud vendor?

Can I modernize apps with minimal disruption?

Do I need other tools to manage my cloud and on-premises (or hybrid) environments?

I'm out of support, but not ready to upgrade. What are my options?

I am ready to migrate but have questions

Is there a framework?

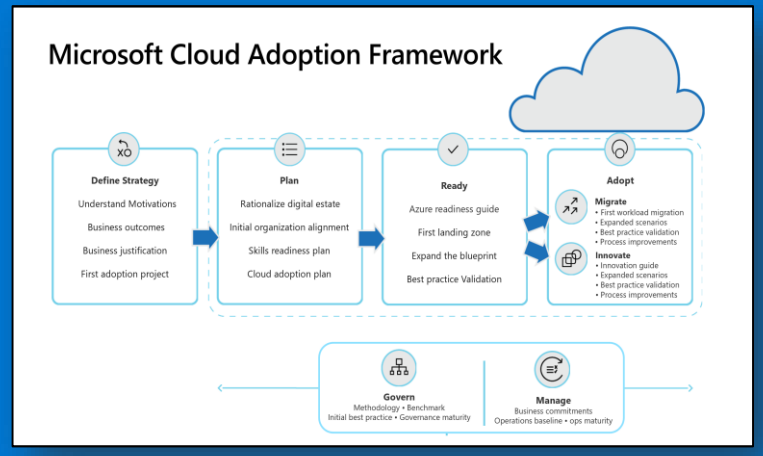
Where do I evaluate the different scenarios and tools that can help me execute my migration strategy?

How do I discover my infrastructure and applications?

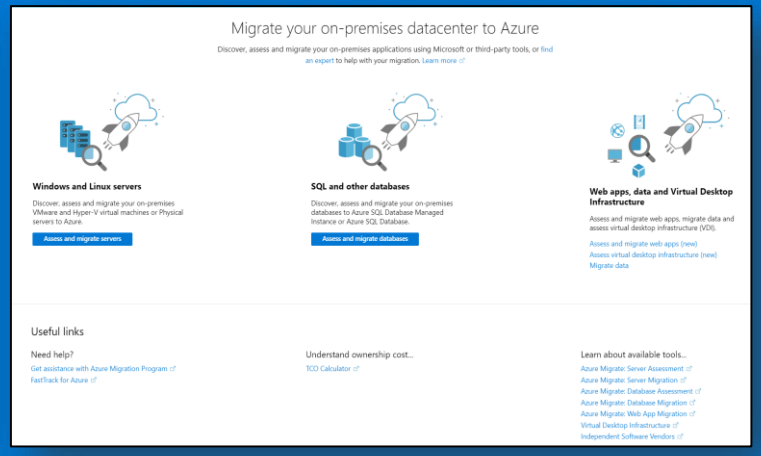
How do I perform migrations for servers, databases, and more?

Can Microsoft help?

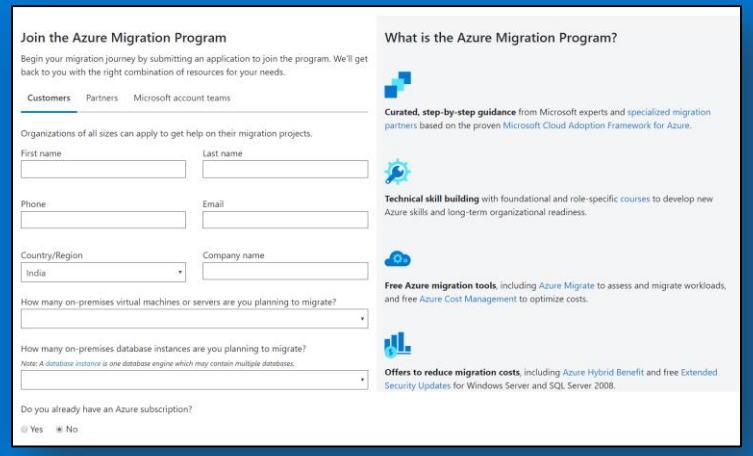
Azure Migration—process, product, and program



Microsoft Cloud Adoption Framework

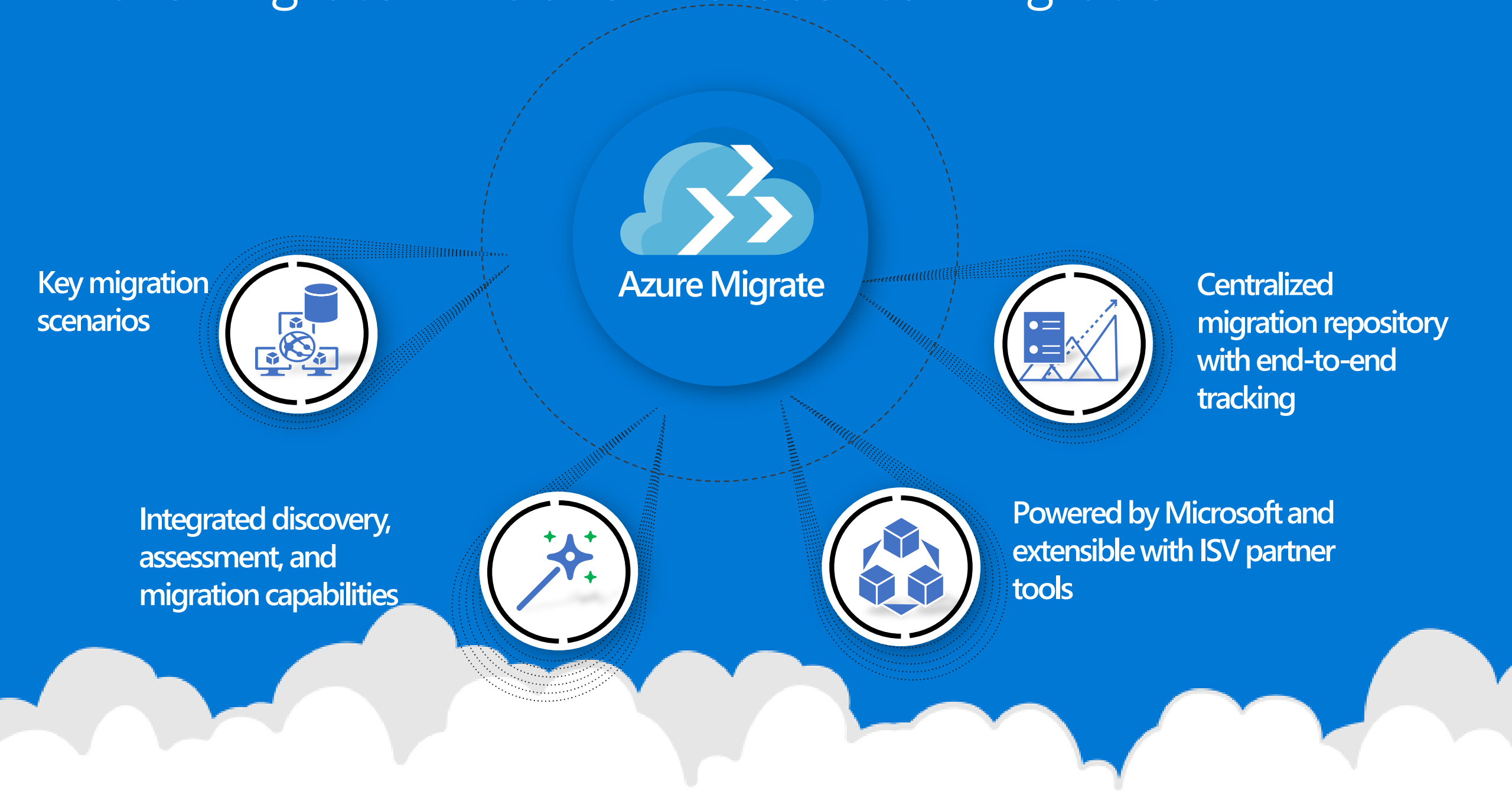


Azure Migrate



Azure Migration Program

Azure Migrate – Hub for Datacenter Migration



GRAZIE!