FP + PROFESSIONAL EDUCATION

Tech Club

tajamar.

HTTPS://TECHCLUB.TAJAMAR.ES

WWW.MEETUP.COM/TECHCLUBTAJAMAR/

@TECHCLUBTAJAMAR

WWW.YOUTUBE.COM/TECHCLUBTAJAMAR

STUDENTTECHCLUB@TAJAMAR365.COM

plain concepts

Infraestructuras seguras en Azure

José María Genzor
Cloud Team Lead– Plain Concepts
jmgenzor@plainconcepts.com

plain concepts

http://www.plainconcepts.com
http://geeks.ms/enterprise

AGENDA

- **Acceso seguro a contenidos públicos en Azure**
    - Acceso seguro a través de un WAF.
    - Creación de una DMZ.
- **Acceso a aplicaciones locales a través de las aplicaciones empresariales en Azure AD.**
    - Publicación de una aplicación local a través del conector de application proxy.
    - Securización de la aplicación a través de Azure AD.
- **Almacenamiento en Azure.**
    - Creación de una infraestructura de almacanemiento seguro en Azure.

plain concepts

ACERCA DE PLAIN CONCEPTS

XAMARIN PREMIUM CONSULTING PARTNER

12 MICROSOFT MOST VALUE PROFESSIONAL

Xbox PREMIER DEVELOPER PARTNER LIVE Apps

ALM PARTNER OF THE YEAR FOR 7 CONSECUTIVE YEARS

AGILE ALLIANCE CORPORATE MEMEBER

MICROSOFT GOLD CLOUD PLATFORM

MICROSOFT GOLD APP DEVELOPMENT

MICROSOFT GOLD LIFECYCLE MANAGEMENT APPLICAITON

MICROSOFT SILVER APP INTEGRATION

MICROSOFT SILVER COLLABORATION AND CONTENT

WINDOWS 8 APPLICATIONS PARTNER OF THE YEAR

PIXEL SENSE PREMIER PARTNER

ACERCA DE PLAIN CONCEPTS

desde
2006

100+
empleados

10+
tecnologías

3
continentes

1000+
proyectos

ACERCA DE PLAIN CONCEPTS

Barcelona

Bilbao

Madrid

Sevilla

Dubai

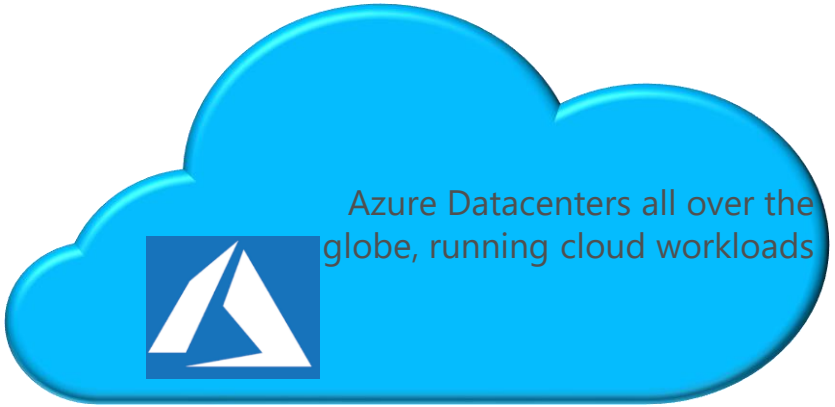
London

Seattle

AZURE NETWORKING

plain concepts

AZURE NETWORKING PICTURE



Virtual Network

- "Bring your own network"
- Segment with subnets and security groups
- Control traffic flow with user defined routes
- Network Security Groups

AZURE NETWORKING PICTURE

Front-End Access

- Load Balancing Solutions
- Public & Private Ips
- Azure DNS
- DDoS Protection
- Direct VM Access (RDP/)

Virtual Network

- "Bring your own network"
- Segment with subnets and security groups
- Control traffic flow with user defined routes
- Network Security Groups

plain concepts

AZURE NETWORKING PICTURE

Front-End Access

- Load Balancing Solutions
- Public & Private Ips
- Azure DNS
- DDoS Protection
- Direct VM Access (RDP/SSH)

Back-End Access

- VPN Gateways
  - Point-to-Site VPN
  - Site-to-Site VPN
  - ExpressRoute
- VNet Peering

plain concepts

AZURE NETWORKING PICTURE

Front-End Access

- Load Balancing Solutions
- Public & Private Ips
- Azure DNS
- DDoS Protection
- Direct VM Access (RDP/SSH)

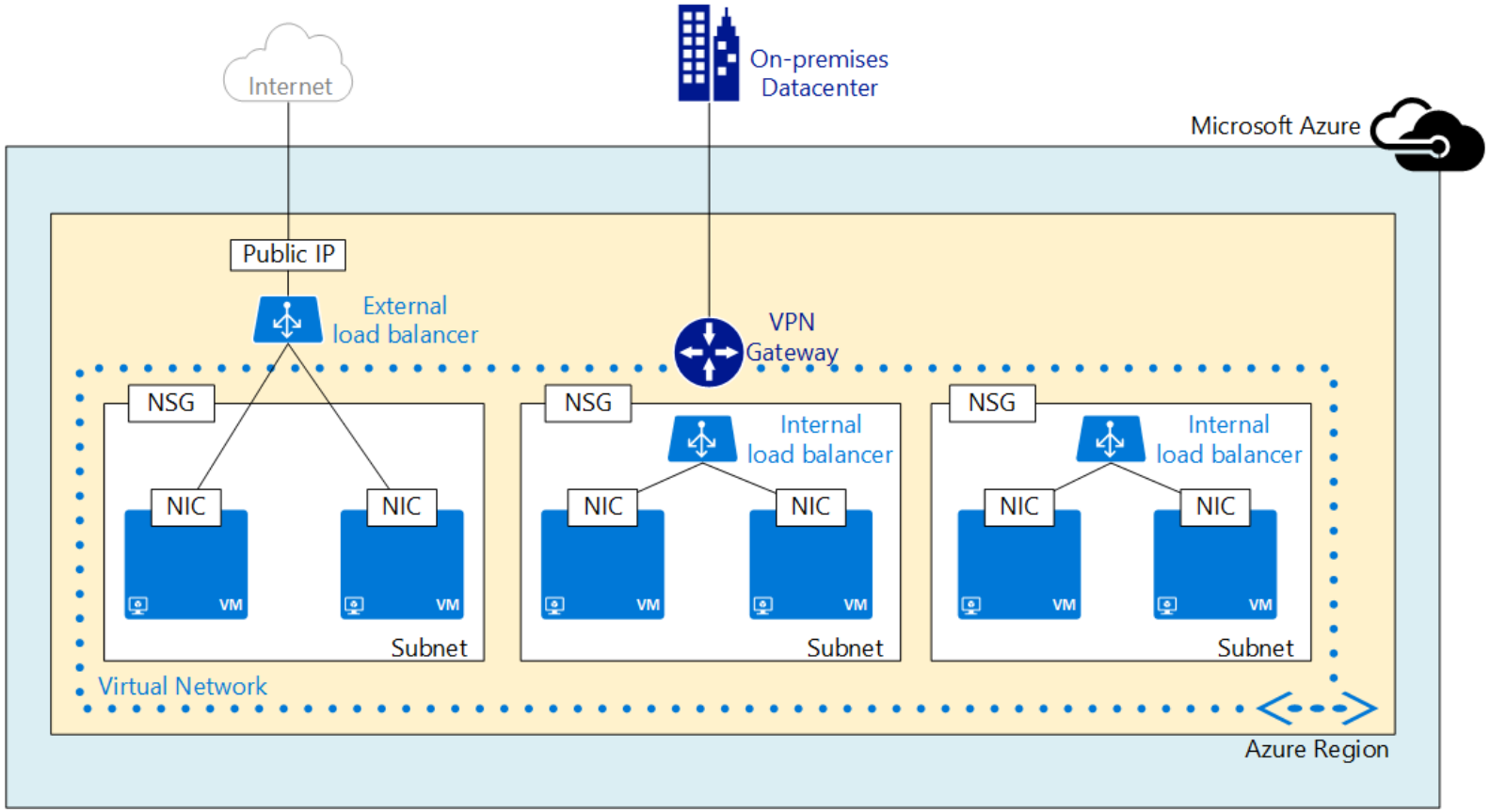
Azure Provides End-to-End Enterprise Ready Networking Solutions

Back-End Access

- VPN Gateways
  - Point-to-Site VPN
  - Site-to-Site VPN
  - ExpressRoute
- VNet Peering

plain concepts

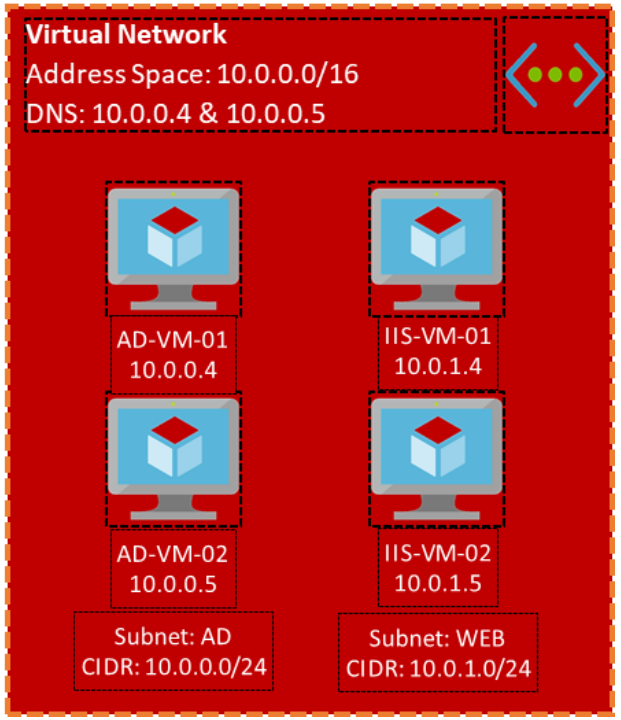
AZURE NETWORKING COMPONENTS



plain concepts

MICROSOFT AZURE VIRTUAL NETWORKS (VNETS)

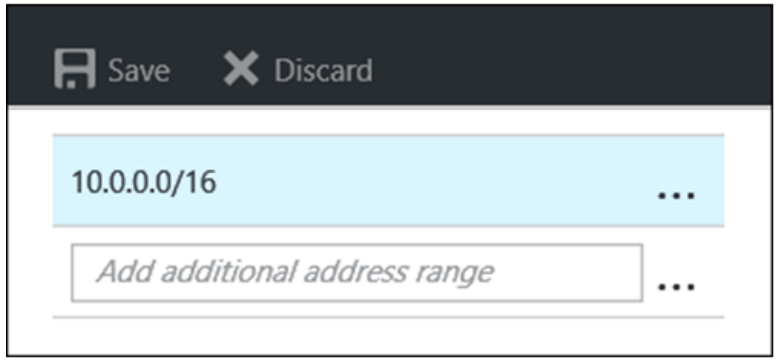
- Logical isolation with control over the network
- Create subnets and isolate traffic with network security groups
- Support for Static IP addresses
- Support for Internal Load Balancing
- DNS support
- Hybrid Connectivity Support
  - Site-to-Site
  - Point-to-Site
  - ExpressRoute



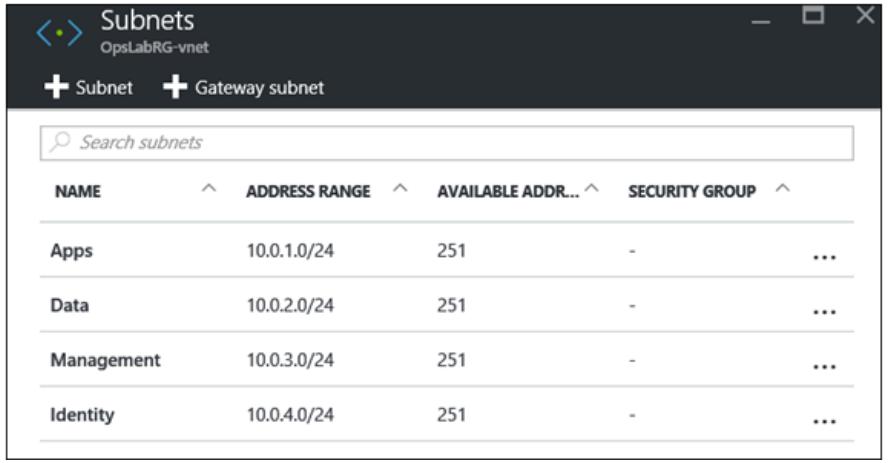
ADDRESS SPACE AND SUBNETS

- One more non-overlapping address spaces
- Define subnets out of the available address spaces in the virtual network using Classless Internet Domain Routing (CIDR)

Address Spaces



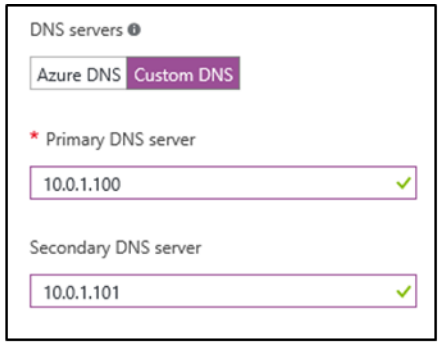
Subnets

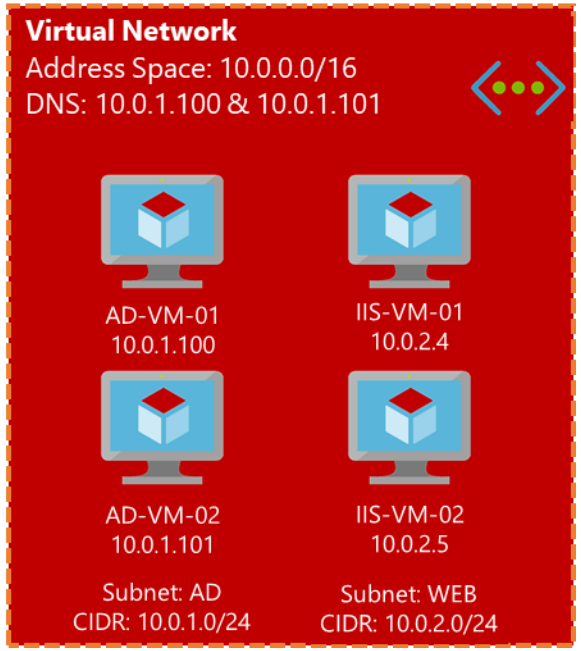


BRING YOUR OWN DNS

- Specify DNS Servers at the Virtual Network Level
  - Hosted in an Azure VM
  - External
  - On-Premises (with hybrid connection)

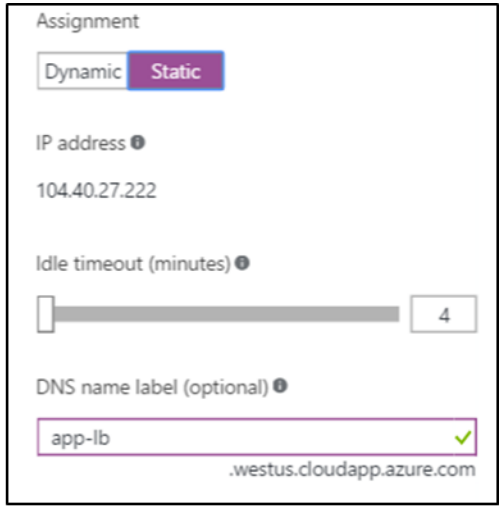
- Virtual Machines are assigned specified DNS at boot
  - If DNS is added after a virtual machine is running a reboot is required for assignment.

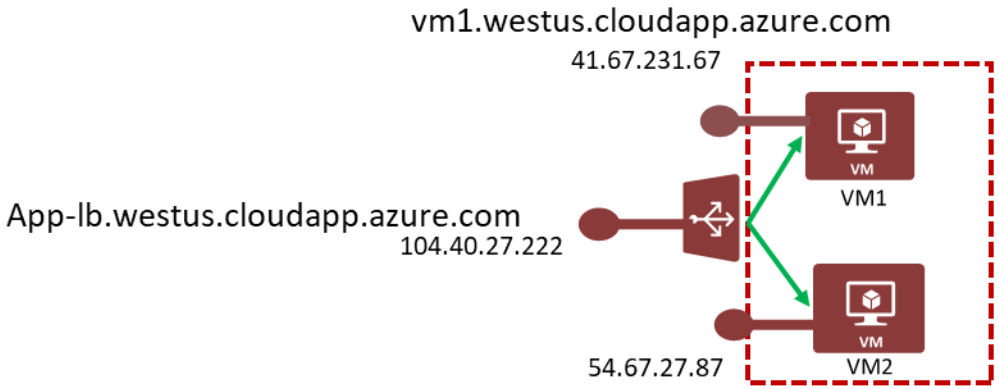




PUBLIC IP ADDRESS

- A public IP can be assigned directly to a network interface or a load balancer
- Supports static (reserved) or dynamic assignment
- Optionally supports specifying a DNS label
- Configurable idle timeout
- First 5 static IPs are free





PRIVATE IP ASSIGNMENT RULES

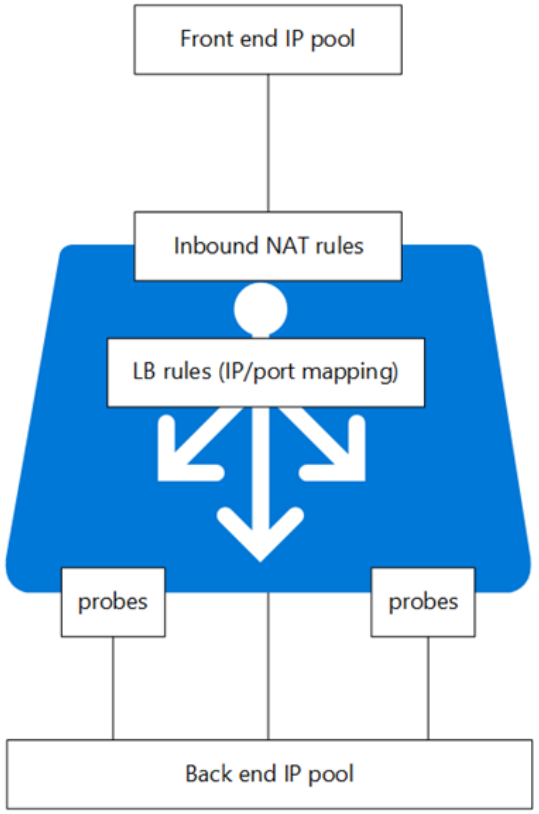
- IPs are allocated based on order of provisioning of Network Interface Cards
- (1st 4 IPs are reserved)
- Subnet Web: 10.0.1.0/24
  - 1. NIC-01 = 10.0.1.4 Initial Provisioning
  - 2. NIC-02 = 10.0.1.5 Initial Provisioning

- Use Static Private IP addresses to retain IP regardless of order

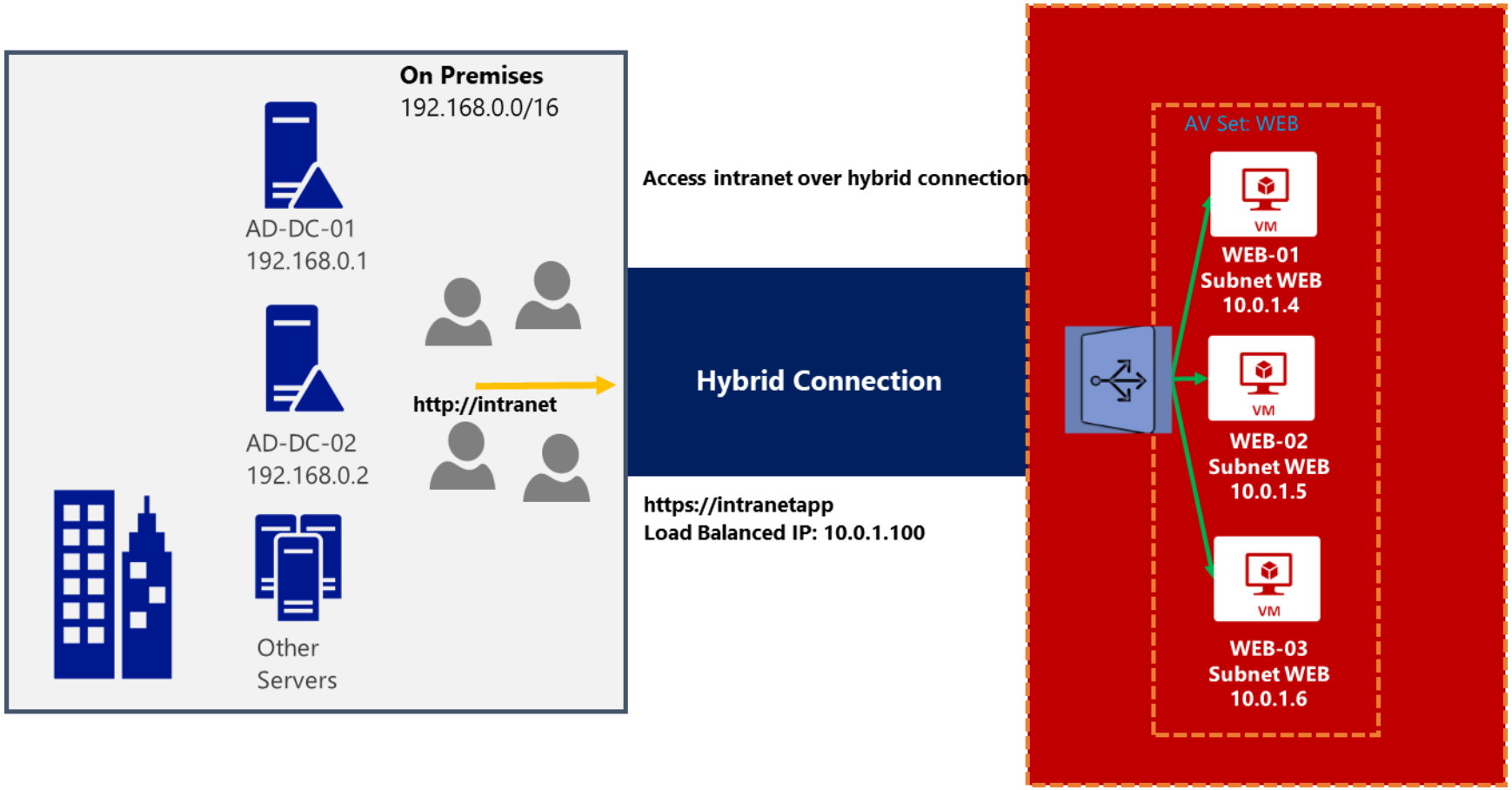
AZURE LOAD BALANCING SOLUTIONS

1) Azure Loadbalancer

- "Typical Load Balancing" on Layer 4
- External or Internal Load Balancing
- Support for TCP and UDP Protocols
- Health Probe (http or tcp)

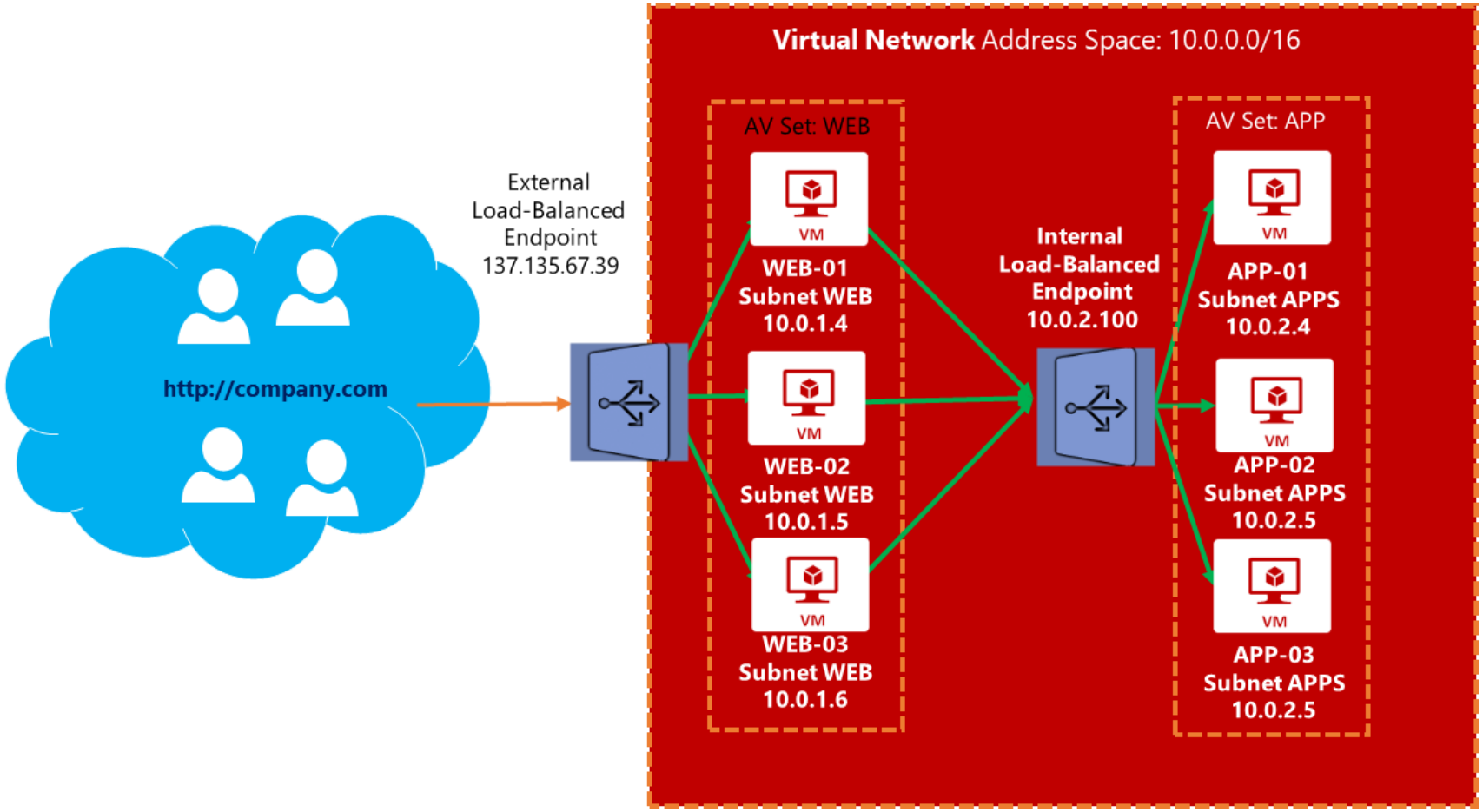


INTRANET SOLUTION USING INTERNAL LOAD BALANCER



plain concepts

N-TIER APPLICATION WITH LOAD-BALANCED MIDDLE TIER

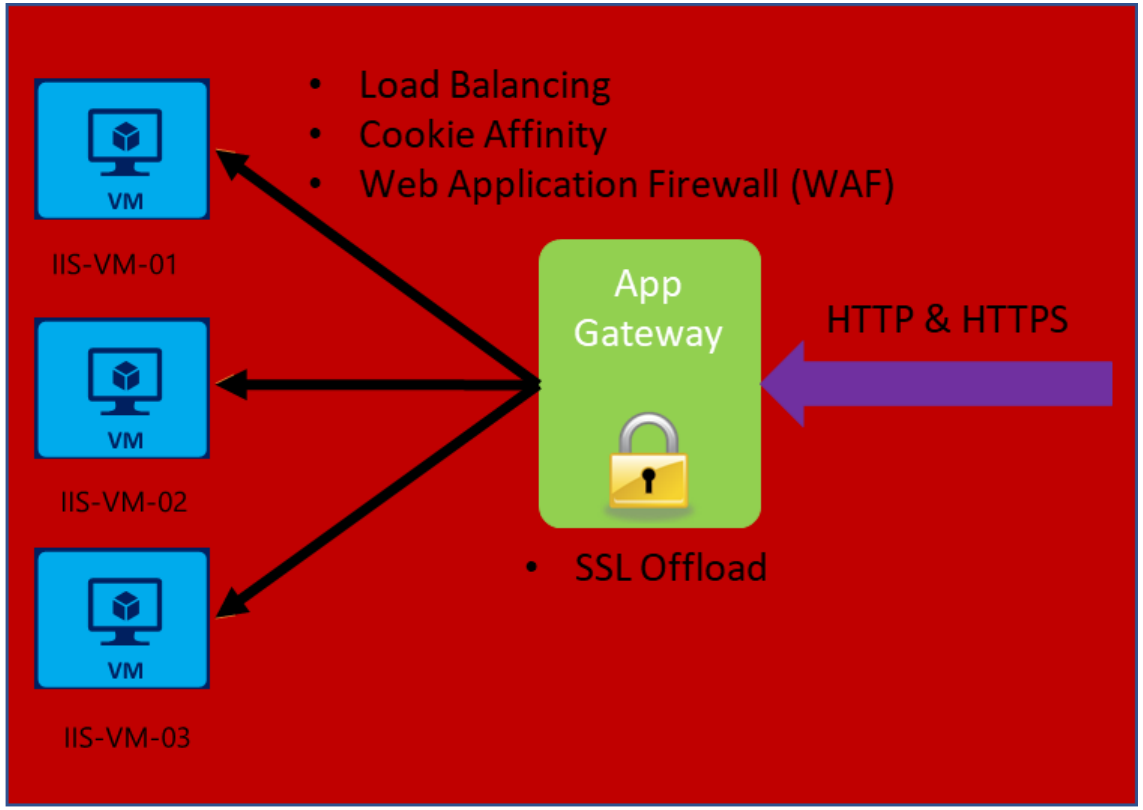


plain concepts

AZURE LOAD BALANCING SOLUTIONS

2) Azure Application Gateway

- Application Load Balancing on Layer 7
- HTTP/HTTPS protocols only
- Session cookie affinity
- SSL offloading
- URL rerouting



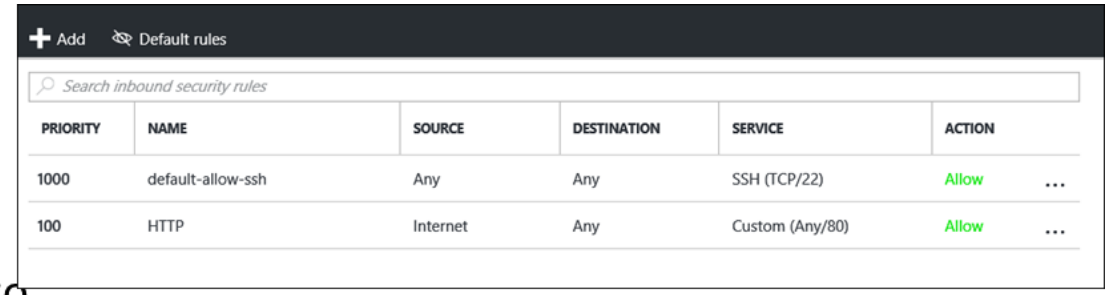
NETWORK SECURITY GROUPS OVERVIEW

Enables network segmentation & DMZ scenarios

NSG contains a list of ACL Rules that Allow/Deny Network Traffic to VMs in a Virtual Network

Restrict traffic from or to external or internal sources, but only within the region where it was created

Manage using Portal, Template, or Command line

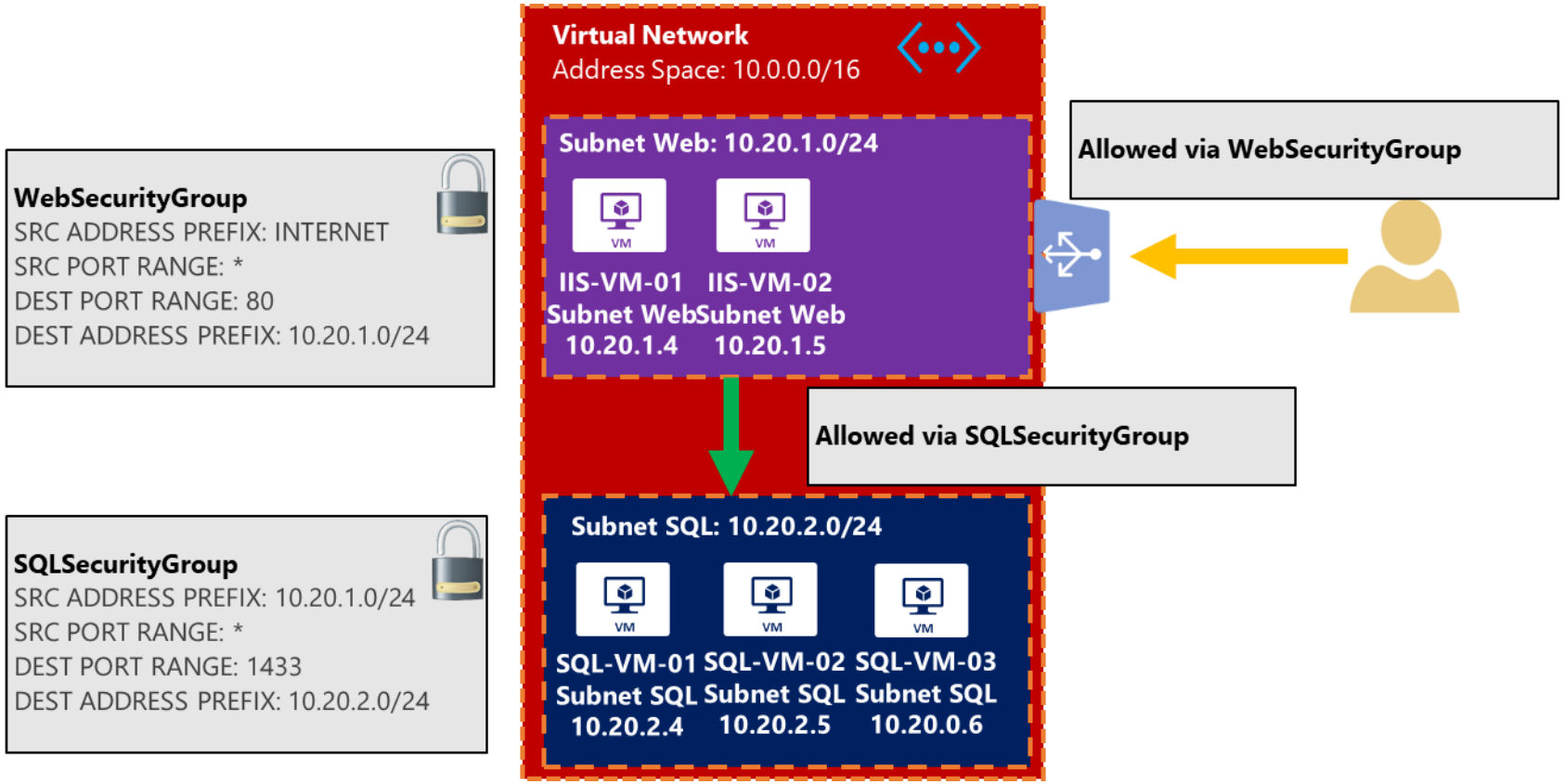


PRIORITY	NAME	SOURCE	DESTINATION	SERVICE	ACTION	
1000	default-allow-ssh	Any	Any	SSH (TCP/22)	Allow	...
100	HTTP	Internet	Any	Custom (Any/80)	Allow	...

Property	Limits
Number of NSGs associated to a subnet, VM, or Network Interface	1
NSGs per region per subscription	100*
NSG rules per NSG	200*

plain concepts

NETWORK SECURITY GROUPS EXAMPLE



plain concepts

AZURE DEFAULT NETWORK ROUTING

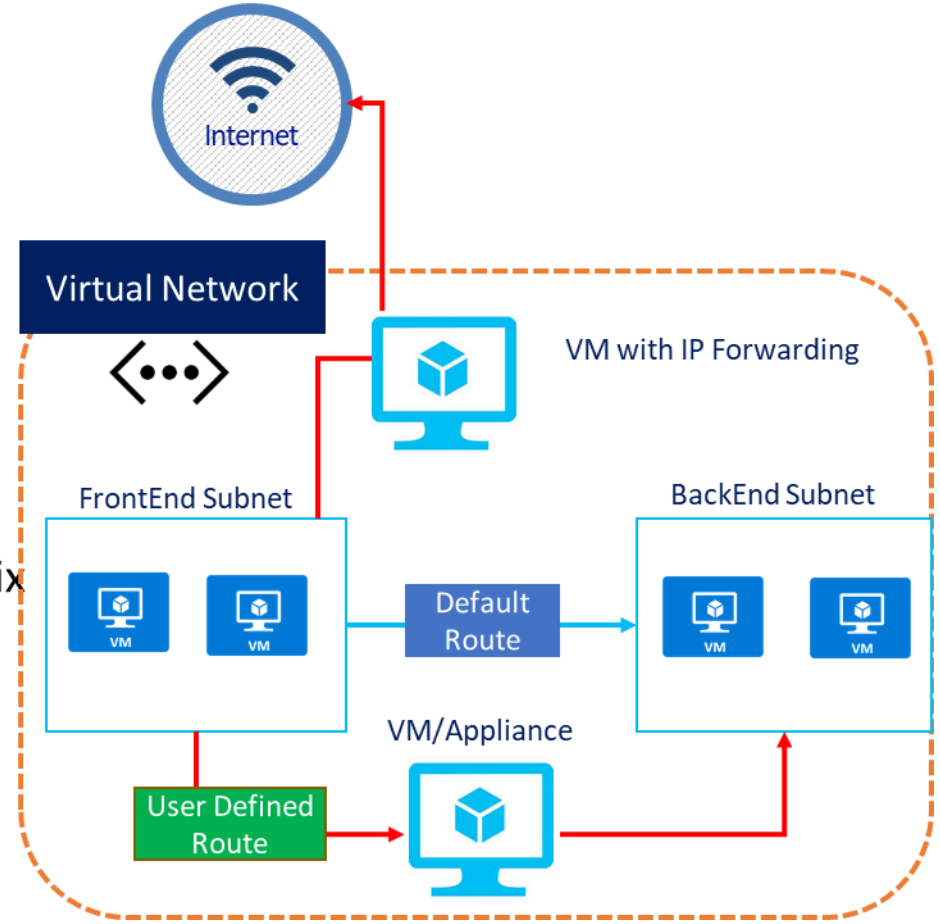
Traffic automatically flows between virtual machines in different subnets and even address spaces

Azure has built in default routes:

- Routing within a subnet
- From a subnet to another subnet in the same virtual network
- To the Internet
- Virtual Network to Virtual Network using a VPN Gateway
- Virtual Network to on-premises using a VPN Gateway

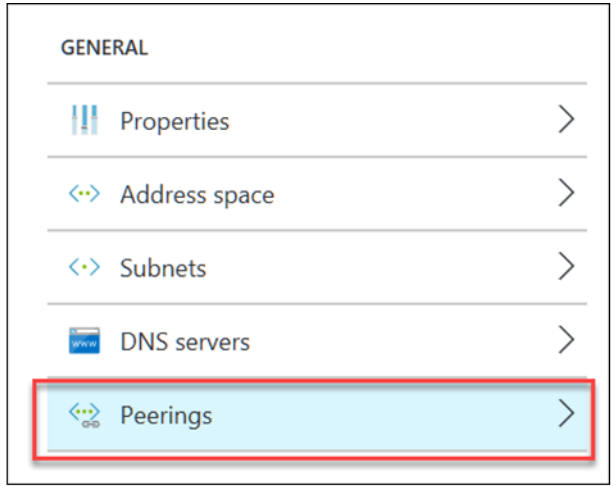
USER DEFINED ROUTES

- Control traffic flow in your network with custom routes
- Attach route tables to subnets
- Specify next hop for any address prefix
- Set default route to force tunnel all traffic to on-premises or appliance



VNET PEERING

- Connect two VNETs in the same region
- Utilizes the Azure Backbone network
- Appear as one network for connectivity
- Managed as separate resources

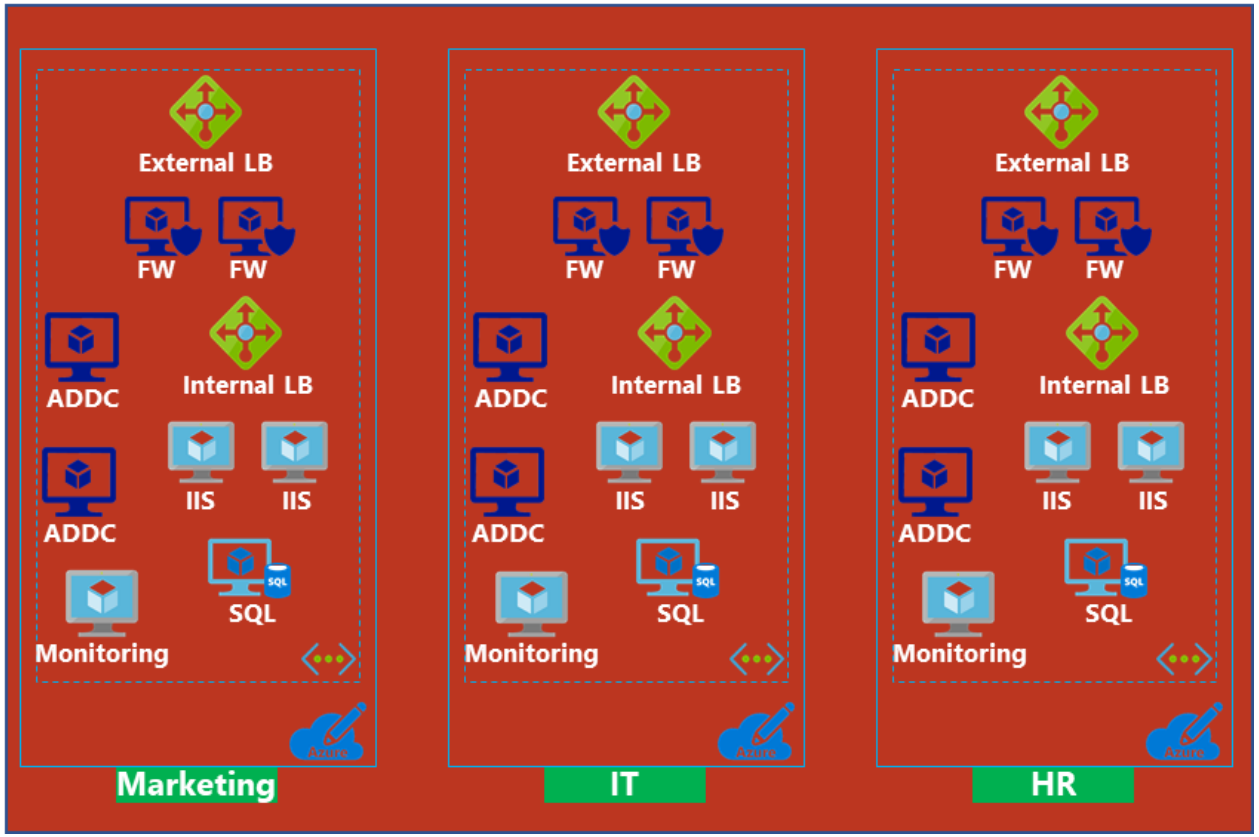


Virtual Machines will experience the exact same throughput for Peered VNET as they do on the same VNET

WHY HAVE MULTIPLE VNETS?

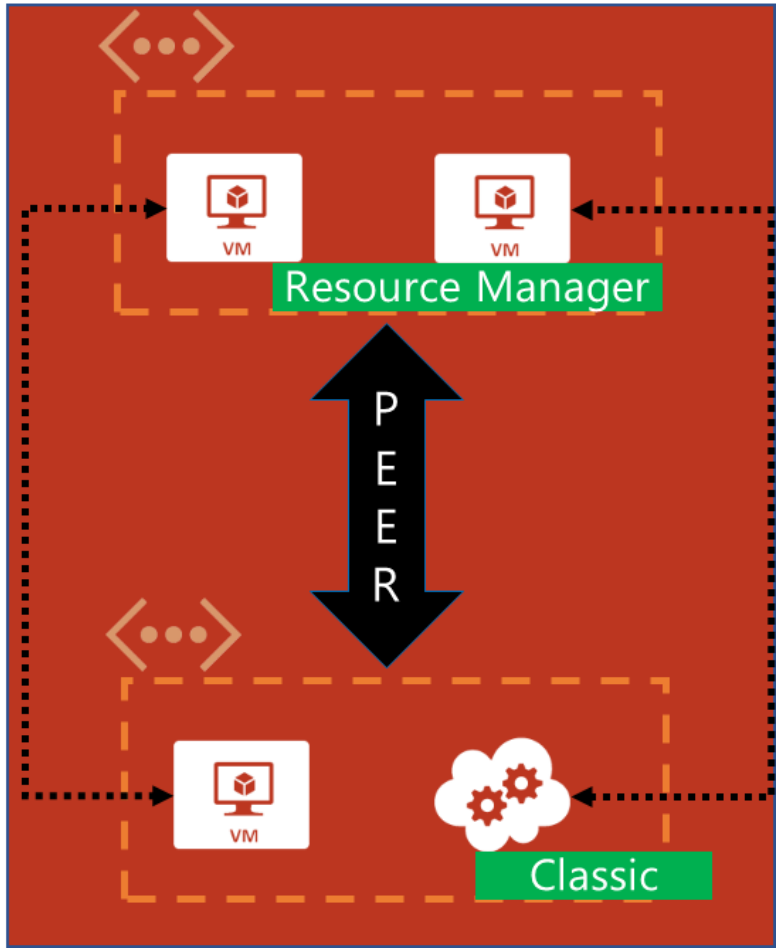
- Most common in Enterprise Agreements with multiple subscriptions
  - Segregating Billing
  - Segregating Admin

- A VNet cannot span subscriptions



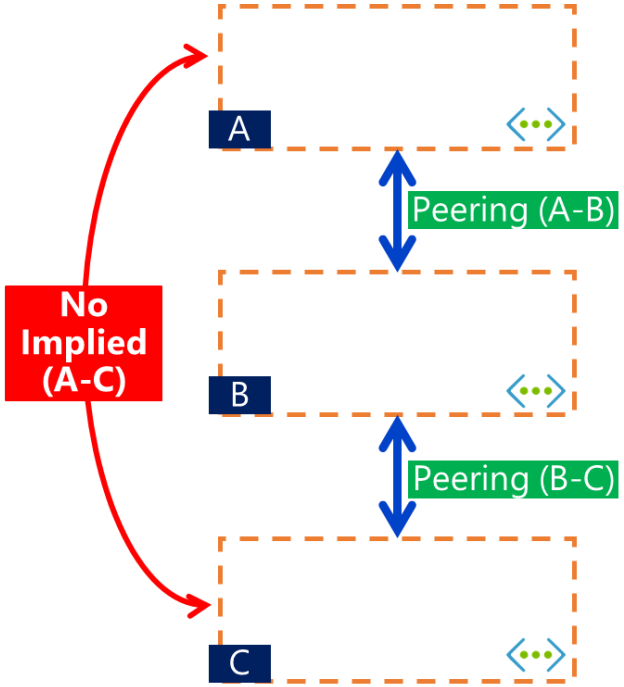
BENEFITS OF VNET PEERING

- Low-latency, high-bandwidth connection between resources in different VNETs
  - No bandwidth restriction (besides those imposed on VM series/size)
- Ability to use resources as transit points in a peered VNET (between ARM VNets only)
  - Reduced Infrastructure
- Connect VNETs that use ARM model to a VNET that uses Classic model and enable full connectivity between resources (same subscription only)



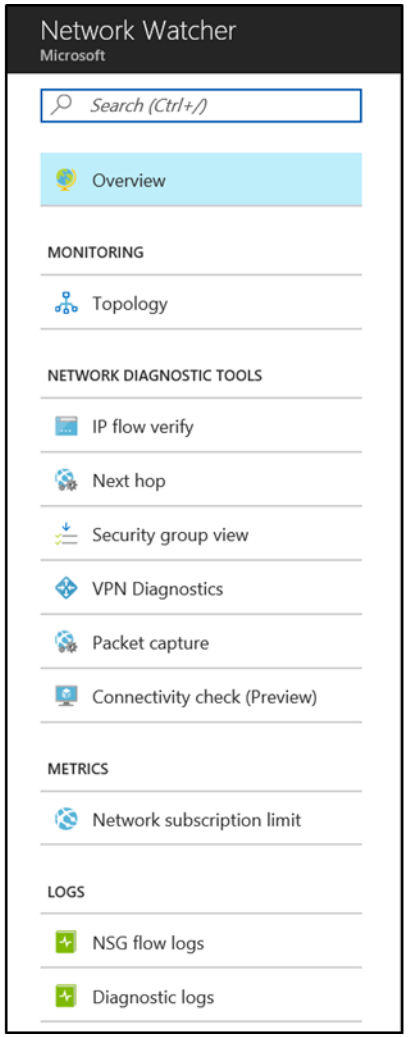
CAVEATS OF VNET PEERING

- Vnet peering is between 2 virtual networks, and there is no derived transitive relationship
- Vnet address spaces cannot overlap
- Peered Vnets can be in different subscriptions
  - Must be linked to the same Azure AD tenant
  - Exception – If 1 Vnet is ARM and the other is Classic
- Inter-Vnet traffic is not encrypted
- Must bring your own DNS
- Default limit of 10 peerings per Vnet (Max 50)



AZURE NETWORK WATCHER

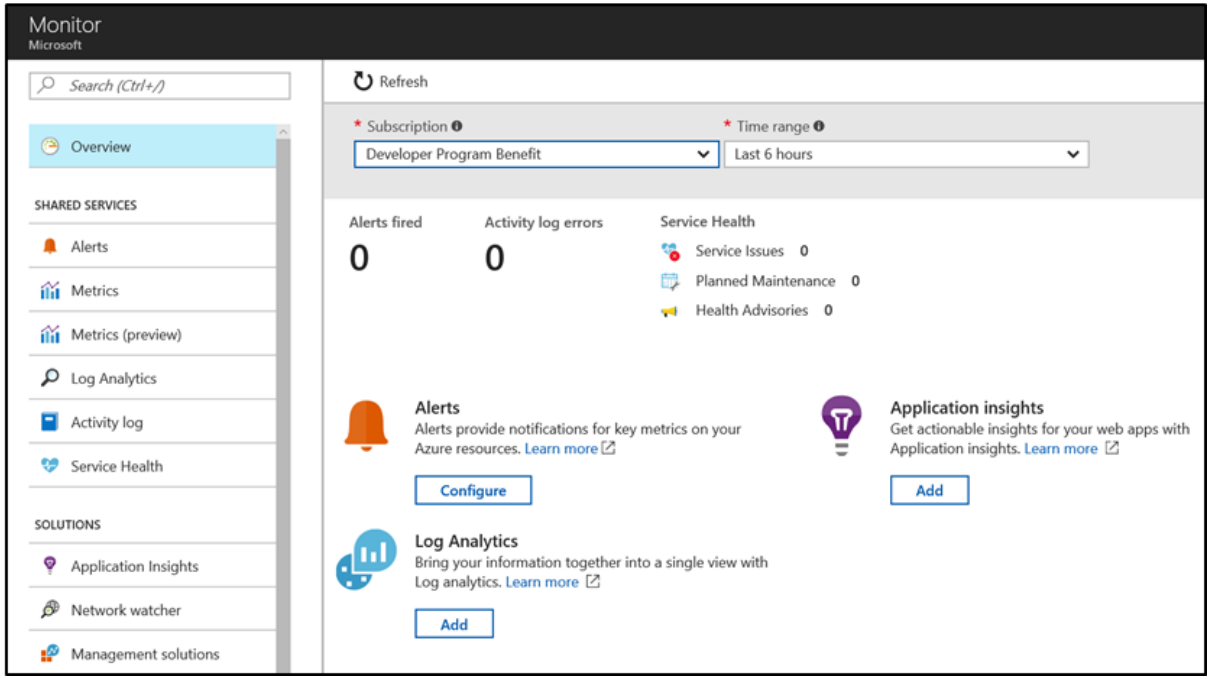
- Recently added Networking feature, providing
  - Topology
  - Variable Packet Capture
  - IP Flow Verify
  - Next Hop
  - Diagnostics Logging
  - Security Group View
  - NSG Flow Logging
  - VPN Gateway Troubleshooting
  - Network Subscription Limits
  - Role Based Access Control
  - Connectivity



plain concepts

AZURE NETWORK MONITOR

- Centralized hub for different Azure Resources Monitoring aspects:
  - Alerts
  - Metrics
  - Log Analytics
  - Service Health
  - Application Insights
  - Network Watcher

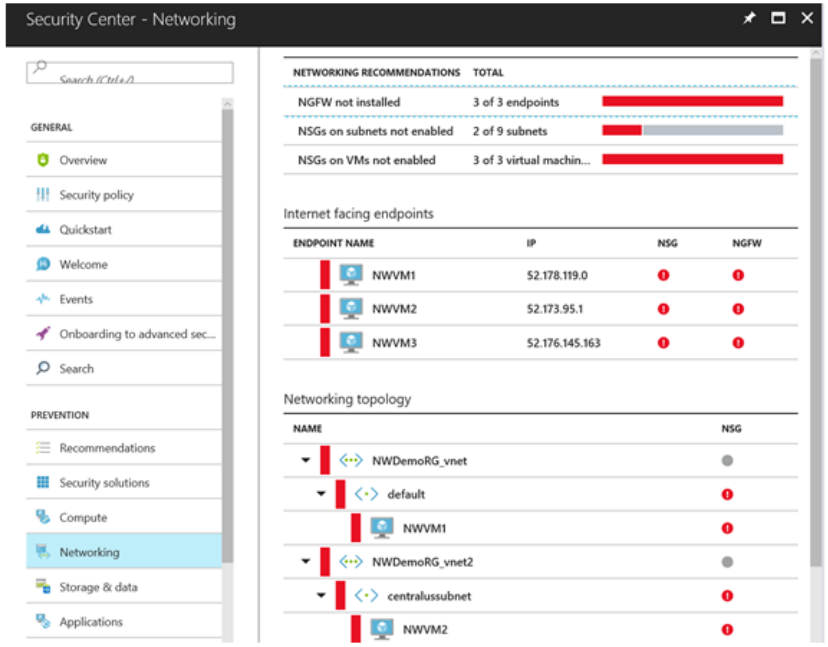


AZURE SECURITY CENTER

- Centralized Dashboard, focusing on Security posture of Azure and hybrid systems and applications

- Active in 3 different areas:
  - General Security View
  - Prevention
  - Detection

- Networking Features:
  - Networking Recommendations
  - Internet Facing Endpoints security view
  - Networking Topology security view

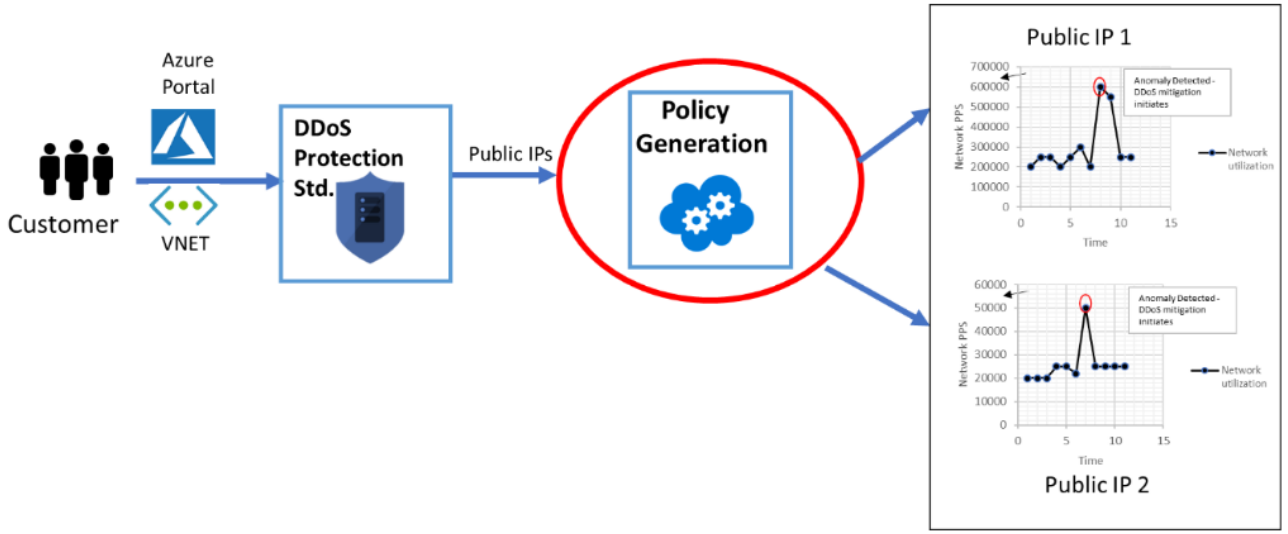


plain concepts

AZURE DDOS PROTECTION

DDoS Protection Standard mitigation

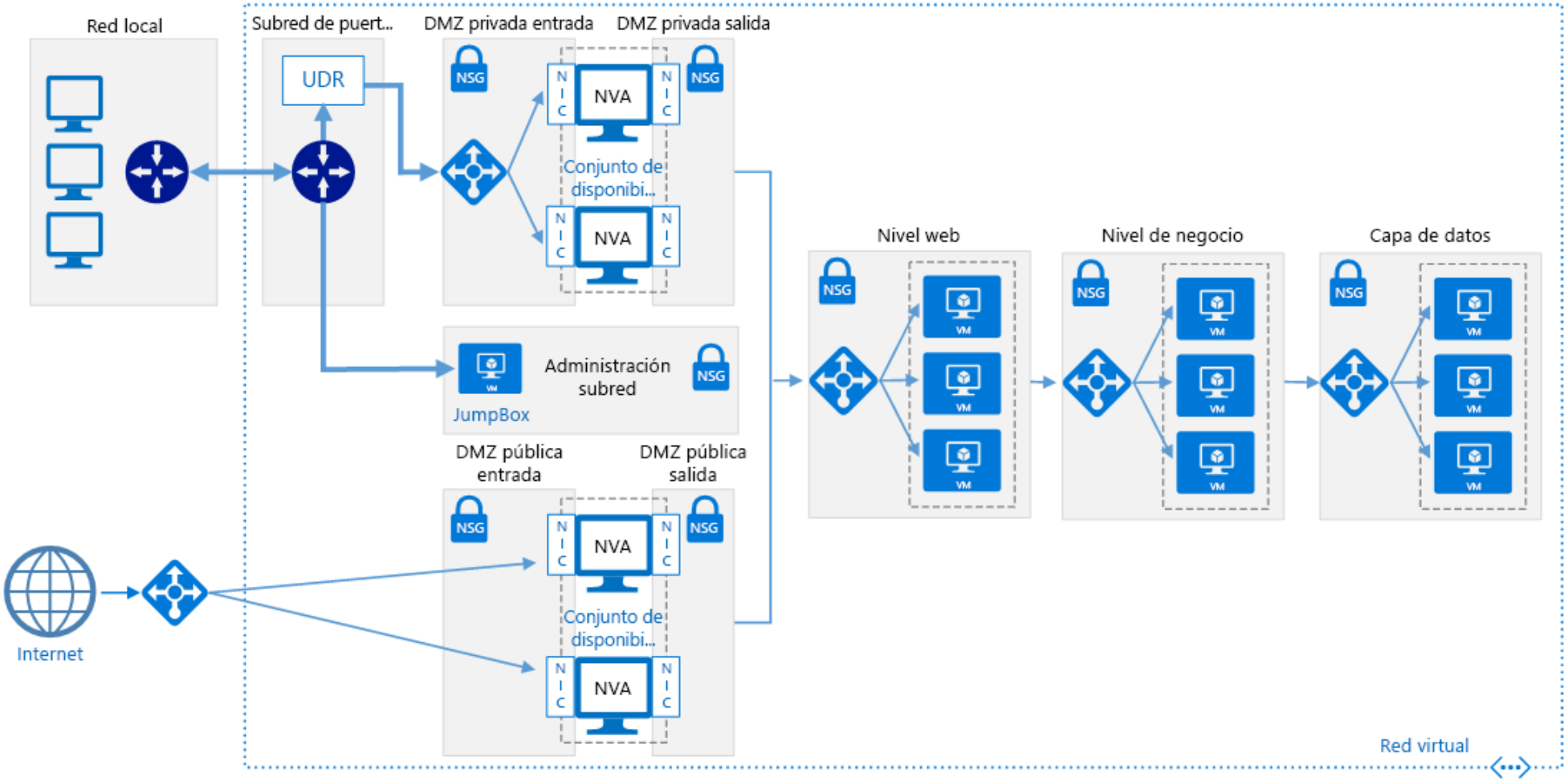
DDoS Protection Standard monitors actual traffic utilization and constantly compares it against the thresholds defined in the DDoS Policy. When the traffic threshold is exceeded, DDoS mitigation is initiated automatically. When traffic returns below the threshold, the mitigation is removed.



During mitigation, traffic sent to the protected resource is redirected by the DDoS protection service and several checks are performed, such as the following checks:

- Ensure packets conform to internet specifications and are not malformed.
- Interact with the client to determine if the traffic is potentially a spoofed packet (e.g: SYN Auth or SYN Cookie or by dropping a packet for the source to retransmit it).
- Rate-limit packets, if no other enforcement method can be performed.

HOW TO CREATE DMZ IN AZURE



plain concepts

PRÁCTICAS PUBLICACIÓN WEB SEGURA

Generar el siguiente escenario

- Crear un grupo de recursos
  - Zona oeste Europa
- Crear una Vnet
  - Una subred Default
  - Una subred WAF
- Crear dos NSG
  - VM
    - Permitir el Puerto 3389
    - Asignar a la subred default
  - WAF
    - Permitir puertos 65200-65535
    - Permitir el Puerto 80
    - Asignar a la subred WAF
- Crear una MV windows.
  - Tamaño A1v2
  - Con ip pública.
  - Windows 2016.
  - Asignar a la subred Default
  - Instalar el rol web y no bloquear por fw de Windows
  - Verificar el acceso por locahost y por ip pública

plain concepts

PRÁCTICAS PUBLICACIÓN WEB SEGURA

- Crear un WAF
  - WAF V2
  - Autoescalado
  - Nombre DNS ejemplo
    - Tajawaf. .westeurope.cloudapp.azure.com
  - Protocolo HTTP
  - Modo de FW detección
  - Asignar la MV al grupo Backend creado por defecto
  - Agregar un sondeo de estado
    - HTTP
    - Localhost
    - Ruta de acceso “/”
  - Asignar como Backend el servidor creado por el Puerto 80
  - Crear y asignar un Puerto de escucha por el Puerto 80
  - Probar el acceso por la ip pública del WAF al sitio web
  - Eliminar la IP pública asignada al servidor y probar de nuevo

IDENTIDAD AZURE

plain concepts

MICROSOFT AZURE ACTIVE DIRECTORY

What is it?

A multi-tenant service that provides enterprise-level identity and access management for the cloud.

Built to support global scale, reliability and availability.

Backed by a 99.99% SLA for Azure AD Premium or Basic

What can I do with it?

Manage users and access to cloud resources.

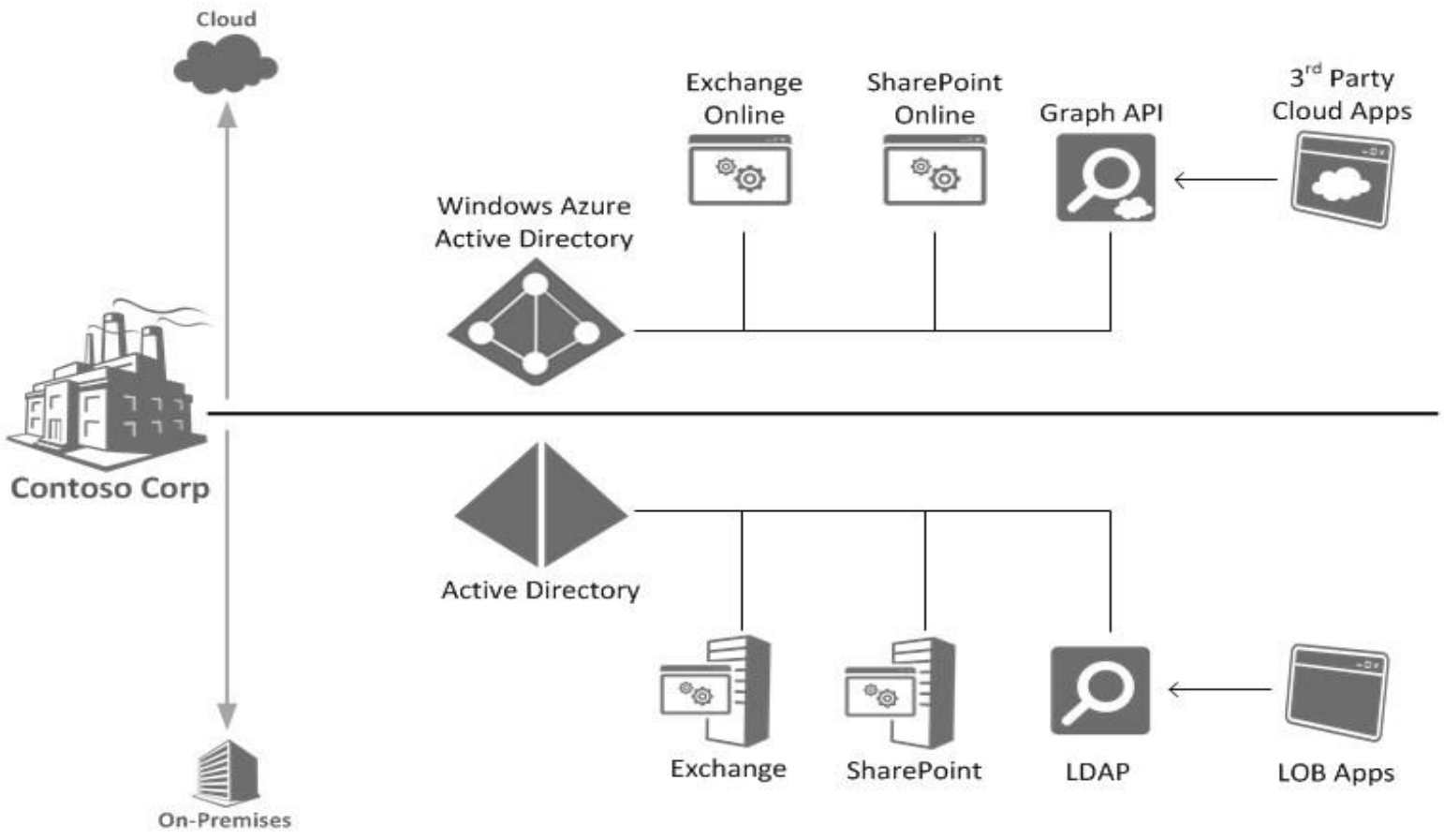
Extend your on premise Active Directory to the cloud.

Provide single-sign-on (SSO) across your cloud applications.

Reduce risks by enabling multi-factor authentication.

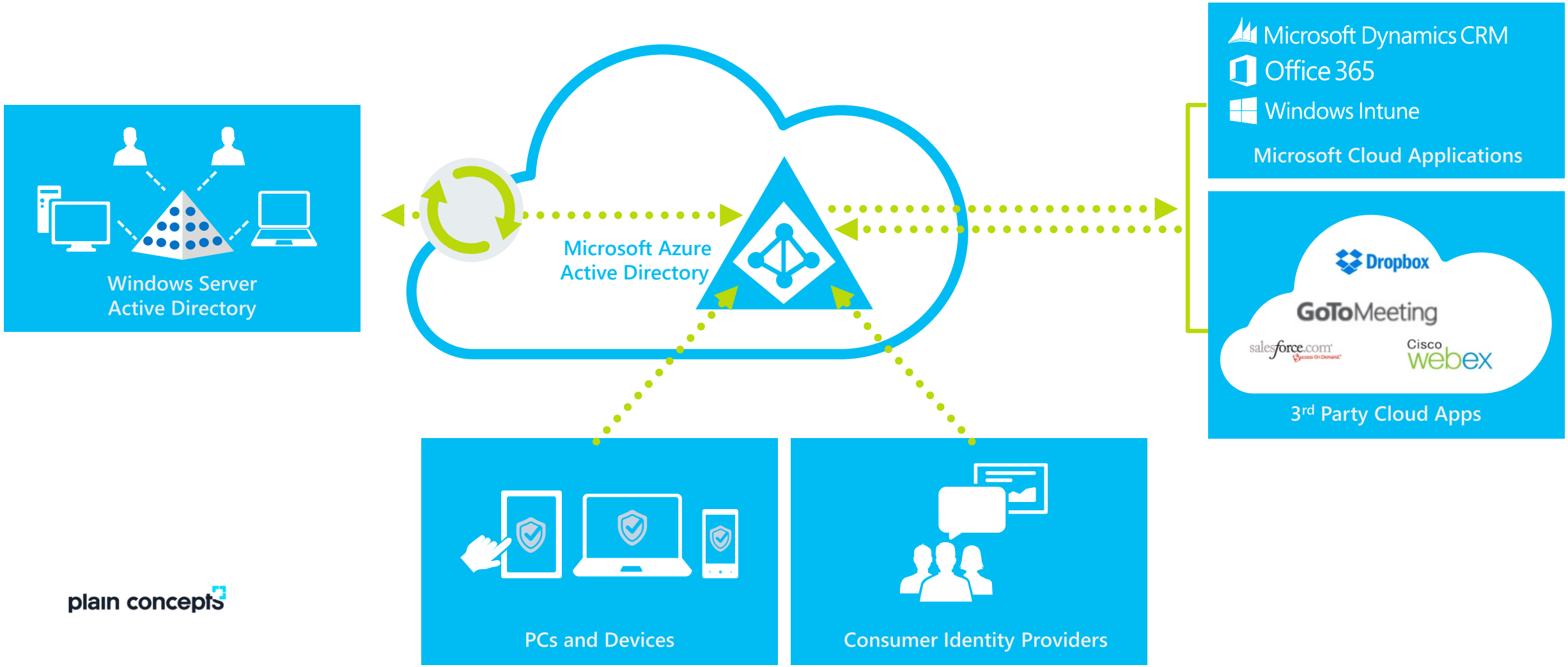
Support development's need to build secure directory integrated applications for the enterprise.

SIMILARITIES BETWEEN ACTIVE DIRECTORY & MICROSOFT AZURE ACTIVE DIRECTORY



plain concepts

IDENTITIES EVERYWHERE



plain concepts

AZURE AD FEATURES BY SKU

	FREE	BASIC	PREMIUM
Price (per user)	Free	Contact your Enterprise Agreement representative	Contact your Enterprise Agreement representative
Directory as a Service	✓	✓	✓
User and Group Management	✓	✓	✓
Directory Objects [1]	500K	Unlimited	Unlimited
End User Access Panel	✓	✓	✓
SSO for SaaS Apps	10 Apps / User [2]	10 Apps / User [2]	Unlimited
Directory Synchronization	✓	✓	✓
User-based Access Management and Provisioning	✓	✓	✓
Basic Security Reports	✓	✓	✓
Logon/Access Panel Branding Customization		✓	✓
Group-based Access Management and Provisioning		✓	✓

AZURE AD FEATURES BY SKU (CONTINUED)

Self-Service Password Reset for Cloud Users	✓	✓
Self-Service Password Reset for Users w/ writeback to on-premises directories		✓
Self-service group management for cloud users		✓
Multi-Factor Authentication (for cloud and on-premises applications)		✓
Advanced Usage and Security Reports		✓
Microsoft Identity Manager Server and User CAL		✓
Service Level Agreement	99.9%	99.9%

APPLICATION ACCESS OVERVIEW

Software-as-a-Service (SaaS) Applications

Organizations increasingly rely on SaaS applications to support business activities.

Microsoft Azure AD enables easy integration to many of today's popular SaaS applications, such as Salesforce, Box, Google Apps, DocuSign, DropBox. etc.

Tenets of Integrating SaaS Apps w/Microsoft Azure AD

Single Sign-On (SSO) enables users to access their applications using their organizational ID.

Account synchronization enables user provisioning/de-provisioning into application based on changes in Windows Server AD and/or Microsoft Azure AD.

Centralized application access management.

Unified monitoring and reporting.

SUPPORTED SINGLE SIGN-ON

Federation-based Single Sign-On

Users are automatically signed in to applications using their credentials from Microsoft Azure AD.

Password-based Single Sign-On

Users are automatically signed in to applications using their credentials from the 3rd party application

ACCESS PANEL

http://myapps.microsoft.com

This is where users can discover the applications they have access to.

Features of the Access Panel

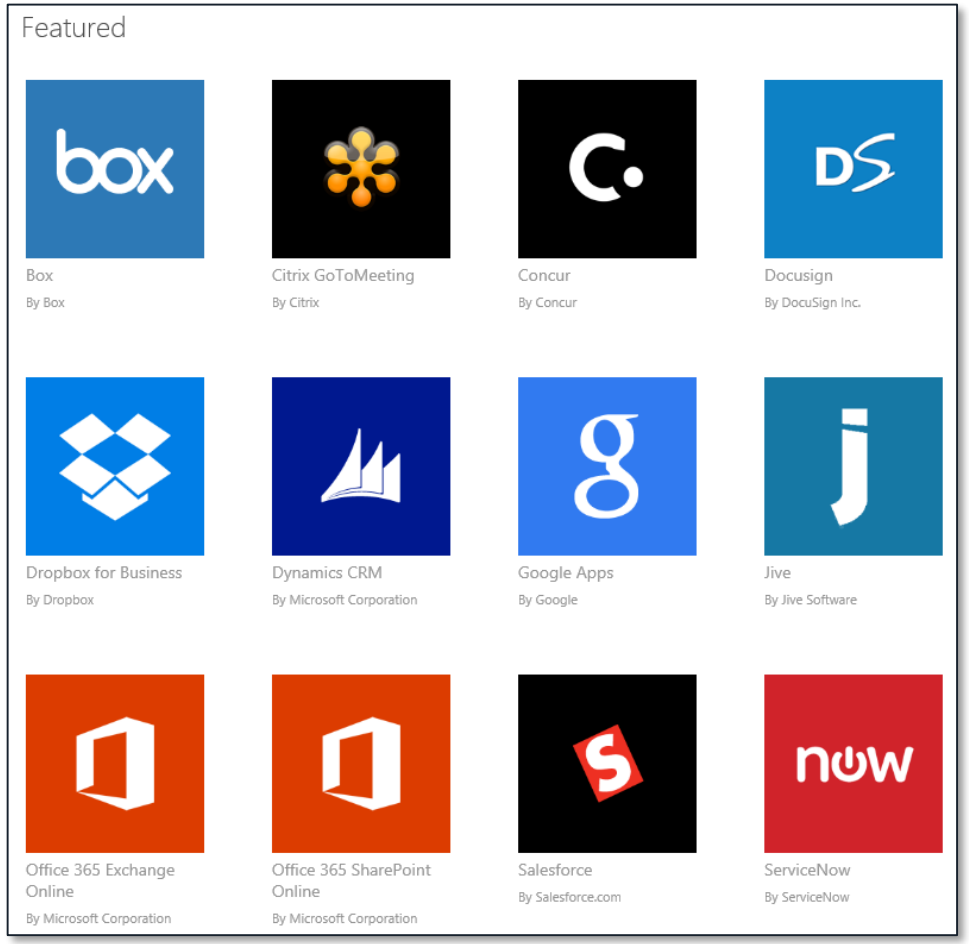
Users can change the password associated with their organizational account.

Users can edit multi-factor authentication-related contact and preference settings.

Users can view details about their account.

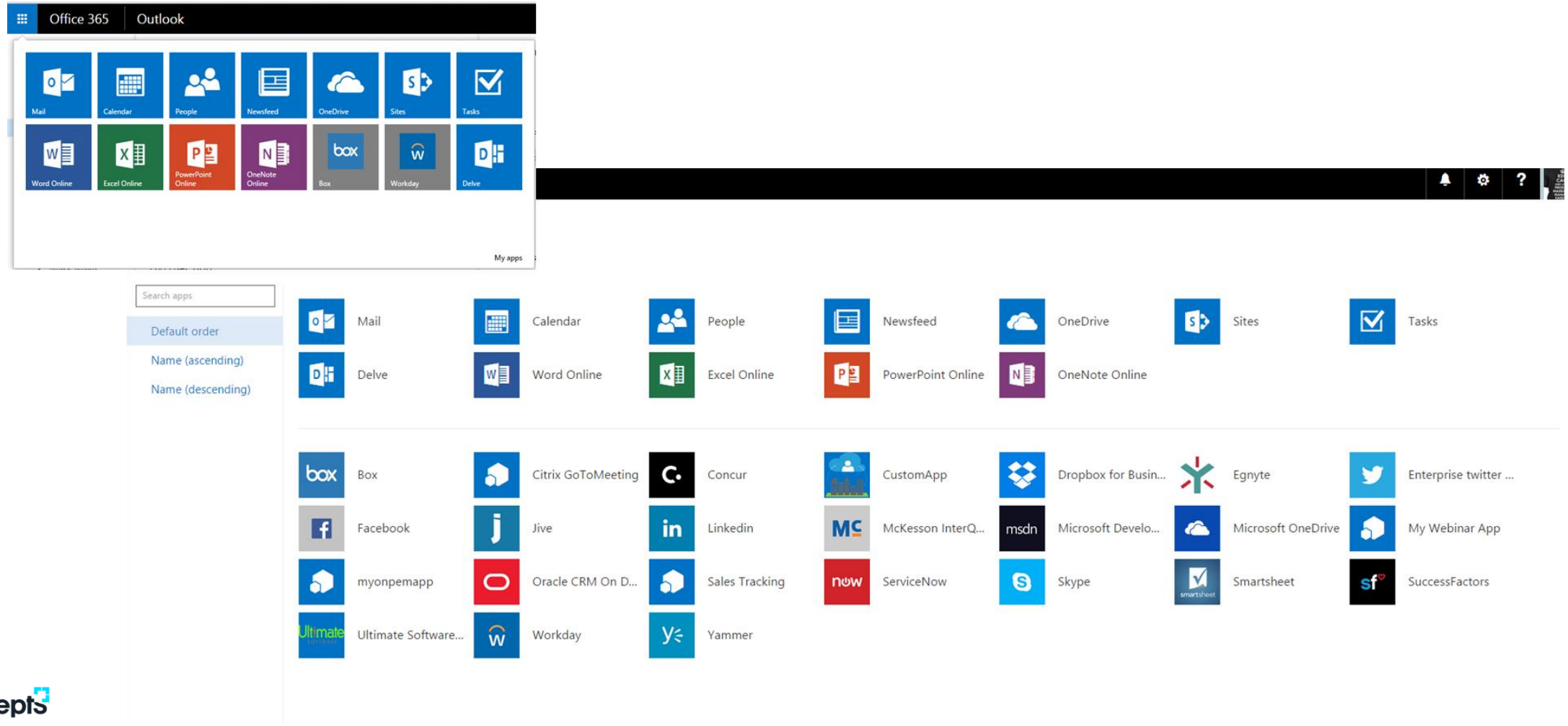
PUBLIC-FACING APPLICATION GALLERY

Discover Available SaaS Applications Without Signing into the Azure Management Portal



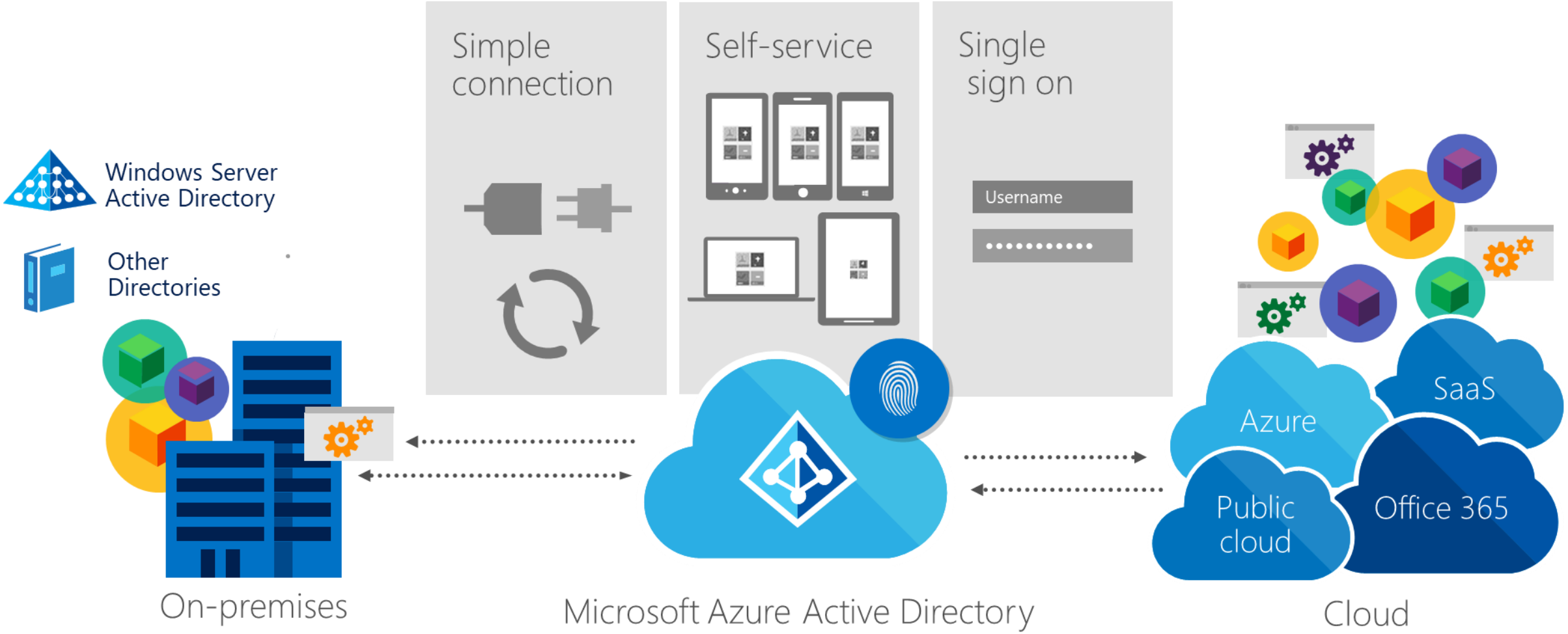
plain concepts

ACCESS YOUR APPS FROM OFFICE 365 “WAFFLE”



plain concepts

IDENTITY AS THE CONTROL PLANE



plain concepts

AZURE AD APPLICATION PROXY

Reverse-Proxy as a Service

Builds on the Web Application Proxy capabilities in Windows Server 2012 R2.

Supports browser-based applications - http(s).

Cloud Connector Pattern

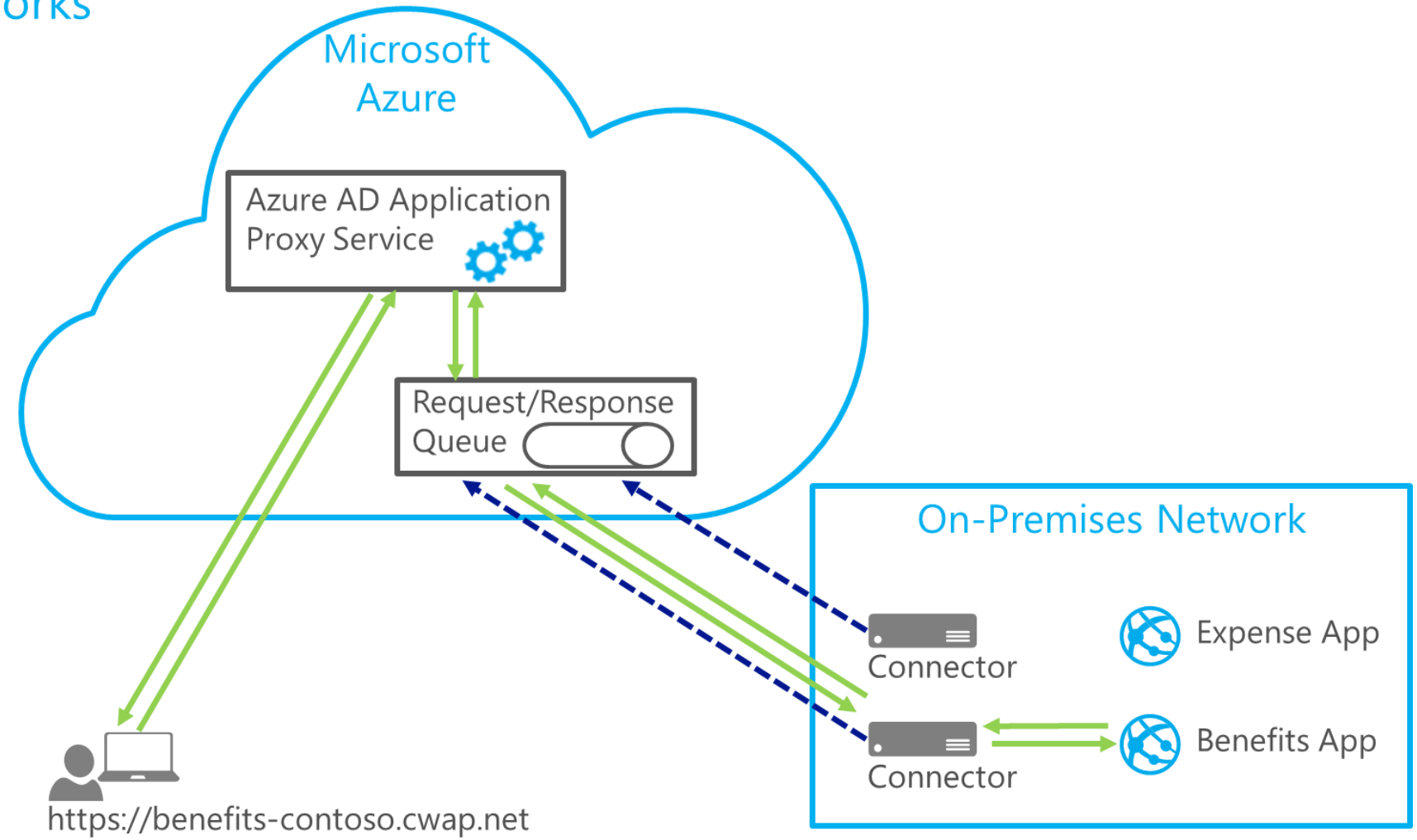
Simpler On-Premises Deployment

Connectors can be redundant for HA

Stateless Architecture (as compared to WAP with AD FS)

AZURE AD APPLICATION PROXY

How it works



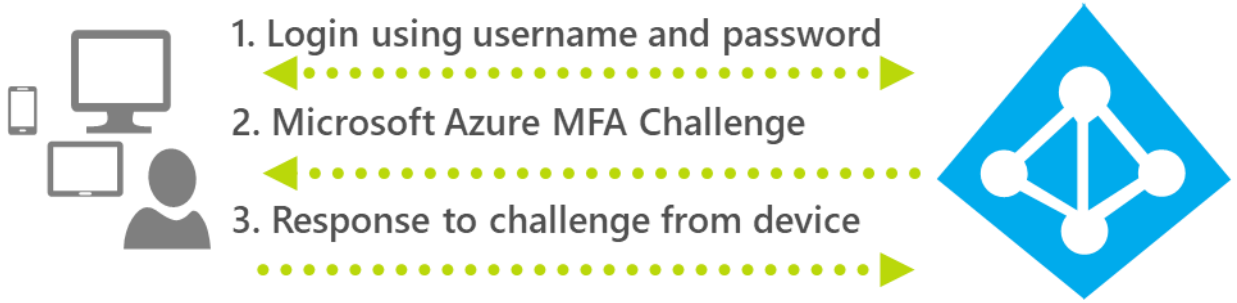
plain concepts

MULTI-FACTOR AUTHENTICATION (MFA)

What is it?

A method of authentication requiring the use of more than one verification method to authenticate a user.

- Mobile Application
- Automated Phone Call
- Text Message



How it works?

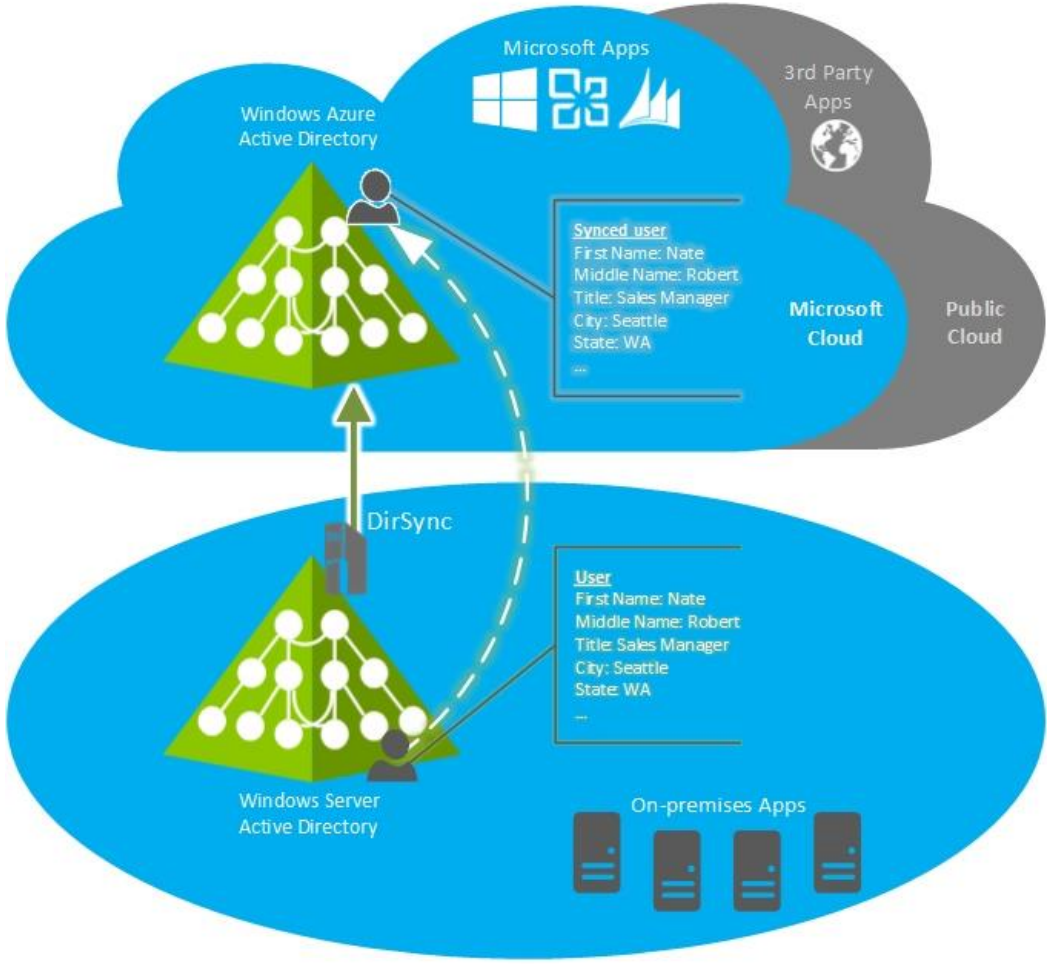
Requiring any two or more verification methods

- Something you know (typically a password)
- Something you have (a trusted device that is not easily duplicated, like a phone)

DIRECTORY SYNC

Synchronizes Users, Groups, and Contacts to Windows Azure AD.

Users will have a different password in Windows Azure AD than they have for the on-premise AD.

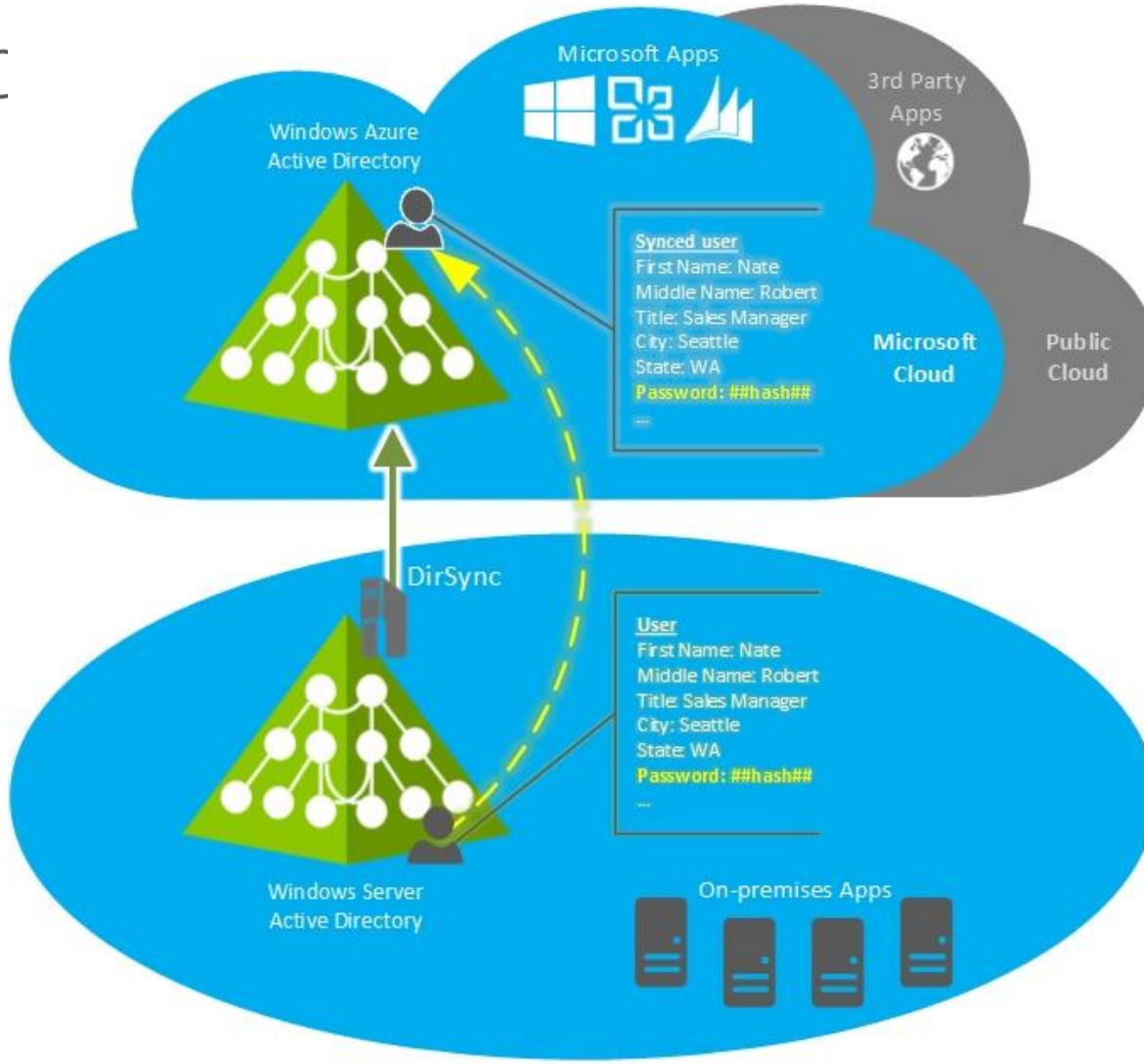


plain concepts

DIRECTORY SYNC W/PASSWORD SYNC

An extension of 'Directory Sync that also synchronizes a "hash" of the user's password.

Enables users to sign-in to cloud applications using their same on-premise password.



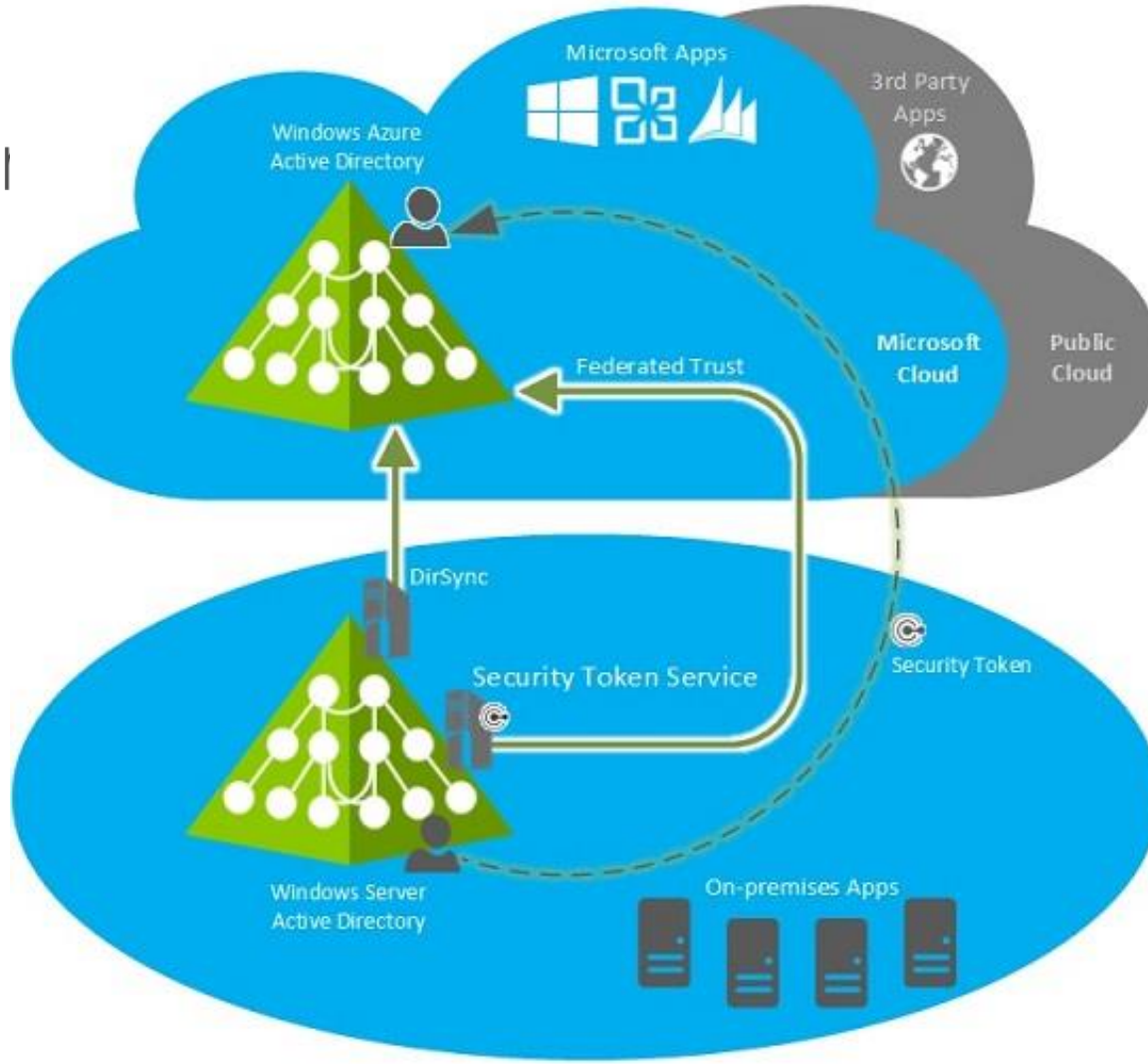
plain concepts

DIRECTORY SYNC W/SINGLE SIGN-ON

Users won't be challenged to enter username/password when accessing cloud applications.

Authentication occurs in the on-premise directory.

Requires an on-premises STS, such as ADFS.



plain concepts

DIRECTORY SYNC WRITEBACK CAPABILITY ("DIRSYNC")

Self-Services Password Reset with Writeback

Writeback capability enables password resets to be persisted back to on-premises Server AD

A feature of the Azure Active Directory "DirSync" Tool

Only available in Azure AD Premium

PRÁCTICAS PUBLICACIÓN APP PROXY

Generar el siguiente escenario

- Crear una MV windows.
  - Tamaño A1v2
  - Con ip pública.
  - Windows 2016.
  - Asignar a la subred Default
  - Configurar un nombre DNS en Azure.
  - Instalar el rol web y no bloquear por fw de Windows
  - Verificar el acceso por locahost y por ip pública
- Crear un conector de applications proxy
  - Utilizar como url interna el nombre DNS.
- Descargar el conector de application proxy e instalar en la MV
- Intentar acceder a la aplicación a través de la url externa
- Desde Enterprise applications daros permisos sobre la aplicación creada, asignando vuestro usuario
- Intentar acceder de nuevo.
- Crear una política de acceso condicional
  - Sobre la aplicación publicada
  - Bloquear cualquier ubicación
  - Acción bloquear.
- Probar a acceder a la aplicación
- Crear una localización con vuestra ip como localización de confianza
- Crear una exclusion a la localización con las zonas de confianza y probar de nuevo

plain concepts

ALMACENAMIENTO EN AZURE

plain concepts

AZURE STORAGE OVERVIEW

Azure Services: SQL Data Warehouse, HDInsight, Data Lake Store, Event Hubs, IoT Hubs…
Microsoft Services: Office 365, OneDrive, XBox, Skype…

Azure Storage

Foundational Building Block of Azure

Azure Services: SQL Data Warehouse, HDInsight, Data Lake Store, Event Hubs, IoT Hubs…
Microsoft Services: Office 365, OneDrive, XBox, Skype…

Hyper Scale	>30 million transactions per second, trillions of objects
Durable	Never lose your data. Multiple redundancy options. Automatic data checks
Secure	Encryption at Rest. Client side Encryption. Integration with KeyVault
Highly Available	Fault tolerance to hardware/software issues. Automatic load balancing
Open	REST API, Open sourced Client Libraries – .NET, Java, C++, Python, Node.js, iOS, Android, Xamarin…
Hybrid	Extensive partner ecosystem. Azure Stack for private/hosted clouds.

AZURE STORAGE OVERVIEW

IaaS

Storage | Virtual machines | Networking

Disks

Persistent disks for Azure IaaS VMs

Standard Storage Disks: Magnetic disk based, low IOPS, moderate latency

Premium Storage Disks: SSD based, high IOPS, low latency

Managed Disks

Files

Fully Managed File Shares in the Cloud

SMB and REST access

"Lift and shift" legacy apps

Blobs

Highly scalable, REST based cloud object store

Block Blobs: Sequential I/O, Hot, Cool and Archive Tiers

Page Blobs: Random-write pattern data

Append Blobs

Tables

Massive auto-scaling NoSQL store

Dynamic scaling based on load

Scale to PBs of table data

Fast key/value lookups

Queues

Reliable queues at scale for cloud services

Decouple and scale components
Message visibility timeout and update message to protect against unreliable dequeuers

Built on a unified Distributed Storage System

Durability, Encryption at Rest, Strongly Consistent Replication, Fault Tolerance, Auto Load-Balancing

AZURE STORAGE OVERVIEW

plain concepts

AZURE STORAGE OVERVIEW

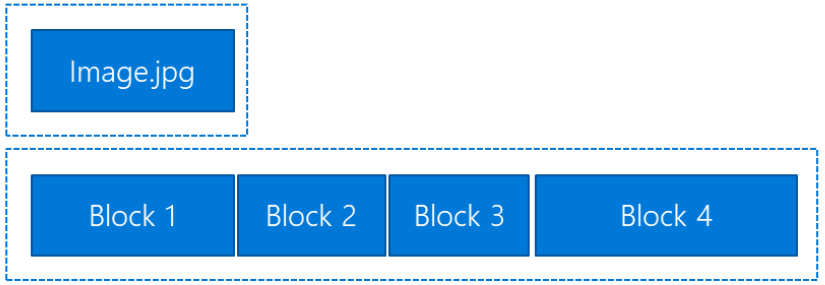
What is the Blob Storage Service?

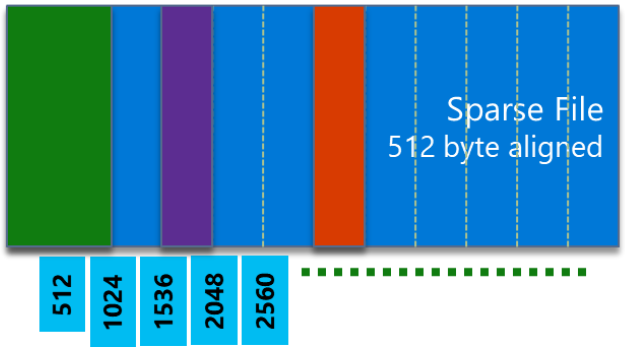
Azure's Object Storage platform

- Store and serve unstructured data
  - App and Web scale data
  - Backups and Archive
  - Big Data from IoT, Genomics, etc.

Types of Blobs

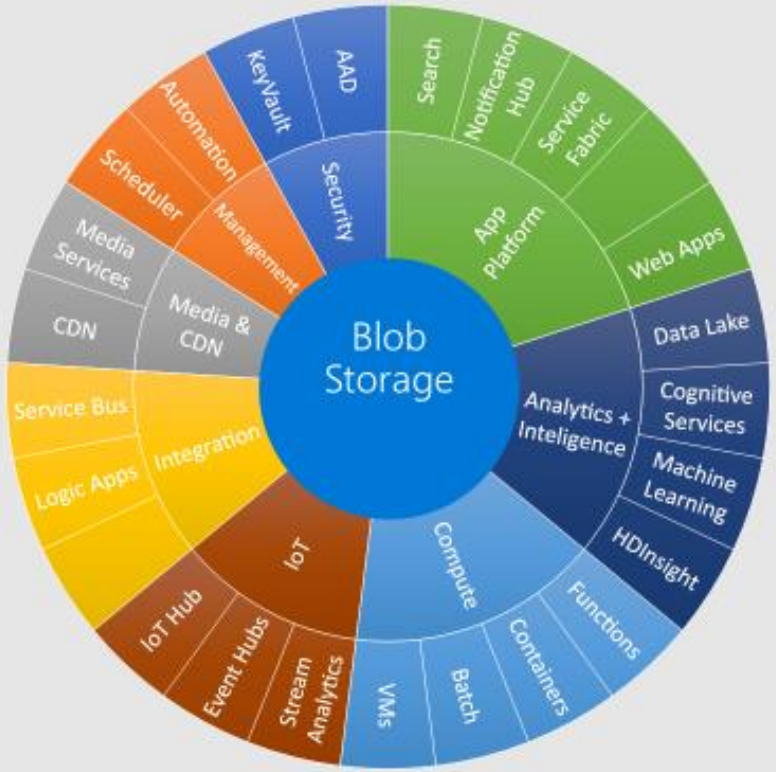
- Block Blobs - Most object storage scenarios
- Append Blobs - Multi-writer append only scenarios
- Page Blobs - Page aligned random reads and writes





AZURE STORAGE OVERVIEW

Azure Ecosystem and Blob Storage



Broad integration for Blobs across Azure services

Enables many scenarios

AZURE STORAGE OVERVIEW

BLOB STORAGE: IDEAL FOR PAAS

Why?

- Limitless Scale
- Globally accessible
- Cost Efficient

Scenarios for PaaS usage of Blob Storage:

- Live Data Repository
- Big Data Analytics
- IoT/sensor data
- Active or Deep Archive

BLOB STORAGE – ARCHITECTURAL PILLARS

Durable & Available

Secure & Compliant

Manageable & Cost Efficient

Scalable & Performant

Open & Interoperable

BLOB STORAGE – ARCHITECTURAL PILLARS

BLOB STORAGE – ARCHITECTURAL PILLARS

Durability & Availability

Azure Storage Blobs Durability & Availability

Strong Consistency
3 replicas + erasure coding

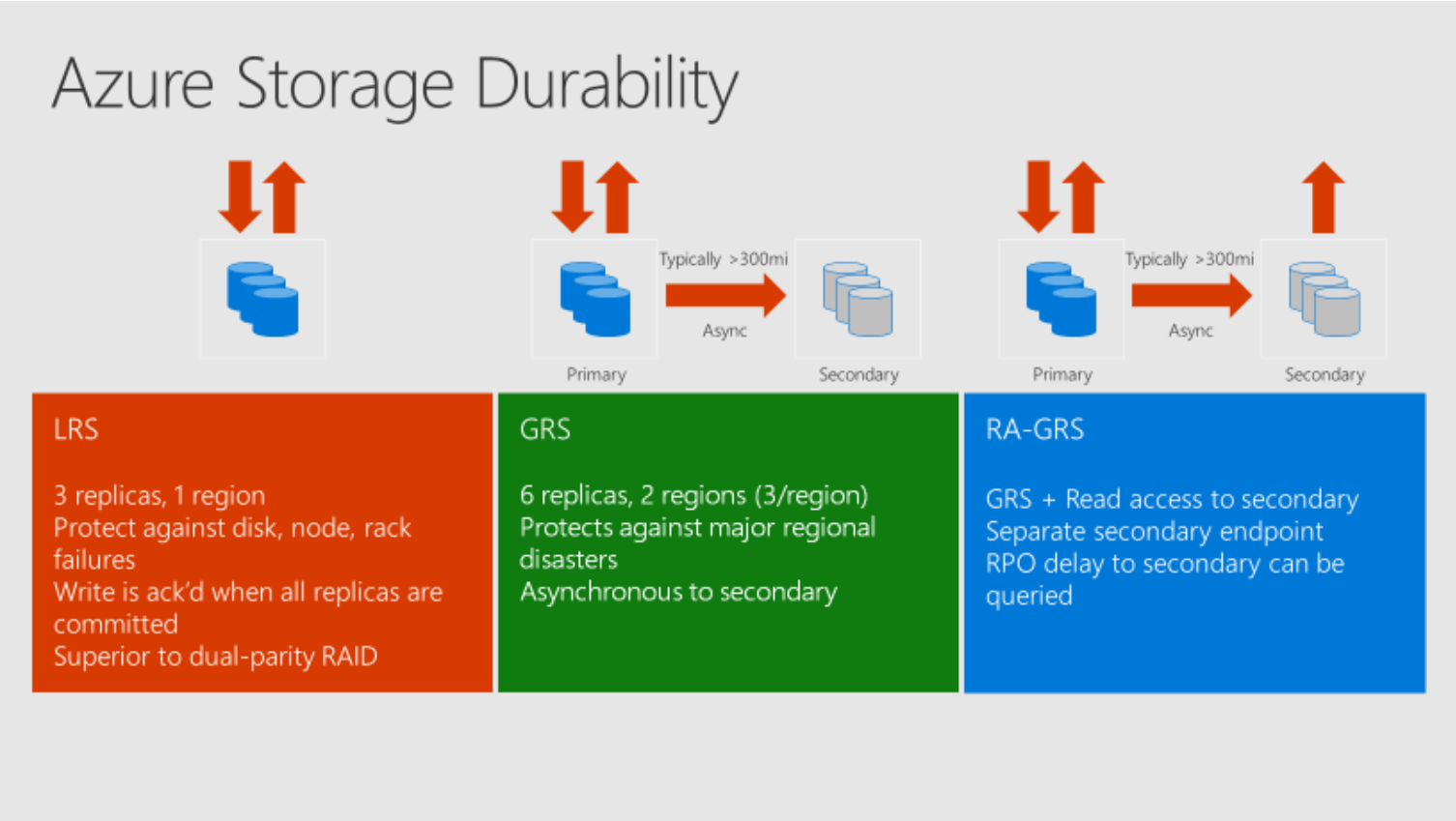
Data Integrity
MD5 hash on ingress/egress
CRC checksum & "bit rot" protection

Disaster Recovery (BCDR)
Geo-redundant storage (GRS)

High Availability (HA)
99.9% availability SLA
99.99% for reads with RA-GRS

BLOB STORAGE – ARCHITECTURAL PILLARS

Durability & Availability



BLOB STORAGE – ARCHITECTURAL PILLARS

plain concepts

BLOB STORAGE - ARCHITECTURAL PILLARS

Secure & Compliant

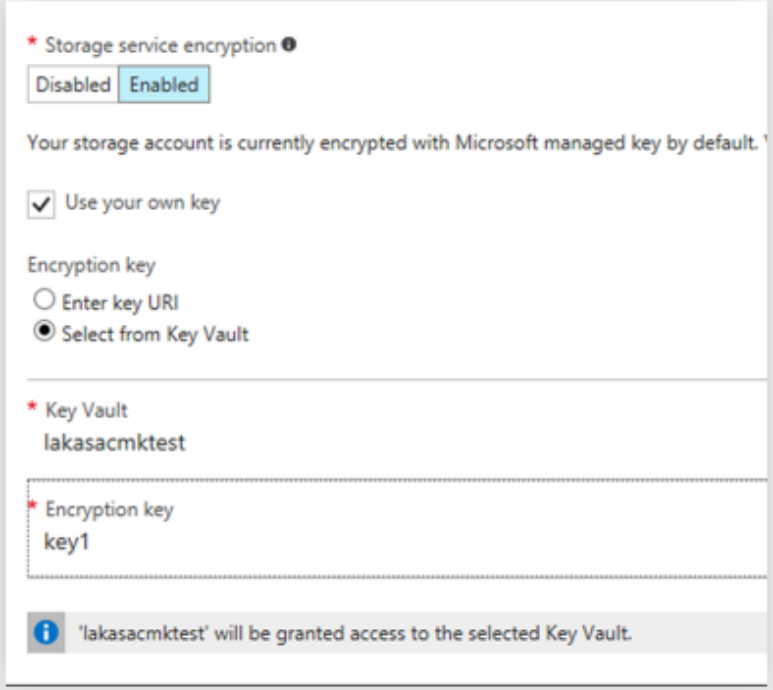
Encryption At Rest – Storage Service Encryption

Prevents data disclosure from physical disk compromise

Available for Blobs with MS managed keys

New – Encryption enabled for all accounts – Coming soon

New - Customer managed encryption keys – In Preview



BLOB STORAGE – ARCHITECTURAL PILLARS

Secure & Compliant

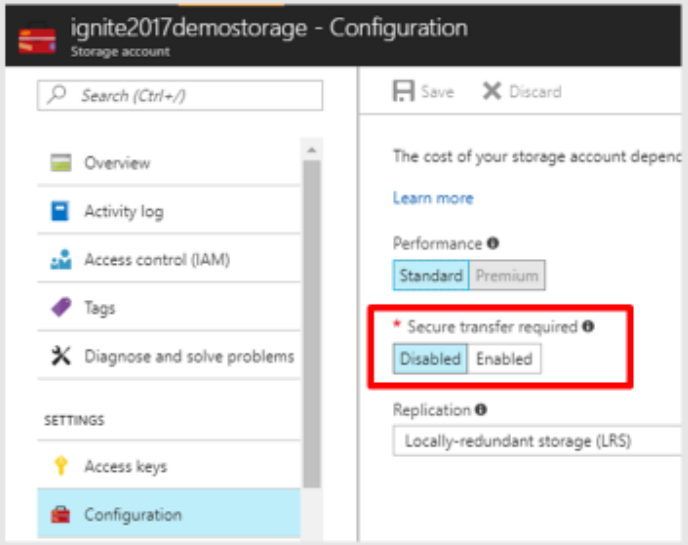
Encryption In Transit

Storage REST APIs support HTTPS

SAS Tokens can be restricted for HTTPS only

New - "Secure Transfer" option

- Limit *all* access to HTTPS only
- Enables control via ARM Policy and monitoring via Azure Security Center
- Available now



BLOB STORAGE – ARCHITECTURAL PILLARS

Secure & Compliant

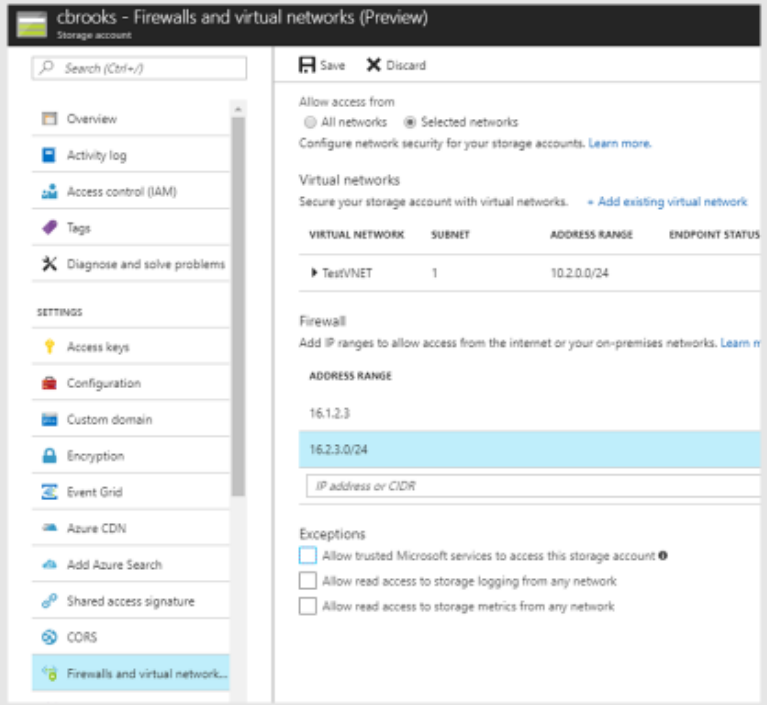
New - Firewalls and Virtual Networks

Layered security for Storage

Protection from key disclosure threats

Limit access to specific Azure VNETs or external internet IP address ranges

Annnouncing Public Preview



plain concepts

BLOB STORAGE – ARCHITECTURAL PILLARS

Secure & Compliant

New - AAD Authentication and RBAC

Currently support AAD, OAuth and RBAC on Storage Resource Provider via ARM

Adding AAD and OAuth support to Blob Storage REST API

Integrating with Azure RBAC for Authorization

- Role assignments down to container scope

On Roadmap

RESOURCE TYPE	READ	WRITE	DELETE
Microsoft Storage			
Location			
Name Availability	✓		
Operations	✓		
Storage Accounts	✓	✓	✓
Blob Services	✓	✓	
Containers	✓	✓	✓
Blobs	✓	✓	✓

BLOB STORAGE – ARCHITECTURAL PILLARS

Secure & Compliant

New - Immutable (WORM) Storage

Feature Overview

Write-modify-delete protection

Retention-interval based policy

Audit logging

Available for all blob tiers (hot, cool, archive)

Feature Benefits

SEC 17a-4(f) compliance

Legal hold support

Low cost for compliance archives

Immutably store hot and cold data in a single storage account

Preview in late CY17, GA in H1 CY18

BLOB STORAGE – ARCHITECTURAL PILLARS

Blob Storage Pillars

Durable & Available	Secure & Compliant	Manageable & Cost Efficient	Scalable & Performant	Open & Interoperable

plain concepts

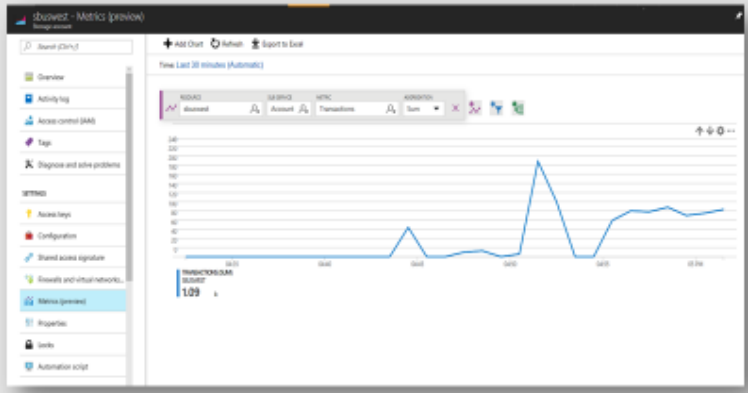
BLOB STORAGE – ARCHITECTURAL PILLARS

Manageable & Cost efficient

Storage Metrics/Logs - Azure Monitor Integration

Benefits

Access from unified Azure Monitor APIs
Setup charts and alerts based on metrics
Archive analytics data into storage account
Stream analytics data to Event Hub, OMS, etc.
Access from Azure Portal, REST, SDK, Powershell, CLI



Timeline

Metrics in Azure Portal - Public preview now
Metrics with SDK (REST API) – Public preview now
Stream metrics data into storage account – Public preview now
Diagnostic logs – Public preview in H1 2018

BLOB STORAGE - ARCHITECTURAL PILLARS

Manageable & Cost efficient

New - Data Protection – Soft Delete

Recovery from accidental deletions

Configurable

Number of days to retain (max: 365)

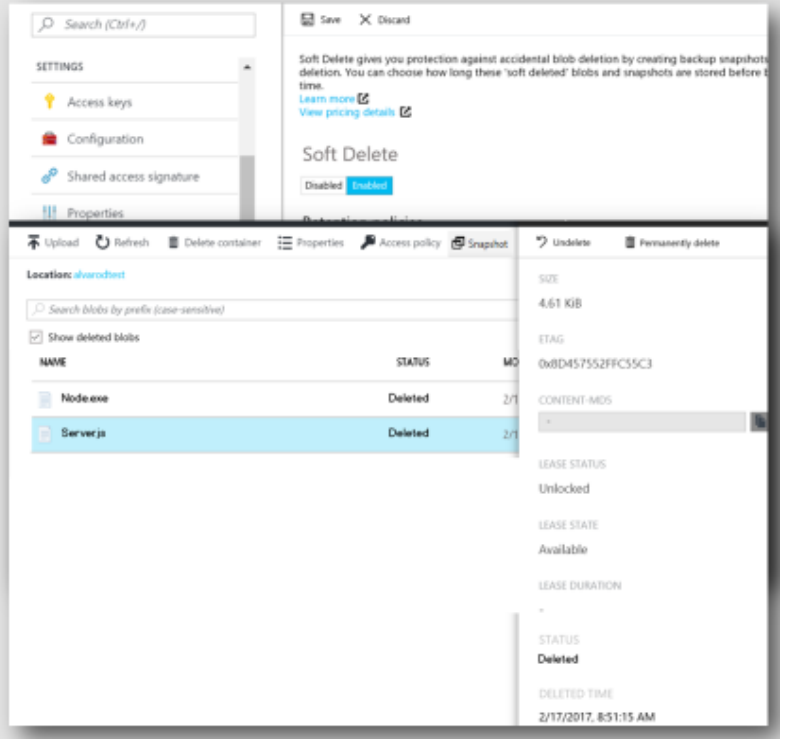
Can be turned off

Blob level

DeleteBlob call results in an entry

GA: H1 CY18

Future: Object Versioning



plain concepts

BLOB STORAGE – ARCHITECTURAL PILLARS

Manageable & Cost efficient

Tiered Object Storage

Cost Efficiency and Scale are core tenets of Object Storage

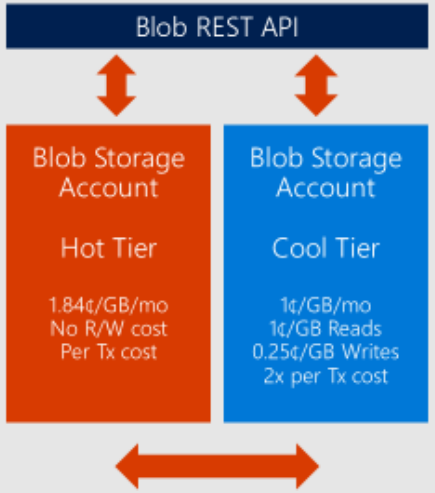
Data has different "temperatures" over its lifecycle

Blob Storage: Offered at different tiers and cost

Two tiers currently: Hot and Cool

Milliseconds to first byte for both tiers

API is 100% identical



BLOB STORAGE – ARCHITECTURAL PILLARS

Manageable & Cost efficient

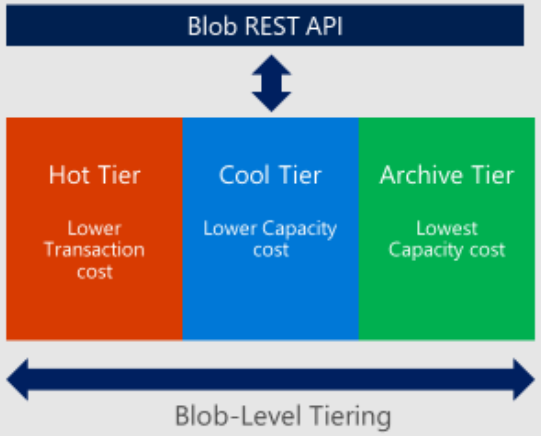
New - Blob Level Tiering

Introducing Blob-Level Tiering
- Individual blobs can move between tiers
- All tiers co-exist in the same storage account

New API to set blob tier: *SetBlobTier*
- Acknowledged immediately from service

Get APIs *(GetBlobProperties and ListBlobs)* return current tier and archive status
- New headers "*x-ms-access-tier*" and "*x-ms-archive-status*"

Future: Automated Lifecycle Management



BLOB STORAGE – ARCHITECTURAL PILLARS

Manageable & Cost efficient

Archive Storage Scenarios

Long-term backup and disaster recovery datasets

Original data retention (e.g. raw media files after transcoding)

Healthcare - medical records, medical imaging (e.g. X-rays, ultrasounds)

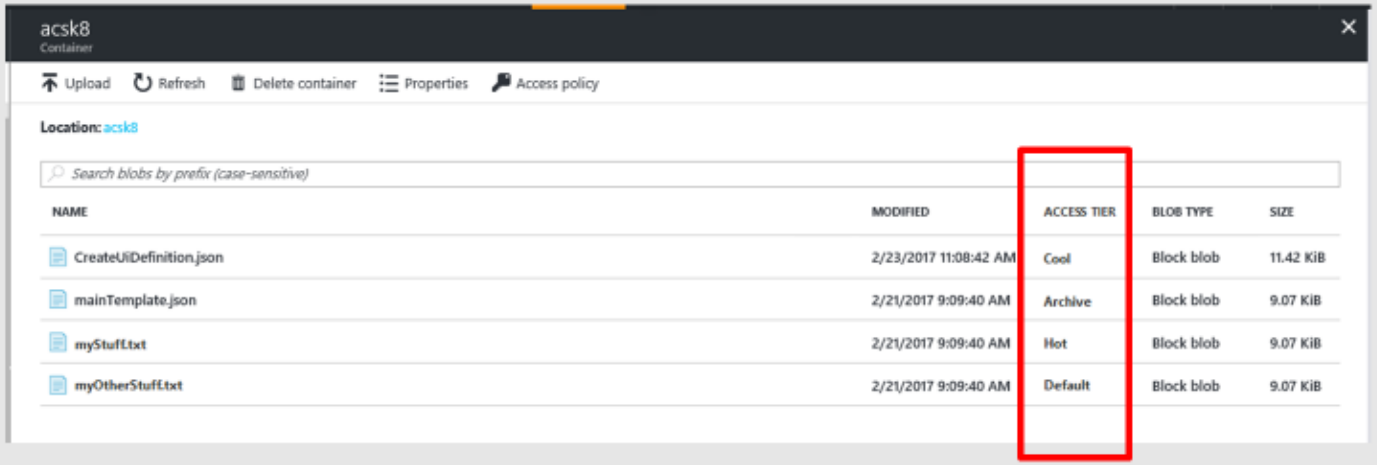
Business compliance data (e.g. security camera footage, call recordings)

Legal compliance (e.g. financial/tax records, employee information)

BLOB STORAGE – ARCHITECTURAL PILLARS

Manageable & Cost efficient

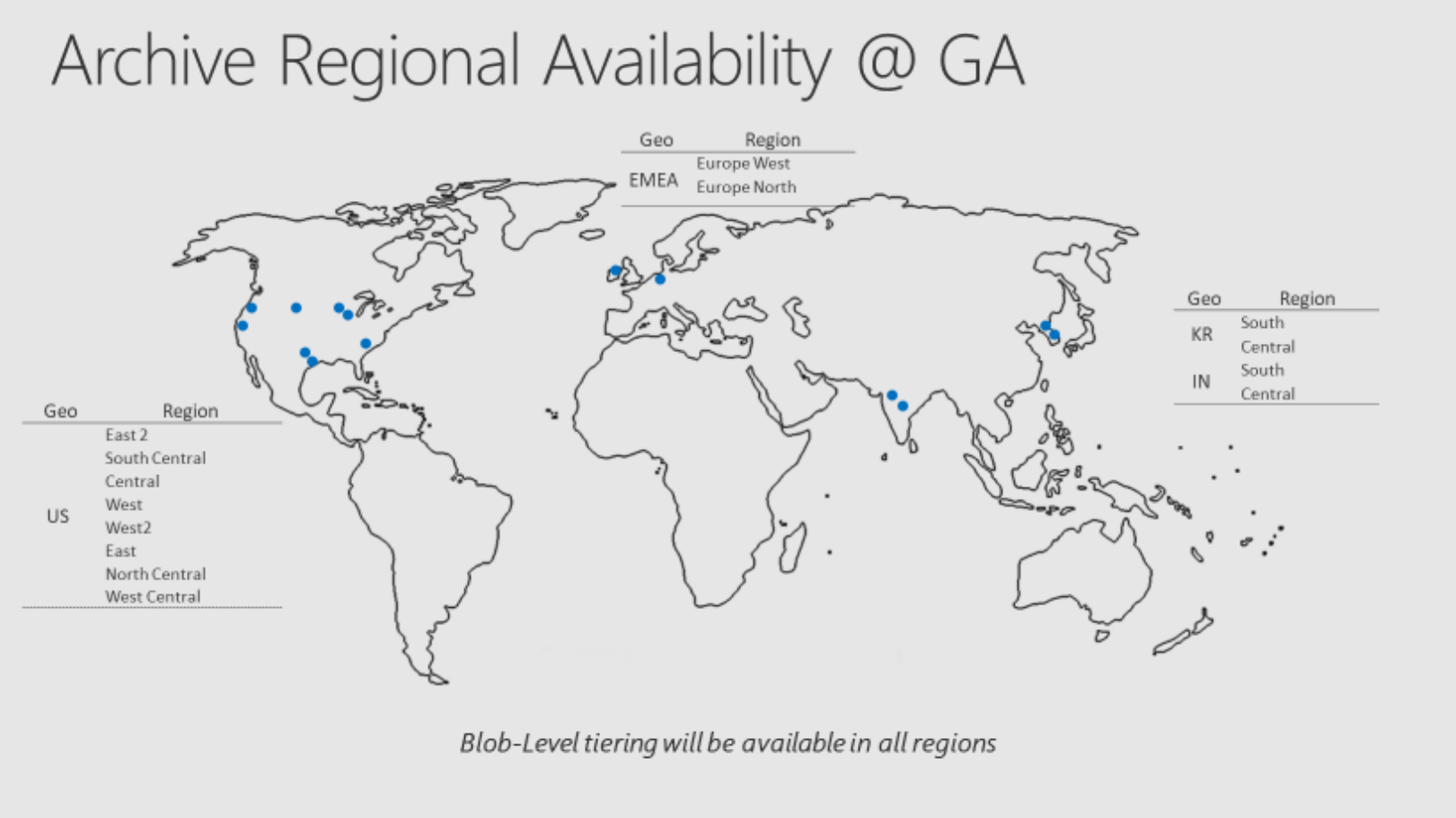
Tiered Storage



plain concepts

BLOB STORAGE – ARCHITECTURAL PILLARS

Manageable & Cost efficient



plain concepts

BLOB STORAGE – ARCHITECTURAL PILLARS

Blob Storage Pillars

Durable & Available	Secure & Compliant	Manageable & Cost Efficient	Scalable & Performant	Open & Interoperable

BLOB STORAGE – ARCHITECTURAL PILLARS

Scalable & Perfomant

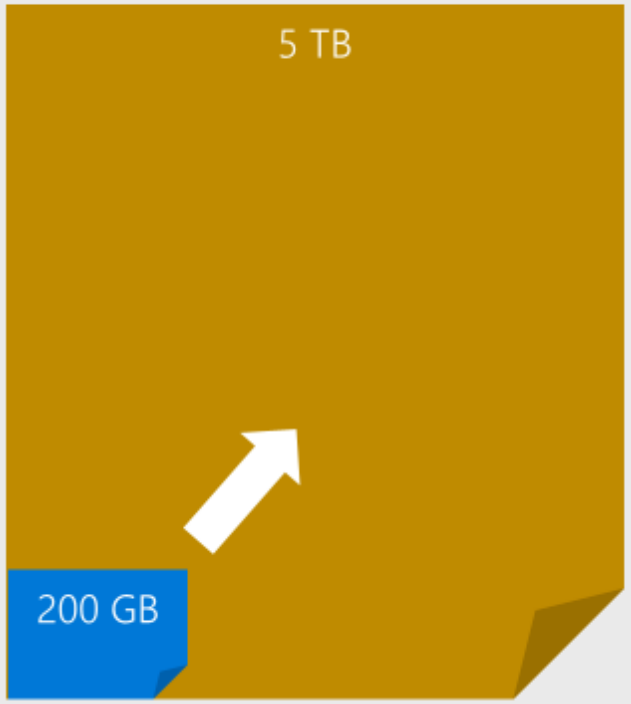
Individual Blob Performance & Scale Improvements

Large Block Blobs

Single Blob max increased 25x to 5TB
Write throughput improvements

Small Block Blobs

Improved read latency for blobs <4MB



BLOB STORAGE – ARCHITECTURAL PILLARS

Scalable & Perfomant

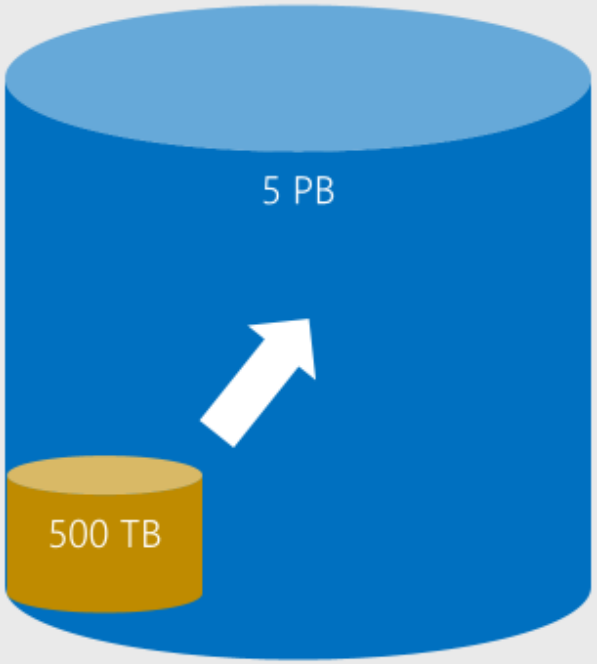
New - Storage Account Scalability

Scale Target increases per account

500TB → 5 PB storage capacity
20K → 50K Requests/sec
20 Gbps → 50 Gbps Bandwidth

More coming in late CY17 & CY18

Optimized for rapid storage scale out for HPC and big data



BLOB STORAGE – ARCHITECTURAL PILLARS

Scalable & Perfomant

Data Ingestion at Scale - Online

Over Internet

- Possible bottleneck – Internet bandwidth out of your location
- Partner solutions for accelerated uploads – Aspera, Signiant

Using Express Route

- Secure, provisioned connection to Azure
- Up to 10Gbps links, with multiple 10Gbps links supported
- Active/Active with double the provisioned bandwidth
- 10Gbps = 3.2PB of ingress/egress per month

BLOB STORAGE – ARCHITECTURAL PILLARS

Scalable & Perfomant

Data Ingestion at Scale - Offline

Azure import/export service
Disk based import - Up to 10TB SATA drives
Available in many regions
Requires disks and prep/load on to disks

BLOB STORAGE – ARCHITECTURAL PILLARS

Scalable & Perfomant

New - Azure Data Box PREVIEW

Fast and Easy

Rent an Azure Data Box and transfer 100 TB of data to Azure in around a week

Data Box uses standard NAS protocols

Safe and Secure

Azure Data Box is tamper-resistant and ruggedized for shipping

Data is protected with AES-256 encryption for safe transit

Sign up today:
https://aka.ms/azuredatabox

SECURITY AZURE STORAGE

Security & Compliance

Initial concern

60%

cited concerns around data security as a barrier to adoption

45%

concerned that the cloud would result in a lack of data control

Realized benefit

94%

experienced security benefits they didn't previously have on-premise

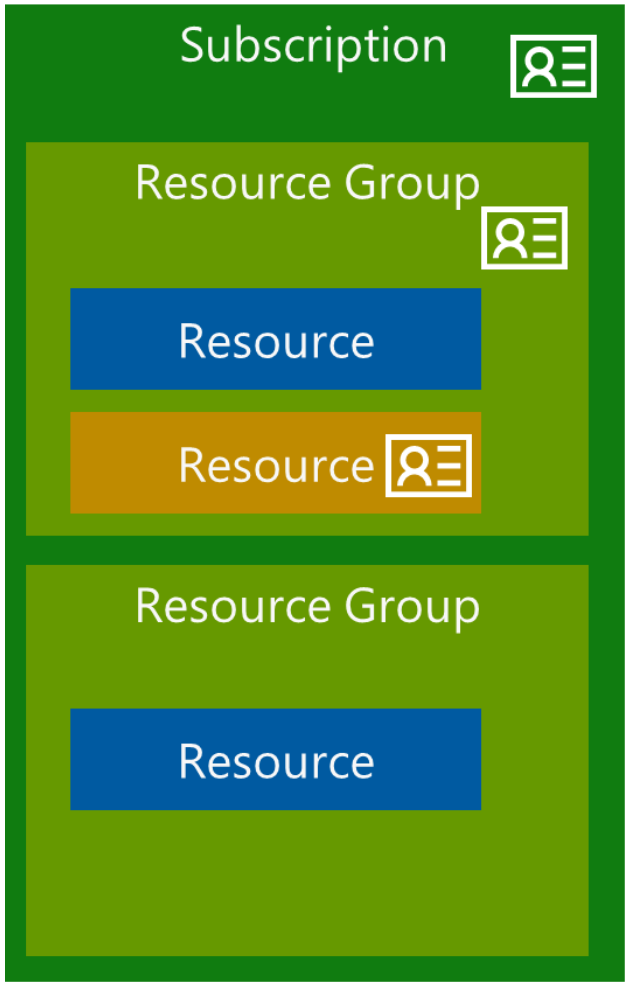
62%

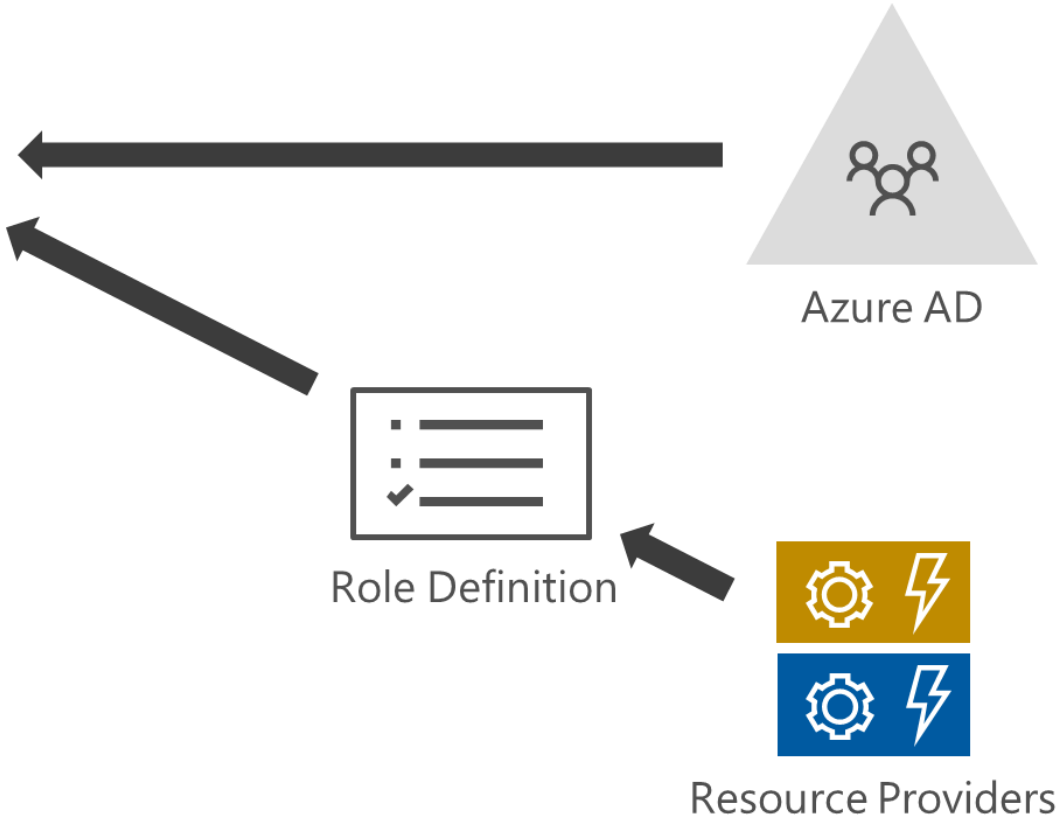
said privacy protection increased as a result of moving to the cloud

plain concepts

SECURITY AZURE STORAGE

RBAC





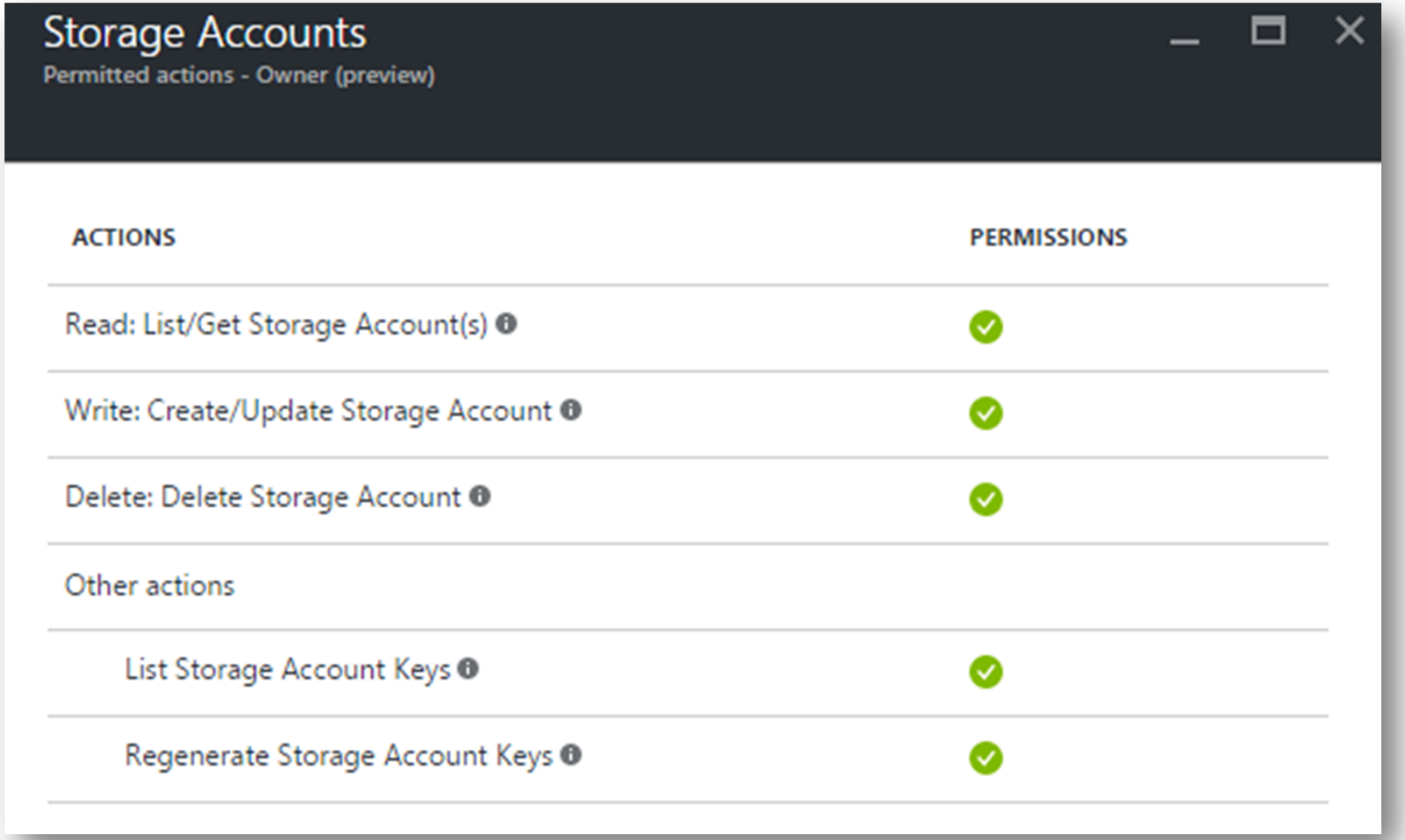
Learn more:

- *BRK3203 Manage and control your applications with Microsoft Azure Resource Manager*

plain concepts

SECURITY AZURE STORAGE

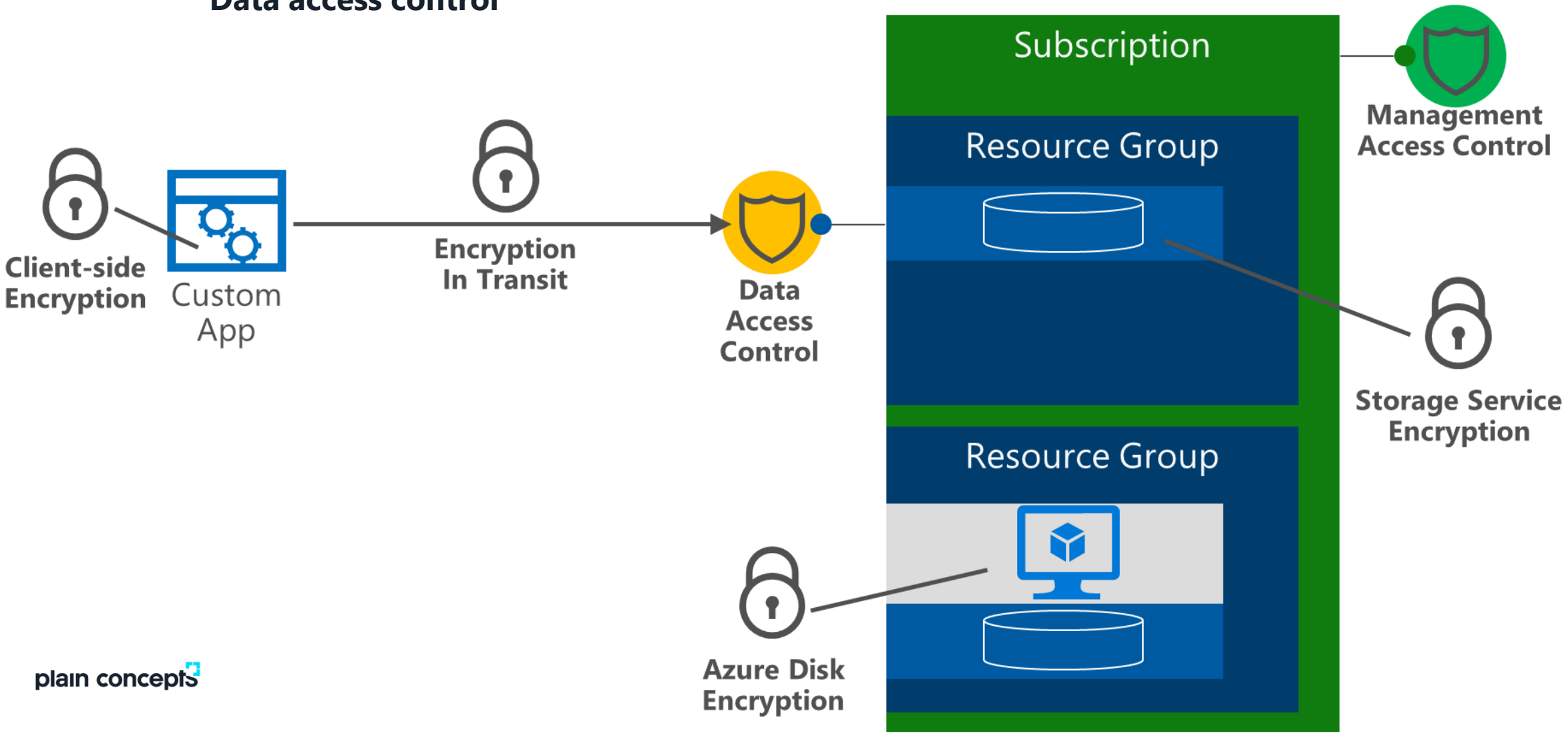
Storage Resource Provider Permissions



plain concepts

SECURITY AZURE STORAGE

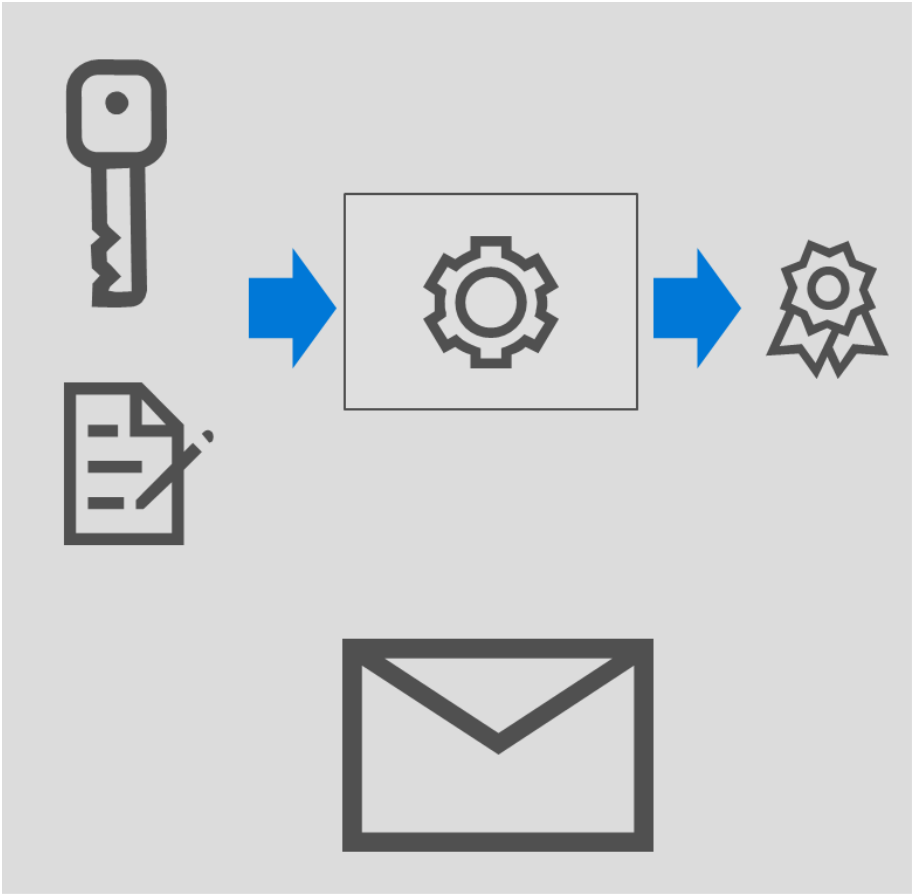
Data access control



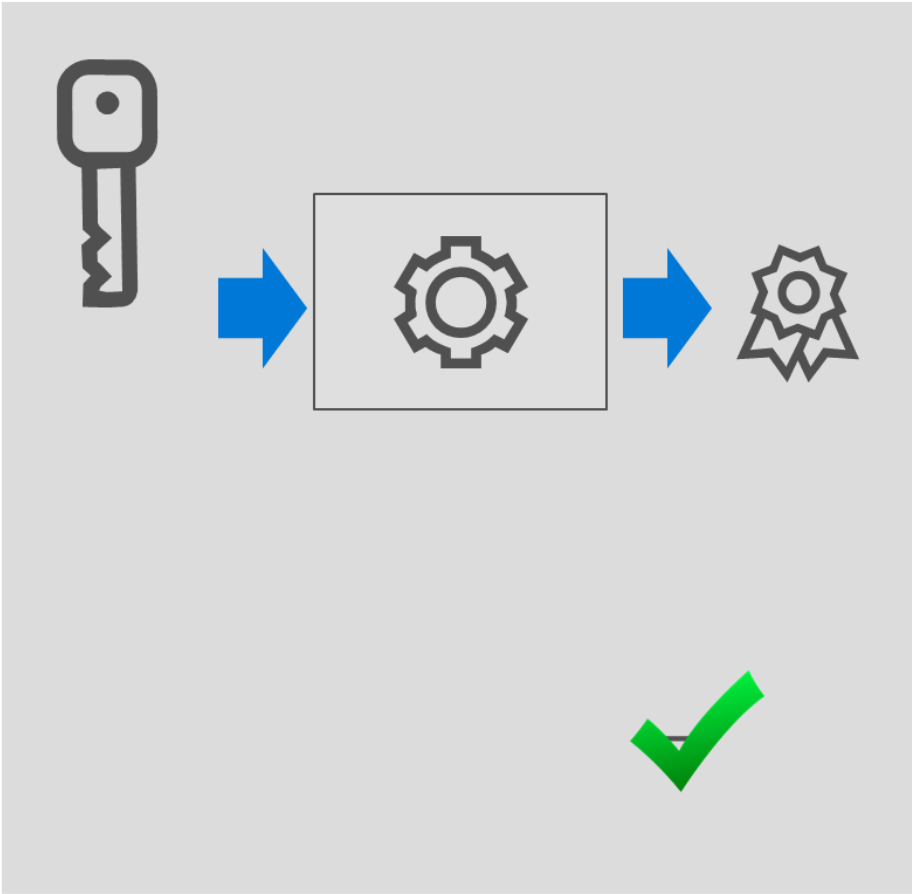
plain concepts

SECURITY AZURE STORAGE

Shared key security



Client



Service

plain concepts

SECURITY AZURE STORAGE

Client side encryption

Encrypt Data in Your Applications

Scenario: Customer wants to encrypt data within their client applications prior to sending to Azure

- Support for Blob, Table and Queue Storage
- Uses AES 256 cipher
- Provides option to integrate with on-premises Key Management and Azure Key Vault
- Storage Service never sees the keys nor the unencrypted data
- Supported in .NET, Java and Python, Windows and Linux client libraries

Key Management

- Can generate and manage your own encryption keys.
- Can use keys generated by the storage client library.
- Can have Azure Key Vault generate/store the root keys.

SECURITY AZURE STORAGE

Azure security center

Understand your security posture

Gain visibility into security across your Azure subscriptions

Enable security at cloud speed

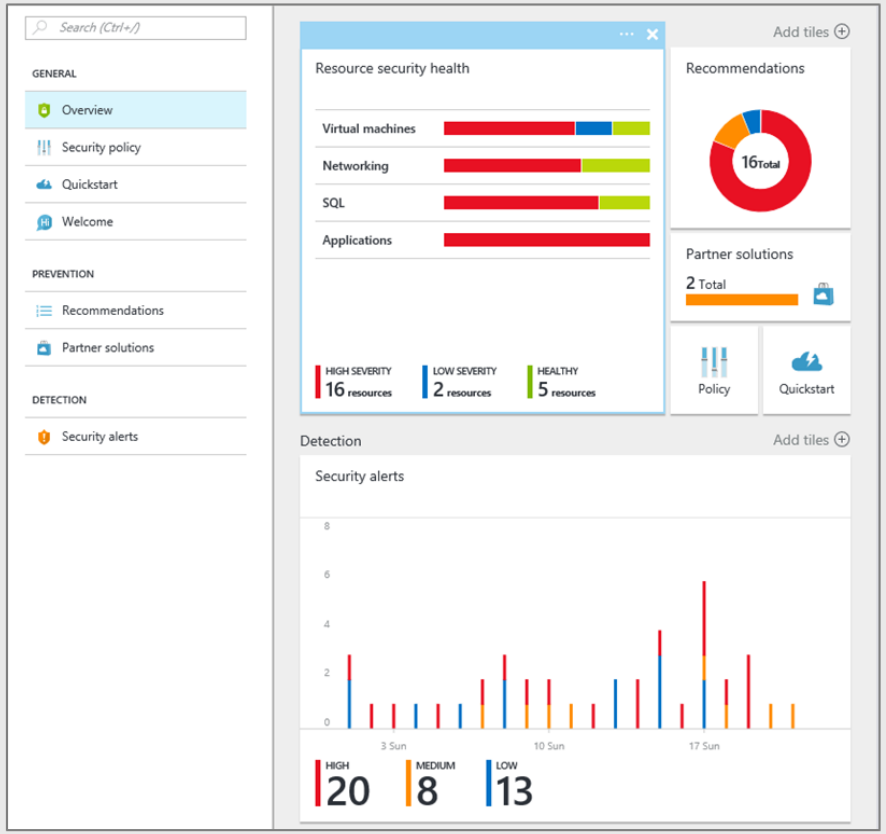
Use security policies to monitor cloud resources even as they change – quickly find and fix vulnerabilities

Detect attacks early

Get alerted to attacks detected using advanced security analytics and Microsoft global threat intelligence

Act quickly to mitigate damage

Arm yourself with information about an attacker's actions, mapped across the kill chain, as well as their known objectives and tactics



CONFIGURACIÓN CUENTA ALMACENAMIENTO

Escenario a crear:

Crear una cuenta de almacenamiento:

- (StorageV2 (uso general v2))
- Zona Oeste Europa
- Replicación local (LRS)
- Rendimiento estándar
- Solicitar transferencia segura
- Habilitar integración redes virtuales
    - Usar la Vnet del grupo de recursos
    - Usar la subred para MV

Cambiar el tipo de acceso a frecuente

Cifrar el almacenamiento en la cuenta con la integración con Key Vault

- Setting→Encryption→Habilitar
    - Crear Key Vault
    - Crear key
- Impedir que ningún servicio de MS se conecte con la cuenta de almacenamiento.
- Volver a permitirlo.
- Crear un contenedor y subir un archivo

plain concepts

CONFIGURACIÓN CUENTA ALMACENAMIENTO

- ¿Podéis subir el archivo?
- Hacer una copia de seguridad del archivo
- Eliminar la instantanea y posteriormente recuperarla
- Cambiar el access tier del fichero subido a “archive”.
- Abrir el archivo.
- Volver el archivo a access tier “hot”
- Generar una SAS.
- Acceder al archivo por la URL.