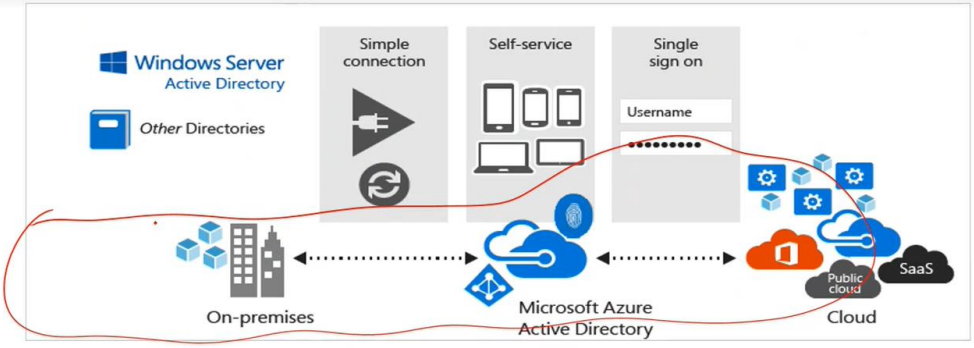
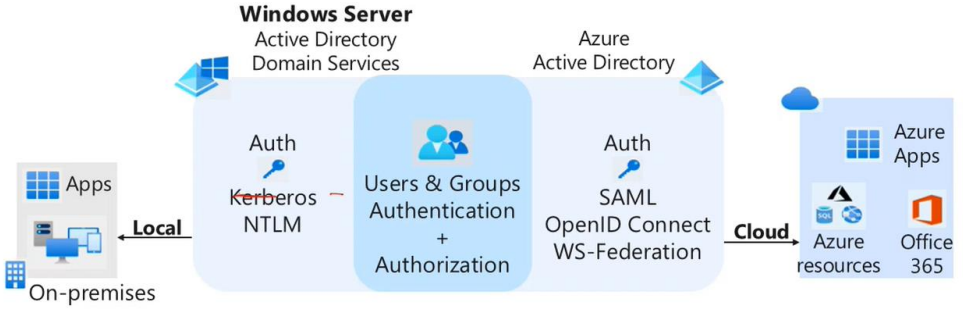
Azure Active Directory Features



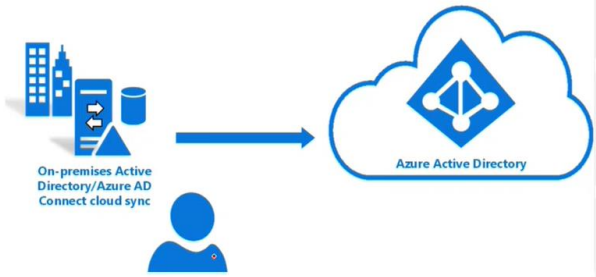
Microsoft's multi-tenant cloud-based directory and identity management service	Identity management capabilities and integration	Integrates with Windows Server Active Directory	Provides SSO access

Azure AD versus Active Directory Domain Services (AD DS)



Service	Authentication	Structure	What it's used for
Azure Active Directory	Includes SAML, OpenID Connect (based on OAuth), WS-Federation	Tenants	Internet-based services and applications like Office 365, Azure services, and third-party SaaS applications
Active Directory Domain Services	Kerberos, NTLM	Forests, domains, organizational units	Authentication and authorization for on-premises printers, applications, file services, and more

Azure AD Connect cloud sync



Alternate method to integrate your on-premises directories with Azure Active Directory

Uses the Azure AD cloud provisioning agent

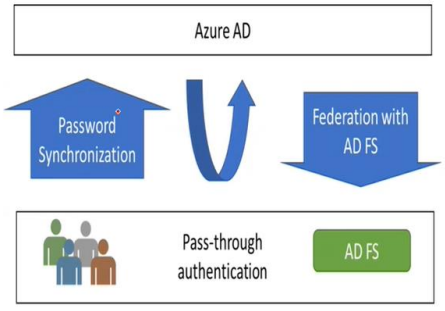
Runs stand-alone or along-side Azure AD Connect

Authentication Options

Password Hash Synchronization (PHS) can synchronize an encrypted version of the password hash for user accounts

Pass-through authentication (PTA) authenticates the username and password with the on-premises domain controllers

AD FS is the Microsoft implementation of an identity federation solution that uses claims-based authentication

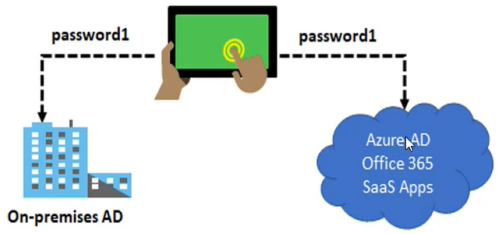


Password Hash Synchronization

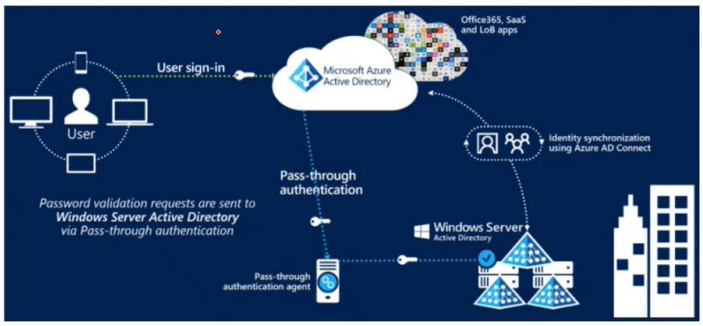
Password hash synchronizes user passwords from on-premises Active Directory to cloud-based Azure AD

Sign into Azure AD services using the on-premises password

Improve the productivity of your users and reduce your helpdesk costs



Pass-through Authentication



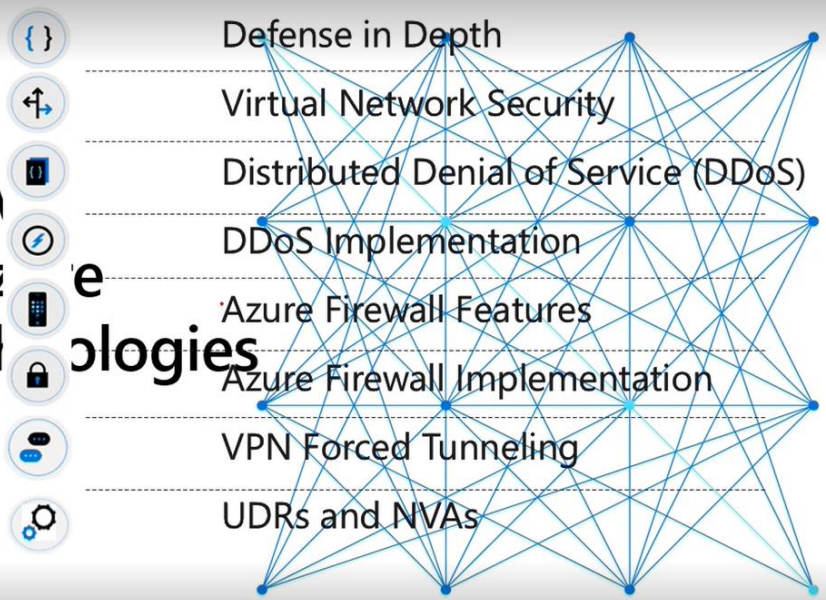
Supports user sign-in into all web browser-based applications and into Microsoft Office client applications

Is a free feature and can be enabled via Azure AD Connect

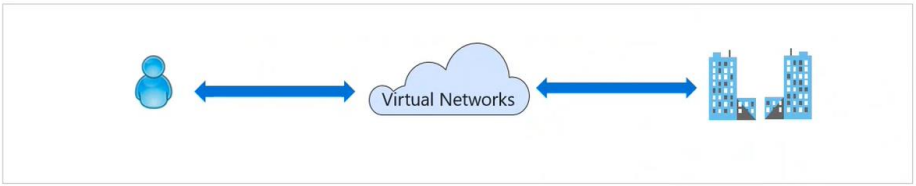
Is not only for user sign-in but allows an organization to use other Azure AD features – MFA and Self-Service Password Reset

Infra sec:

Perimeter Security



Virtual Network Security

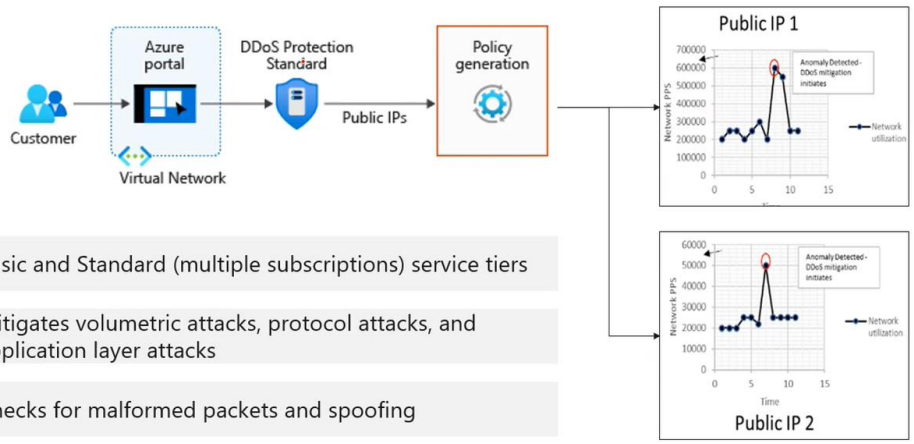


- Dynamic and reserved public IP addresses
- Direct virtual machine access
- Load balancing
- DNS hosting
- Traffic management
- DDoS protection

- Bring your own network
- Segment with subnets
- Add network security groups
- Create user defined routes

- Point-to-site for dev/test
- VPN Gateways for site-to-site
- ExpressRoute for private connectivity

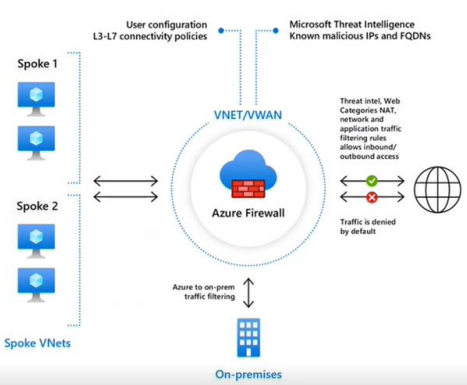
DDoS Implementation



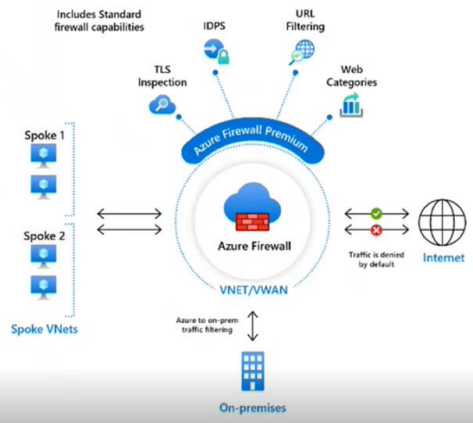
- Basic and Standard (multiple subscriptions) service tiers
- Mitigates volumetric attacks, protocol attacks, and application layer attacks
- Checks for malformed packets and spoofing

Azure Firewall

Azure Firewall Standard

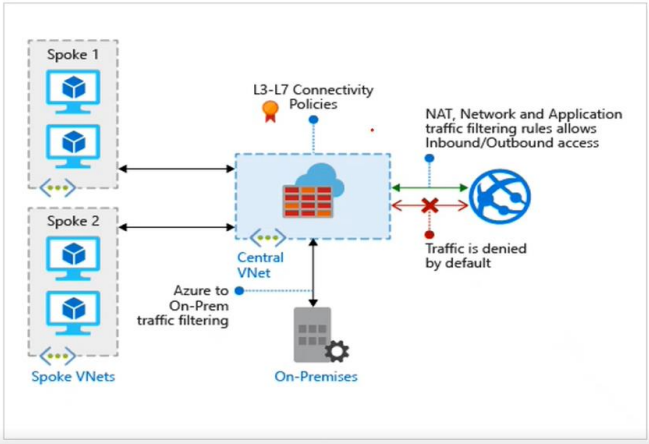


Azure Firewall Premium



Azure Firewall Implementation

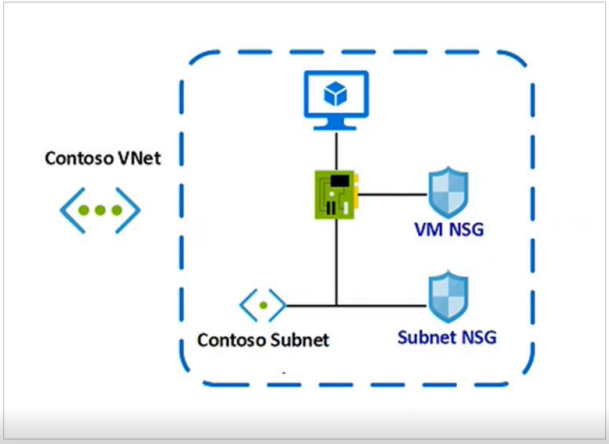
- Application FQDN filtering rules
- Network traffic filtering rules
- FQDN tags
- Outbound SNAT
- Inbound DNAT support
- L3-L7 connectivity policies
- Separate firewall subnet
- Static public IP address



- Forced tunnelling – Push all internet traffic for specific next hop (example – on-premises device).

Network Security Groups (NSG)

- Limit virtual network traffic
- Can be associated to a subnet or a network interface
- Uses security rules to allow or deny network traffic
- Default inbound and outbound rules allow virtual network and load balancers – all other traffic denied



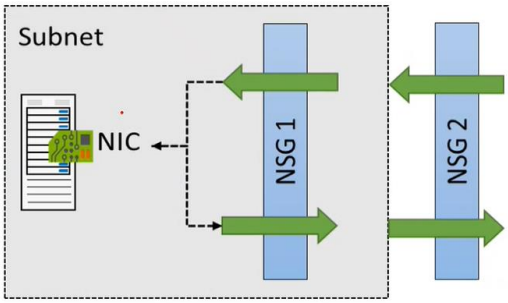
NSG Implementation

NSGs are evaluated independently for the subnet and NIC

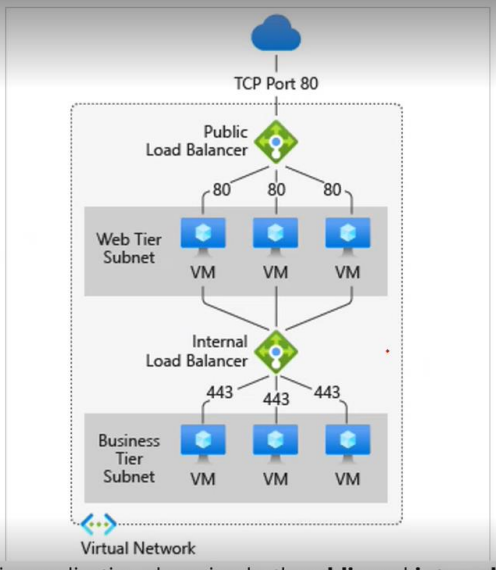
An "allow" rule must exist at both levels for traffic to be admitted

You can add more rules – many preconfigured selections (SSH, RDP, FTP…)

Troubleshoot with the Effective Security Rules link



Load Balancer



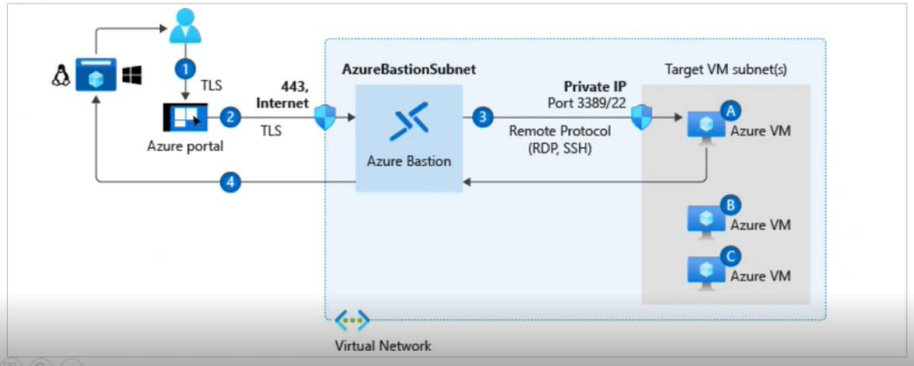
Balancing multi-tier applications by using both **public** and **internal** Load Balancer

Host Security

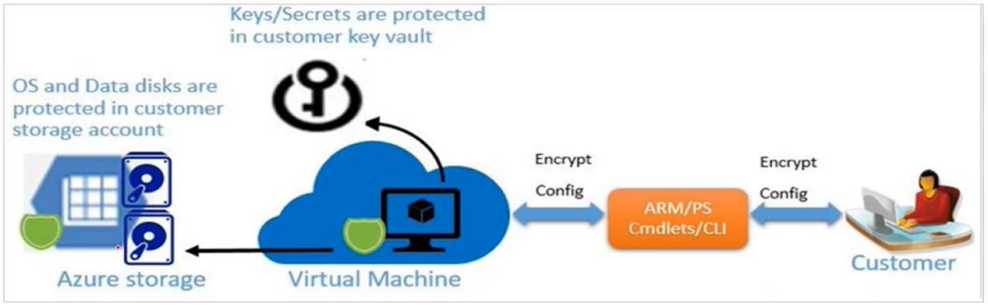
- Endpoint Protection
- Privileged Access Workstations
- Virtual Machine Templates
- Remote Access Management
- Update Management
- Disk Encryption
- Microsoft Defender
- Security Center Recommendations
- Securing Azure Workloads

Remote Access Management

Remote Desktop Protocol (RDP) for Windows-based virtual machines	Secure Shell Protocol (SSH) for Linux based virtual machines	Bastion Subnet for RDP/SSH through the Portal over SSL



Disk Encryption



Provides encryption of the operating system and data disks

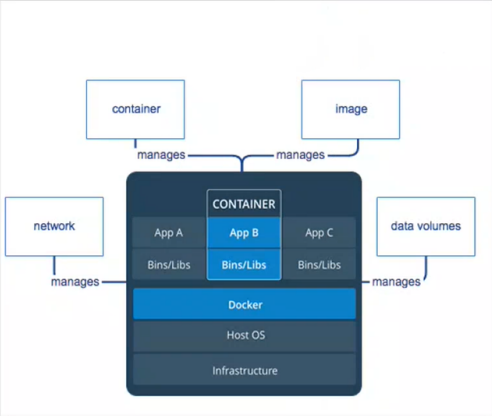
Windows VMs (BitLocker) and Linux VMs (DM-Crypt)

Stores encryption keys in a customer-managed key vault

Container Security

- Containers
- ACI Security
- Azure Container Instances (ACI)
- Azure Container Registry (ACR)
- ACR Authentication
- Azure Kubernetes Service (AKS)
- AKS Terminology
- AKS Architecture
- AKS Networking
- AKS Storage
- AKS and Active Directory

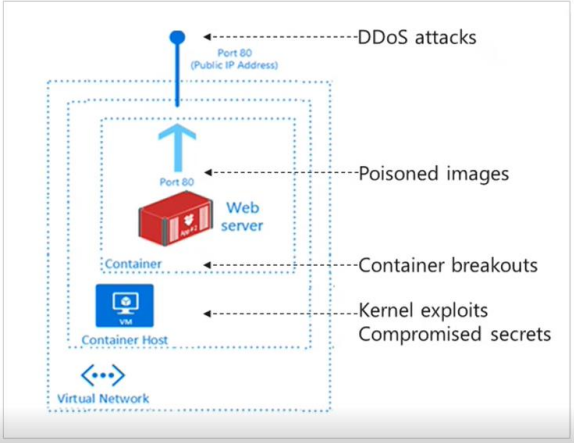
Containers



Feature	Containers
Isolation	Typically provides lightweight isolation from the host and other containers but doesn't provide as strong a security boundary as a virtual machine.
Operating system	Runs the user mode portion of an operating system and can be tailored to contain just the needed services for your app, using fewer system resources.
Deployment	Deploy individual containers by using Docker via command line; deploy multiple containers by using an orchestrator such as Azure Kubernetes Service.
Persistent storage	Use Azure Disks for local storage for a single node, or Azure Files (SMB shares) for storage shared by multiple nodes or servers.
Fault tolerance	If a cluster node fails, any containers running on it are rapidly recreated by the orchestrator on another cluster node.

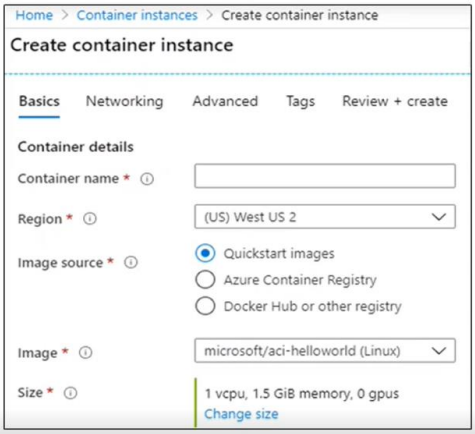
ACI Security

- Continuously scan registry images
- Use approved images – chain of custody, signing
- Run with least privileges
- "Allow List" files the container can access
- Maintain network segmentation
- Monitor and log activities



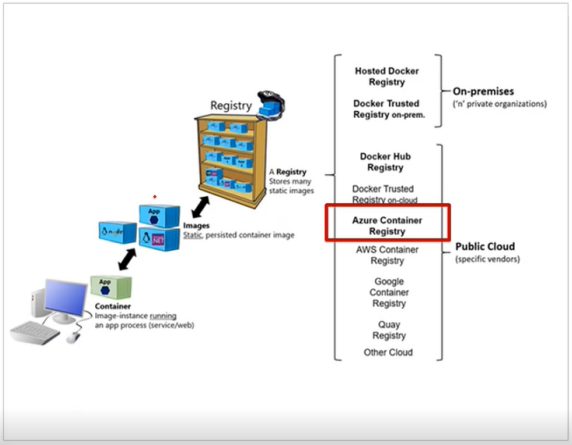
Azure Container Instances (ACI)

- PaaS Service
- Custom sizes - fast startup times
- Public IP connectivity and DNS name
- Hypervisor-level security
- Isolation features
- Co-scheduled groups
- Persistent storage
- Linux and Windows containers
- Virtual network deployments



Azure Container Registry (ACR)

- Docker registry service
- Private and hosted in Azure
- Build, store, and manage images
- Push and pull with the Docker CLI or the Azure CLI
- Access with Azure AD
- RBAC to assign permissions
- Automate using DevOps



ACR Authentication

Require authentication for all operations – unauthenticated access is not supported.

Identity	Usage Scenario	Details
Azure AD identities including user and service principals	Unattended push from DevOps, Unattended pull to Azure or external services	Role-based access – Read, Contributor, Owner
Individual AD identity	Interactive push/pull by developers and testers	
Admin user	Interactive push/pull by individual developer or tester	By default, disabled.

Azure Kubernetes Service (AKS)

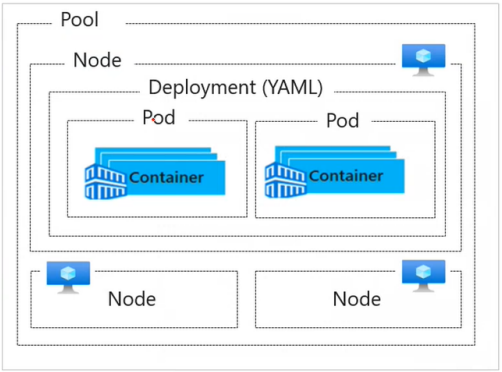
Portable, extensible open-source platform for automating deployment, scaling, and the management of containerized workloads.

- Fully managed
- Public IP and FQDN (Private IP option)
- Accessed with RBAC or Azure AD

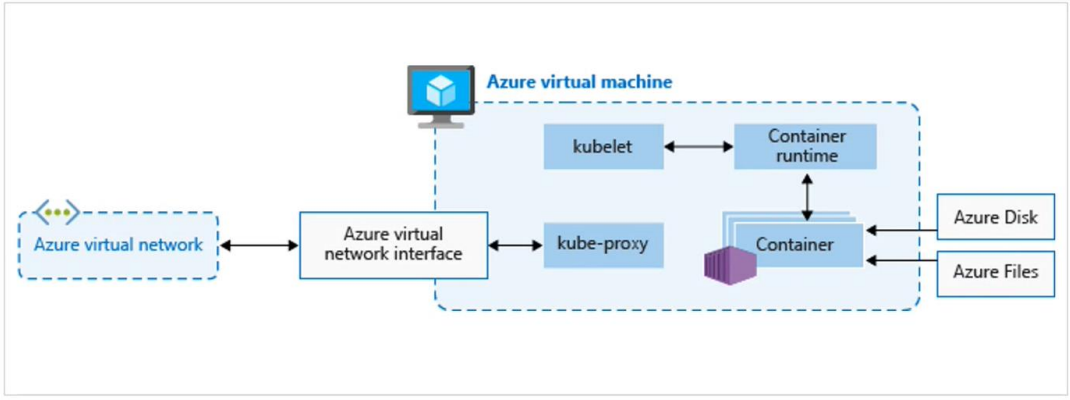
- Dynamic scale containers
- Automation of rolling updates and rollbacks of containers
- Management of storage, network traffic, and sensitive information

AKS Terminology

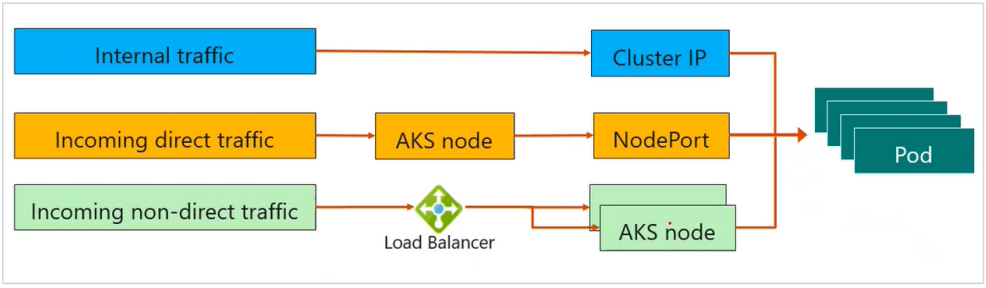
Term	Description
Pools	Groups of nodes with identical configurations.
Nodes	Individual VM running containerized applications.
Pods	Single instance of an application. A pod can contain multiple containers.
Deployment	One or more identical pods managed by Kubernetes.
Manifest	YAML file describing a deployment



AKS Architecture



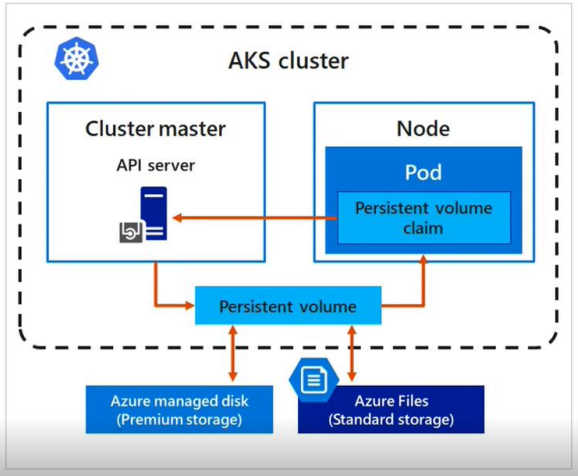
AKS Networking



- Pods run an instance of your application
- Services group pods together to provide network connectivity
- Cluster IP provides internal traffic access
- NodePort provides mapping for incoming direct traffic
- Load balancer has external IP address for incoming non-direct traffic

AKS Storage

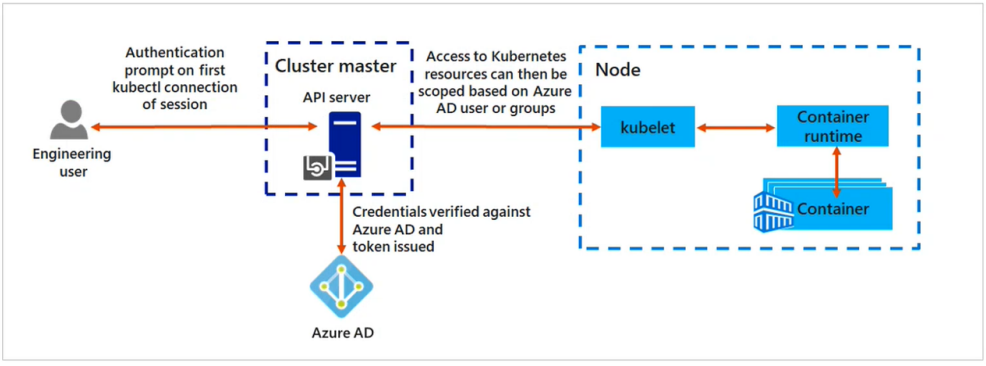
- Local storage on the node is fast and simple to use
- Local storage might not be available after the pod is deleted
- Multiple pods may share data volumes
- Storage could potentially be reattached to another pod



AKS security capabilities

Authentication and authorization	Network security
• Azure AD integration with Azure Kubernetes Service • Azure RBAC, Kubernetes RBAC • Headless services and applications use Service Principals / Managed Identities • Pod managed identities	• Deploy private AKS cluster – API server only has private IP addresses • NSG, Firewall to control the traffic to/from AKS nodes • Use Kubernetes Network Policy to secure traffic between pods • Protect data – Least privilege RBAC, Azure Key Vault

AKS and Azure Active Directory



Use Azure AD as an integrated identity solution

Use service accounts, user accounts, and role-based access control

Additional Study – Container Security

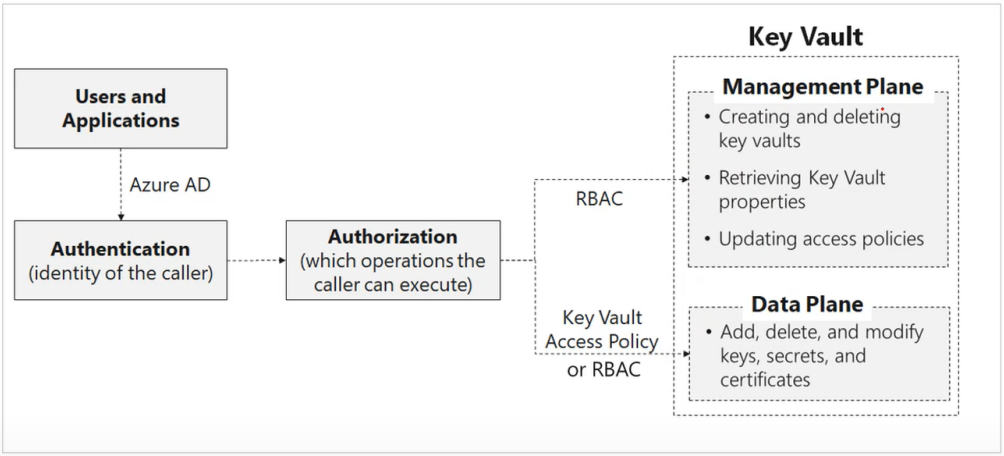
Module Review Questions	Microsoft Learn Modules (docs.microsoft.com/Learn)
	Core Cloud Services - Azure compute options Build and store container images with Azure Container Registry (Exercise) Build a containerized web application with Docker (Exercise) Introduction to Docker containers Run Docker containers with Azure Container Instances (Exercise) Azure Kubernetes Service Workshop (Exercise)

Azure Key Vault Features

- Tokens, passwords, certificates, API keys, and other secrets
- Public and private SSL/TLS certificates
- Hardware security modules (HSMs) protected keys
  - Premium license
- Not intended for user passwords
- Two service tiers—standard and premium

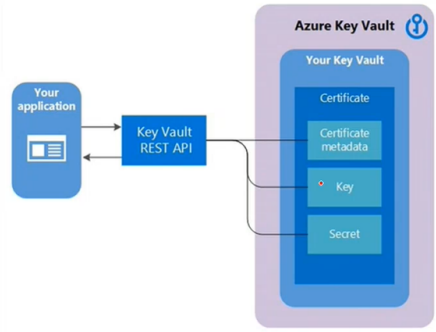
Safeguard cryptographic keys and secrets that cloud applications and services use

Key Vault Access

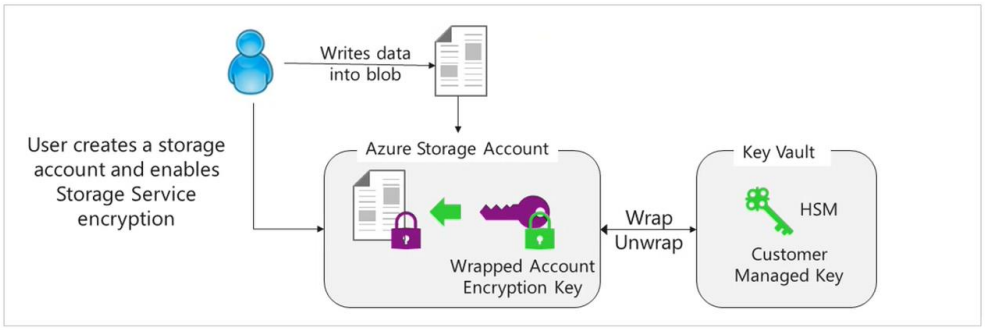


Key Vault Certificates

- Manages X509 v3 certificates (PFX, PEM)
- Created by the Key Vault or by import
- Self-signed and Certificate Authority certificates
- Lifecycle management including automatic renewal and contact notification
- Minimum 2048-bit encryption
- RSA or RSA HSM with certificates



Customer Managed Keys



Update keys and secrets without affecting applications

Updates can be manual, programmatic, or automated

Azure AD Application Scenarios

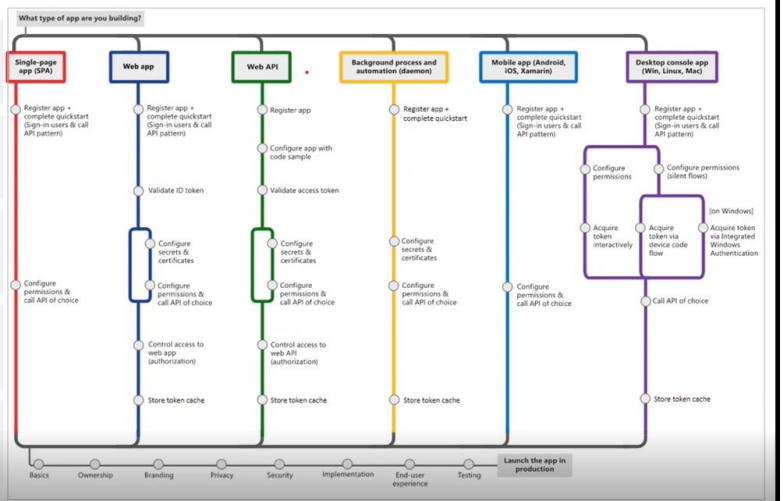
Single page frontends that run in a browser

Web browser to a web application

Web API on behalf of a user

Web applications that need resources from a web API

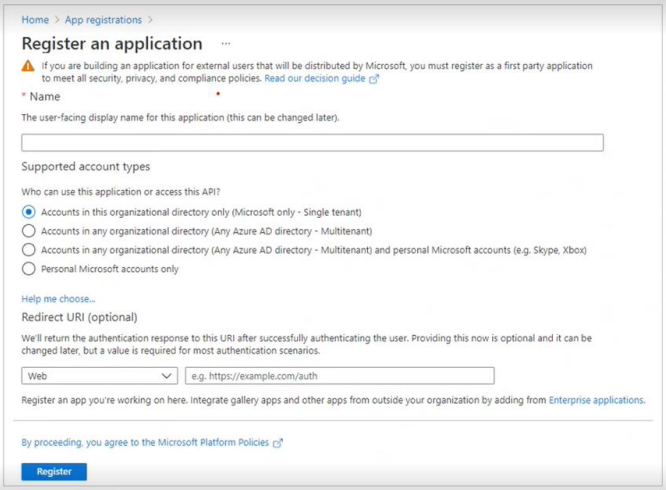
Daemon or server application that needs resources from a web API



App Registration

Any application that outsources authentication to Azure AD must be registered in a directory

Registration creates token information including a unique application id.

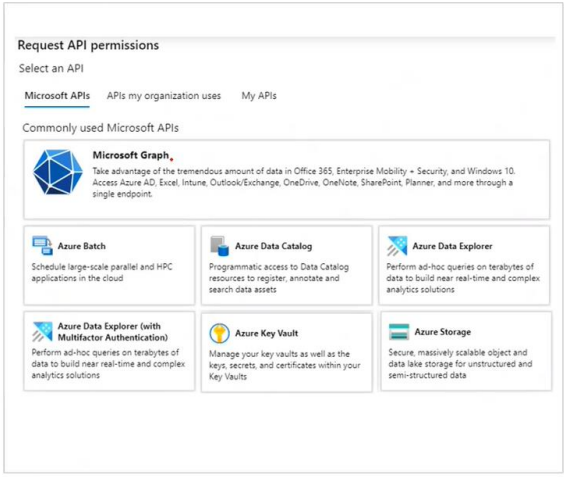


Microsoft Graph Permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process

Delegated permissions are used by apps that have a signed-in user present

Application permissions are used by apps that run without a signed-in user present

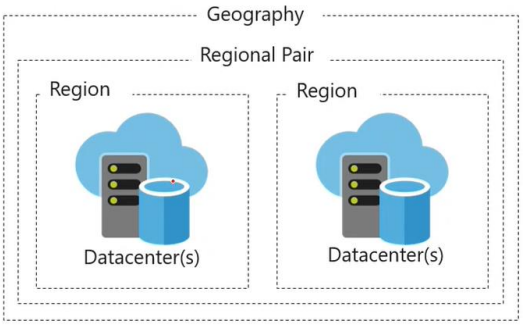


Storage Security

- Data Sovereignty
- Azure Storage Access
- Shared Access Signatures
- Azure AD Storage Authentication
- Storage Service Encryption
- Blob Data Retention Policies
- Azure Files Authentication
- Secure Transfer Required

Data Sovereignty

- Physical isolation
- Platform-provided replication
- Region recovery order
- Sequential updates
- Data residency



Facilitates compliance with data location laws

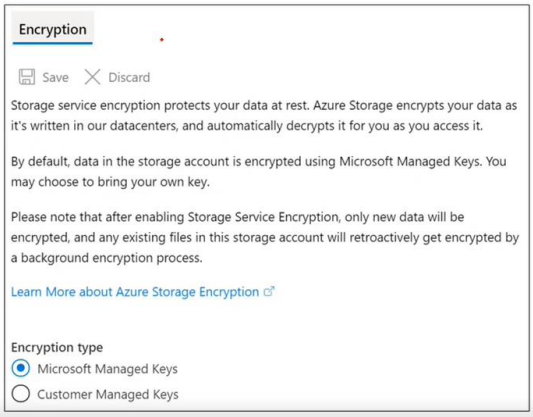
Azure Storage Access

Every storage request must be authorized. There are various authorization methods, including anonymous.

Storage	Storage Account Shared Key	Shared access signature	Azure Active Directory	Active Directory Domain Services (on-prem AADS)	Anonymous public read access
Azure Blobs	Supported	Supported	Supported	Not supported	Supported
Azure Files (SMB)	Supported	Not supported	Supported, only with Azure AD Domain Services	Supported, credentials must be synced to Azure AD	Not supported
Azure Files (REST)	Supported	Supported	Not supported	Not supported	Not supported

Storage Service Encryption

- Protects your data for security and compliance
- Automatically encrypts and decrypts your data
- Encrypted through 256-bit AES encryption
- Is enabled for all new and existing storage accounts and cannot be disabled
- Is transparent to users



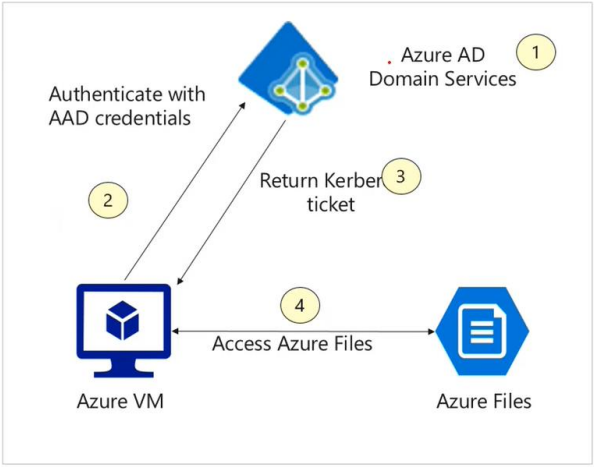
Azure Files Authentication

Enable identity-based authentication

Use Azure AD DS or on-premises AD DS

Use RBAC roles to assign access rights to the file shares

Enforces standard Windows file permissions at both the directory and file level



Database Security

- SQL Database Authentication
- SQL Database Firewalls
- Database Auditing
- Data Discovery and Classification
- Vulnerability Assessment
- Advanced Threat Protection
- Dynamic Data Masking
- Transparent Data Encryption
- Always Encrypted

SQL Database Firewalls

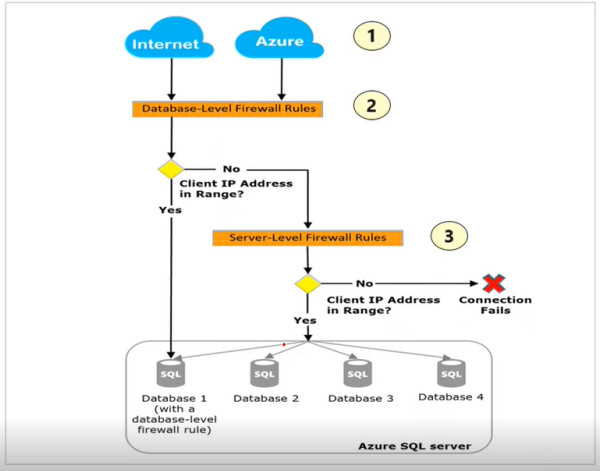
By default, firewall denies all access

Database-level firewall rules add allowed client IP addresses access to specific databases (including Master database).

T-SQL only

Server-level firewall rules enable client and Azure services access to the entire database server.

Portal, T-SQL, or PowerShell



Database Auditing

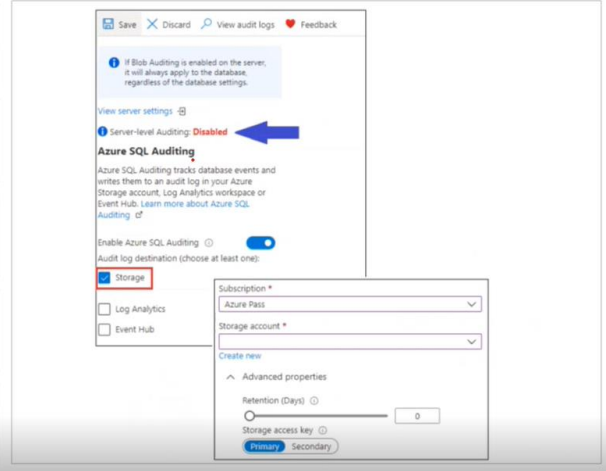
Retain an audit trail of selected events

Report on database activity and analyze results

Configure policies for the server or database level

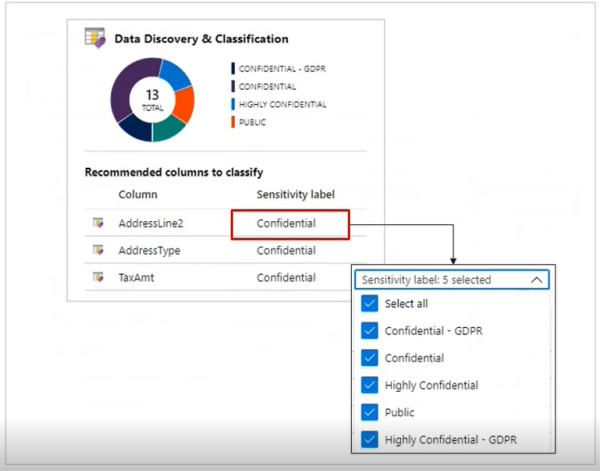
Configure audit log destination

A new server policy applies to all existing and newly created databases



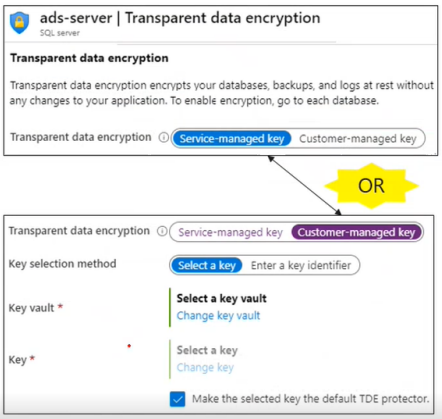
Data Discovery and Classification

- Built-in to Azure SQL Database
- Scans your database and identifies columns that contain potentially sensitive data
- Provides classification recommendations and reports
- Let's you apply sensitivity-classification labels



Transparent Data Encryption

- Protects databases, backups, and logs at rest – server level
- Real-time page level encryption and decryption - service or customer managed keys
- Supports Azure SQL Database (enabled by default), SQL Managed Instance , and Azure Synapse Analytics



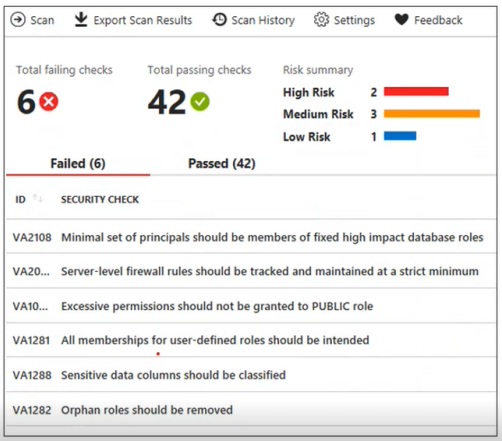
Vulnerability Assessment (Defender for SQL in Security Center)

Scans for database security vulnerabilities organized by severity

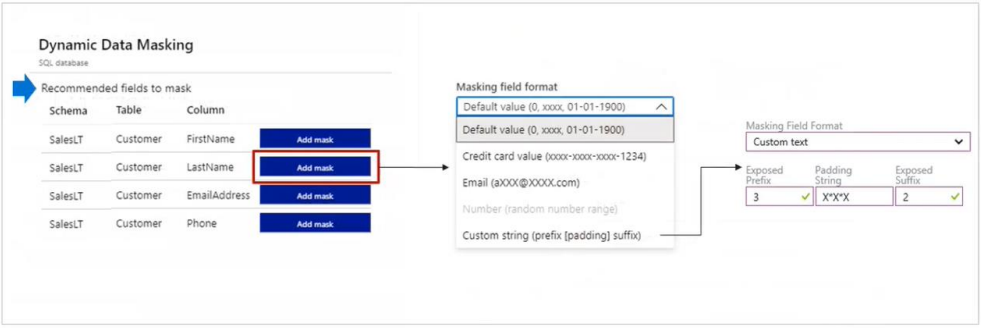
Findings provide actionable steps to remediate the issue

Set up periodic recurring scans and export reports

Covers database-level and server-level security issues



Dynamic Data Masking



Masks sensitive data for non-privileged users

Administrators are excluded; you can add others

Rules apply the masking logic; several formats are available